CWU919KD

Threat Detection: Linux Defensive Capabilities

Instructor: Maj Patrick “Shrink” Vinge

USAF Weapons School • Nellis AFB

So What?

- Linux systems make up a small portion of the AFNet, but make up a large portion of non-AFNet CPT missions
- To be an effective defender *you must know how to use the tools available to you effectively and what normal looks like*
- There are a *plethora of capabilities indigenous on most Linux platforms and knowing how to use them can allow you to mitigate most threats*

"If you know the enemy and know yourself,
you need not fear the result of a hundred battles"
– Sun Tzu

Objectives

- List and illustrate the boot sequence for a Linux Operating System
- Describe the daemon start sequence
- Describe why defenders care about patching configuration / events
- List eight native commands that can be used during an investigation
- Describe FLUFFE

Overview

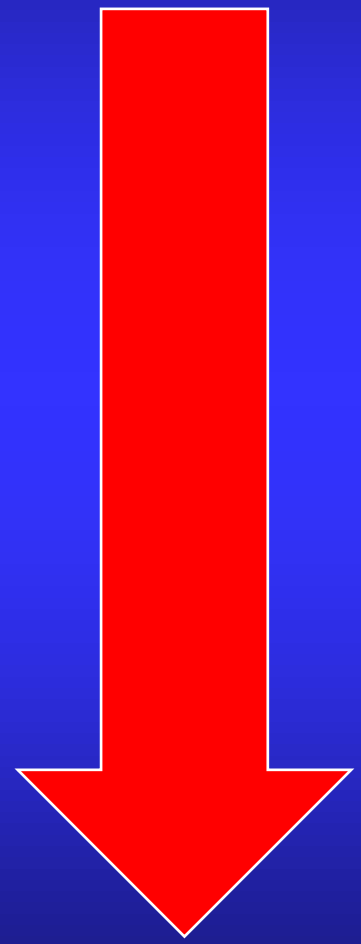
- System hardening
- Software patching
- Integrity checking
- System auditing
- Investigation

Overview

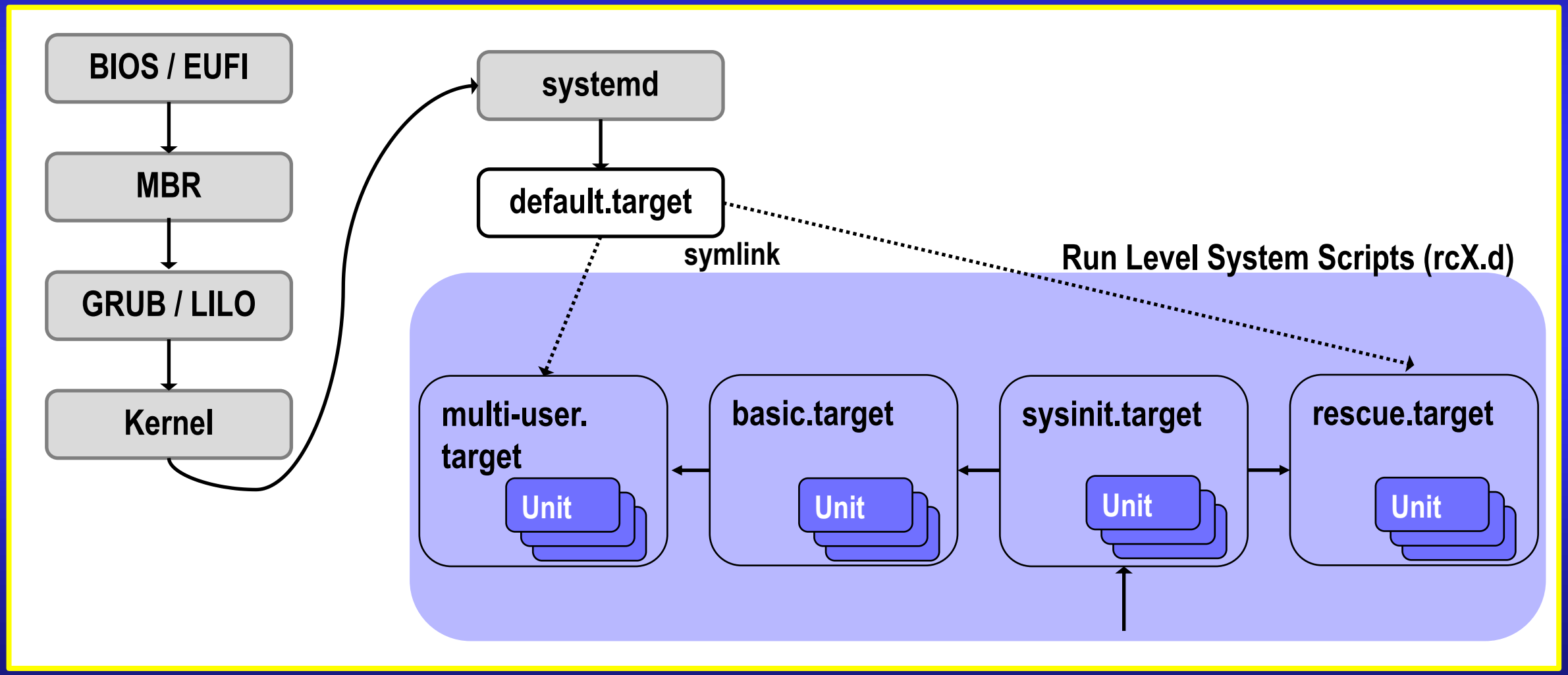
- *System hardening*
- Software patching
- Integrity checking
- System auditing
- Investigation

