University of New Haven
300 Orange Avenue West Haven CT 06516

Info-Security Master Class

Focused on Your Success

Computer Forensics

Information Technology Master Class

Class Outline and Overview

Focused on Your Success

- Properties of the evidence
- What is computer forensics all about
- How do people use and abuse computer systems
- What kind of evidence
  - What does it look like
  - What does it tell us
  - Where and how do we get it
  - When can we get it
  - When does it go away
- How do we interpret it
- How do we validate it
- What are the limits
  - How long does it last
  - How valid is it
    - admissibility
    - accuracy
    - timeliness
- Chain of custody issues
- Resources for Cyber Cops
- Presenting the evidence

Lets get on-line

Focused on Your Success

- Secure shell to the UNH Cyber-Cops Network
  - login: <User ID>
  - password: <Password>
  - prompt>
- The address: 24.1.84.100
- The port: 22
- The User ID and Password - from the instructor
  - For class purposes ONLY - only authorized users - no sharing UID and Password with others - only authorized activities and actions - when in doubt ASK

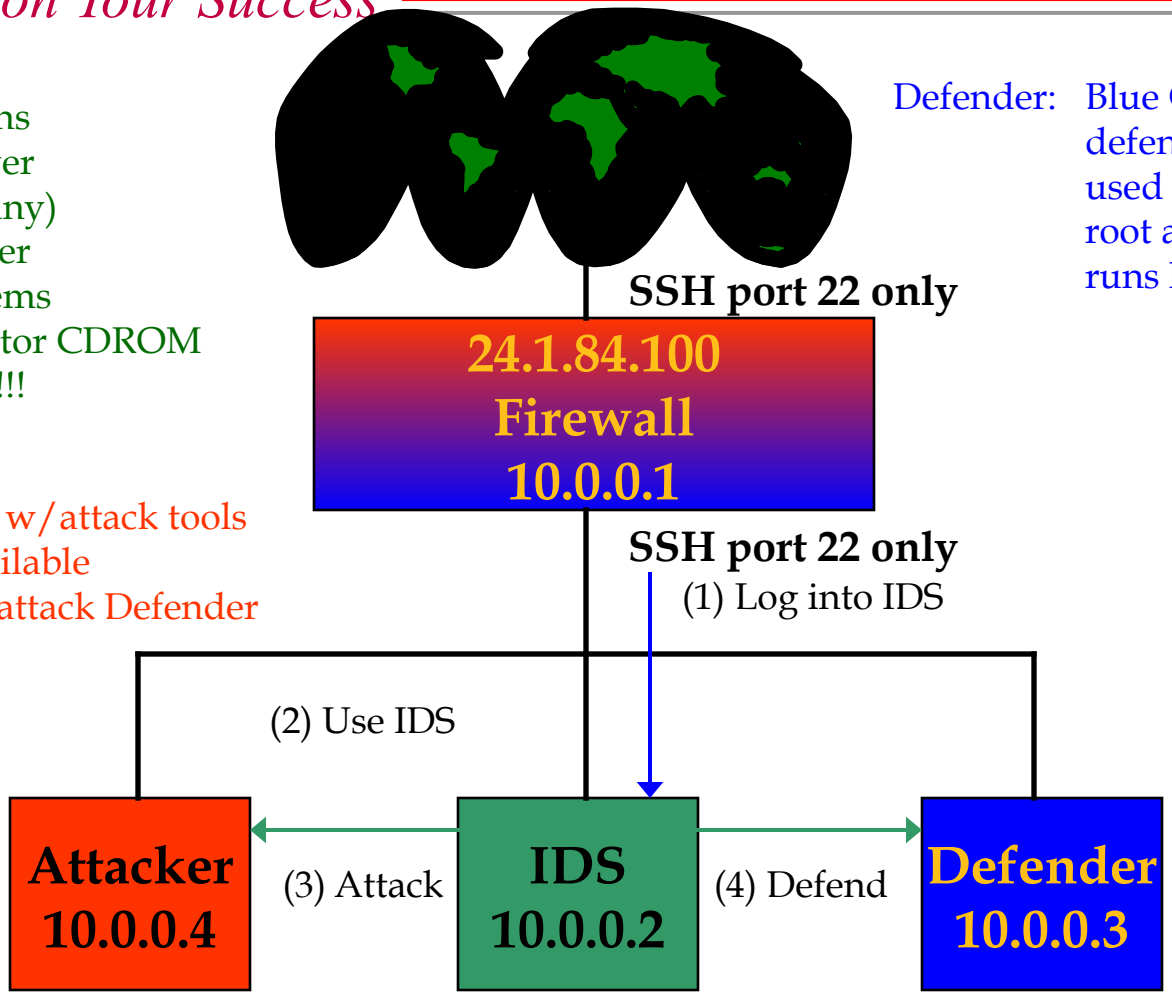
The Setup

Focused on Your Success

IDS: user logins
mail server
DNS (if any)
web server
IDS systems
investigator CDROM
DO NOT ROOT IDS!!!

Attacker: Red CD w/attack tools
root available
used to attack Defender

Defender: Blue CD
defender tools
used to practice defense
root available
runs lots of services



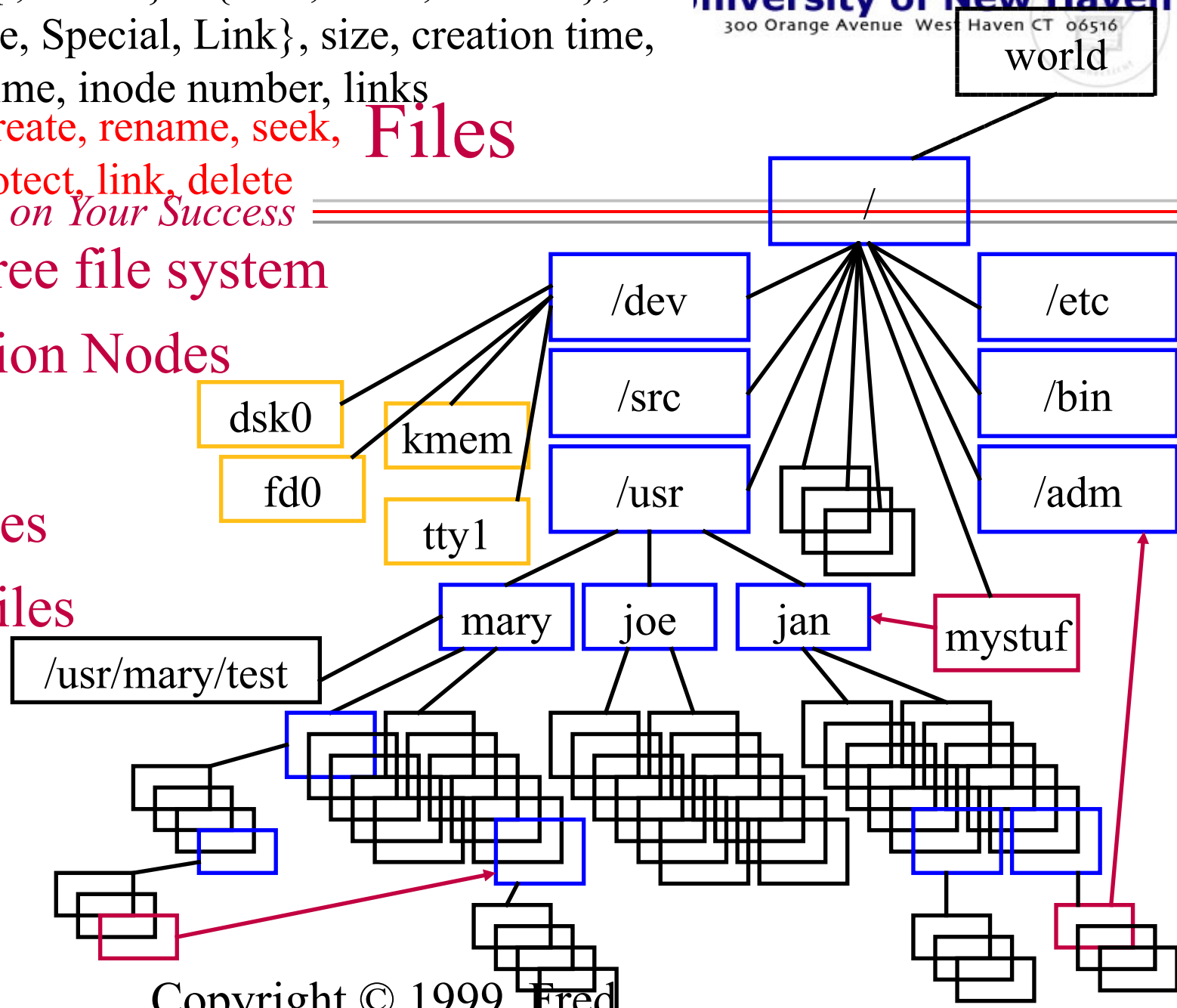
Files

{Owner, Group, World} x {read, write, execute}, {Directory, File, Special, Link}, size, creation time, modification time, inode number, links

