Digital Forensics
Lecture Week 8

Linux artifacts

Nelson Chapters 3 and 7
Readings

Linux forensics

- I need to run forensics Linux tools
- How?

- “Our Linux Server has been infected”
- Why and How?

Linux boxes

- Where do I get a Linux box to examine?
- Use WSL on Windows 10
  - Note: A VM will not show kernel activity as this is on the host
- Use a terminal window on MacOS
- Use a Linux VM
- Hire a Linux Server on AWS for $6 a month

A Linux Server Case Study

- A company used an ftp server to distribute software updates
- One day it stopped working as the OS had been erased
- The IDS logs had three high priority events
- These indicated a WU_FTP attack and a file upload to the ftp server
- Log file analysis showed the file to be mount.tar.gz
- Using strings and grep on output of log files showed well known root kit files being installed
- A backdoor was installed, but the Firewall prevented files been sent out of the network
- http://www.linuxsecurity.com/content/view/117644/

Objectives

- To understand basic Linux
- To understand the Linux system
- To locate volatile evidence
- To locate non volatile evidence
- To examine log files

Linux OS components

- The kernel
  - talks to the CPU and Hardware
  - modular
- The operating system tools (GNU)
  - compliers and libraries
  - the shell and command line tools
- The user interface (environment)
  - gui
  - Touch
- The applications
  - Do useful things like run a web server

Linux OS Distributions

- Assemble the components in a particular flavour
- Debian GNU(1993) Descendants
  - Knoppix
  - Ubuntu (2004)
    - Backtrack, Kali
- Red Hat (1994-2004) Descendants
  - Fedora (free)
  - CentOS (2003)
  - Red Hat Enterprise (RHEL) (mainly in USA)
- Open SUSE (Novell) 1994
  - Mainly in Europe

Debian Releases – Aug 2020

4.0	Etch	2007-04-08	Etch, the Etch-A-Sketch
5.0	Lenny	2009-02-14	Lenny, the binoculars
6.0	Squeeze	2011-02-06	Squeeze toy aliens
7	Wheezy	2013-05-04	Wheezy the penguin
8	Jessie	2015-04-26	Jessie the cowgirl
9	Stretch	2017-06-17	Rubber octopus from Toy Story 3
10	Buster	2019-07-06	Andy's pet dog
11	Bullseye	Not yet released	Woody's horse
	Sid	"unstable"	The next door neighbour

OS Distribution Packages

- Download as a DVD image (.iso) file or a VM
- Debian
  - Includes Kali, Knoppix and Ubuntu
  - use the apt package manager
- Fedora
  - includes CentOS, RHEL
  - use the yum package manager
- Distro ranking and latest news
  - http://distrowatch.com/

Page Hit Ranking

Last 6 months

Rank	Distribution
1	MX Linux
2	Manjaro
3	Mint
4	Ubuntu
5	Debian
6	elementary

Linux user interfaces

- The gui interfaces
  - Use X Windows (also called X11) for bit mapped displays
  - KDE (Windows like)
  - Gnome (Apple like)
  - Blackbox (minimal X11)
- The cli Interface
  - command line interface
  - like Cisco cli and windows cmd
  - use a shell, usually bash

Linux applications

- Usually issued as a package
- Downloaded and installed using a package manager
- The package manager also specifies a package format
- RPM for Red Hat
- APT for Debian using the dpkg format
- Licencing
  - all code must be compatible with version 2 of the GNU General Public License (GPLv2)
  - all code must be signed
  - All commands support the - -help option

Linux and Malware

- Small companies often use Linux as the server platform
  - Web server, ftp server, mail server, db server
  - Thus a target for web application based attacks
- Attackers often use Linux as their C & C Server
  - Many Linux servers are not well protected
  - Some infections last for years undetected