Boot Sequence

- *1. Basic Input Output System (BIOS) / Unified Extensible Firmware Interface (EUFI)*
- *2. Master Boot Record (MBR)*
- *3. GRand Unified Bootloader (GRUB) / Linux Loader (LILO)*
- *4. Kernel*
- *5. Initialization Daemon (systemd)*
  - Parent process to all Linux daemons
- *6. Run Level System Scripts (rcX.d)*
  - System Daemons



Boot Sequence



Bootloaders

- Linux uses one of two bootloaders
  - GRand Unified Bootloader (GRUB) or Linux Loader (LILO)
- Linux allows a lot of access to someone who can control the boot sequence
- Attackers who can reboot your system can:
  - Choose which kernel to boot into
    - Allows for:
      - Single-user boot – which gives default root privileges
      - Command-line access!
  - Cause a denial-of-service by taking the system offline
- *Mitigation: Add a password to the bootloader*

Listing 1-1. *Sample* `lilo.conf` *File*

```
prompt
timeout=50
default=linux
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear
password=secretpassword
restricted
```

Listing 1-2. *Generating a Grub Password*

```
puppy# grub
grub> md5crypt
Password: ********
Encrypted: $1$2FXKzQo$I6k7iy22wB27CrkzdVPe70
grub> quit
```

Daemons

- Daemon start sequence is IMPORTANT!
  - Can create security vulnerabilities (e.g., starting the IPTables and Syslog Daemons *after* your network daemon could *lead to unblocked and unlogged connections)*
- *1. Systemd executed*
  - *Parent over all processes*
  - *Limited processes without a parent*
    - What about kthreadd?

```
ubuntu@ubuntu:/etc/systemd/system/sysinit.target.wants$ ps -ely
S   UID     PID    PPID  C PRI  NI    RSS    SZ WCHAN  TTY          TIME CMD
S     0       1       0  0  80   0 10008 42032 -      ?        00:00:08 systemd
S     0       2       0  0  80   0     0     0 -      ?        00:00:00 kthreadd
I     0       3       2  0  60 -20     0     0 -      ?        00:00:00 rcu_gp
I     0       4       2  0  60 -20     0     0 -      ?        00:00:00 rcu_par_gp
I     0       6       2  0  60 -20     0     0 -      ?        00:00:00 kworker/0:0H-kblockd
I     0       9       2  0  60 -20     0     0 -      ?        00:00:00 mm_percpu_wq
S     0      10       2  0  80   0     0     0 -      ?        00:00:01 ksoftirqd/0
I     0      11       2  0  80   0     0     0 -      ?        00:00:02 rcu_sched
S     0      12       2  0 -40   -     0     0 -      ?        00:00:00 migration/0
S     0      13       2  0   9   -     0     0 -      ?        00:00:00 idle_inject/0
S     0      14       2  0  80   0     0     0 -      ?        00:00:00 cpuhp/0
```

- *2. Mounts the filesystems as defined by /etc/fstab*

Daemons

- *3. Starts reading configuration files from /etc*
- *4. Reads default.target file to determine target environment to boot into*
  - By default, desktop will be run level 5, servers are run level 3
- *5. Starts at default (lower functionality services) and executes all system scripts until target environment reached*

SystemV Runlevel	systemd target	systemd target aliases	Description
	halt.target		Halts the system without powering it down.
0	poweroff.target	runlevel0.target	Halts the system and turns the power off.
S	emergency.target		Single user mode. No services are running; filesystems are not mounted. This is the most basic level of operation with only an emergency shell running on the main console for the user to interact with the system.
1	rescue.target	runlevel1.target	A base system including mounting the filesystems with only the most basic services running and a rescue shell on the main console.
2		runlevel2.target	Multiuser, without NFS but all other non-GUI services running.
3	multi-user.target	runlevel3.target	All services running but command line interface (CLI) only.
4		runlevel4.target	Unused.
5	graphical.target	runlevel5.target	multi-user with a GUI.
6	reboot.target	runlevel6.target	Reboot
	default.target		This target is always aliased with a symbolic link to either multi-user.target or graphical.target. systemd always uses the default.target to start the system. The default.target should never be aliased to halt.target, poweroff.target, or reboot.target.

Daemons

- *So what can we do with this information?*
- We can use it to:
  - Know what 'Good' looks like to start identifying possible bad
  - Know what services we can turn off to harden
    - 'Minimalist' security strategy
    - Unused services create unnecessary risks

Table 1-1. *Starting Services for Red Hat and Debian*

Service	Description	Remove?
anacron	A variation on the cron tool	Yes
apmd	Advanced Power Management	Yes
atd	Daemon to the at scheduling tool	Yes
autofs	Automount	Yes
crond	The cron daemon	No
cups	Printing functions	Yes
functions	Shell-script functions for init scripts	No
gpm	Mouse support for text applications	Yes
irda	IrDA support	Yes (unless you have IrDA devices)
isdn	ISDN support	Yes (unless you use ISDN)
keytable	Keyboard mapping	No
kudzu	Hardware probing	Yes
lpd	Printing daemon	Yes
netfs	Mounts network file systems	Yes
nfs	NFS services	Yes
nfslock	NFS locking services	Yes
ntpd	Network Time Protocol daemon	No
pcmcia	PCMCIA support	Yes
portmap	RPC connection support	Yes
random	Snapshots the random state	No
rawdevices	Assigns raw devices to block devices	Yes
rhnsd	Red Hat Network daemon	Yes
snmpd	Simple Network Management Protocol (SNMP) support	Yes
snmptrap	SNMP Trap daemon	Yes
sshd	Secure Shell (SSH) daemon	No
winbind	Samba support	Yes
xfs	X Font Server	Yes
ypbind	NIS/YP client support	Yes