Open, close, create, rename, seek, read, write, protect, link, delete

Focused on Your Success

- Rooted tree file system
- Information Nodes
- Links
- Directories
- Special files



Try the file system out

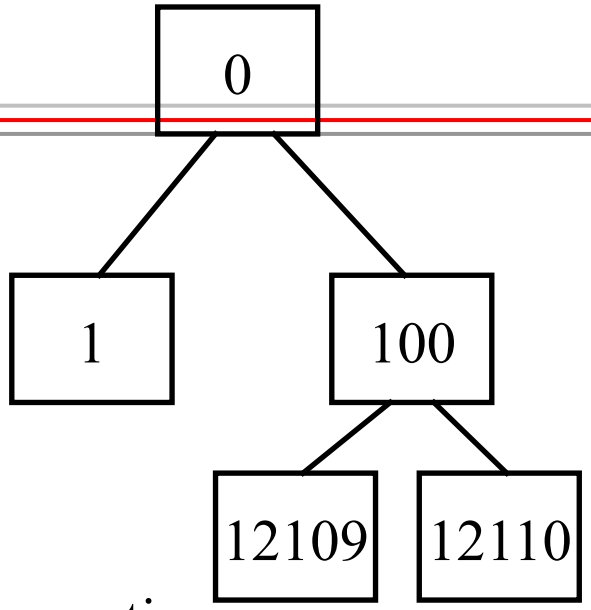
Focused on Your Success

- Try these commands:
  - ls
  - ls /
  - ls /etc
  - ls -l
  - pwd
  - ls -la
  - ls -R /usr/local
  - cd /etc;ls -R;pwd;cd;pwd
  - cat /etc/passwd
  - cat .profile
  - ln .profile prof;ls -la
  - cat prof;rm prof;ls -la
- And these:
  - find /usr/local -print
  - find . -print
  - find / -name “*ls*” -print
  - mkdir test
  - ls -ld test
  - cd test
  - cat > test
  - OK ^D
  - cat test
  - rm test
  - cd;ls;rm -r test;ls

Processes

Focused on Your Success

- Process table create, signal, kill, stop, start, swap, connect to files & ports
- Ownership fork, exec, read, write, run
- Group membership
- Parents and children

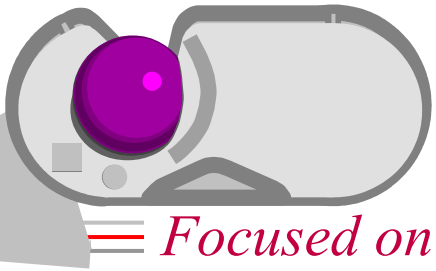


Pid	ppid	owner	grp	state	name	times
0	0	root	0	W	init	0.0 0.0 0.0
1	0	root	0	W	swap	0.1 1.1 1.2
…						
100	0	fc	23	SW	sh	0.1 0.0 0.1
...						
12109	100	fc	23	IO	grep	1.1 1.2 1.2
12110	100	fc	23	R	less	0.2 0.1 0.1

Try out processes

Focused on Your Success

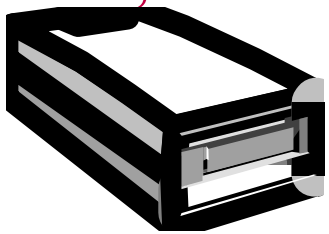
- Try these out
  - ps
  - ps -aux
  - ps -aux | grep root
  - sleep 30&
    - observe the <pid>
  - ps
  - kill -9 <pid>
  - ps
- These are simple commands to look at processes.
- There are far more complex process issues that we will get into later
- There are more options:
  - man ps
  - man kill
  - man grep
  - man bash

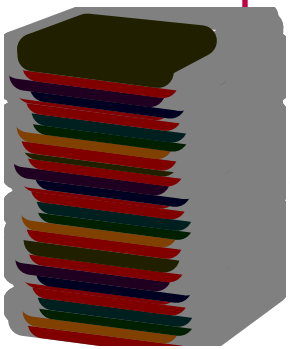


Devices

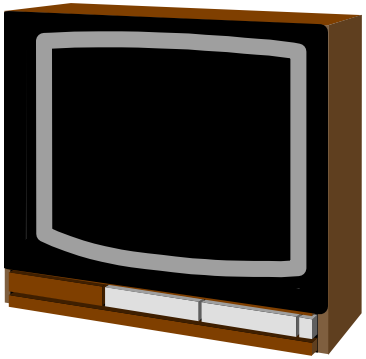
Focused on Your Success

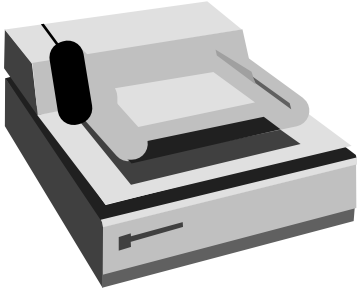
- File representations of physical or logical devices, with IO corresponding to file IO
  - network links, remote computers
  - disks, memory, tapes, CDs, cameras, microphones
  - PC boards, PCMCIA cards, network boards,
  - printer ports, terminal ports, keyboard, mouse, etc.





open, close, read, write, seek





Look at some devices

Focused on Your Success

- Try these:
  - ls /dev
  - ls -l /dev/tty*
  - cat /dev/tty
    - type a bit
    - end with ^D
  - ls -l /dev/cdrom
  - cat /dev/cdrom
    - ^C to stop this!!!
  - ls -l /dev | less
    - look at some of the details
- Special files
- Character type
  - terminals
  - serial ports
- Block type
  - disks
  - tapes (both)
- Links
  - for naming convenience
- Note protection settings

Users and Groups

Focused on Your Success

- Users as defined in the /etc/passwd file
- Groups as defined in the /etc/groups file

```
root:dflkjhsdf:0:0:Root:/:/bin/sh
bin:*:1:0:Binaries:/bin:/dev/null
…
fc:sdfjhlkj:100:100:Fred Cohen:/u/fc:/bin/sh
...
```

user, encrypted password, UID, GID, description, home directory, default shell

```
users:100:100,221,203,205
system:0:0,1,10
```

group name, GID, UIDs

Some user and group details

Focused on Your Success

- Try these
  - who
  - ls -lg
  - less /etc/passwd
  - less /etc/groups
  - ls -l ..
  - ls -lg ../*
  - ls -lgR /etc | less
  - ls -lRg /usr | less
  - echo “test file” > test-file
  - ls -lg test-file
- File protections
  - chmod 400 test-file
  - ls -lg test-file
  - cat test-file
  - echo “fix” > test-file
  - cat test-file
  - chmod 600 test-file
  - echo “fix” > test-file
  - cat test-file
  - ls -l test-file
  - chmod 644 test-file
    - you can r/w
    - group and world can read

Programs

Focused on Your Success

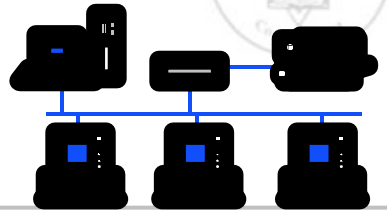
- Files with the 'executable' bit set
- Interpreted by looking at the 'magic number'
  - #!executable — interpreted by executable
  - <valid magic number> — load into memory and start
  - alphanumeric character — interpreted by /bin/sh
- Execution by other executable:
  - run the other executable with this file opened as FD=0
- Load and start:
  - 'fork' parent process and 'exec' this file

