CYBER502x
Computer Forensics

Week 4: Linux/Unix Forensics Analysis Technologies

R·I·T

Investigating Linux/Unix systems

- Evidence Collection
- Preservation
- Analysis
  - Event reconstruction with timestamps
  - password entries, log files, history files, hidden files, suid/sgid files, recently modified binaries, recently created files, deleted files
  - keyword search, hash analysis….
- Report

Analysis

- General steps:
  - Start an analysis by looking at the partition table on the suspect drive
  - Retrieve deleted files
  - Examine MAC times
  - Keyword search for terms related to your case
  - Check for password, logs, hidden data, suid/sgid files
  - Examine emails
  - …

Hard-drive usage

- CynanLine LLC discovered this feature
- Self Monitoring Analysis Reporting Tool (SMART) displays
  - how many times has the hard-drive been turned on
  - for how many hours has it been used

Identify partitions

- Use Linux fdisk

```
$ fdisk /dev/hdd
```

or

```
$ fdisk /mnt/case1
```

(if case1 is the mount point for case1.dd mounted loopback)

Disk /dev/hda: 64 heads, 63 sectors, 1023 cylinders

Units = cylinders which is 64 * 63 * 512 bytes82 Linux swap

Device	Boot	Start	End	Blocks	Id	System
/dev/hda1	?	1	990	1995808+	83	Linux
/dev/hda2		991	1023	66528	5	Extended
/dev/hda3		xxx	xxxx	xxxxx	82	Linux swap

Identify partitions (cont'd)

- mmls (media management) from sleuthkit
  - http://www.sleuthkit.org/sleuthkit/man/mmls.html
  - `-t mmtype`
  - `-o offset` (in sector) into the image
- Examples
  - `# mmls disk_image.dd`
  - `# mmls –t dos -o 12345 disk.dd`

Separate each partitions for sleuthkit

```
# mmls -t dos sda.dd
DOS Partition Table
     Units are in 512-byte sectors

        Slot      Start         End           Length        Description
00:     -----     0000000000    0000000000    0000000001    Primary Table (#0)
01:     -----     0000000001    0000000031    0000000031    Unallocated
02:     00:00     0000000032    0001800031    0001800000    Linux (0x83)
03:     00:01     0001800001    0002000000    0000200000    Linux Swap
```

```
# dd if=sda.dd skip=32 count=1800000 of=sda1.dd
# dd if=sda.dd skip=1800001 count=200000 of=sda2.dd
```

mmls for gpt

- mmls –t gpt /dev/sdg
- GUID Partition Table (EFI)
- Offset Sector: 0
- Units are in 512-byte sectors

```
      Slot     Start        End          Length       Description
00:   Meta     0000000000   0000000000   0000000001   Safety Table
01:   Meta     0000000001   0000000001   0000000001   GPT Header
02:   Meta     0000000002   0000000033   0000000032   Partition Table
04:   00       0000000040   0000409639   0000409600   EFI System Partition
05:   01       0000xxxxxx   0xxxxxxxxx   0xxxxxxxxx   Untitled
06    -------  0xxxxxxxxx   0xxxxxxxxx   0000xxxxxx   unallocated
```

Mount ’em up!

- Mount what you think is the root f/sys
  - Do not modify in any way!
  - Mount with read-only option
  - `Mount –o ro,loop /my_hda1.dd /mnt/hacked`
    - Assume `my_hda1.dd` is a raw dd image representing a disk partition.