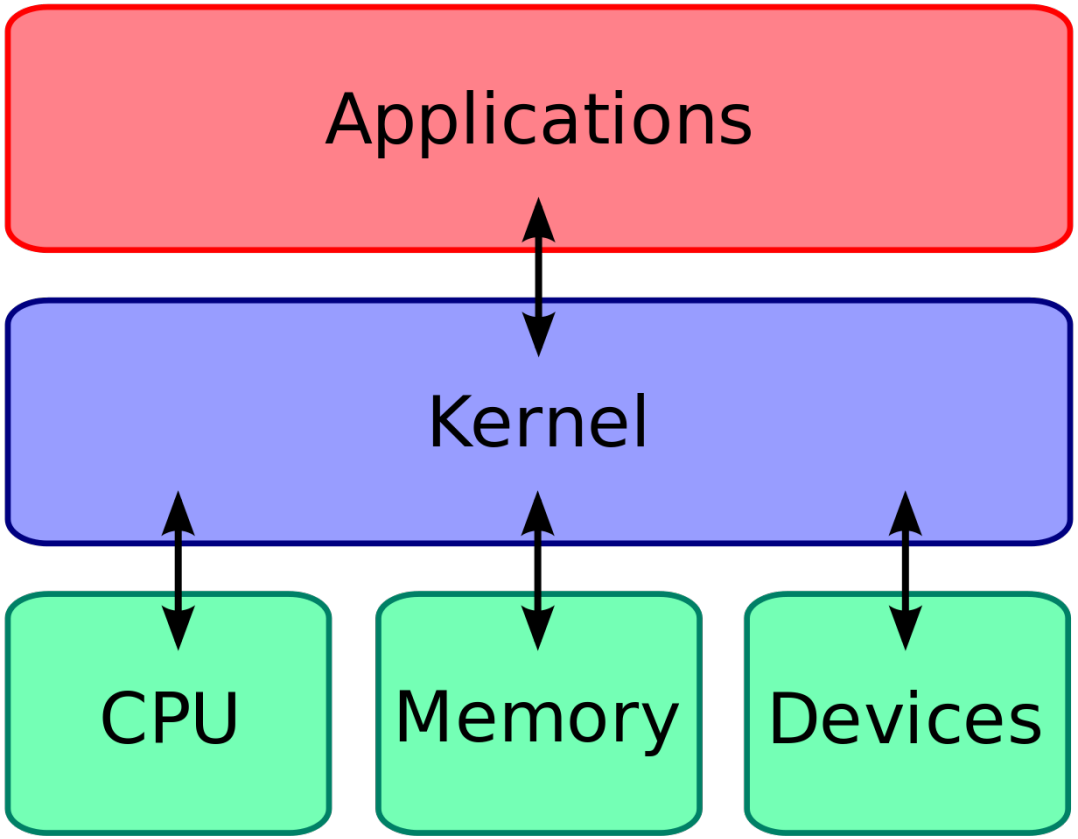
Linux Security Features

- iptables – the Linux Firewall
- http://en.wikipedia.org/wiki/Iptables
- Virus Scanners
  - not common on Linux, clamav is one
  - http://www.debianhelp.co.uk/clamav.htm
- Use of private key Certificates for networking
  - openssl, ssh, openvpn, etc
- Sudo (superuser do)
  - privilege escalation as required
- https://wiki.debian.org/sudo

Objectives

- To understand basic Linux
- To understand the Linux system
- To locate volatile evidence
- To locate non volatile evidence
- To examine log files

The Linux Kernel



The Linux Kernel Archives

Protocol	Location
HTTP	https://www.kernel.org/pub/
GIT	https://git.kernel.org/
RSYNC	rsync://rsync.kernel.org/pub/

Latest Release
5.8.1

mainline:	**5.8**	2020-08-02
stable:	**5.8.1**	2020-08-11
stable:	**5.7.15**	2020-08-11
longterm:	**5.4.58**	2020-08-11
longterm:	**4.19.139**	2020-08-11
longterm:	**4.14.193**	2020-08-07
longterm:	**4.9.232**	2020-07-31
longterm:	**4.4.232**	2020-07-31
linux-next:	**next-20200814**	2020-08-14