Lets write a program

Focused on Your Success

- A little program
  - cat > test-file
  - ls -l
  - cat $0
  - chmod 000 test-file
  - rm test-file
  - chmod 600 test-file
  - ^D
  - chmod 755 test-file
  - ls -l test-file
- Now let's run it
  - test-file /etc/passwd
  - test-file test-file
  - rm test-file
  - cat .profile
  - ls -l .profile
  - which ls
  - ls -l `which ls`
  - ls -l `which bash`
  - bash
  - ^D

Protocols and Networking



Focused on Your Success

- Services:
  - Program opens a network port and waits for input
  - As input arrives, the program does its thing
    - Web server waits for 'get' and types out files
    - Mail server waits for email and delivers it
    - Telnet server waits for connection for login program
    - Ftp waits for file transfer requests and transfers files
    - IRC waits for chat sessions and relays content
- Clients:
  - Program opens up port for output, makes request, awaits responses, shows to user, interacts

Let's look at the network

Focused on Your Success

- Try these
  - ifconfig -a
  - hostname
  - traceroute attacker
  - traceroute defender
  - traceroute firewall
  - traceroute ids
  - traceroute all.net
  - ping attacker
  - telnet attacker
  - ftp attacker
- Now for network tools
  - nc attacker 25
  - finger @ids
  - telnet defender 80
    - get /
  - ls /usr/sbin/in.*
    - try some of the services
  - cat /etc/hosts
  - vi /etc/services
  - vi /etc/inetd.conf
  - vi /etc/hosts.allow

Properties of the evidence*

Focused on Your Success

- Latent in nature
  - It can only be seen, understood, analyzed, and presented with and through tools.
- Often fragile and time sensitive
  - Sometimes exists for very short periods of time
  - Can be easily destroyed or modified
  - Can be easily mishandled
- Meaning is only clear in context
  - Patterns of information combine to provide substance
  - Like a puzzle you put together to get a picture
- Easily misinterpreted
  - Often misleading
  - Often patently false

Latent in nature

Focused on Your Success

- It can only be seen, understood, analyzed, and presented with and through tools.
- There are a lot of different types of systems and corresponding types of tools
- A lot of effort may go into getting the information via subpoenas, assistance, etc.
- Examples:
  - physical trace evidence on devices and in area
  - date and time stamps on data in the computers
  - telephone records
  - ISP access records
  - stored email
  - backups on tape and disk
  - network access logs
  - deleted sectors
  - web logs at remote sites

Latent evidence example

Focused on Your Success

- Let's look for some
  - grep failed /var/log/mess*
    - failed attempts to use services are stored here
  - lastlog | less
    - last time various users logged in are stored here
  - last | less
    - whole history of logins
  - lastcomm | less
    - who ran what when (root)
  - ls -l /var/log
    - look at the other logs and see what you can see
- Some less obvious ones
  - ls -lag
    - note the time and date stamps on all the files
  - ps -aux | less
    - note all the process information on usage time, IO, names of programs

Often fragile and time sensitive

Focused on Your Success

- Sometimes exists for very short periods of time
- Can be easily destroyed or modified
- Can be easily mishandled
- Tends to be temperature sensitive
- Often damaged by shaking or jolting of systems
- Can be erased easily
- Sensitive to magnetic fields

- Examples:
  - data in transmission only exists as it passes through
  - access records purged daily, weekly, etc.
  - backups retained only for days, weeks, months
  - file data overwritten by newer files
  - PDA data lost when battery runs out
  - FLASH cards erased in seconds

Temporary evidence

Focused on Your Success

- Network traffic
  - /u/local/bin/tcpdump
    - ^C pretty soon
    - you are seeing the packets generated by your own process as well as others
  - /u/local/bin/shownet -f
    - this will show all the traffic in text form - better ^C
    - note that much of the traffic was encrypted - ssh!
- Network traffic is VERY transitory
- It persists only as it passes an interface
- It is so voluminous it can not be stored in its entirety
- Real-time separation based on IP address or service is typically used

Meaning is only clear in context

Focused on Your Success

- Patterns of information combine to provide substance
- Like a puzzle you put together to get a picture
- Often involves many types of sources
  - paper
  - logs from many systems
  - purchase records
  - sequences of events
- Case Study:
  - Who posted the information?
  - Combine:
    - data provided by user
    - email records of knowledge
    - date and times of actions
    - access to systems used
    - date and time of accesses
    - motive shown in emails
  - Means, motive, opportunity

Example - audit trails

Focused on Your Success

- Find the password guessing
  - a failed login appears in the /var/log/messages log file
  - It is only accessible from root
    - unless specially configured
  - less /var/log/messages
  - grep failed /var/log/messages
- Which are guessing attacks
- Which are simple mistakes
- Put it in context
  - Where is it coming from?
  - What else came from there?
  - What account were they trying to get into?
  - What else is there to know about that account?
  - Correlate it to other events

Easily misinterpreted

Focused on Your Success

- Often misleading
- Often patently false
- Forgery commonly used
- Intermediaries used
- Groups cover each other
- Records intentionally deleted
- Insider obstructions
- Low quality experts
- People with an axe to grind

- Case Study:
  - Special Master made claims:
    - May have been altered data
    - Date and times unreliable
    - System never worked
    - Programs destroyed
    - Data not present
  - All refuted:
    - recorded statements
    - videotape of process
    - physics of forgery
    - correlation with other records

Example - who posted the email?

Focused on Your Success

- Try to forge an email
  - telnet ids 25
  - helo 10.0.0.3
  - mail from: <fc@10.0.0.3>
  - rcpt to:<UID@10.0.0.2>
  - data
    - enter a message here
  - .
  - quit
- NOTE:
  - don't try this at home!
- Now read the email
  - elm
    - this mailer will allow you to look at the mail in different ways
    - this new message should appear in the incoming mail
  - h
    - this should show the headers of the message - note the details of where it came from

What computer forensics is about*

Focused on Your Success

- Establishing a crime
  - by figuring out what happened when
  - by documenting the criminal activity
- Identifying the responsible parties
  - who, what, where, when
- Trace and trap
  - where are they
  - getting a warrant
  - getting better evidence
- Getting the evidence
  - ceasing it
  - searching it
  - interpreting it
- Explaining it
  - presenting the evidence
  - establishing evidence quality
  - establishing its meaning

Establishing a crime

Focused on Your Success

- Case Study:
  - NE University vs. graduate student X
    - NE has student testing computer security
    - Student reports results and is thanked
    - Student continues 'tests' unsupervised
    - Systems administrator claims student broke in
    - Student is brought before university disciplinary committee on charges - possible result - expulsion
    - Case outcome hinges on audit trails from computers

How do people use and abuse?

Focused on Your Success

- In order to understand the issues, you need to understand normal and abnormal use of systems
- Mostly this comes from experience
  - so we will try to give you some…
- Let's try an attack
  - sniffing for passwords on a LAN
  - then logging in

What does it look like

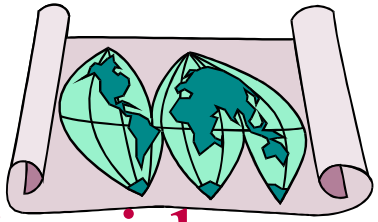
Focused on Your Success

- TCPdump files
  - 05:43:01.870000 1.2.3.4.13104 > 1.2.3.5.23: . ack 13280 win 32120 (DF)
- TCP show files
  - from IP.port -> to IP.port service-type content
  - **1.2.3.4.13197 -> 3.4.5.6.pop3 over TCP USER fred.**
  - **3.4.5.6.pop3 -> 1.2.3.4.13197 over TCP**
  - **3.4.5.6.pop3 -> 1.2.3.4.13197 over TCP +OK Password required for fred..**
  - **1.2.3.4.13197 -> 3.4.5.6.pop3 over TCP PASS mypassword.**
  - **3.4.5.6.pop3 -> 1.2.3.4.13197 over TCP**
  - **3.4.5.6.pop3 -> 1.2.3.4.13197 over TCP +OK fred has 0 messages (0 octets)..**
  - **1.2.3.4.13197 -> 3.4.5.6.pop3 over TCP STAT.**
  - **3.4.5.6.pop3 -> 1.2.3.4.13197 over TCP +OK 0 0.**
  - **1.2.3.4.13197 -> 3.4.5.6.pop3 over TCP QUIT**

Find my password

Focused on Your Success

- Turn on the sniffer
  - /u/local/bin/shownet -n 10.0.0.3 | tee zz
    - looking for defender data
    - 10.0.0.3 = defender
- I will log in
  - see if you can catch it
  - my password should appear in plaintext as part of the login sequence
- Now you have it
  - log in as me!
- Once logged in…
  - we could look around
  - or setup to come in again
    - cat .rhosts
    - echo '10.0.0.2' >> .rhosts
  - now log out and you should be able to come in with rsh…
    - you're in again and again
    - rsh 10.0.0.3
    - rm .rhosts
  - but not under Linux!
  - look at /var/log/messages!!!

