Computer & Network Forensics

(18 August, 2002)

Be Proactive - Defense in-Depth

- Implement Risk Management.
- Protect Individual Host.
- Protect Network
- Review/Create Policies and Procedures.
- Develop Acceptable Use Policies.
- Establish an Incident Response Team.
  - Identify a Forensics Team
- Create a Forensics Toolkit.
- Conduct Training

Forensic Guidelines

Investigative Thoughts

- Forensics, whether network or computer, involves the **preservation**, **identification**, **extraction**, **documentation** and **interpretation** of network or computer data.
- Every investigation should be treated as if it will end in court.
- The goals of Forensics analysis are to:
  - Determine **what** happened
  - The **extent** of the problem
  - Determine **who** was responsible
- It is used by both
  - **Internal investigators** of Private organization and
  - **Law Enforcement** when computers are involved in illegal activity.

Investigative Thoughts

- **Acquire the evidence** without altering or damaging the original.

  - **Acquiring the data**

    Opt 1- Perform the analysis on a live system?

    - Utilities have most likely been modified by intruder.
    - Least defensible in court.

    Opt 2 - Examine a forensic copy of the original data.

    - Most defensible in court

    Opt 3 - Pull the plug.

    - Damage is in progress.

Investigative Thoughts

- **Handling the Evidence**.
  - Maintain a **Chain of custody**: Evidence form and locker.
    - Who, How and Why was it collected..
    - Who took possession of it?
    - How was it stored and protected.
    - Who and why was it taken out of storage?
  - **Collect everything**.
    - **ISP** normally maintain logs for about 30 days.
    - Assign an **evidence custodian**.
    - Work in **pairs**.
  - **Identify and label everything**.
    - Case number, description, signature, date and time.
  - **Photograph/video tape** the crime scene.

Investigative Thoughts

Handling the Evidence Contd.

Evidence Transportation

- Static free,Bubble wrap.
- Signature across the seal.

Evidence Storage.

- Evidence Locker.
- Evidence log.
- Primary and Alternate custodian.

http://www.cybercrime.gov/searchmanual.pdf

Investigative Thoughts

- **Documenting the Investigation.**
  - **Work in Pairs**.
    - Investigator.
    - Documenter.
  - **Documentation includes.**
    - Software used and Version Numbers.
    - Collection tools.
    - Methods used.
    - Explanation of why this analysis.

NOTE: The case may not go to court for 1-2 years.

Investigative Thoughts

- **Authenticate** your recovered evidence.
  - Create an **Electronic Hash** of all electronic evidence.
  - MD5SUM, SHA or Tripwire.
- **Analyze** the data without modifying it.
  - Make **two backups** of the original data.
  - Perform a **bit by bit (bit stream)** backup.
    - Create a hash of each backup prior to analysis.

Investigative Thoughts

Examination

- Start a **script** with time, name and date.
- **Examine** the partition and directories on the hard drive.
- Use the **Hex editor** to view suspect areas.
  - Search for terms related to case.
- Retrieve **deleted** files.
- Check **unallocated** and **slack** space.
- If **evidence** is found specify the cylinder, head and sector.

Investigative Thoughts

- **Court Presentation**.
  - The Discovery process
    - Checklists, notes, comments, email, etc.
  - Chain of Custody
  - Business Attire.
  - Respect he Judge.
  - Be honest.
  - Ask for questions to be repeated.
    - Give your attorney a chance to object.
  - Review your notes before court
    - Always use your notes to answer questions.

NOTE: A lawyer will not ask a question if he does not already know the answer.

Investigative Thoughts

- **Final Thoughts on Evidence.**
  - The majority of computer security incidents do not become civil or criminal cases
    - Most of them are handled **administratively.**
  - The majority of those cases that do become a legal case never go to court.
    - Most are **plea bargained**.
    - You must proceed as it if will go to court.

Tool Kits

Hardware Toolkit - Example

- High-End Processor - 1 Ghz Plus
- 512 MB Ram Plus
- Large Capacity IDE Drives - 50 GB Plus
- Large Capacity SCSI drives - 50 GB Plus
- 40x CD-RW Drive
- 8-mm Exabyte Tape - 20 GB Plus
- Zip 250 MB Drives
- 10/100 NIC - Promiscuous Mode
- Removable metal drives
- Printer

http://www.forensic-computers.com/main.htm
http://www.cftco.com//
http://www.exabyte.com/

Supplies - Examples

- Power Extension cords
- Power strips
- Uninterruptible Power Supply (UPS))
- Cds and Labels
- Zip Media
- Permanent Markers
- Folders/labels for evidence.
- Digital Camera
- Toolkit
- Lockable Storage Cabinet
- Printer Paper
- Burn Bags

Software Toolkit - Examples

- All utilities should have **trusted Binaries**.
  - Various commands can be trojaned.
- Each machine should have dual-boot **multiple OSs.**
  - Win 98, 2000, linux.
- **Drive Imaging** Tools
  - **Safeback -** http://www.forensics-intl.com/safeback.html
  - **EnCase -** http://www.guidancesoftware.com/html/forensic_software.html
  - **DiskPro -** http://www.e-mart.com/www/index.html
  - **SnapBack -** http://www.snapback.com/
  - **Ghost -** http://www.symantec.com
  - **dd -** Standard Unix drive imaging utility.

Software Toolkit - Examples Contd

- Viewers
  - **Quickview Plus -** http://www.jasc.com/
  - **Conversion Plus -** http://www.dataviz.com
  - **ThumbsPlus -** http://www.cerious.com/thumbsplus.shtml
- CD-R Utilities
  - **CD-R Diagnostics -** http://www.cdrom-prod.com/public.html
- Text Searches
  - **dtsearch -** http://www.dtsearch.com
- Disk Wiping
  - **DiskScrub -** http://forensics-intl.com/thetools.html

Software Toolkit - Examples Contd

- **Forensic** Programs
  - **Forensic Toolkit -**
    http://www.foundstone.com/rdlabs/tools.php
  - **The Coroner's Toolkit (TCT) -**
    http://www.fish.com/tct/
  - **ForensiX -**
    http://www.all.net/
  - **New Technologies Inc (NTI) -**
    http://forensics-intl.com/thetools.html

Computer Forensics

Computer Forensics

- Computer Forensics Principles.

  P1: Preserve the evidence in an unchanged state.

  P2: Thoroughly and completely document the Investigative Process.

Instructor Recommendation: Handle the corporate investigation as if Law enforcement will be called in and the attackers will be prosecuted.