The WSL Kernel

- Here the Kernel is modified to run on Windows
  - Windows Subsystem for Linux (WSL)
- Looking at the kernel inside Linux will fail

```
$ whatis uname
uname (1)          - print system information
uname (2)          - get name and information about current kernel

$ uname -r
4.4.0-20190-Microsoft          # Returns Windows version of Linux
```

- You need to ask wsl

```
C:\Users\graha>wsl --update --status
Windows Subsystem for Linux was last updated on 24-Jun-20
WSL automatic updates are on.
Kernel version: 4.19.121.1
```

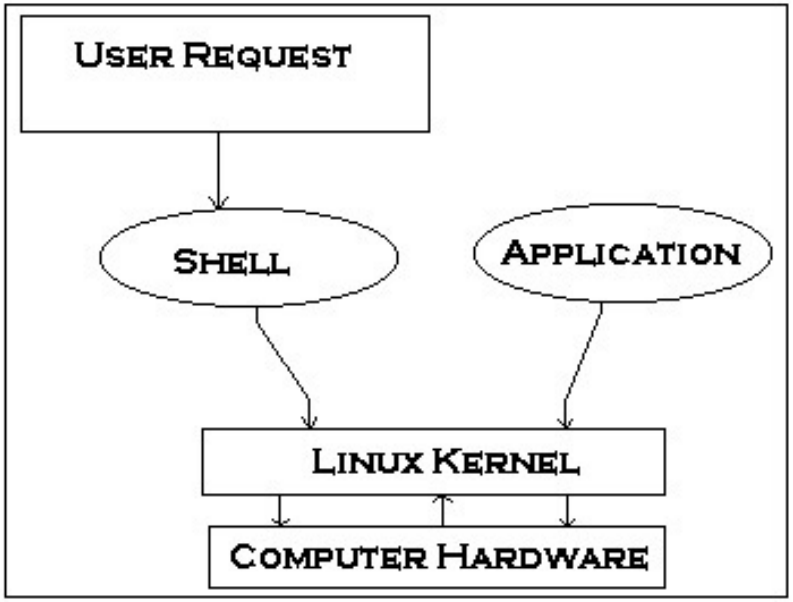
- More about wsl in readings

The Linux system

- A bootloader
  - GNU GRUB or LILO
  - loads the kernel from a file into RAM
- init
  - the top of the process tree, launched by the kernel
  - launches other processes
- libraries
  - contain code used by other processes
  - GNU C library (glibc)
  - like dlls in Windows

The Linux system #2

- The GNU C Complier gcc
  - compiles and links the programs used by Linux
- the user interface
  - a shell or gui
- Shells
  - the CLI to talk to the kernel
  - takes commands from stdin
  - supports regular expressions
  - keeps a history