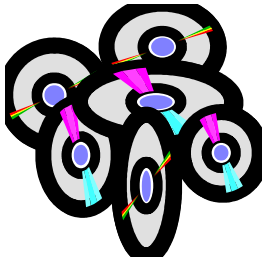


University of New Haven
300 Orange Avenue West Haven CT 06516

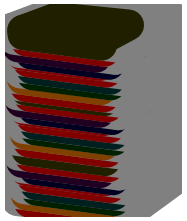
What kind of evidence do we get

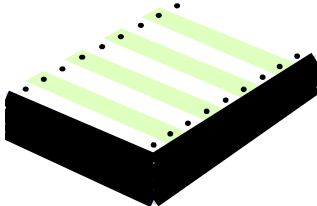
Focused on Your Success

- Electronically collected
- Records of activity
- In various forms
- From various sources
- Generated for various purposes
- Often normal business records
- Sometimes the system is altered to gather the data



- Typical audit trails include:
  - Date and time
    - of creation, last use, modification
  - Identification information
    - program names
    - function performed
    - user names, owners, groups
    - IP addresses, port numbers
    - protocol types
    - portions / all of the content
    - protection settings





What does it look like

Focused on Your Success

- System log files (syslog / messages / …)
  - Jan 27 05:38:22 Web.pl[32136]: twist proxy.gv-nmc.unisource.nl to /u/fc/bin/Web.pl 194.151.95.22
- Program-specific files
  - 1999/01/27 05:38:23 Allow 194.151.95.22 GET /game/HackMove?Q0=L1%2FUnixSendmail HTTP/1.0
- Directory listings
  - file type (d=directory, s=special, - = data/program file)
  - links, user, group, size (bytes) modification date/time, filename
  - drwxr-xr-x 2 fc users 1024 Jan 26 16:48 bin.
  - drwx------ 9 fc users 1024 Jan 13 06:56 clisp
  - drwxr-xr-x 4 fc users 2048 Jan 22 07:28 emacs
  - -rw-r--r-- 1 fc users 693 Jan 25 19:48 setup
  - drwx------ 3 fc users 1024 Jan 22 07:33 src
  - -rw-r--r-- 1 fc users 56496 Jan 26 22:50 tcpshow.c
  - -rw-r--r-- 1 fc users 1148549120 Jan 27 06:00 u.tar

What does it look like

Focused on Your Success

- Process status information

```
root        1  0.0  0.0   776    64  ?  S   Jan 17   0:31 init [3]
root        2  0.0  0.0     0     0  ?  SW  Jan 17   0:13 (kflushd)
root        3  0.0  0.0     0     0  ?  SW< Jan 17   0:20 (kswapd)
root       13  0.0  0.0   756    40  ?  S   Jan 17   0:50 update (bdflush)
root       89  0.0  0.0   908    12  ?  S   Jan 17   0:00 (klogd)
root       93  0.0  0.1   792    80  ?  S   Jan 17   0:35 /usr/sbin/inetd
root      175  0.0  0.0   776    52  ?  S   Jan 17   0:01 gpm -t mman
root      181  0.0  0.0   768     0   6 SW  Jan 17   0:00 (agetty)
root      202  0.0  0.0  1916    44  ?  S   Jan 17   0:00 (xdm)
```

  - the user, process ID, times, process state, date started, total run time, and program name
  - this log indicates clearly…
    - Linux, on the Internet running X11, up for a long time, and that it is missing a number of log entry details

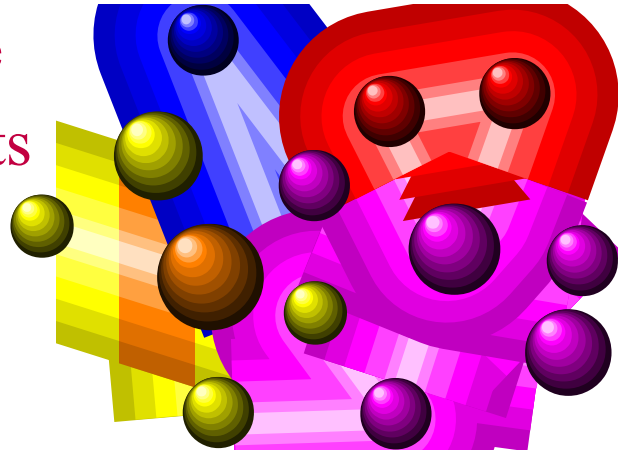
What does it look like

Focused on Your Success

- A Traceroute command

```
traceroute to 207.222.214.225 (207.222.214.225), 30 hops max, 40 byte packets
 1  cr1-hfc1.lvrmr1.sfba.home.net (24.1.84.1)  81.435 ms  30.254 ms  19.458 ms
 2  r1-fe2-0-0-100bt.frmt1.sfba.home.net (24.1.80.1)  25.47 ms  32.153 ms  25.403 ms
 3  10.0.255.245 (10.0.255.245)  22.304 ms  39.679 ms  37.361 ms
 4  bb1-fe0-0-100bt.rdc1.sfba.home.net (24.0.0.2)  17.44 ms  34.294 ms  19.798 ms
 5  172.16.4.74 (172.16.4.74)  19.545 ms  27.381 ms  35.842 ms
 6  mae-west.netcom.net (198.32.136.15)  33.521 ms  31.967 ms  20.851 ms
 7  h10-0-sjx-ca-gw1.netcom.net (163.179.233.213)  33.307 ms  21.738 ms  57.063 ms
 8  h0-0-0-3-dal-tx-gw1.netcom.net (163.179.232.185)  125.816 ms  139.07 ms  108.534 ms
 9  f3-0-dal-tx-gw1.netcom.net (163.179.1.129)  121.259 ms  141.544 ms  98.627 ms
10  other.all.net (207.222.214.225)  132.364 ms  103.101 ms  102.894 ms
```

  - The path from here to there
    - NOT necessarily from there to here
  - Intervening infrastructure elements
  - Response times and IP addresses



Let's find our own attack

Focused on Your Success

- Login as me on defender
  - telnet 10.0.0.3
    - user fred
    - password zippy12
  - look at the log files
    - last login
      - we have corrupted that one
      - we should have come as someone else
    - /var/log/messages
      - note the times and dates
      - note where it came from
- Save the evidence
  - cp /var/log/messages mess
- Work with the copy
  - but secure the original
    - it might go away
      - every day or two it will in RedHat Linux
    - it might get altered
      - attackers use automatic alteration programs for this
- Look for other evidence
  - what might you find?

Let's logout for now

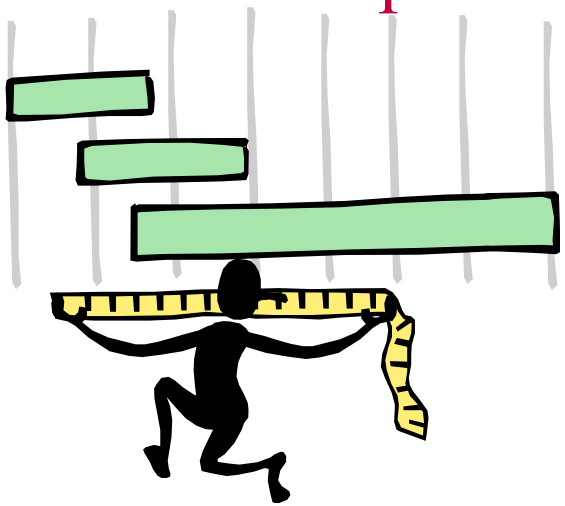
Focused on Your Success

- ^D to logout
- Come back to your window
- Exit the secure shell program
- We'll be back for more - later

