Linux Forensics
(for Non-Linux Folks)

Hal Pomeranz

Deer Run Associates

What's Different About Linux?

- No registry
  - *Have to gather system info from scattered sources*
- Different file system
  - *No file creation dates (until EXT4)*
  - *Important metadata zeroed when files deleted*
- Files/data are mostly plain text
  - *Good for string searching & interpreting data*

Accessing the File System

- Can be complicated
- Encryption, RAID, Logical Volume Mgmt, …
- Multiple partitions to mount

http://computer-forensics.sans.org/blog/2010/10/06/

http://deer-run.com/~hal/CEIC-dm-crypt-LVM2.pdf

What Should We Look At?

/etc [%SystemRoot%/System32/config]

- *Primary system configuration directory*
- *Separate configuration files/dirs for each app*

/var/log [Windows event logs]

- *Security logs, application logs, etc*
- *Logs normally kept for about 4-5 weeks*

/home/$USER [%USERPROFILE%]

- *User data and user configuration information*

Basic System Profiling

Linux distro name/version number:

- /etc/*-release

Installation date:

- Look at dates on /etc/ssh/ssh_host_*_key files

Computer name:

- /etc/hostname (also log entries under /var/log)

IP address(es):

- /etc/hosts (static assignments)
- /var/lib/dhclient, /var/log/* (DHCP)

Default Time Zone

- /etc/localtime stores default time zone data
- Binary file format:
  - Use "zdump" on Linux
  - Look for matching file under /usr/share/zoneinfo

User Accounts

- Basic user data in /etc/passwd

  Any UID 0 account has admin privs
- MD5 password hashes in /etc/shadow

  (brute force with "John the Ripper")
- /etc/sudoers may indicate users w/ admin privs
- Group memberships in /etc/group

User Login History

- /var/log/wtmp
  - Shows user, source, time, and duration of login
  - Need to use Linux "last" command to view

- Other logs that may contain useful data:
  - /var/log/auth.log
  - /var/log/secure
  - /var/log/audit/audit.log

There's No Place Like $HOME

- /home/<user> is common convention
- Home dir for admin user is /root

- "Hidden" files/dirs have names starting w/ "."
  - Contain app-specific configuration information
  - Sometimes executed at login
  - Possible back-door or persistence mechanism

Web Browser Artifacts

- Firefox and Chrome are common browsers
- File formats the same as Windows (SQLite DBs)
- Files under user home directories:
  - Firefox: $HOME/.mozilla/firefox/*.default
  - Chrome: $HOME/.config/chromium/Default

Nautilus

- Linux graphical file browser
- Like Windows Explorer
- Thumbnails:	$HOME/.thumbnails
- Recent files:	$HOME/.recently-used.xbel

Command History

- $HOME/.bash_history
- Unfortunately not time-stamped by default
- Can be modified/removed by user

- Sudo history in:
  - /var/log/auth.log
  - /var/log/sudo.log

SSH

- Standard remote access/file xfer mechanism
- Useful files in $HOME/.ssh:

  known_hosts – hosts user connected to from here

  authorized_keys – public keys used for logins to here

  id_rsa – private keys used to log in elsewhere

Things to Watch Out For

- Persistence mechanisms
- Back doors
- Other suspicious files and directories

Persistence Mechanisms

- Service start-up scripts

  /etc/inittab, /etc/init.d, /etc/rc.d (traditional)

  /etc/init.conf, /etc/init (Upstart)

- Scheduled tasks ("cron jobs")

  /etc/cron*

  /var/spool/cron/*

Back Doors

- Deliberate malware/Trojan horse installs
- In /etc/passwd and /etc/shadow:
  - – Extra UID 0 accounts
  - – "Application" accounts with active passwords
- New $HOME/.ssh/authorized_keys entries
- Back doors via [x]inetd

  /etc/inetd.conf

  /etc/xinetd.conf, /etc/xinetd.d

Also Watch Out For…

- Rogue "set-UID" files
- Directories w/ names that start with "."
- Regular files under /dev directory
- Recently modified files
- Large files

Wrapping Up

- Any final questions?
- Thanks for listening!

Hal Pomeranz

hal@deer-run.com Twitter: @hal_pomeranz

http://www.deer-run.com/~hal/

http://computer-forensics.sans.org/blog/author/halpomeranz/

http://www.sans.org/security-training/instructors/Hal-Pomeranz