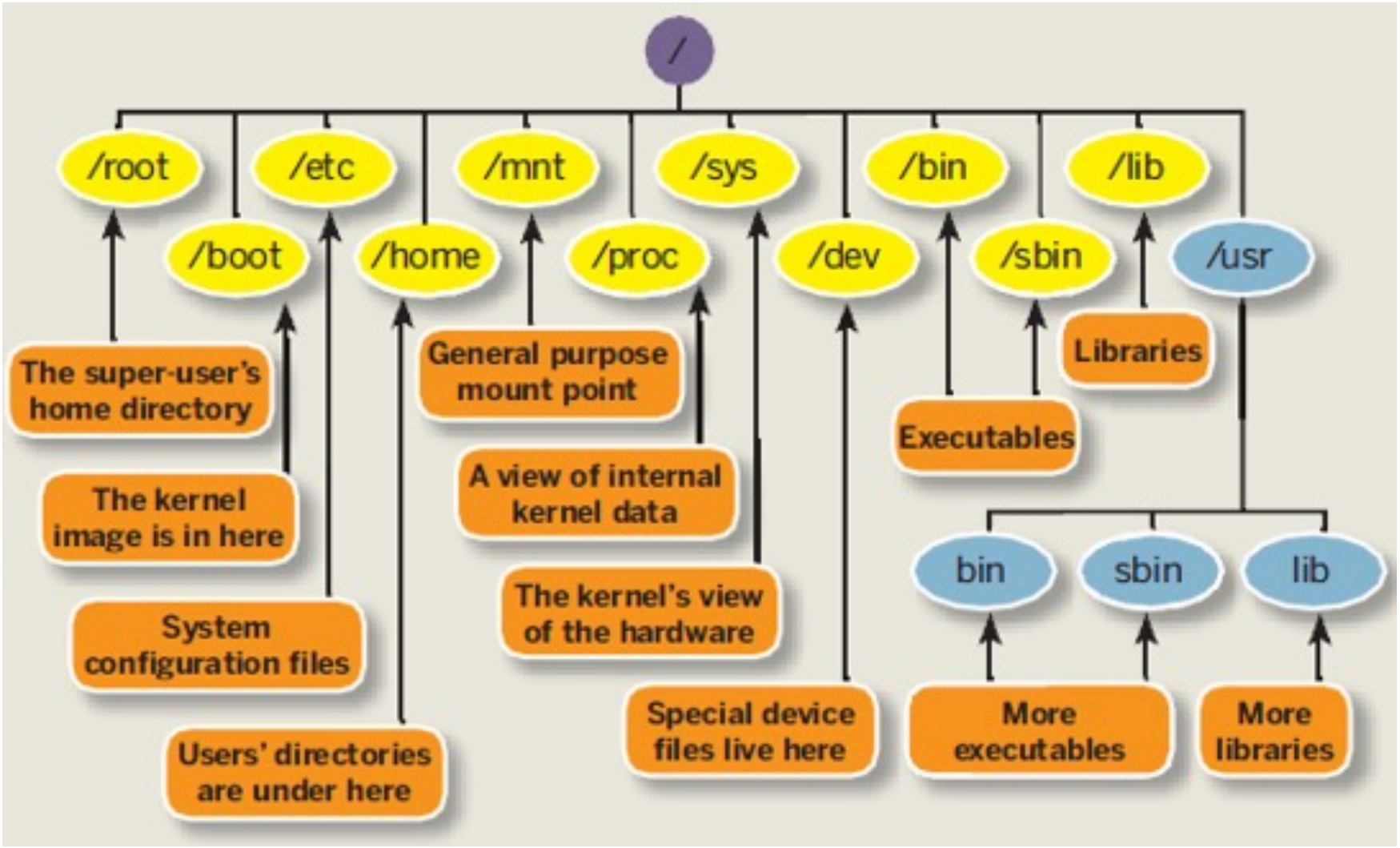
Shell versions

- bash
  - Bourne Again Shell, part of GNU Linux
- csh
  - The C Shell, uses C syntax
- sh
  - the system default shell
  - often the Dash shell for speed (Derived Almquist Shell)
- Other shells
  - Korn Shell, Tenex C Shell