Auto-Start Programs

- Once all the daemons are started and we are booted into our target environment, auto-start programs will be executed by systemd
  - NOTE: Great place to store persistence mechanisms …
- Auto-start location
  - /etc/xdg/autostart/

```
ubuntu@ubuntu:/etc/xdg/autostart$ ls
at-spi-dbus-bus.desktop                      org.gnome.SettingsDaemon.A11ySettings.desktop      org.gnome.SettingsDaemon.Wwan.desktop
geoclue-demo-agent.desktop                   org.gnome.SettingsDaemon.Color.desktop             org.gnome.SettingsDaemon.XSettings.desktop
gnome-initial-setup-copy-worker.desktop      org.gnome.SettingsDaemon.Datetime.desktop          print-applet.desktop
gnome-initial-setup-first-login.desktop      org.gnome.SettingsDaemon.DiskUtilityNotify.desktop pulseaudio.desktop
gnome-keyring-pkcs11.desktop                 org.gnome.SettingsDaemon.Housekeeping.desktop      snap-userd-autostart.desktop
gnome-keyring-secrets.desktop                org.gnome.SettingsDaemon.Keyboard.desktop          spice-vdagent.desktop
gnome-keyring-ssh.desktop                    org.gnome.SettingsDaemon.MediaKeys.desktop         tracker-extract.desktop
gnome-shell-overrides-migration.desktop      org.gnome.SettingsDaemon.Power.desktop             tracker-miner-fs.desktop
gnome-software-service.desktop               org.gnome.SettingsDaemon.PrintNotifications.desktop tracker-store.desktop
gnome-welcome-tour.desktop                   org.gnome.SettingsDaemon.Rfkill.desktop            ubuntu-report-on-upgrade.desktop
im-launch.desktop                            org.gnome.SettingsDaemon.ScreensaverProxy.desktop  update-notifier.desktop
nm-applet.desktop                            org.gnome.SettingsDaemon.Sharing.desktop           user-dirs-update-gtk.desktop
orca-autostart.desktop                       org.gnome.SettingsDaemon.Smartcard.desktop         vmware-user.desktop
org.gnome.DejaDup.Monitor.desktop            org.gnome.SettingsDaemon.Sound.desktop             xdg-user-dirs.desktop
org.gnome.Evolution-alarm-notify.desktop     org.gnome.SettingsDaemon.Wacom.desktop
```

Cronjobs

- Cronjobs are equivalent to schtasks on Windows
- Crontab can be used to list all cronjobs
  - Crontab –l
    - Lists root cronjobs
  - Crontab –u username –l
    - Lists specified user cronjobs
- Cronjobs are located in:
  - /etc
    - /cron.d
    - /cron.hourly
    - /cron.daily
    - /cron.weekly
    - /cron.monthly

Executable Program Locations

- /bin
- /sbin
- /usr/bin
- /usr/sbin
- /usr/local/bin
- /usr/local/sbin
- /usr/share
- /home/$USER/.local/share/applications