Computer Forensics Definitions

- **Evidence Media:** The original media to be investigated whether subject or victim.
- **Target Media:** A forensic duplicate of the evidence media. The forensic evidence transferred to the target media.
- **Restored Image**: A copy of the forensic image restored to its bootable form.
- **Native Operating System**: The OS utilized when the evidence media or forensic duplicate is booted for analysis.
- **Live Analysis**: A analysis conducted on the original evidence media.
- **Offline Analysis:** Analysis conducted on the Forensic Image.
- **Trace Evidence:** Fragments of information from the free space, etc.

Best Evidence Rule

- **Common Mistakes** include:
  - Altering time and date stamps.
  - Killing rogue processes.
  - Patching the system before the investigation.
  - Not recording commands executed on the system.
  - Using untrusted commands and binaries.
  - Writing over potential evidence by:
    - Installing software on the evidence media
    - Running programs that store their output on the evidence media.

Evidence Chain of Custody

- The prosecution is responsible for proving that which is presented in court is that which was originally collected.
  - An **Evidence Chain of Custody** must be maintained.
- Create an **Evidence Tag** at the time of evidence collection.
  - A designated **Evidence Custodian** with a Laptop to generate the Evidence Tags.
    - Date and Time
    - Case Number
    - Evidence Tag number
    - Evidence Description
    - Individual receiving the evidence and Date
  - Each time the evidence moves from one **person** to another or from one **media** to another must be recorded.

Typical Evidence Tag

EVIDENCE TAG

DATE	TAG NO.	CASE FILE NO.	LOCATION OF OFFICE OF INVESTIGATION	LOG PAGE
5/30/2002	AZ3456	AB29-5-30-02	Rm 138B, Woodbridge	29

On 5/30/2002 (Date) at Apt 24, South Complex, Woodbridge, Va (Place)

the property described below was ☐ received from ☐ seized from ☒ obtained during search of:

DESCRIPTION (If property is to be returned, include condition and claimed value.)

A Toshiba hard drive, serial number 1234 manufactured on 01/03/00.

SIGNATURE OF WITNESS	SIGNATURE OF PERSON RECEIVING PROPERTY
Bill Drake, #8967	Jerry Oney, #1234

Typical Chain of Custody

CHAIN OF CUSTODY RECEIPT				
RELEASED BY (Printed name and signature)	DATE	PURPOSE	RECEIVED BY (Printed name and signature)	DATE
Jerry Oney #1234 5/30/2002	5/30/2002	Analysis	Johnny Dollar #5678	

Preparation

- Tool Preparation
  - Use Command line and not GUI tools
  - Maintain the tools on both a Read Only CD and/or Write protected floppies.
  - Check the file access of each tool prior to use.
  - Checksum each tool in the toolkit.
- Evidence gathered by the tools should be burned to a CD or to a write protected floppy.
  - Chain of custody tags should be completed for each CD or floppy.

Thoughts Contd

- Determine whether or not an unlawful, unauthorized or unacceptable activity has occurred.
- Don't destroy or alter any evidence.
- Initial Response toolkit of trusted utilities.
- Initial Response Script.
- Run md5sum against all collected volatile data.
- Create a log of all actions taken during the initial response.

Uni

x

Unix Tools

- System commands are trojaned by Hackers in order to hide their activities.
- The Investigator needs his own command toolkit.
  - Every variation of Unix requires a unique toolkit.
  - May version of programs are not backward or forward compatible.
- All tools musts be compiled with the ***-static*** option.
  - Not dependent upon any system shared libraries.
  - Trusted, independent binaries.

http://www.incident.response.org

Unix Trusted Binaries

ls	dd	des	file	pkginfo
find	icat	lsof	md5sum	netcat/cryptcat
netstat		pcat	perl	ps	strace
strings		truss	df	vi	cat
more	gzip	last	w	rm
script	bash	modinfo	lsmod	ifconfig

Most Common Unix Utilities

Name	Description
w,who	Shows current logins
ps	Process status. Displays a lit of all running processes with details about their context and state.
top	Real-time display of most CPU-intensive processes. A useful tool to when the system is running slowly.
lsof	List Open Files. Provides a list of all current open files and the processes that have opened them.
fuser	File User. Identifies which processes are using a specific file or network Socket.
strace	System trace Call. Lists all system calls being made by all running processes.
truss,ktrace	Earlier versions of system call trace.
ltrace	Library routine trace.

Suggested NT Tools

Norton Ghost	**Creates a Forensic duplicate.**
windump	**Capture Network traffic.**
Nmapnt	**Scan ports and services on local/remote hosts.**
L0pht's Antisniff	**Detects Sniffers.**
L0phtcrack	**NT Password Cracking utility.**
pwdump	**Dump password hashes.**
Netcat	**"TCP/IP Swiss Army Knife".**
DumpSec	**Produces a list of shares.**
NTFS DOS	**Mount an NTFS files system fro DOS prompt.**
PGP	**Securing disks or files.**

Suggested NT Utilities

cmd.exe	Command prompt for NT and 2000.
loggedon	Shows all users connected locally and remotely.
rasusers	Shows which users have remote access privileges.
netstat	Enumerates all listening ports and all current connection to those ports.
fport	Enumerates all process that opened any TCP/IP ports.
pslist	Enumerates all running processes on the system.
listdlls	Lists all running processes, their command-line arguments and their dynamic linked libraries (DLL).

Suggested NT Utilities Contd

nbtstat	lists most recent NetBios connections.
arp	Shows most recent MAC addresses used by the system.
kill	A command to terminate a process.
md5sum	Creates md5 file hashes.
rmtshare	Displays shares on a remote machine.
cryptcat	Transfers encrypted data between target and forensics system.
doskey	Displays the command history on the target system.

Recovering Unix Volatile Data

Volatile Data

- Capture volatile data before it is lost.
  - System date and time.
  - Currently running processes.
  - Currently open sockets.
  - Applications listening on open ports.
  - Users currently logged on.
  - Systems with recent connections.

Volatile Data

- **Volatile Data** reflects the current, active information reflecting the machines current operating state.
- It includes:
  - **Open** sockets.
  - Running **Processes**.
  - Contents of **system Ram**.
  - **Unlinked** files (files marked for deletion when powered off).
    - Unix allows the hacker to delete a file after they have started it running.
    - That is, the program is running but the file has been deleted from the hard drive.