Linux File structure

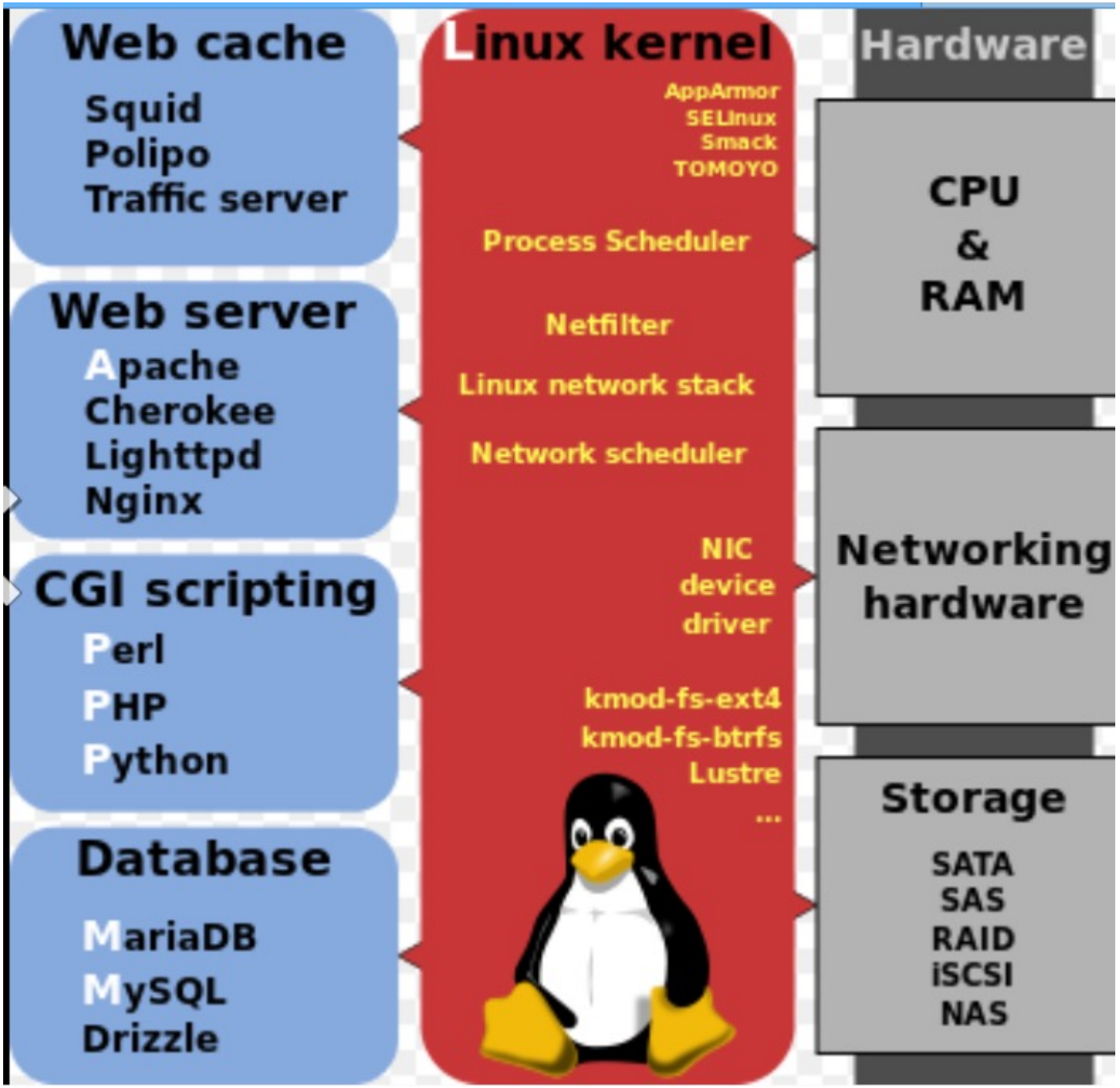
- / - root
- /bin – binaries (executables)
- /lib – libraries (dlls)
- /dev – devices (disks, ram, usb)
- /etc – config files (registry)
- /home – user folders
- /var – logs, swap files, mailboxes, caches

Linux File structure #2



LAMP

- Many small Linux Servers run LAMP
- An open source solution stack that works
- High Availability, Heavy Duty
- Linux (L) OS
  - Debian and Ubuntu share 60% of Linux web servers
- Apache2 (A) Web Server (56%) - some nginx (25%)
- MySQL (M) Database – also PostgreSQL
- PHP (P) Dynamic Web Pages – also Perl, Python