IPTables / NFTables

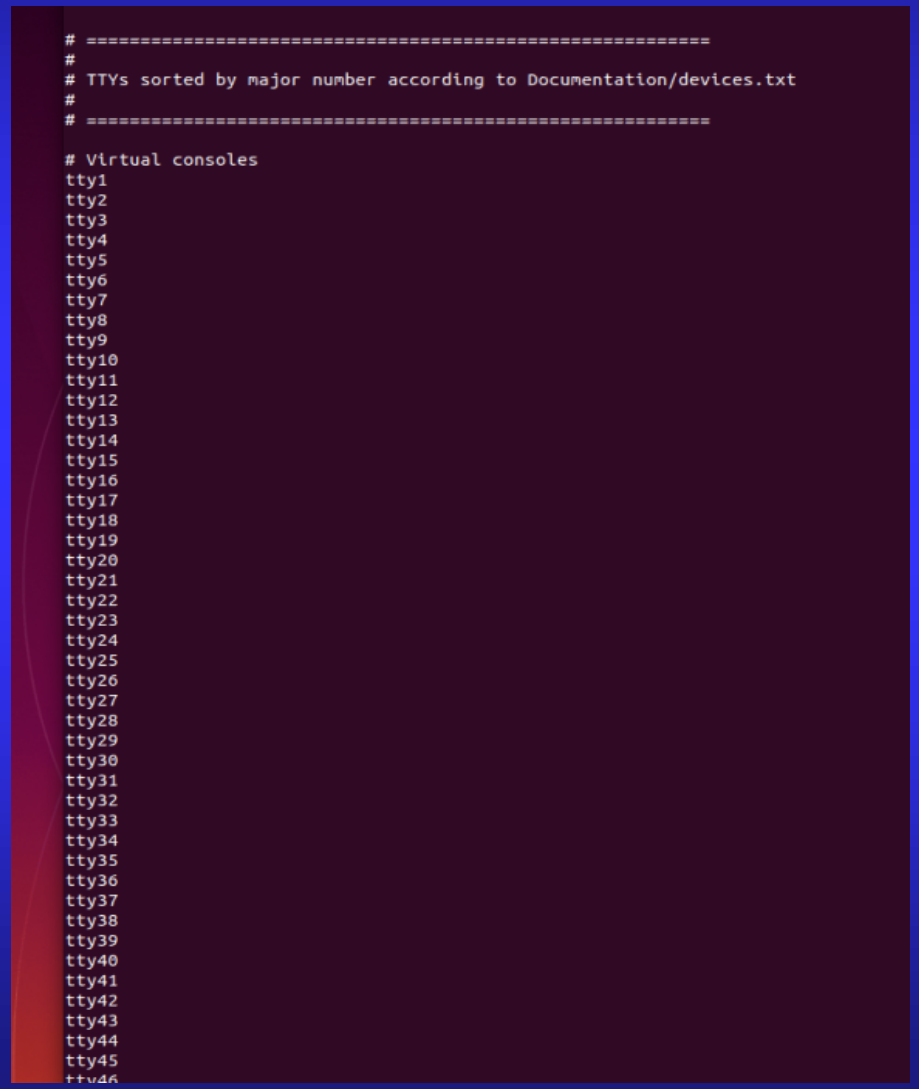
- Command-line firewall utility that uses policy chains to allow or block traffic
- IPTables is slowly being replaced by NFTables (network filter tables)
  - Connection tries to establish itself on system, iptables / nftables looks for a rule match
  - Does not find one, resorts to the default action
- Almost always comes preinstalled on any Linux distribution
  - List policy chains:
    - # iptables or # ip6tables or # nft
  - Location:
    - /etc or /etc/alternatives or /etc/sysconfig
- ***Adversaries will create or delete firewall rules to enable communication!***

iptables vs nftables

	iptables	nftables
Events reporting	no	Yes
XML / Json	weak	Yes
Public library / API	no	Yes
Built-in data sets	no	Yes
Fast updates	no	Yes

Console

- Remote access like SSH and FTP is crucial to control / manage, but removing is not the only solution
- Console connections can also be restricted from the system level
  - By default LOTS of root consoles are authorized!
- Linux systems authorize remote console connections via the configuration file found at: /etc/securetty



```
# ============================================================
#
# TTYs sorted by major number according to Documentation/devices.txt
#
# ============================================================

# Virtual consoles
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
tty12
tty13
tty14
tty15
tty16
tty17
tty18
tty19
tty20
tty21
tty22
tty23
tty24
tty25
tty26
tty27
tty28
tty29
tty30
tty31
tty32
tty33
tty34
tty35
tty36
tty37
tty38
tty39
tty40
tty41
tty42
tty43
tty44
tty45
tty46
```

Users / Groups

Three locations to look for malicious accounts

- /etc/password
  - Username : password : UID : GID : GECOS :
    … Home Directory : Shell
- /etc/shadow
  - Username : Pass : Date pass changed : min days between
    … pass change : pass expiry time: pass expiry warning :
    … number of days after pass : expiry account is disabled :
    … date since account disabled
- /etc/group
  - Name : pass : GID : member , member

```
ubuntu@ubuntu:/etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

```
ubuntu:$1$WfPMQl8m$kqCzW3Ike68ryiMAs5dy6/:18338:0:99999:7:::
```

```
ubuntu@ubuntu:/etc$ cat group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
```

Users / Groups

Why do we care about understanding users / groups?

Table 1-6. *Default Users*

User	Purpose	Remove?
adm	Owns diagnostic and accounting tools	Yes
backup	Used by packing for backing up critical files	No
bin	Owns executables for user commands	No
daemon	Owns and runs system processes	No
desktop	KDE user	Yes
ftp	Default FTP user	Yes
games	Games user	Yes
gdm	GDM user	Yes
gnats	GNATS (bug tracking) user	Yes
gopher	Gopher user	Yes
halt	/sbin/halt user	No
identd	User for identd daemon	Yes
irc	Internet relay chat (IRC) user	Yes
list	Mailman user	Yes (if not using mailman)
lp	Printing user	Yes (if no printing)
lpd	Printing user	Yes (if no printing)
mail	Default user for Mail Transfer Agent (MTA)	Maybe
mailnull	Sendmail user	Yes (if no Sendmail)
man	Man-db user	No
news	Default news user	Yes
nfsnobody	NFS User	Yes
nobody	Default user for Apache or NFS	Maybe
nscd	Name Service Cache Daemon user	Yes (if not using nscd)
ntp	Network Time Protocol user	No
operator	Ops user	Yes
postgres	Postgres default user	Yes (if no Postgres)
proxy	Default proxy user	Yes
root	Root user	No
rpc	RPC user	Yes
rpcuser	Default RPC user	Yes
rpm	RPM user	No
shutdown	Shutdown user	No
sshd	Privilege split sshd user	No
sync	Sync user	Yes
sys	Default mounting user	No
telnetd	Telnetd default user	Yes
uucp	Default uucp user	Yes
vcsa	Virtual console memory	No
www-data	Owns www data	Yes (if not Web server)
xfs	X Font Server	Yes

Users / Groups

Groups that can be removed:

- Lp
- News
- Uucp
- Proxy
- Postgres
- www-data
- Backup
- Operator
- List
- Irc
- Src
- Gnats
- Staff
- Games
- Users
- Gdm
- TelnetD
- Gopher
- ftp
- Nscd
- Rpc
- Rpcuser
- Nfsnodboy
- Xfs
- Desktop

Process Accounting

- Process accounting (psacct or acct)
- /var/log/account/pacct or savacct or usracct
  - Install
    - Sudo apt-get install acct
    - cd /etc/init.d
  - Account log-in times
    - ac
  - Summary of account commands
    - sa –u
  - Pull details associated with the last time a specified command was run
    - Lastcomm sudo