Order of Volatility

- **CPU Storage**: As short as a Single clock cycle.
- **System Storage**: Until host is shut down.
- **Kernel Tables**: Until host is shut down.
- **Fixed Media**: Until overwritten or erased.
- **Removable Media**: Until overwritten or erased
- **Paper Printouts**: Until Physically destroyed

Order of Volatility Contd

Registers	Minimal Utility
Caches	Captured as part of system memory
Volatile Ram	Current screen capture
Static Ram	Includes information on all running processes.
Network state	Examine network activity and for backdoors.
Running Processes	Examine for authorized activity.
Swap Space	Swapped kernel data.
Queue Directories	Information on running processes, incomplete activities, outgoing mail and print jobs.
Temp Directories	/tmp or /usr/tmp serves as a scratch pad and working directory for system.
Log Directories	Used for reconstructing events

Recovery Guidelines

- **Command lines tools are best.**
- **Use tools you know work. Safe, tested, trusted binaries.**
- **Volatile Tools should be on write protected floppies or CD.**
  - **Run your tools from the floppy or CD.**
- **Create a checksum of each tool and store it on the toolkit.**

Recovering Volatile Data

- **A Trusted Shell.**

  - Log onto the local console with **root privilege** in order to prevent network traffic from being generated.

  - Go to a **Command Line Interface (CLI)** and mount the floppy or CD containing your tools.

  - Execute a **trusted command shell** from your CD or floppy.

    - Sometimes Hackers will trojan shells.

  - Set the **PATH variable** to dot (.) in order to reduce the likelihood of executing untrusted commands.

Documentatio

- **Investigative Documentation**
  - Use the ***script*** command to send the investigative output to both the screen and a specified file.

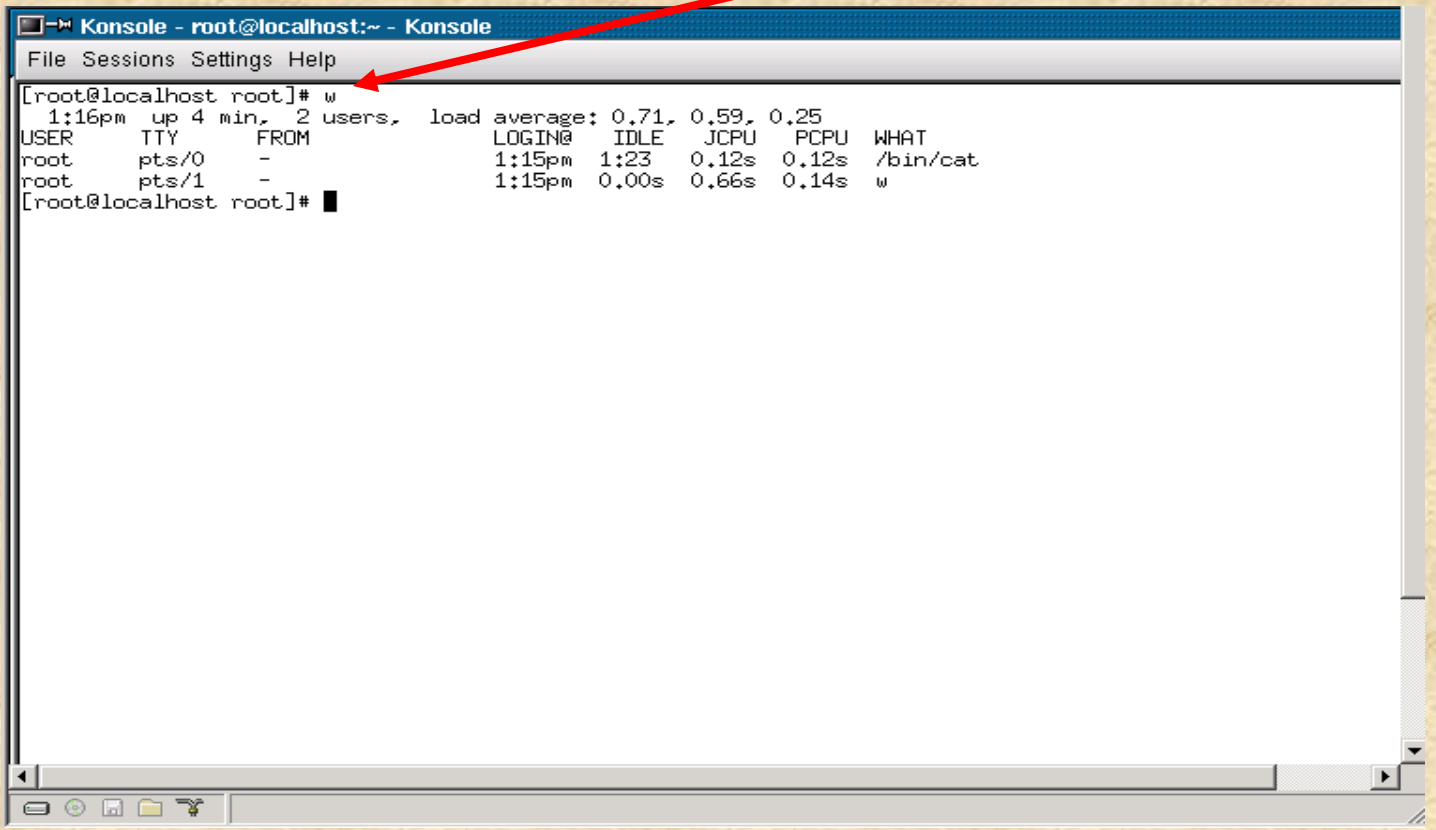
# ***script > script.txt***	Put everything into the script.txt file
# ***date***	1st put in the date and time
# ***uname -a***	2nd put in the host name

- Mount the tool CD and set the path variable so that the CD is the only thing in your path.

# ***mount -t iso9660 /dev/cdrom /mnt/cdrom***	Mount the CD.
# ***path=/mnt/cdrom***	Set the PATH variable.
# ***echo $PATH***	Verify the PATH
/mnt/cdrom	Path verified.