First analyzing MAC times…

- Key to every forensic investigation
- Modification (`mtime`): last time the file was written
- Access (`atime`): last time the file was read
- Change (`ctime`): last time the file's inode was changed
  - (on Windows C=file Creation time)

MAC times

- Installation of a rootkit / LKM / application leaves a number of files with timestamps very close to one another

MAC times can be changed easily

- utility for Linux/Unix file systems
    - touch can change both atime and mtime
- utility for Windows file systems
    - timestomp can change all three timestamps

Be nice to your MAC times

- MAC times are sensitive to change
- Collect MAC times before running other commands on system.
- You will use MAC times to create a timeline of activity.

mactime

- A tool in The Sleuth Kit
- A perl script that takes data files as input and sort the data to create a timeline

How to run mactime

- Step1: Create an intermediate data file

```
fls -f ext3 -m “/” –r images/root.dd > data/body
```

OR

```
ils -f openbsd -m  images/root.dd > data/body
```

- Step 2: Sort the data to create a timeline with mactime

```
mactime –b filename [time range]
```

Timeline example

```
Sat Dec. 12 2016 16:40:20 1234 .a. –rwxr-xr-x root root /bin/file_a
Sat Dec. 12 2016 16:40:23 4096 .a. d/drwxr-xr-x 0 0 31400 /dev/inet
                          32768 .a. d/drwxr-xr-x 0 0 15974/dev/cciss
                          ….
                          ....
                          ....
                          .....
                          .....
Sat Dec. 12 2016 16:45:56 4096 mac d/drwxr-xr-x 0 0 47163 /bin/file_b
                          1234 m.c –rwxr-xr-x root root /bin/file_a
```

Timeline reading

- Look for suspicious activity in the timeline
- Find deleted files
- For example, use fls + mactime, you get…

```
Wed Mar 20 2012 16:56:12 0 ..c s/srwxrwxr-x 500 500 127 /tmp/socket1
(deleted)
Fri Aug 23 2012 16:56:12 11 .a. l/-rw-r--r-- 0 0 34689 /tmp/file1 (deleted-realloc)
                         11 .a. -/-rw-r--r-- 0 0 34689 /etc/sysconfig/desktop
```

Other evidences

- Deleted files, log files and history files
  - Review as many as you can find
    - “Stupid” hackers will leave lots of clues
    - More sophisticated ones will try to cover their tracks
  - `/var/log/*`
  - `~/.bash_history`
  - `~/.history`
- emails
- pictures
- visited websites

Files and inodes in an abnormal location

- Recently created files *regular* files in /dev
- Finding clues using inodes
- Hash analysis to detect
  - known malware and rootkits
  - modifications to system binary files and configuration files.

Binaries that are often replaced by rootkits:

- Chfn
- Chsh
- Crontab
- Du
- Find
- Ifconfig
- Inetd
- Tcpd
- pidof

- Killall
- Login
- Ls
- Netstat
- Passwd
- Ps
- Rshd
- Syslogd
- Top
- ssh

Use find command

- to find hidden files/dir (start w/’.’ or “ “)