```
ubuntu     0.00 cpu     4622k mem      0 io apparmor_parser
ubuntu     0.00 cpu     4622k mem      0 io apparmor_parser *
ubuntu     0.00 cpu     4622k mem      0 io apparmor_parser
ubuntu     0.01 cpu    79664k mem      0 io snap
ubuntu     0.07 cpu     9688k mem      0 io command-not-fou
ubuntu     0.00 cpu     4842k mem      0 io bash           *
ubuntu     0.00 cpu      622k mem      0 io run-parts
ubuntu     0.00 cpu     5090k mem      0 io systemctl
ubuntu     0.00 cpu     4178k mem      0 io readlink
ubuntu     0.00 cpu     5090k mem      0 io systemctl
ubuntu     0.00 cpu     5090k mem      0 io systemctl
ubuntu     0.01 cpu     5090k mem      0 io systemctl
ubuntu     0.00 cpu      650k mem      0 io acct
ubuntu     0.00 cpu      624k mem      0 io ac
ubuntu     0.00 cpu      624k mem      0 io ac
ubuntu     0.00 cpu      624k mem      0 io ac
ubuntu     0.00 cpu      965k mem      0 io sa
root       0.00 cpu      650k mem      0 io 01-ifupdown
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
root       0.00 cpu     2558k mem      0 io systemd-udevd  *
```

```
ubuntu@ubuntu:/etc/init.d$ lastcomm sudo
sudo            S     ubuntu   pts/0      0.00 secs Thu Apr  9 12:32
sudo            S     ubuntu   pts/0      0.00 secs Thu Apr  9 12:32
sudo            S     root     pts/0      0.00 secs Thu Apr  9 12:31
```

Compilers / Dev Tools

- rpm / yast / dselect Tools allow you to find compilers currently installed
- Install
  - Apt-get install rpm
- Find compilers / dev tools
  - Rpm -qg Developers/Languages Developers/Compilers
- *Why would I care if a system had development tools installed on it?*

Overview

- System hardening
- *Software patching*
- Integrity checking
- System auditing
- Investigation

Updates / Patching

- There are lots of different update / patching options on Linux depending on the distribution but the main ones are:
  - Apt-get, yum and Red Hat Package Manager (RPM)
- A major security vulnerability in many operating systems is simply the lack of updating software with current patches / bug fixes
- *From a defensive perspective*
  - *Unscheduled update may be a sign that a system has been compromised*
    - Adversaries will patch systems after compromise to ensure no cohab
  - *Last patch date may show a system that is vulnerable*
    - Can validate with vulnerability scan
  - *Repository addition might be used for persistence*

Updates / Patching Apt-Get

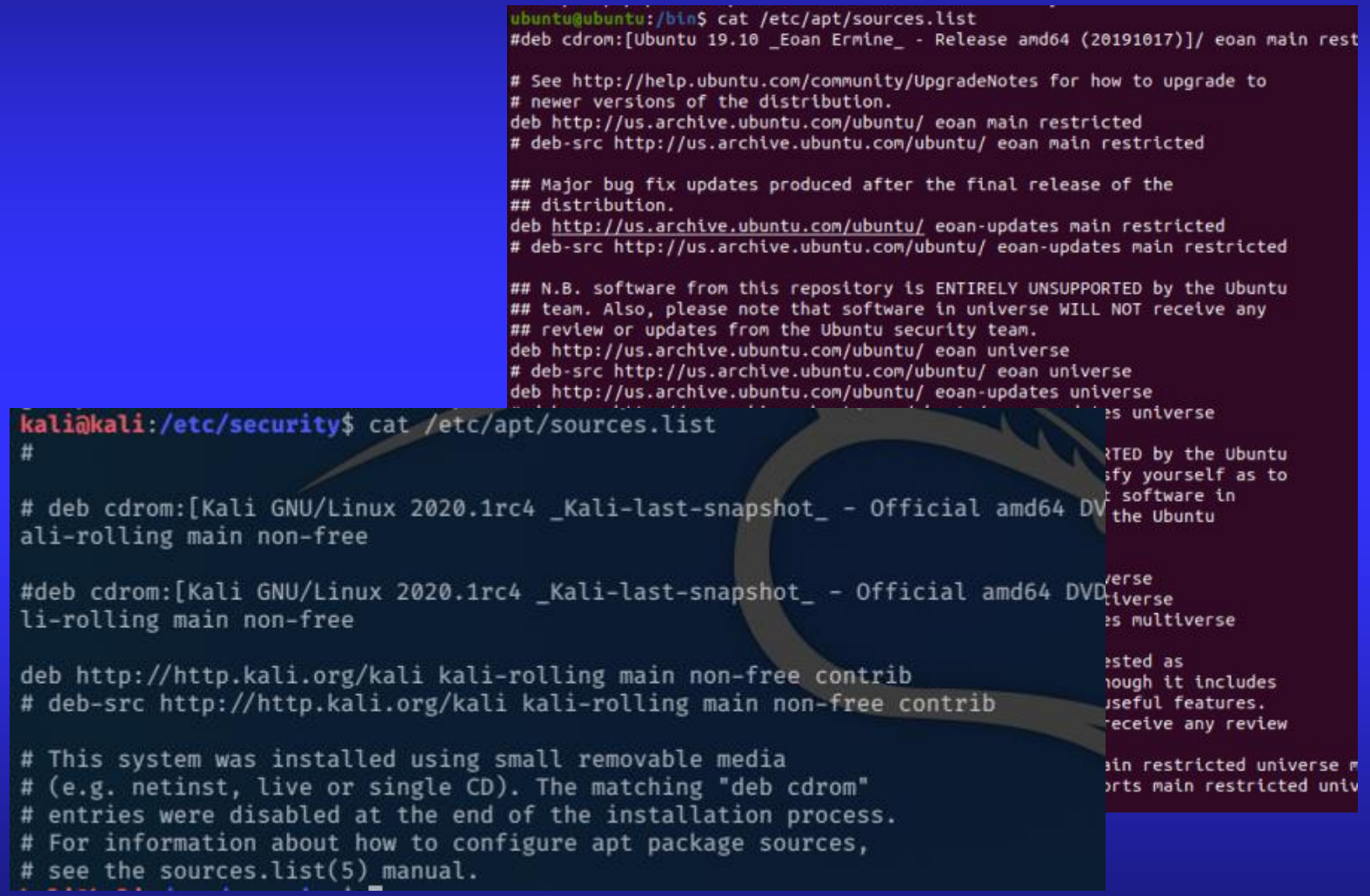
There are a lot of places you can look to see when the last apt-get was run and by whom:

- You can use acct (discussed previously) to see when the apt-get / apt-config command was run
- You can look at the access times in the /var/lib/apt/lists folder to see when they were accessed last
- You can look in the apt-get file repository / log folders to pull information that may be useful