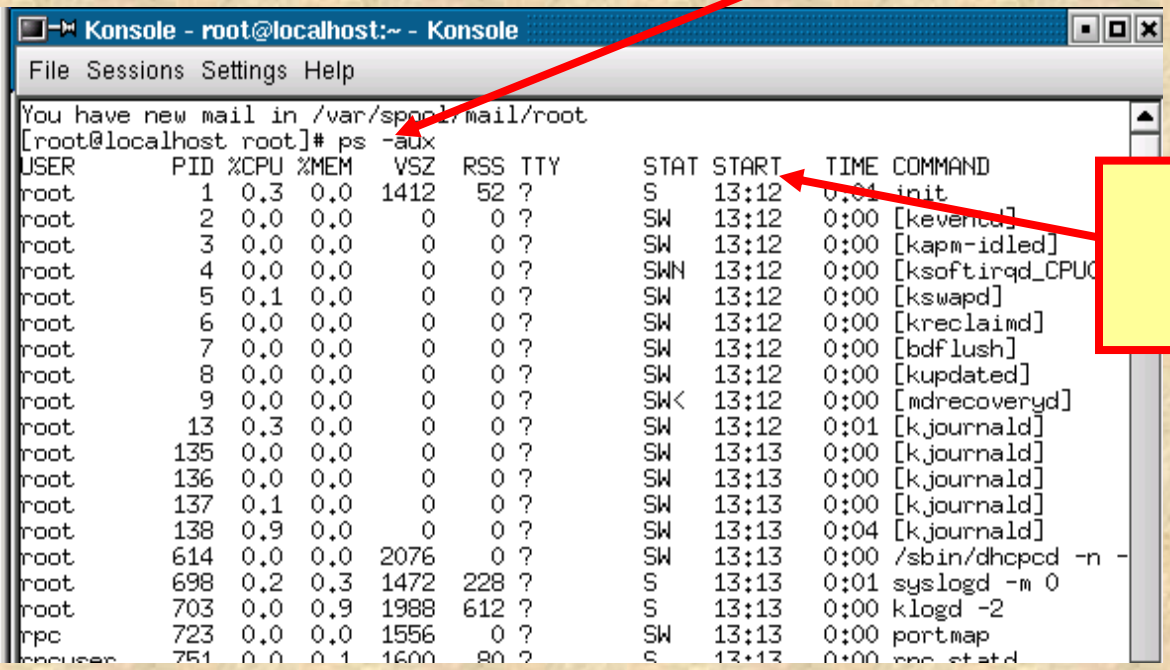
The Who Command

- Determine **who is logged** onto the system with the ***w*** (what) command.



The PS Command

- Determine the **running processes** with the ***ps*** (process status) command.

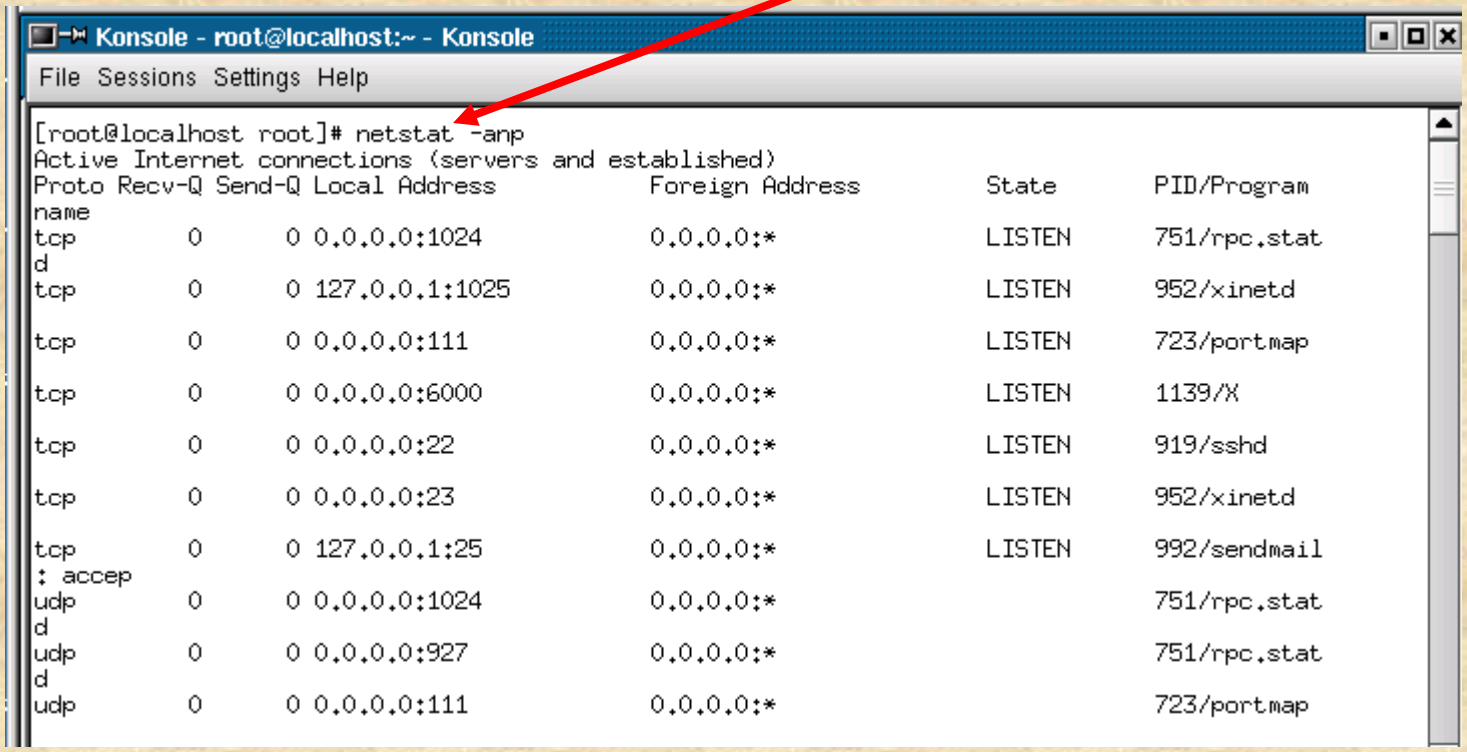


- Look for unusual processes.
- If unusual process are present then execute ***netstat***.

To detect any IP addresses.