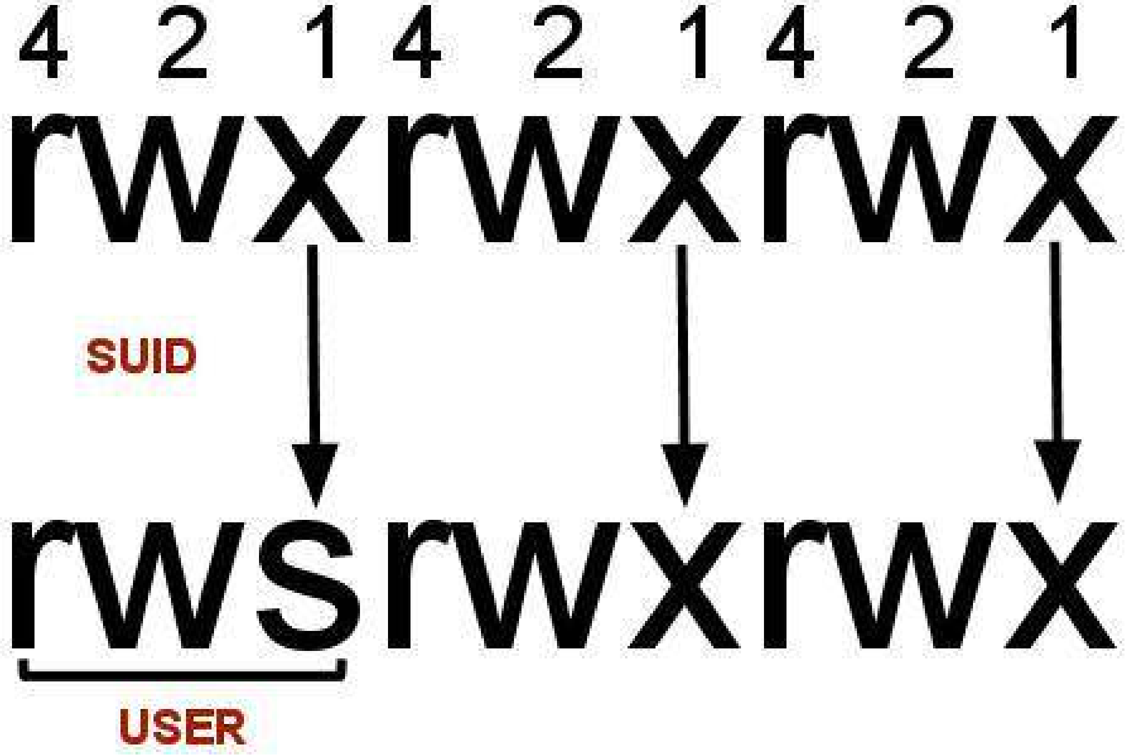
```
sudo find / -name “[. ]* -type f
sudo find / -name “[. ]* -type d
```

- to list all world-writeable files/dir:

```
find / -type f \( -perm -2 -o -perm -20 \) -exec ls -l {} \;
find / -type d \( -perm -2 -o -perm -20 \) -exec ls -ld {} \;
```

What does SUID/SGID programs do?

- Sets a permission that allows users to run an executable with the permissions of the executable's owner/group



Use find command (cont'd)

- To find all SUID/SGID files

    -
      ```
      find / \(-perm -4000 –o –perm -2000\) –type f
      ```

Use find command (cont'd)

- To find binary files that were modified in 1 day

```
find /directory_path –type f –a=x –mtime -1 -
print
```

- to find files that were created in less than 24 hours

```
find /directory_path –type f –a=x –bmin -24 -
print
```

Data carving tools

- foremost
  - Searches for files of known file types using foremost.conf
- Scalpel (not required)
  - With foremost, only files up to 4 Gigabytes could be carved, while with Scalpel the limitation is 16 Exabytes
- Magic rescue (not required)
  - Use a recipe file that describes how to recognize the beginning of the file and what to do when a file is recognized.
- PhotoRec/TextDisk (not required)
  - http://www.cgsecurity.org/wiki/PhotoRec

Other Free Forensics Analysis Tools

- Digital Forensics with Open Source Tools by Cory Altheide and Harlan Carvey, 2011
- TCT (The Corners Toolkit)
  www.porcupine.org/forensics/tct.html
- Sleuthkit/Autopsy
  www.atstake.com
- Digital Forensics Framework
- SANS Investigative Forensics Toolkit – SIFT

bootables

- Caine - http://www.caine-live.net
- Helixs/Helix3 Pro
- Kali
- Penguin Sleuth
- F.I.R.E
- Snarl

Commercial tools

- Guidance Software’s Encase
- AccessData’s Forensic Toolkit (FTK)
- ProDiscover Basic
- …

Analysis procedure

- Create a case
- Add evidence to a case
- Perform thorough analysis
- Obtain basic analysis data
- Export files
- Generate report

Practice

- http://www.honeynet.org/scans/scan29/
- http://www.sleuthkit.org/case/sotm_29/index.html
- http://www.honeynet.org/scans/scan29/sol/carrier/index.html