Web cache
Squid
Polipo
Traffic server
Web server
Apache
Cherokee
Lighttpd
Nginx
CGI scripting
Perl
PHP
Python
Database
MariaDB
MySQL
Drizzle
Linux kernel
AppArmor
SELinux
Smack
TOMOYO
Process Scheduler
Netfilter
Linux network stack
Network scheduler
NIC
device
driver
kmod-fs-ext4
kmod-fs-btrfs
Lustre
...
Hardware
CPU
&
RAM
Networking
hardware
Storage
SATA
SAS
RAID
iSCSI
NAS

Objectives

- To understand basic Linux
- To understand the Linux system
- To locate volatile evidence
- To locate non volatile evidence
- To examine log files

Linux forensic shell commands

- Many tools are the same as for Windows
  - netstat, ifconfig (ipconfig), date, ping
- Some are Unix based
  - ps (process), df (mount points), du (disk usage)
  - uname (OS version), w (logged on users)
- Some require root privilege (sudo)
  - fdisk, crontab, viewing logs
- Some will not work on VMs such as WSL
- See the labs for details

sudo

- SuperUser Do (sudo)
- Ubuntu supports restricting dangerous commands to the SuperUser called root
- To run a root command as User just prefix sudo
- sudo ifconfig

```
group11@kali:~$ sudo ifconfig

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for group11:
```

who can sudo?

- root is su so root can sudo
- To see who else can sudo look at the sudo group

```
root@kali:~# cat /etc/group | grep sudo
sudo:x:27:group11
```

Volatile evidence

- who is logged on remotely?
  - w nice and simple
- running processes
  - ps –af local processes
  - ps –Af system processes
- services
  - service - -status-all
  - ls /etc/init.d startup processes

```
$ service --status-all | grep +
 [ ? ]  apport
 [ ? ]  cryptdisks
 [ ? ]  hwclock.sh
 [ + ]  irqbalance
 [ + ]  iscsid
 [ + ]  lvm2-lvmetad
 [ + ]  lvm2-lvmpolld
 [ ? ]  networking
```

```
$ ls /etc/init.d
acpid
apparmor
apport
atd
bootmisc.sh
checkfs.sh
```

Folders of forensic interest

- /etc/passwd – user names
- /etc/shadow – password hashes
- /etc/init.d – services
- /var/www – web server pages
- /var/log - log files
- /var/lib/mysql – database data files also PostgreSQL

Objectives

- To understand basic Linux
- To understand the Linux system
- To locate volatile evidence
- To locate non volatile system evidence
- To examine non volatile log files

non volatile Evidence

- Linux keeps memory information in /proc
- This is a virtual folder – a link to memory
- /proc/cmdline show how the boot image is loaded
  - the boot file name
- /proc/cpuinfo shows some CPU details
  - CPU model, speed and flags
- /proc/meminfo shows the memory manager details
  - total memory, swap file details, Virtual Memory details

/proc/ examples

```
$ cat /proc/cpuinfo | grep processor
processor       : 0
processor       : 1
processor       : 2
processor       : 3

$ cat /proc/cpuinfo | grep 'model name' | uniq
model name      : Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz

$ cat /proc/meminfo | grep Mem
MemTotal:       8259836 kB
MemFree:        4543520 kB
```

Objectives

- To understand basic Linux
- To understand the Linux system
- To locate volatile evidence
- To locate non volatile system evidence
- To examine non volatile log files

Linux log files

- The main logs are in /var/log (some not used in a VM)
  - (Fedora has different logs to Debian)
- apache2 web server access
  - access.log – web visitors
  - ssl-access.log – ssl visitors
- auth.log authentication (password)
- mail.log mail
- mysql.log database
- lpr.log line printer
- syslog app logging

journalctl

- Modern Linux uses systemctl instead of init.d to launch processes. (may not be visible in a VM)
- systemctl has its own log – journalctl
- Check with hostnamectl for device details

```
ubuntu$hostnamectl
   Static hostname: ip-172-26-5-152
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 0eaed5dbe31548e38562f54383ed1376
           Boot ID: 8fbc0ef2f0fa497fb36226922559bc0a
    Virtualization: xen
  Operating System: Ubuntu 16.04.3 LTS
            Kernel: Linux 4.4.0-1049-aws
      Architecture: x86-64
```

journalctl options

Reference – not assessed

- journalctl | grep -i GHz # look for CPU info
- journalctl -u ssh # look for unit
- journalctl -t sshd # look for syslog identifier
- journalctl -t dhclient | grep bound # to interface
- journalctl -p 3 # set warning level
- journalctl --since -1w # open archive, w = week