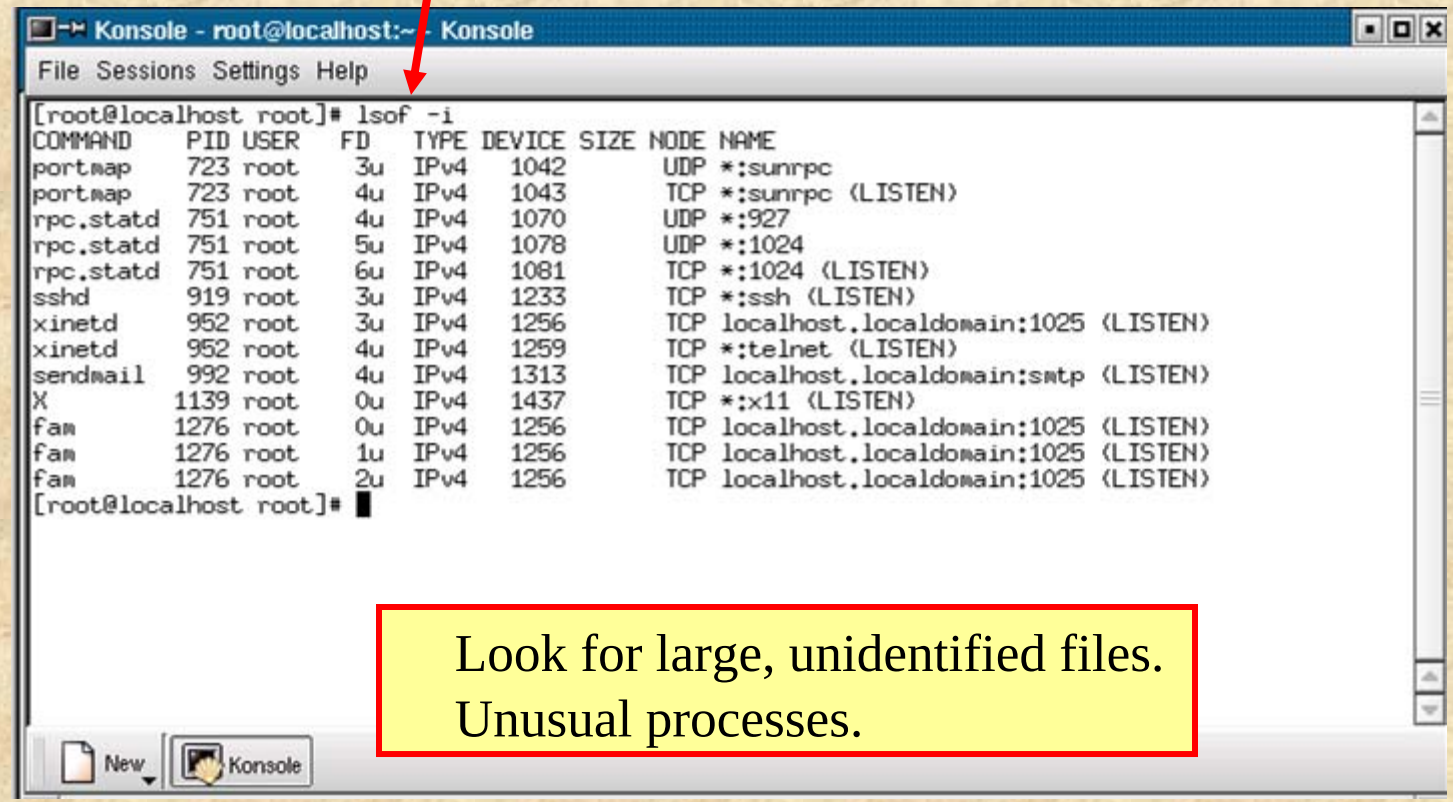
The netstat Command

- Determine the open ports with the ***netstat*** (network statistics) command.



The lsof Command

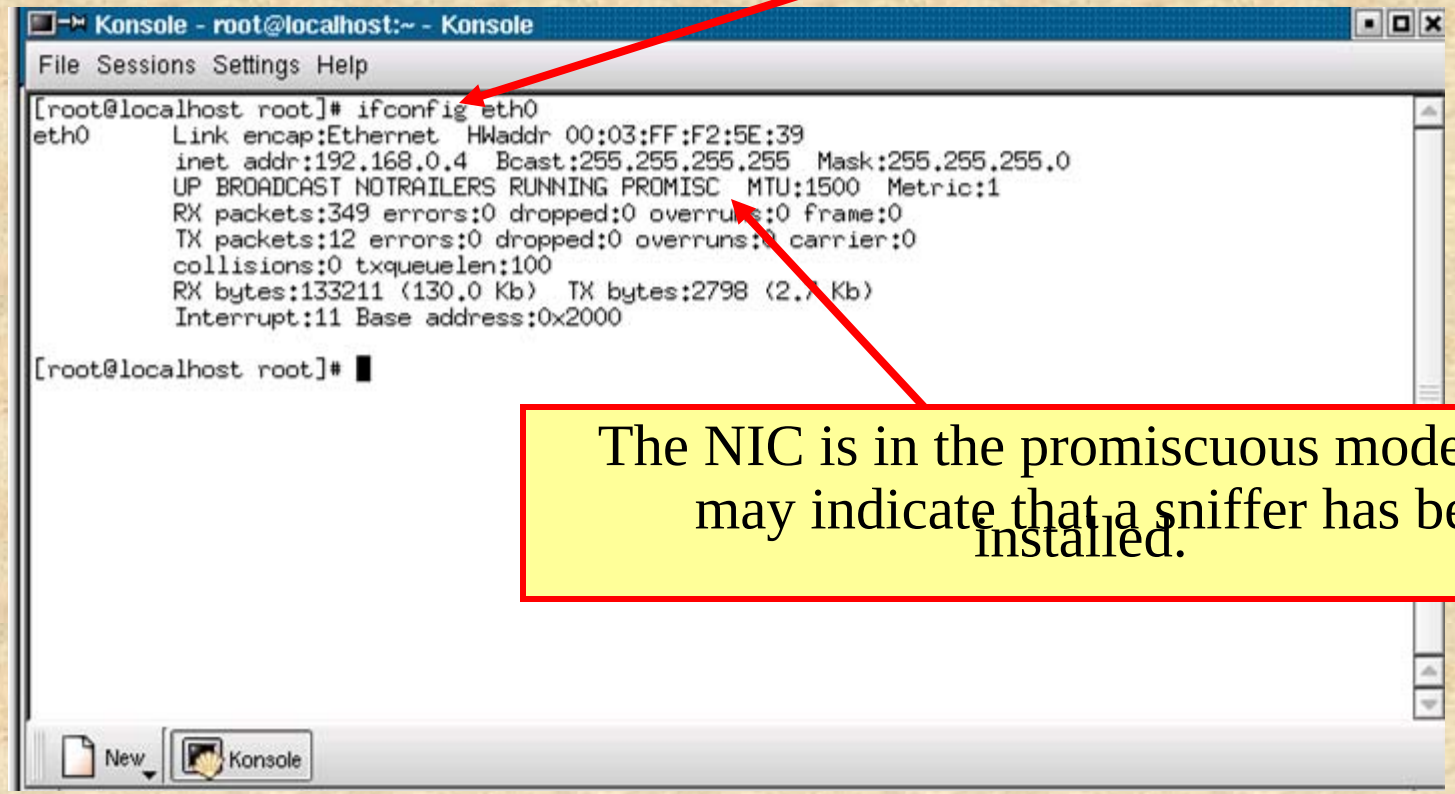
- Map the open port to the running process by employing the ***lsof*** (list open files)command.