What does it tell us

Focused on Your Success

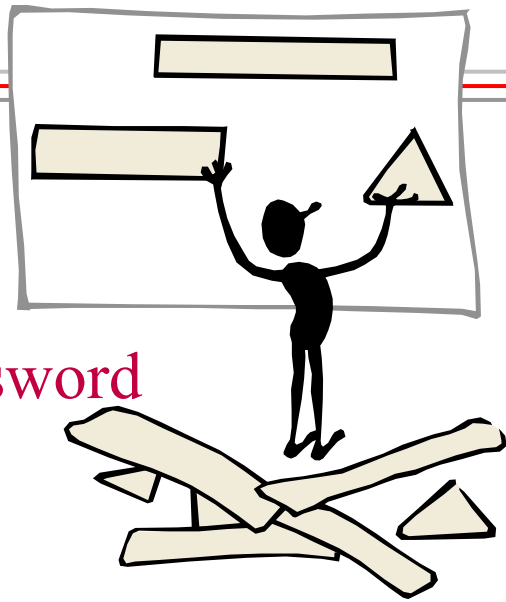
- Details of things that happened inside of computers
  - At this time
  - This thing was done
  - By this program
  - Acting for this user
  - With this result



- The timeline and pattern of these is interpreted to demonstrate criminal activity, cause, & intent

Case example

Focused on Your Success



- Suppose the audits tell us this:
  - Someone tried to telnet into the computer
  - They guessed 47 times before finding a password
  - Finally they got a good one and logged in
  - The ran a list of different programs
  - They got data from a list of files
  - They planted a hole for remote access as the user
  - They left for now
  - They returned later and started to delete files
- What can we conclude?

Some educated guesses

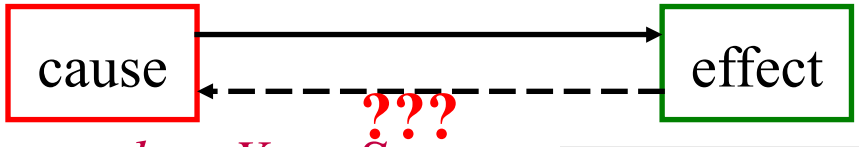
Focused on Your Success

- Tried to telnet into the computer
- 47 guesses to find a password
- Got a good one and logged in
- Ran a list of different programs
- Got data from a list of other files
- Planted a hole for remote access as the user
- Left and returned later and started to delete files

- No other attack methods - weak
- We had weak passwords
- They meant to break in
- It depends on the programs
- They intended to take data
- They intend to return and repeat attacks - not just a casual visit
- They are malicious and are intent upon causing real harm

Also: they were not apparently very skilled, they were persistent, they acted like crackers - not hackers, they may think we are watching and want to avoid being caught, they may be opposed to something we are or do.

How certain are we of this?



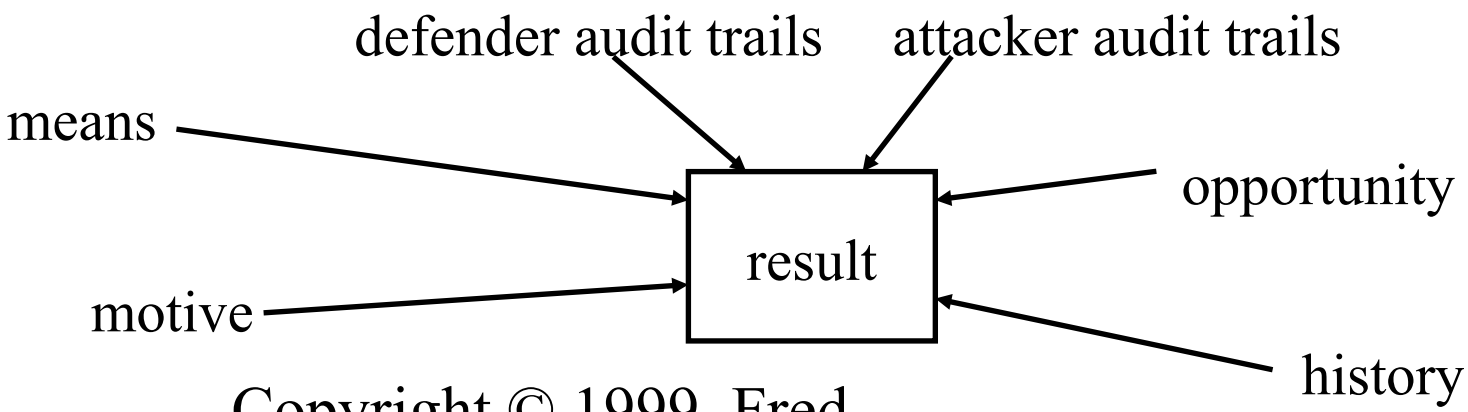
Other causes may result in the same effect

- The more details the closer we come to certainty.
- At the level of the last problem, they are guesses.
- Experience and the ability to do experiments in support of forensics can take us a log way:
  - Start with detailed audit results
  - Do real attacks that produce similar results
  - Generate a nearly identical results in a demonstration
  - This shows that the behavior could have generated these audit trails
  - BUT not that this is the only way to generate them

How to be more certain...

Focused on Your Success

- More related facts limits alternative explanations
- Other forms of evidence help convince juries
- In some cases we can do mathematical analysis
  - to show that specific other explanations are unlikely
  - to show how complex it would be to generate in other ways



Where and how do we get it

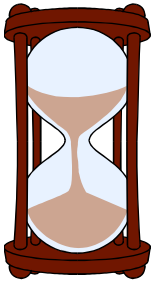
Focused on Your Success

- We get it from computers
  - by knowing
    - what to ask for (syslog file, messages, directory listing, …)
    - how to get it (cat it, do an ls -la, print it, save it to disk, ...
    - how to read it (when, what happened, by whom, how, …)
    - what it means (somebody broke in and stole data)
- People help us get it
  - by examining the computers (hardware and software)
  - by electronically analyzing things
    - programs to search, organize, extract, present, etc.

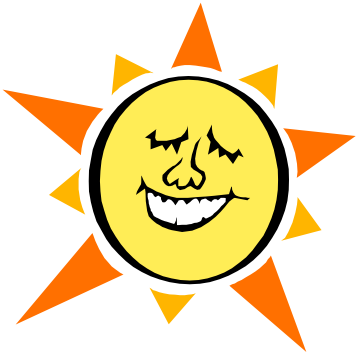
When can we get it

Focused on Your Success

- Time is the enemy
  - log files are not usually kept for very long
  - 24 hours for ISPs is typical
  - different logs retained for different time periods
  - billing records often kept
  - detailed records take a lot of time and space -> cost
  - system logs tend to stay for a long time - sometimes years



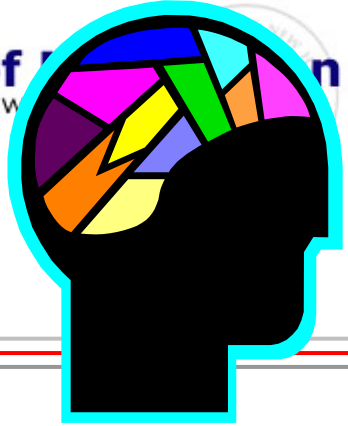
- File information is often retained
  - in backup tapes
  - dates and times only change with reuse
  - on-line backups
  - deleted file space is not always cleared
  - copies are often kept around by the OS



When does it go away

Focused on Your Success

- The more detail, the faster it goes away
  - connection records often disappear immediately
  - logins often stay for weeks or longer
  - file changes may stay for months or years
  - backups are retained for many years
- The more detailed the less often kept at all
  - keystrokes go away as they are typed
  - encrypted information is usually discarded ASAP
  - private session keys are gone at the end of sessions
  - file encryption keys often retained
  - process information changes by the second



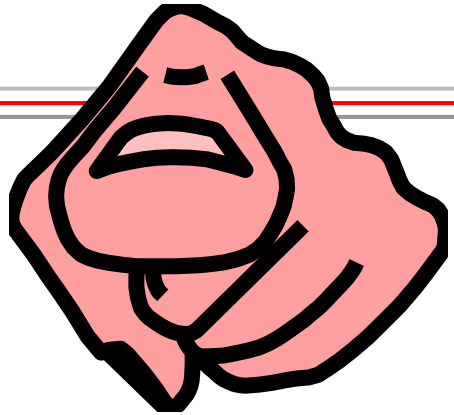
How do we interpret it

Focused on Your Success

- Expert interpretation is often required
  - similar looking things can be quite different
  - little details may mean a great deal if you see them
  - experience is a very good teacher
  - normal system experience as well as under-attack experience helps
- A major site was under attack
  - audit trails of network packets were taken during the attack cycle

Case Study

Focused on Your Success

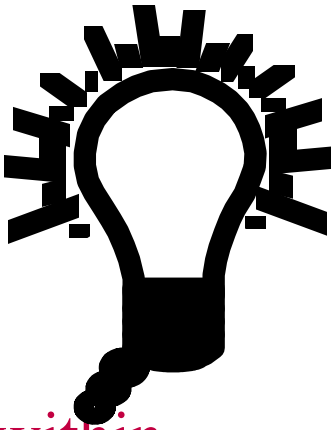


- A similar audit trail to a real case
  - 22:11:39.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:40.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:41.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:42.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:43.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:44.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:45.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:46.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
  - 22:11:47.820000 4.1.8.10 < 20.222.24.225: icmp: echo request
- The source address (in the actual case) is identified by lookup in the NIC as being on the other side of the world.
- The destination is a machine in the victim's site
- Any conclusions from this audit trail?

