INF 528
Computer Forensics

Linux Investigations

Overview

- Linux File System
  - ext2/3
- Overview of Distributions
- Tracking Activity
- Print Spools
- Swap Space

Linux File System - recap

- Most linux systems today use either ext3 or ext4 file systems
  - – Alternatives: UFS, ReiserFS, ZFS)
- Disks are broken up into partitions (like windows)
  - – Partitions are broken up into groups
  - – Groups contain superblock, group descriptor, block bitmap, inode bitmap, inode table, and data blocks

Groups

- Superblock – stores all important information about the block
  - If it is wiped out, it must be recreated – ext2 stores a copy of the superblock in each group
  - If someone tries to wipe the filesystem, you could possibly recreate it with ext2fschk
- Group Descriptor – contains information about the group, such as which blocks are allocated and which are unallocated

Files & Directories

- Files are represented by inodes, and directories are files which contain a list of entries and pointers to those files
  - For more information, see the hard disks presentation
- Special Directories in Linux:
  - Root – represented by a single slash (/) – superdirectory
  - Current Directory – single dot (.)
  - Previous Directory – double dot (..)

Important Linux Directories

- Root - / - superdirectory
- **/home** – contains user directories
- /bin – contains commands for startup. May be used by normal users
- /sbin – also commands for startup, but is not normally used by users
- /proc – contains processor and hardware information. Does not actually exist, but resides as a virtual directory
- /tmp – temporary files
- /opt – software and packages not part of default install

Important Linux Directories

- /usr – contains commands, programs, libraries, and man pages for users – most often referenced by normal users
- /boot – files used by the bootstrap loader
- /lib – files needed by multiple programs
- /dev – device files, such as hard disks and removable drives
- **/etc** – configuration files
- **/var** – contains files that change regularly, such as log files
- /mnt or /mount – mounted devices used by the administrator

Overview of Linux Distributions

- Determining which release:
  - Look in the /etc directory
    - There could be a directory called redhat-version or debian-release
  - Look at the /etc/issue file
    - Contains the welcome banner, in which most distributions announce themselves
  - Look at the /var/log/dmesg or /var/log/messages
    - Startup log, which normally contains the distribution type
  - If self-compiled linux, good luck ☺

Linux Distributions

- RedHat/Fedora/CentOS
  - Most programs are installed using a .rpm file
  - RPM database contains installed programs
- SuSE/openSUSE
  - YaST/Tumbleweed is the package manager
- Gentoo Linux
  - Everything is compiled – as close to self-compiled linux as you can get
  - Package (program) manager is called portage/emerge
- BSD/Debian/Ubuntu/Mint/Tails/Kali/elementary OS
  - Package management is done using APT
- Arch/Manjaro
  - Uses pacman package distribution
- Once you've discovered the type of distribution, study information about that distribution that will help you in your investigation

Linux Investigations

- EnCase
  - 7/8 are better for Linux than 6
- SMART
  - Commercial forensic tool for Linux
  - Highly recommended by others, but I have never used it
- **Autopsy**
  - Open Source investigation tool for Linux and Windows
- Forensic Explorer
  - Fairly good but be careful of parsed metadata
- **X-Ways**

Linux Shells

- Linux shells are command interpreters for using Linux Systems
    - Similar to the command prompt for windows systems, but is much more sophisticated
- Two most popular shells are Bash and Tcsh

Bash

- Most common (and default) shell on Linux systems
- Very sophisticated, with startup and shutdown programming and shell scripting
- Audits the user's activities for us!!!
- In the user's directory, normally /home/*user_name*, there are important files for us to look at
  - .bash_profile or .bashrc – stores commands that are started upon logging in to the system
  - .bash_history – audit trail of commands the user has run (there are no time/date stamps)
  - .bash_logout – stores commands that are run upon logging off of the system

Tcsh

- Normally for people who are used to Unix csh who are moving to Linux
- Important files in the user's home directory:
  - .history – audit trail of commands, with no time/date stamps
  - .logout or csh.logout – set of commands that are run upon logging off of the system
  - .tcsrc or .cshrc – commands that are run when logging on to the system

Subverting the shell’s auditing

- Deleting the files
  - If you investigate the system and do not see these files in the home directory of a user, then either the user account has not been used or the files have been deleted
  - Use the file recovery tool in your favorite tool to recover the history files
- Symbolic Linking to Null
  - /dev/null – Linux black hole
  - If the user has linked his .bash_history file to /dev/null, then he does not track his bash history (that means he cannot hit the up arrow to get his last command).
  - At this point, find another trail to follow

Printing in Linux

- Old Unix – LPR
  - /var/log – look for lpr.log to find the log of files printed
- New Linux – CUPS
  - /var/log/cups – there are multiple log files
- If you cannot find the printer log files, then look in the /etc directory for the configuration files

Logging

- Syslog
  - Linux logging program
  - Not set up by default – must be set up by administrator
  - Configuration file: /etc/syslog.conf
    - Will tell you where the logs are stored

Usernames and passwords

- /etc/passwd
  - Password file contains all the users with passwords
  - Salted – random characters inserted into passwords
    - Rainbow Tables are nearly impossible
  - Encrypted
    - Can use John the Ripper to break the passwords
    - Can take several days if it is a difficult password

Linux INvestigations

- Determine the role of the system
  - Destkop
  - Server
    - LAMP (Linux, Apache, MySQL, PhP) – web server
    - File Server
    - Mail Server
    - Application Server
    - DNS
- Examine configuration files
  - Misconfigured services and settings are the most common cause of penetration into Linux systems
- Pray that syslog is configured because it is robust and comprehensive

Linux Investigations

- When tackling a Linux case, just like any other case, identify the scope and the role of the system
- Research the distribution to understand the structure of binaries and data files
- Intrusions – check logs and config files
- User artifacts – look at hidden files in /dev/
  - This is the equivalent of hiding malware in system32
- Rootkits – very hard to detect and purge