Look for large, unidentified files.
Unusual processes.

The ifconfig Command

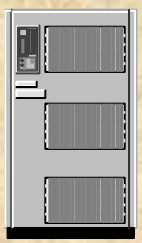
- Determine the status of the NIC with the ***ifconfig*** command.



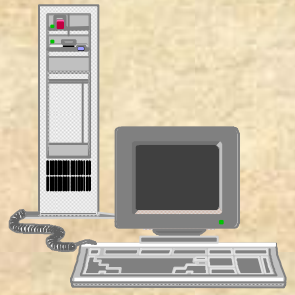
- Look for sniffers.

Collecting Data

Forensics Station



Target Station



time/date

who

ps

netstat -an

lsof

arp

ifconfig

ls

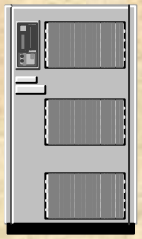
time/date

- Employ ***netcat*** to move volatile data from the target to the forensics machine.
- ***Cryptcat*** can be employed to move data across an insecure link.
- Run ***md5sum*** against the output file with a witness.

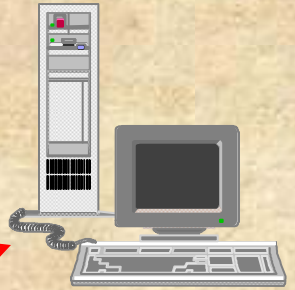
Using Netcat contd

Forensics Station

Target Station



netcat data



Step 1. Start the **Forensics Station** Netcat program listening on port 10,005.

 # nc -1 - p 10005 > suspect.netstatus.txt

Step 2. On the **Target Station** Netcat data to the Forensics station.

 # (data; netstat -p; netstat -rn; arp -v) | nc 192.168.0.2 10005 -w 3

- **Perform an md5sum on the data after receipt.**

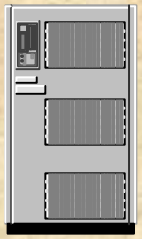
-p will associate the process with a specific network connection.

-rn displays the routing table.

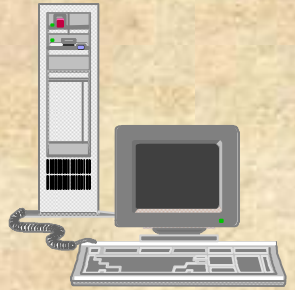
-v displays information in a verbose mode.

Using Netcat

Forensics Station



Target Station



netcat passwd file

Step 1. Start the **Forensics Station** Netcat program listening on port 10,000

nc -1 - p 10000 > tmp/nc.suspect.passwd_file

Step 2. On the **Target Station** Netcat data to the Forensics station.

cat /etc/passwd /etc/shadow | nc 192.168.0.2 10000 -w 3

- **Perform an md5sum on the data after receipt.**

Volatile Data Problems

- Intruder Presence.
- Hacker Booby Traps.
- Impact on continued operations.
- Involvement of law Enforcement.

Online Unix Analysis

Online Unix Analysis

- Data retrieved from a host that **must remain on-line**.
  - Generally not defensible.
  - Can be used to prove an allegation.
- Data to be retrieved.
  - Time/date of the files.
  - System Logs
  - Configuration files.
  - System Ram.

Online Unix Analysis

- Data retrieval tools.
  - ***dd*** - Data Dumper. A Unix utility that can be used to create a forensic copy.
  - ***cat*** - display files.
  - ***netcat*** - Creates a communication channel between two different systems.
  - ***des*** - Data Encryption Standard used to encrypt data.
  - ***cryptcat*** - Same as netcat but the data transfer is encrypted.

File Time and Dates

- Retrieve all **time/date stamps** of the file system
- Use a trusted ***ls*** binary utility to obtain the access, modification and creation times of each file.
- Save the output to a trusted floppy.

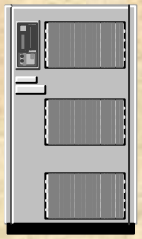
```
ls -alRu   >        /floppy/access
ls -alRc   >/floppy/modifications
ls -alR    >   /floppy/creation
```

Important Log Files

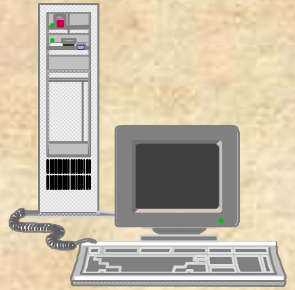
utmp	Keeps track of who is logged onto the system. Accessed via the ***w*** utility.
wtmp	Keeps track of logins and logouts. Accessed via the ***last*** utility.
lastlog	The last time each user logged onto the system. Accessed via the ***lastlog*** utility.

Using Netcat to Copy a Log File

Forensics Station



Target Station



netcat Log file

Step 1. Start the **Forensics Station** Netcat program listening on port 2222.

nc -1 - p 2222 | des -d -c -k password |dd of = messages md5sum messages

Step 2. On the **Target Station** Netcat log file to the Forensics station.

dd if =/var/log/messages | des -e -c -k password | nc 192.168.0.2 2222 -w 3

if is the input file

of is the output file

Important Configuration Files

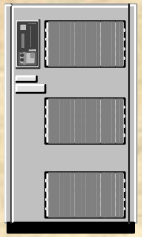
/etc/passwd	Password file. Look for unauthorized user accounts and privileges.
/etc/shadow	Encrypted password file. Every account should require password authentication.
/etc/groups	The group to which each individual belongs. Look for privilege escalation and access scope.
/etc/hosts	Matches host name to IP addresses. List the local entries.
/etc/hosts.equiv	Contains a list of trusted hosts. review the trust relationship.
~/.rhosts	Trusted hosts applicable only to a particular user. Review the user-based trusted relationship.
/etc/allow	TCPWrapper Allow rules
/etc/deny	TCPWrapper deny rules
/etc/rc	Start up files
crontab files	A list of scheduled events
/etc/inetd.conf	List of services that are listened for.