Interpretation of the audit trail

Focused on Your Success

- A series of very regular network scan packets
- An apparent source across the globe
- BUT - regularity within 1 ms
- This is inconsistent
  - because packet jitter from around the world is not within milliseconds
  - the source was likely fairly local - and in the path to the forged remote location
- Traceback found culprit two hops away

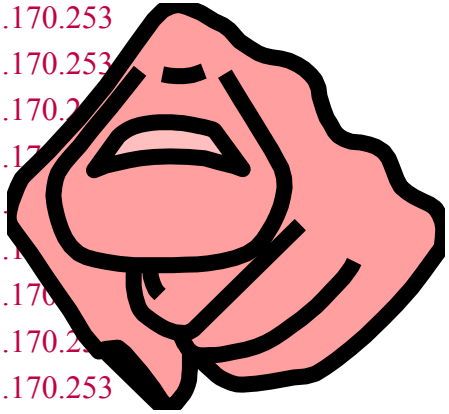


Case Study - refused telnet attempts

Focused on Your Success

- During a large-scale attack

- 198.133.170.253 unknown 1996/03/13 19:56:33 in.telnetd 24601 all refused connect from 198.133.170.253
- 198.133.170.253 unknown 1996/03/13 20:01:45 in.telnetd 25009 all refused connect from 198.133.170.253
- 198.133.170.253 unknown 1996/03/13 20:02:01 in.telnetd 25046 all refused connect from 198.133.170.253
- 198.133.170.253 unknown 1996/03/13 20:03:02 in.telnetd 25138 all refused connect from 198.133.170.253
- 198.133.170.253 unknown 1996/03/13 20:03:57 in.telnetd 25228 all refused connect from 198.133.170.2
- 198.133.170.253 unknown 1996/03/13 20:08:58 in.telnetd 25630 all refused connect from 198.133.17
- 198.133.170.253 unknown 1996/03/13 20:13:57 in.telnetd 26141 all refused connect from 198.133.
- 198.133.170.253 unknown 1996/03/13 20:18:57 in.telnetd 26542 all refused connect from 198.133.1
- 198.133.170.253 unknown 1996/03/13 20:23:57 in.telnetd 26930 all refused connect from 198.133.170
- 198.133.170.253 unknown 1996/03/13 20:28:57 in.telnetd 27317 all refused connect from 198.133.170.2
- 198.133.170.253 unknown 1996/03/13 20:33:57 in.telnetd 27715 all refused connect from 198.133.170.253
- 198.133.170.253 unknown 1996/03/13 20:38:55 in.telnetd 28108 all refused connect from 198.133.170.253
- 198.133.170.253 unknown 1996/03/13 20:43:56 in.telnetd 28499 all refused connect from 198.133.170.253
- 198.133.170.253 unknown 1996/03/13 20:48:56 in.telnetd 28890 all refused connect from 198.133.170.253
- ...
- 198.133.170.253 unknown 1996/03/13 22:10:07 in.telnetd 6022 all refused connect from 198.133.170.253



During a major attack

Focused on Your Success

- These audit trails were observed
  - the systems administrator was traced down at home in the evening - it turned out to be a university site
  - somebody had broken into a root account
  - they tried a few times manually - then automated
- They set up a program to retry every 5 minutes
  - regularity indicated early that this was automation
  - even with automation, there was some jitter because of there being several hops & most computers are not regular to the second for such things

How do we validate it

Focused on Your Success

- For evidence, we have issues of validity
- For investigation, we need only probably cause to obtain a search warrant
  - validity is not of as high a standard
- The search normally exposes the real crime
- Validation is done by expert witnesses:
  - better if they have tools to aide them
  - better if they present evidence well
  - better if they know what they are talking about

Validation - case study

n Your Success

- Civil trial - expert witness for one side turned into a special master for the court
- The 'special master' was clearly biased and had made many unsupportable statements
- In the end, two things won out:
  - refutation of several 'expert' opinions by physical evidence (analysis of a video tape, limits of time to do things the claimant was accused of by the SM)
  - evidence of the defendant violating the court's order by perpetrating acts during the search and seizure

Getting it - Case Study

Focused on Your Success

- Somebody has been posting insider information
  - to Yahoo in a company forum
  - this is impacting stock as well as revealing future moves
  - we need to find out about the people posting it
- Start at your Web browser and find the URLs
  - figure out what the Yahoo URLs look like
  - write a small program to fetch the whole bunch
- Get the related information on posters
  - get a warrant if you can, find the little that Yahoo knows
  - use posted information to figure out who did it.

Getting it from Yahoo

Focused on Your Success

- Use the browser
  - go to a forum
  - look at a posting
  - get the URL
  - look at another posting
  - compare the URLs
  - try making up your own URL
  - now that you have the form
    - magic happens…
    - you write a few tiny programs to get and manipulate the data
- Instructor demonstration:
  - write a short shell script
  - use 'webget' to fetch the files
  - use grep - find related articles
  - turn them into a report
    - keep the downloads clean
      - get a copy and hold it
    - work on copies and temp files to get the answers
    - keep the process documented and the intermediate files on hand
    - write it up

What are the limits of the evidence*

Focused on Your Success

- How long does it last
- How valid is it
- Admissibility
- Accuracy
- Timeliness
- Chain of custody issues
- What can go wrong

How long does it last?

Focused on Your Success

- Tape, CDs, disks
  - 1-3 years if kept well
  - can fail in minutes
    - excessive heat
      - a car on a sunny day
      - a radiator or heater
      - a match
  - or in seconds
    - electromagnetic
      - a strong magnet
      - high impulse vibrations
      - overwritten
- Paper (non-acid)
  - hundreds of years
  - can fail in minutes
    - excessive heat
      - fire
      - heaters / radiators
    - shredding
      - a shredder
      - eating it
- Audit trails
  - some are never stored
  - others last minutes, hours, days, weeks, months, years

Case Example: ISP records gone

Focused on Your Success

- Typical ISP contacted within minutes of an attack attempt against systems via their systems
  - The person who deals with LE is not in
    - The operator isn't sure what to do
    - We await a call back
  - Two days later, the contact person calls back
    - I'd be happy to help…
    - But those records are only retained for 24 hours
    - You should have shown up with a search warrant

How long does it last

Focused on Your Success

- Attacks are not instant either…
  - Take down 100 computers w/LAND: 30 seconds
  - Crack to guess fairly easy passwords: 5-10 minutes.
  - Researching a target over the Web: hours-days
  - Program some new attacks for a serious attack: days
  - Spreading a virus from source to target: weeks
  - Salami attacks and kiting schemes: weeks to months
- If you are there when the attack is underway:
  - How fast do you need to act to catch them in the act?

How valid is it?

Focused on Your Success

- Computer data is easily altered
  - by attackers it is done in the normal course of events
  - by defenders to make it look like an attack?
  - by accident all of the time
    - but rarely by hardware faults
    - sometimes by software faults
- It's usually fairly easy to tell if it was altered
  - it's gone completely over a portion of time
  - inconsistencies show up across audit trails
- It's hard to alter undetectably

Case study: Is the audit altered?