```
ubuntu@ubuntu:/var/lib/apt/lists$ ls -al
total 176880
drwxr-xr-x 4 root root     16384 Apr 10 06:54 .
drwxr-xr-x 5 root root      4096 Apr 10 06:33 ..
drwxr-xr-x 2 _apt root      4096 Oct 17 05:34 auxfiles
-rw-r----- 1 root root         0 Oct 17 05:34 lock
drwx------ 2 _apt root     20480 Apr 10 06:54 partial
-rw-r--r-- 1 root root     97502 Apr 10 06:02 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root   1275386 Apr  9 08:13 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root    735746 Apr  9 08:13 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root     18515 Apr  7 11:19 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      8328 Apr 10 03:25 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      4827 Mar 24 03:53 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      9699 Mar 24 03:53 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root    747232 Apr  9 08:13 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      2024 Mar 12 08:21 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      2916 Mar 12 08:21 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root        57 Apr 24  2019 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      1052 Oct 23 15:51 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root    132329 Apr  9 08:13 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root        57 Apr 24  2019 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root     60479 Apr  9 08:13 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root   1232807 Apr  7 08:55 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root   1186263 Apr  7 08:55 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root     44062 Apr  7 11:19 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      5384 Apr 10 03:27 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root      9061 Apr  9 08:09 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root     11554 Apr  9 08:09 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root    500698 Apr  7 08:55 security.ubuntu.com_ubuntu_dists_eoan-