Important Memory

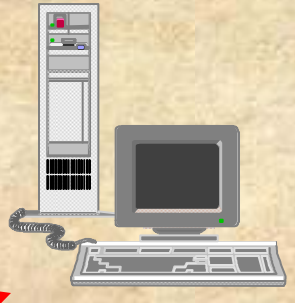
/proc/kmem	Contains the contents of system RAM. It is used for string searches

Using Netcat to Copy Memory

Forensics Station



Target Station



netcat Memory file

Step 1. Start the **Forensics Station** Netcat program listening on port 2222.

nc -1 - p 2222 > suspect.mem.images&

Step 2. On the **Target Station** Netcat log file to the Forensics station.

dd bs=1024 < /proc/kmem | nc 192.168.0.2 2222 -w 3

bs is the block transfer size

Offline Analysis

Forensic Thoughts

- If the network is in danger then unplug the machine from the network.
  - Collect the volatile date.
- If the system needs to remain on-line then
  - Collect on-line data
- If the incident represents no current threat then
  - Collect the volatile data.
  - Power the machine down.
- Create two forensic copies of the disk image.

The Best Evidence Rule

- **Federal Rules of Evidence (FRE).**

  "to prove the content of a writing, recording, or photograph, the original writing, recording or photograph is required, except as otherwise provided in these rules or by Act of Congress."

- **FRE 1001(3)** is an exception

  "...if data are stored on a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an '**Original.**"

- This allows forensic analysts to create an accurate representation of the original data that may be introduced as evidence.

BIOS Review

- Review the Target **Basic Input/Output System (BIOS)** before beginning a duplication to determine:
  - **Basic geometry** of the hard drive on the target System.
    - Document the hard drive settings to include maximum capacity, cylinders, heads, and sectors.
    - For proper recovery by the original OS the partitions should be aligned on the cylinder boundaries.
  - Determine the **Boot Sequence** on the target System.
    - Floppy drives.
    - CD-Rom
    - Hard Drive.
    - PCMCIA Card.

Forensic Duplication

- **Three** Forensic Duplication Approaches**.**

Opt 1 - Remove the storage media and connect it to a Forensics Workstation.

- Document the system details to include serial number, jumper settings, visible damage, etc.
- Remove media from the target system and connect it to the Forensics workstation.
- Image the media using **Safeback**, the Unix **dd** utility or **EnCase**.

Forensics Workstations	http://www.computer-forensics.com/
Safeback	http://www.forensics-intl.com/safeback.html
EnCase	http://www.guidancesoftware.com/
DiskPro	http://www.e-mart.com/www/cnr.html

Forensic Duplication Contd

- Three Forensic Duplication Approaches Contd**.**

Opt 2 - Attach a hard drive to the Target Computer.

- Make sure the target computer works as expected.

Opt 3 - Image the storage media by transmitting the disk image over a closed network to the Forensics Workstation.

- Establish a **point-to-point interface** from the evidence system to the forensics workstation using an Ethernet Switch of Ethernet cross-connect cable.
  - The ***netcat*** utility seems to be the best for this option.
- Perform **MD5** computation on both the original and target system.

Looking for Evidence
- Windows NT/2000-

Where to Look for Evidence

- Volatile Data
- Slack Space
- Free Space
- Damaged Clusters
- Event Logs
- Security Logs
- Application Logs
- Registry
- Swap File
- History File
- Browser Cache
- Temporary Files
- Recycle bin
- Printer Spool
- EMail
- Logical files

Accessing the system

- Accessing the operating system if the password is unknown.
  - Opt 1
    - Boot the system to DOS with a Floppy.
    - Mount the NTFS DOS and copy the SAM database to a floppy.
    - Use L0ptcract to crack the password hashes.
  - Opt 2
    - Boot the system to DOS.
    - Delete the SAM file.
  - Opt 3
    - Access the registry and circumvent the normal authentication process.

Preparation

- The forensic image should be mounted in a read-only mode. View the partition(s) and its content with
  - **NTFSDOS** http://www.sysinternals.com.
  - **Linux** http://www.linux.org/
  - **VMware** http://www.vmware.com
  - ptable http://www.forensics-intl.com/
- Crack the password in the SAM
  - **John the Ripper** http://www.openwall.com/john/
  - **L0phtcrack** http://www.atstake.com.
  - **chntpw** http://home.eunet.no/~pnordahl/ntpasswd
  - **Access Data** http://www.accessdata.com/
  - **Passware Kit** http://www.lostpassword.com

Forensic Analysis

- **Physical Analysis.** Performed on the forensic Image.
  - Perform a **String Search.**

String Search http://www.maresware.com/maresware/forensic1.htm
DS2 http://www.forensics-intl.com/
dtsearch http://www.forensics-intl.com/

  - Perform a Search and Extract.
    - Looks for file types.

File Formats http://www.wotsit.org/

  - Extract File slack and/Free Space.
    - **Free Space:** Hard Drive space not allocated to a file and deleted file fragments.
    - **Slack Space:** Space left when a minimum block size is not filled by a write operation.

NTI Tool Suite http://www.forensics-intl.com/

Forensic Analysis Contd

- Logical Analysis.
  - A partition by partition analysis of each file.
  - A typical process includes:
    - Mount each partition in Read-Only mode under Linux.
    - Export the partition via ***SAMBA*** to the Forensics System.
    - Examine each file with the appropriate file viewer.

Quick View Plus http://www.jasc.com/product.asp?pf_id=006
HandyVue http://shop.store.yahoo.com/repc/handyvue.html

  - Typical Lists created:
    - Web Sites
    - E-mail addresses
    - Specific Key words, etc

Forensic Analysis Contd

- **Hidden Data**.
  - **Files**
    - NTFS streams.
    - Rename
    - Attribute change
    - Extension change
  - **Slack Space -** The data between the end of the data and the end of the block.
  - **Swap File -** A hidden window file, ***pagefile.sys,*** used by virtual memory.
  - **Unallocated clusters -** Blocks not currently used by a file.
  - **Unused partitions -** Space allocated and formatted but does not appear to contain data.
  - **Hidden files/partitions -** Hidden space that might contains unallocated space used to deliberately hide data.

Forensic Analysis Contd

- Log Analysis.
  - Employ ***Dumpel*** to dump the System Log, Application Log and Security Log.
  - Import into ***Excel*** and analyze.