Focused on Your Success

- A potentially altered audit trail in a civil suit
- Access to copies of audit files provided
- Analysis done by comparing redundant audit entries from different audit trails
- Comparison to file modification dates, etc.
- Final result:
  - No detectable alterations were found
  - Alterations that would be at issue would have been detectable given the time available for the attack

How valid is it?

Focused on Your Success

- Unaltered audit information is not always correct
  - Forged email, sessions, etc. look just as real
  - If I break in to user 'Joe' it looks like 'Joe' did it
  - Audit records fail during high load conditions
  - Audit records fail under unanticipated conditions
  - Some programs don't produce records consistently
- Audits can often be avoided
  - Program audits are easily bypassed by not using the program to alter the data

Case study: kidnapping

Focused on Your Success

- An email ransom note shows up in a kidnapping
  - The apparent source of the email is given by mail headers on the received email
  - The source is tracked quickly and the person whose account it come from is picked up
  - The interview demonstrates that this person was not involved in any way and was unaware of the email
- By the time records that might have revealed the real source were thought to be needed they were no longer available for retrieval

Admissibility?

Focused on Your Success

- Most computer records come in under the business records exemption from heresy
- They come in through expert testimony
  - Systems administrator declares that they were taken in the normal course of business
  - Indicates specific actions taken to collect records
  - Shows them in light of other records taken and kept
  - Expert witness explains and interprets the records
  - Opposing experts make their claims

Let's login again

Focused on Your Success

- Secure shell to the UNH Cyber-Cops Network
  - login: <User ID>
  - password: <Password>
  - prompt>
- The address: 24.1.84.100
- The port: 22
- The User ID and Password - from the instructor
  - For class purposes ONLY - only authorized users - no sharing UID and Password with others - only authorized activities and actions - when in doubt ASK

Accuracy?

Focused on Your Success

- Computer records are NOT ALWAYS accurate
  - Times and dates are often off
    - compare them to a standard
    - http://all.net/
      - press "what time is it?"
    - note your computer's time
    - note the Navy's time
  - File time/date stamps altered
    - echo "test" > aa;cat aa
    - ls -l aa;sleep 60;touch aa
    - ls -l aa;cat aa;rm aa
- Inaccuracies can be intentional
  - cd /u/local/attacks
  - ls genocide/log-wipers
    - 'cloak' and 'cloak2'
      - wipe you from /var/adm/*
      - wipe you from utmp
      - fully automatic
      - need to be root
    - ps hiders
      - change your process names to hard-to-detect ones
  - ls sabotage/rootkit;cd
    - create backdoors

Timeliness?

Focused on Your Success

- Real-time capture
  - network traffic, telephone calls, IRC sessions
- Rapid capture (hours-days)
  - ISP dial-ins, system logs, backups, cache files
    - telnet defender
    - less .netscape/cache/index.db
    - find the evil files
    - 15 minutes
- Timely analysis
  - PDAs
    - run out of power
    - lose memory
  - disks/tapes/CDs
    - 1-2 years expected lifetime
    - some last much longer
    - heat/magnets can destroy
  - data leading to other data
- Example screw-up
  - attack reported FBI 1998-04
  - investigated 1999-01

Completeness?

Focused on Your Success

- Most computer records are fairly minimal
  - date, time, major event
  - sometimes only start, not stop
  - sometimes only stop, not start
  - content often missing
  - user information limited
- Better logs are easy to get
  - keystroke logging
  - tapping specific IPs / ports
  - log files take space
- Computer records can be missing things
  - entire records can be missed
  - attackers try to destroy logs
  - attackers try to avoid logs
  - attackers try to forge logs
  - almost always some evidence of alteration
  - use redundancy
    - example from all.net
      - http://all.net/
      - managing network security
      - incident at all.net

Chain of custody issues?

Focused on Your Success

- Just like any other evidence
  - must get to it in time
  - must collect it properly
  - must transport it properly
  - must hold it securely
  - must analyze it carefully
  - must leave evidence in tact
  - must provide repeatability
  - must be available for defense
  - must be presentable in court
  - must be explainable in court
- Just because it's in a computer doesn't make it right
  - Who got it for you?
  - Who told who else when?
- Example:
  - served ISP
  - ISP called defendant
  - defendant destroyed evidence

What can go wrong?

Focused on Your Success

- Pull the plug or not?
  - astute points on both sides
- Marking it properly
  - bag and tag techniques
- Transport sensitivity
  - shaking
  - temperature
  - dust, fumes, magnets, etc.
- Storage sensitivity
  - time in storage
  - also like transportation
- Analysis errors
  - not working the copy
  - modifying/deleting evidence
  - missing evidence
  - misreading evidence
  - not getting redundant data
  - looking excessively
- Presentation errors
  - talking technical
  - not using pictures
  - denying weaknesses of digital evidence

A Little Exercise

Focused on Your Success

- You are called in on a case
- They tell you that I have broken into their computer
  - Their computer is
    - 10.0.0.3
  - I broke in from outside
    - they say from 10.0.0.4
  - I stole the password file
    - what evidence is there?
  - I ran 'crack' on it and guessed other user passwords
  - I stole a document called "Private-Data"
- Your job:
  - Look for evidence
  - Secure it for analysis
  - Try to determine
    - Is there evidence?
    - What does it show?
    - Does it trace back to me?
    - What else do you need?
- GO!!!
  - Ask if you have em
  - 15 minutes to do it

Some Other Sources of Evidence

Focused on Your Success

- Lets look at other records
  - Email
    - in user storage areas
    - on servers and in pending mail files
    - from's and to's
  - Radius logs
    - from a ppp server
  - Disk dumps
    - let's look at a floppy!
  - Database transaction records
- Still more logs
  - Web / gopher logs
    - in the web area
    - correlate with system logs
  - Back-end logs
    - for back end access
  - Email send/receive logs
    - sender, recipient, time
    - kept independently
  - Telephone call detail logs
  - ISP logs

Email

Focused on Your Success

- In user storage areas
  - review my email on attacker in /u/fc/.Mail
- On servers and in pending mail files
  - review pending email in /var/spool/mail/*
- From's and to's
  - if I send it to you, we may both have records.
    - The combination of the records is more powerful than either one alone
- Example from a recent case:
  - "… Hope you are buying lots of stock. I am considering it - unless you have some insider information for me…"

Based on my email records

Focused on Your Success

- What do you conclude about me as an attacker?
- Who else is involved?
- What do their records indicate?
- Is anything about to happen?
- Can we set up to capture a live session?
- How do we correlate the session with the human?
- What would we do to set up to catch me?

Radius logs

Focused on Your Success

- From a ppp server using Radius
  - Start date and time, end date and time, user ID, IP address used, IP address of originator, which port was used, (lots of other data)
- Find all the records for:
  - albonej
    - cd /u/local/logs/radius
    - grep albonej 19* | less
  - What is their work pattern?
- I claim somebody broke in
  - They took over my account
  - I haven't used it for years
  - I know nothing of these attacks
- Am I lying?
  - What do you do to tell?
  - How can radius logs help?
  - What else do you need?
  - What questions should you ask and who should you ask?

Disk Dumps

Focused on Your Success

- let's look at a disk!
  - dd if=/dev/cd of=/tmp/testfile
    - STOP!!! Too much data!
    - We'll try something smaller
  - I have dd'd a floppy disk to /u/local/logs//floppydump
  - Can you find 'help'?
  - Can you see the partition table and all the DOS messages?
  - Can you see the directory entries and deleted/hidden areas?
- I did this:
  - cd /u/local/logs
  - dd if=/dev/fd0 of=floppydump
    - 2880+0 records in
    - 2880+0 records out
- You try this:
  - cd /u/local/logs
  - less floppydump
    - page through a while
  - /help
  - /
- A very nice way to search a disk

Database transaction records

Focused on Your Success

- Databases leave lots of evidence of transactions
  - Each database record typically has details of a transaction
    - user ID, what was done, done to what record(s), when, success or failure, reason for error (if any)
  - Database records are often available to the cleaver user
    - does the transaction record reconcile with the database state?
  - Backups of databases provide historical records
    - this depends on how well they use the backup mechanisms
  - Let's look at one...