Useful events #1 - User Logon

- Forensics Sequence
- a) Identify the usernames - SID
- b) Find the user sessions – time and PID
- c) Find the log entries

a) Identify the usernames

- Users are registered in the /etc/passwd file
  - many are system users with no shell
  - people have a shell called bash
  - Bourne-again shell (bash) replaces the original Bourne shell

```
root@kali:~# whatis cat
cat (1)              - concatenate files and print on the standard output
```

```
root@kali:~# cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
postgres:x:114:125:PostgreSQL administrator,,,:
group11:x:1000:1000:,,,:/home/group11:/bin/bash
```

b) Find the user sessions

- To see the logged in sessions use last

```
root@kali:~# whatis last
last (1)             - show listing of last logged in users
```

```
root@kali:~# last root
root     pts/2        192.168.198.1    Tue Jan  9 23:18   still logged in
root     pts/1        192.168.198.1    Tue Jan  9 23:00   still logged in
root     pts/0        :0.0             Wed Sep 21 00:54 - down   (00:01)
root     tty7         :0               Wed Sep 21 00:54 - down   (00:01)
```

```
root@kali:~# last group11
group11  pts/0        :0.0             Tue Jan  9 22:40   still logged in
group11  tty7         :0               Tue Jan  9 22:40   still logged in
```

System reboots

- A special user called reboot

```
root@kali:~# last reboot
reboot   system boot  3.7-trunk-686-pa Tue Jan  9 22:40 - 23:59  (01:19)
reboot   system boot  3.7-trunk-686-pa Wed Sep 21 00:54 - 00:55  (00:01)
reboot   system boot  3.7-trunk-686-pa Sat Sep 17 04:09 - 04:10  (00:00)
reboot   system boot  3.7-trunk-686-pa Sat Sep 17 04:05 - 04:09  (00:03)
```

- See system with –x

```
$last -x -n 20
...<output snipped>
runlevel (to lvl 5)   4.4.0-1049-aws   Sun Feb 11 08:25   still running
reboot   system boot  4.4.0-1049-aws   Sun Feb 11 08:25   still running

$last --help | grep '\-n,'
 -n, --limit <number> how many lines to show
$last --help | grep '\-x,'
 -x, --system         display system shutdown entries and run level changes
```

c) Find the log entries

- cat /var/log/auth.log | grep gdm
  - Gnome display manager (gdm) is a local login

```
root@kali:~# cat /var/log/auth.log | grep gdm3:session | grep group11
Jan  9 22:40:29 kali gdm3][3129]: pam_unix(gdm3:session): session opened for user group11
```

- To see remote logins, use ssh

```
root@kali:~# cat /var/log/auth.log | grep sshd

Jan  9 22:40:07 kali sshd[3315]: Server listening on 0.0.0.0 port 22.
Jan  9 22:40:07 kali sshd[3315]: Server listening on :: port 22.
Jan  9 23:00:43 kali sshd[3773]: Accepted password for root from 192.168.198.1 port 2047 ssh2
Jan  9 23:00:43 kali sshd[3773]: pam_unix(sshd:session): session opened for user root by (uid=0)
Jan  9 23:18:15 kali sshd[5430]: Accepted password for root from 192.168.198.1 port 2077 ssh2
Jan  9 23:18:15 kali sshd[5430]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

Useful events #2 - dhcp activity

- a) Get the current ip address details – MAC address
- b) Find the log entries – MAC or ip

a) Get the current ip address details

- Use ifconfig

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b3:49:7b
          inet addr:192.168.198.128  Bcast:192.168.198.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb3:497b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4942 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3747 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:466146 (455.2 KiB)  TX bytes:2670120 (2.5 MiB)
          Interrupt:19 Base address:0x2000
```