-rw-r--r-- 1 root root     88827 Apr 10 06:02 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root        52 Apr 24  2019 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root        58 Apr 24  2019 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root        58 Apr 24  2019 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root     12472 Mar 25 00:21 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root     12464 Mar 25 00:21 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root       199 Mar 26 18:17 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root      8425 Apr 10 03:19 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root        29 Oct 31 08:18 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root        29 Oct 31 08:18 us.archive.ubuntu.com_ubuntu_dists_eoa
-rw-r--r-- 1 root root      3103 Jan  9 00:48 us.archive.ubuntu.com_ubuntu_dists_eoa
```

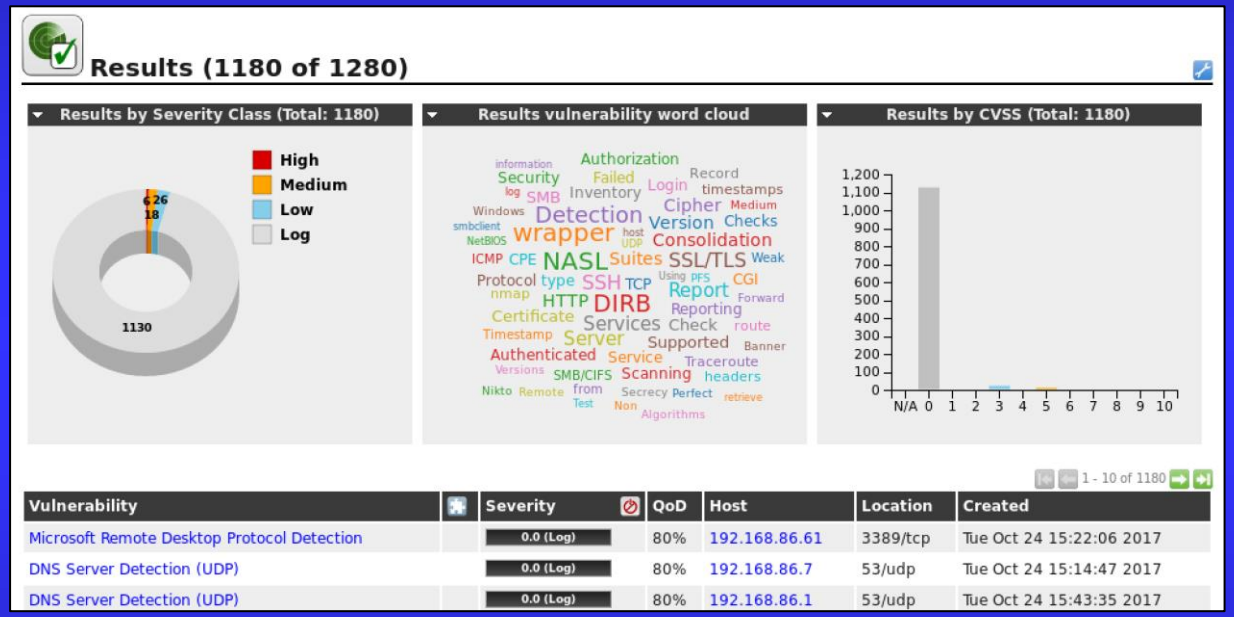
Updates / Patching
Apt-Get

- /etc/apt/sources.list
- /etc/apt/sources.list.d
- /var/lib/apt/lists
- /var/lib/apt/lists/partial
- /var/cache/apt/archives
- /etc/apt/apt.conf
- /etc/apt/apt.conf.d



OpenVAS

- Existing vulnerabilities of a possible compromised system helps identify initial access vectors and direct the investigation
- OpenVAS is a freeware vulnerability scanner that gives current vulnerabilities associated with a system
  - Benefits:
    - Initial access artifacts are often gone by the time a response is initiated
    - Identifies avenues to direct the next step in the investigation

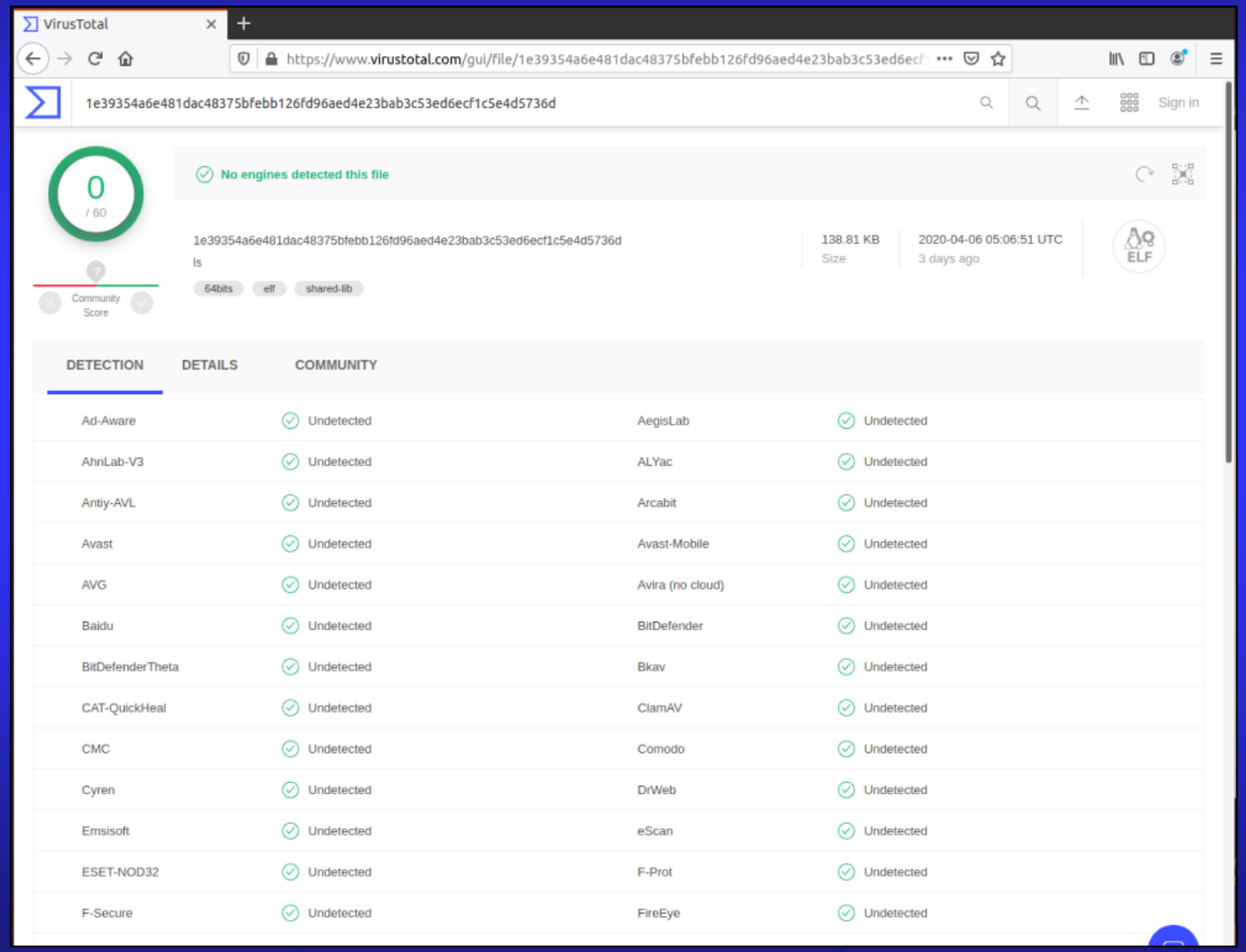


Overview

- System hardening
- Software patching
- *Integrity checking*
- System auditing
- Investigation

File Integrity

- Assume root compromise!