Database records

Focused on Your Success

- A database is stored in
  - /u/local/database
    - cd /u/local/database
    - less nwind.mdb
- Write a program to
  - separate the records out
  - decode the data values
  - produce a 'standard' database
- Then read it with your favorite database or spreadsheet
- What does the database tell you about:
  - Albert Hellstern?
    - grep -i Hellstern * | less
  - Yang Wang?
    - grep -i "yang wang" * | less
  - Could you see deleted records this way?

Web / Gopher logs

Focused on Your Success

- Let's look at one:
  - cd /u/local/logs/web
  - ls -l
  - less 1999-01
  - grep course 19* | less
  - grep attack 19* | less
- Correlate with system logs
  - but I don't have them from the system those logs came from...
- Gopher logs:
  - they are essentially the same for the most part
- Error logs:
  - less err*
  - grep user err* | less
    - looks like somebody has been trying to get into this system by trying user IDs!
    - they are going after the 'vulnerabilities' database

Email send/receive logs

Focused on Your Success

- Sender, Recipient, Time
- Kept independently
- Let's look for them:
  - cd /u/local/logs/sys
  - grep sendmail * | less
  - grep sendmail * | grep -i error | less
- Can we correlate these logs with email logs?
- How do we do it?

Firewall logs

Focused on Your Success

- An increasing priority for law enforcement
- Often contain lots of detail of entry attempts, and may provide the only translation between inside and outside addresses
- From the logs, can you tell me how your packets get through the firewall?
- cd /u/local/logs/log
  - All of the logs from our firewall (for the first day or two of operation) are in here.
  - Look around and tell us everything interesting.
  - Are there any attack attempts?
  - How easy is it to get it right?

Other Logs

Focused on Your Success

- ISP logs:
  - These are the same as the logs we have been looking at all day - plus some more - perhaps
- Telephone logs:
  - Similar to radius logs, usually involving the same information you see on a phone bill
  - More detailed infrastructure logs may be available
  - Substantial database usage in telephone systems
- Back end logs
  - Usually a combination of the logs we have seen

Dealing with cryptography

Focused on Your Success

- Cryptography
  - www.accessdata.com
    - programs to get data from many popular programs
  - Search the Web
  - Go after keys - not messages
  - Get people to reveal the keys
    - by using them
    - by telling you
  - Do experiments with keys
  - Guess easy passwords
  - Break with big computing
- Stegonography
  - Sure you can hidE one message in the Characters of anotheR mEssage Text.
  - There are a lot of techniques that start with a cryptosystem and use it do vary the order or content of messages.
  - Find the secret message in this page.
- Many free applications are available on the Web

Tracking over the Internet

Focused on Your Success

- Programs you may want to use:
  - traceroute
  - whois
  - nslookup
- Then what?
  - Phone calls
  - Warrants
  - Searches

- Joined together in:
  - whoiss
- whoiss 10.0.0.2
- whoiss all.net

Other Online Resources

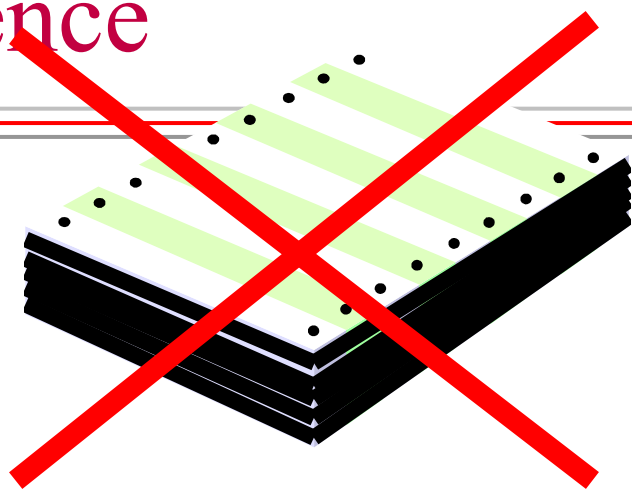
Focused on Your Success

- This pointer list comes from the htcc mailing list and has:
  - Bank Source Information
  - Computer/WWW Issues
  - Consumer Protection Sites
  - Criminal Justice Information
  - Government Web Sites
  - Investigative Sources
  - Legal Sources/Reference
  - Local/State Law Enforcement Web Sites
  - Military Sites
  - Other News Sources
  - Periodicals
  - Professional Associations, Training's, et. al.
  - Search Engines/Tools
  - Search for People/Businesses

all.net/cybercop/pointers.html

Presenting the evidence

Focused on Your Success

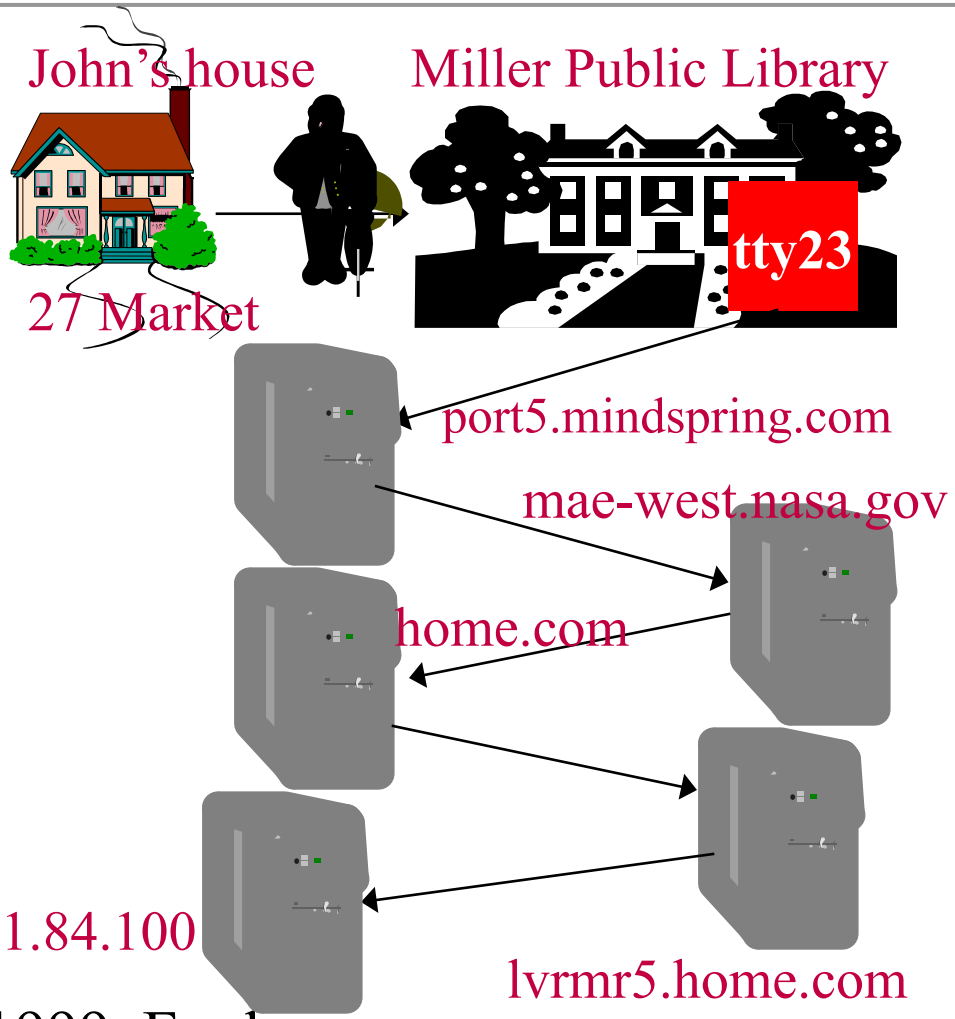


- Juries do NOT understand log files
- You need to explain it to them
  - Demonstrations help a lot
    - show what the user does and how the computer records it
    - Show records of the crime and conclude that they were generated by the perpetrator doing what you showed
  - Are there other ways to generate that? Tell us all about it.
    - Join together multiple sources to form a pattern that makes it harder and harder to figure out a way to come up with it all
- After showing the pictures - get to the details...

The evidence against John Doe

Focused on Your Success

- John left home that morning and went to the Miller Public Library, arriving about 8:45 AM
- He logged into tty23 using his user ID and, using the Internet, attempted to transfer key government files from 24.1.84.100 - a known drop site for Spies-R-Us
- He then took the downloaded information and placed it in a floppy disk, returning to his home at 27 Market



Focused on Your Success

Questions?

Thank You!