b) Find the log entries

date and time, ip address and dhcp server

- We look for an ip address offer from the dhcp server
- cat /var/log/syslog | grep -i dhcpoffer

```
root@kali:~# cat /var/log/syslog | grep -i dhcpoffer
Sep 17 04:05:21 kali dhclient: DHCPOFFER from 192.168.28.254
Sep 21 00:54:08 kali dhclient: DHCPOFFER from 192.168.3.254
Jan  9 22:40:05 kali dhclient: DHCPOFFER from 192.168.198.254
```

- Then we look for a following preinit to bound operation

```
root@kali:~# cat /var/log/syslog | grep -i -A1 preinit
Jan  9 22:40:05 kali NetworkManager[2224]: <info> (eth0): DHCPv4 state changed
Jan  9 22:40:05 kali NetworkManager[2224]: <info>   address 192.168.198.128
```

rotating log files

- Server logfiles fill up quickly
- To keep old logs as long as possible we use rotation
- when a log is full or expired a copy is made.
- When the copy limit is reached, new logs overwrite old ones
- Typically busy server logs only survive 14 days.

Logrotate

- /etc/logrotate.conf looks after two log files
  - wtmp for logins
  - btmp for bad (failed) logins
- other apps look after their own logs in etc/logrotate.d

```
$ls /etc/logrotate.d
apache2  apt   lxd           rsyslog  ufw
apport   dpkg  mysql-server  samba
```

- apache2 is typical

```
$cat /etc/logrotate.d/apache2
/var/log/apache2/*.log {
        weekly
        missingok
        rotate 13
        compress
        delaycompress
        notifempty
```

sample logrotate activity

```
$sudo logrotate -d /etc/logrotate.d/apache2
reading config file /etc/logrotate.d/apache2

Handling 1 logs

rotating pattern: /var/log/apache2/*.log  weekly (13 rotations)
empty log files are not rotated, old logs are removed
considering log /var/log/apache2/access.log
  log does not need rotating
considering log /var/log/apache2/error.log
  log does not need rotating
considering log /var/log/apache2/other_vhosts_access.log
  log does not need rotating
not running prerotate script, since no logs will be rotated
not running postrotate script, since no logs were rotated
```

-d = debug

zipped log files

- often a log file is compressed to save space
- access.log.2.gz
- need to unzip the file using gunzip before using cat.

```
ubuntu$ls
access.log      access.log.3.gz
access.log.1    access.log.2.gz
ubuntu$sudo gunzip access.log.2.gz
ubuntu$ls
access.log      access.log.3.gz
access.log.1    access.log.2
```

tarballs

- A tarball is a group or archive of files that are bundled together using the tar command and have the .tar file extension.
- If your tar file is compressed using a gzip compressor, use this command to uncompress it.

```
$ tar xvzf file.tar.gz
Where,
  x: This option tells tar to extract the files.
  v: The "v" stands for "verbose." This option will
     list all of the files one by one in the archive.
  z: The z option is very important and tells the tar
     command to uncompress the file (gzip).
  f: This options tells tar that you are going to give  it a
     file name to work with.
```

Shell logs

- An intruder or suspect may login and open a bash shell.
- Here she may run shell scripts with malicious intent
- In this case her activities are recorded in her .bash_history file
- Remember shell history in the basic cmds Lab?
  - Part 5 History and Exit

bash shell history log

```
The suspect logs in
The suspect types the following
----
ls
date
./getinfo.sh
cat info.txt
whoami
----
The suspect logs out
----
We look at the suspect's shell history file
cd /home/group11
cat .bash_history
We see all
```

FIN

- Bring an empty USB for the Week 9 Lab
- arrivederci