    Dumpel from the NT Resource Kit (NTRK)
- Recovering Deleted files and Data
  - Undeleting Files

    File Scavenger http://www.quetek.com/prod01.htm

    Disk Search Pro http://www.forensics-intl.com/dspro.html
  - Recycle Bin
  - Temporary Files
  - Backups

Forensic Analysis Contd

- Registry Review.
  - Employ ***regedit*** to identify previously installed software and applications such as steganography tools, sniffer tools, l0phtcrack, etc.
  - Look in:
    - HKEY_CLASSES_ROOT
    - HKEY_CURRENT_USER
    - HKEY_LOCAL_MACHINE
    - HKEY_USERS
    - HKEY_CURRENT_CONFIG

Forensic Analysis Contd

- Swap Files.
  - Swap files are hidden system files used as virtual memory when there is insufficient RAM.
  - Employ **dir /ah** or the **Windows Explorer >Tools>Folder Options>Show Hidden Files.**
- Broken Links
  - Links associate desktop shortcuts or Start menu with an application or document.

  chklnks.exe from NTRK displays broken links.

Forensic Analysis Contd

- Also look at these areas.
  - Web Browser files?
  - Unauthorized User Accounts?
  - Unauthorized Processes?
  - Hidden Files?
  - Unauthorized access points?
  - Patch Level?
  - Administrative shares?
  - Scheduler Service?

Forensic Analysis Contd

- Unexpected Employee Departure
  - Examine the scroll box in the Find dialog box.
  - Examine the Recycle Bin.
  - Examine the files accessed in the last days before departure

    afind http://www.foundstone.com
  - Examine the most recently used files.
  - String search the hard drive for:
    - Project codes
    - Customers, etc

Common Forensics Mistakes

- Failure to Maintain thorough, complete documentation.
- Failure to control access to digital information.
- Underestimate the scope of the incident.,
- Failure to report the incident in a timely manner.
- Failure to provide accurate information.
- No incident response plan.

Network Forensics

Definitions

- **Sniffer**: Hardware or software that passively intercepts packets as they traverse the network. Other name include Protocol Analyzer and Network Monitor.
  - **Silent Sniffers** will not respond to any received packets.
  - **Illegal Sniffers** violate 18 USC 2511 dealing with wiretaps.
- **Promiscuous Mode**. A sniffer operates in a mode that intercepts all packets flowing across the network.
  - A normal NIC only intercepts packets packets addressed only to its IP address and Broadcasts address.
- **Transactional** (Noncontent) information consists only of header information. For example, IP, TCP or UDP headers.
  - Same as a Law Enforcement **Trap and Trace** or **Pen Register**.
- **Content Information** consists of not only the headers but also part or all of the encapsulated data.

Network Forensics Data

- Network data can come from:
  - Routers, Firewalls, Servers, IDS, DHCP Servers, etc.
  - These logs may have different formats, be difficult to find, difficult to correlate and have a broken chain of custody.
- Chain of Custody
  - Strictly controlled network monitoring can maintain a proper chain of custody.
    - Electronic evidence requires tighter control than most other types of evidence because it can be easily altered.
    - A broken chain goes to weight and not admissibility.

Chain of Custody

- Network data Chain of Custody should include:
  - Date and time Recorded.
  - Make, model, serial number and description of recording device.
  - Names of individual recording or the name of individuals recovering the logs.
  - Description of the logs.
  - Name, Signature and date of individual receiving the data.
  - Evidence Tag for this item.
  - Hash value (MD5) of each log file.

Network Monitoring

Monitoring The Network

- What are the **Network Monitoring goals**?
  - Monitor traffic to and from a Host?
  - Monitor traffic to and from a Network?
  - Monitor a specific person?
  - Verify an Intrusion Attempt?
  - Monitor attack signatures?
  - Monitor a specific protocol?
  - Monitor a specific port?
- Check with **corporate legal counsel** prior to starting the monitor.

Instructor's Note: Make sure the corporate policy supports the type monitoring to be performed - non-content or content!

Monitoring The Network Contd

- **Network Monitoring Hardware.**
  - A Portable laptop
  - 512 MB Ram
  - 40 +GB
  - External Zip drive
- **Network Monitoring Software.**
  - NetBSD is reputedly the best..
  - A Silent Sniffer that speaks only TCP/IP with ARP disabled.
  - Employ VLAN with SSH or a Dial-back modem for Remote Administration.

Monitoring The Network Contd

- Possible Network Monitors.
  - tiptop, Ethereal and Snort.
  - Snoop, iptrace, Sniffer Pro, Etherpeek, LANalyzer
  - NetMon, Network Tracing and Logging and Cisco IDS.
- Network Monitor Location.
  - Host Monitoring - On the same Hub or switch. The switch should have Switch Port Analysis (SPAN).
  - Network Monitoring - At the network perimeter.
  - A Physically secure location.

Monitoring Thoughts

- Run a Sniffer detection tool prior to connecting yours.
  - Someone may already be listening to the network.
- Capture the network traffic as close to the source host as possible.
  - Hackers use bounce sites to attack hosts.
- Have the capability of viewing the captured data as a continuous stream.
  - This provides an overview of what the hacker is attempting to do.
  - Reconstruct documents, etc
- Have the capability of viewing the packets at the lowest level.
  - High-level analyzers will sometimes strip off data that is not important for fault analysis but could be important for investigative purposes.
    - Options and fields to identify the OS.
    - Typing speed of user.
    - Printer variables, X display variables , etc.

Common Network Forensics Mistakes

- Failure to **Monitor**.
  - ICMP Traffic
  - SMTP, POP and IMAP Traffic.
  - UseNet Traffic
  - Files saved to external media.
  - Web Traffic
  - Senior Executives Traffic.
  - Internal IP Traffic.
- Failure to **Detect.**
  - ICMP Covert Channels.
  - UDP Covert Channels.
  - HTTP Covert Channels.

Common Network Forensics Mistakes Contd

- Failure to **PlayBack.**
  - Encrypted traffic.
  - Graphics
  - Modeling and Simulation traffic.
- Failure to **Trace.**
  - Denial-of-Service.
  - Distributed Denial of Services.
  - Spoofed EMail.
- Failure to **Detect.**
  - Steganography.
  - Erased Logs
  - File Encryption.
  - Binary Trojans

Monitoring Tools

Dsniff	http://www.monkey.org/~dugsong/dsniff
tcpdump	http://www.tcpdump.org/
WinDump	http://netgroup-serv.polito.it/windump/
ethereal	http://www.ethereal.com/
Snort	http://www.snort.org/
Snoop	http://www.packetstormsecurity,org/

End of Lecture