- Validate required binaries:
  - md5sum
  - sha(1, 224, 256, 384 or 512)sum
- Pair with Virus Total or similar
- Scan with AV engine



File Integrity
ClamAV

- Open-source antivirus engine for detecting Trojans, viruses and malware
- Command-line interface
- Can be used for desktops, servers or even on e-mail gateways
- Supports multiple file formats, file and archive unpacking and multiple signature languages
- NOTE: ClamTK is the GUI version

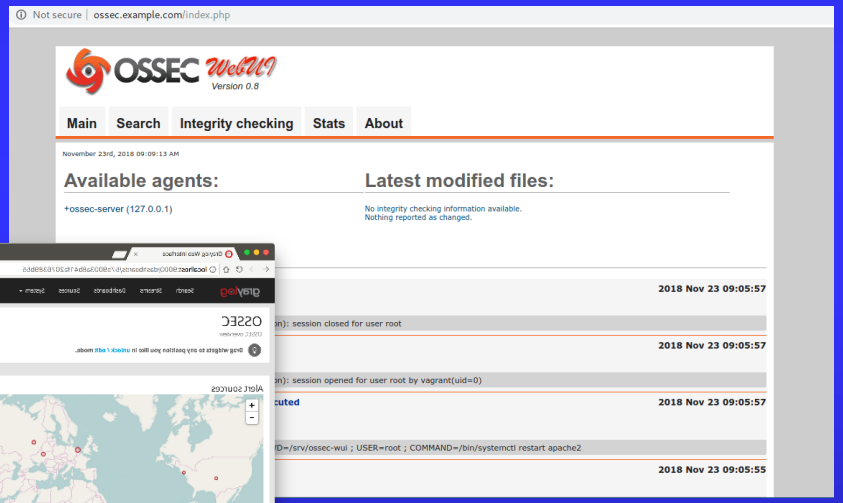
Overview

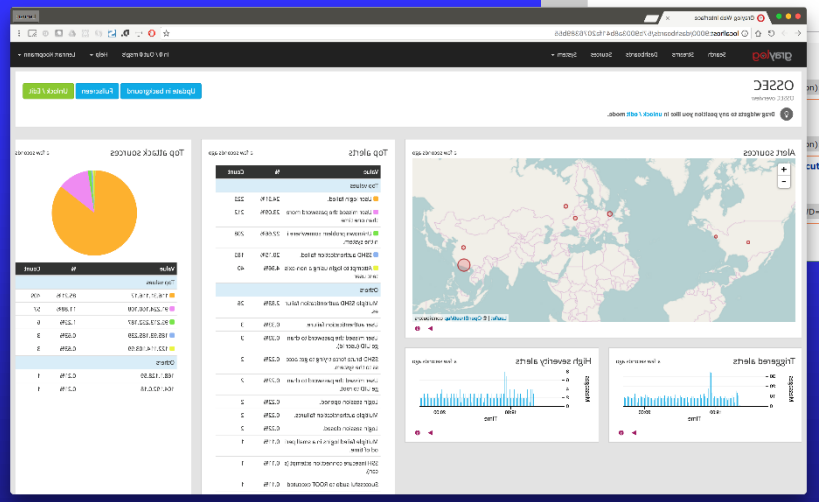
- System hardening
- Software patching
- Integrity checking
- *System auditing*
- Investigation

OSSEC

Host Intrusion Protection System

- OSSEC is a freeware open source scalable, multiplatform, host-based intrusion detection system
- Capabilities
  - Log-based intrusion detection
  - Rootkit and malware detection
  - Active response
  - Compliance auditing
  - File integrity monitoring
  - System inventory





Plaso

- *Computer forensic tool for timeline generation and analysis of system logs*
- *Pulls and analyzes logs from suspect host for timeline analysis and correlation*
- Written in Python
- Modules include:
  - Image_export: Exports file content based on criteria (e.g. extention, path, etc)
  - Log2timeline: Extracts events from individual files, recursing a directory or device
  - Pinfo: Command-line to allow for parsing information from plaso storage file
  - Psort: CLI to post-process plaso storage files to sort and run auto analysis
  - Psteal: CLI combines log2timeline and psort

Overview

- System hardening
- Software patching
- Integrity checking
- System auditing
- *Investigation*

Native Commands

- A lot of information can be gathered using native Linux shell commands:

crontab	*Hostname*	*Who*
ps	*Uname*	*Lsof*
Netstat / SS	*Uptime*	*Dmesg*
Ls	*Date*	*Md5sum*
Cat	*Showmount*	*Sha256sum*
Service	*Mount*	*Sha512sum*
Iptables	*Ifconfig*	*dd*

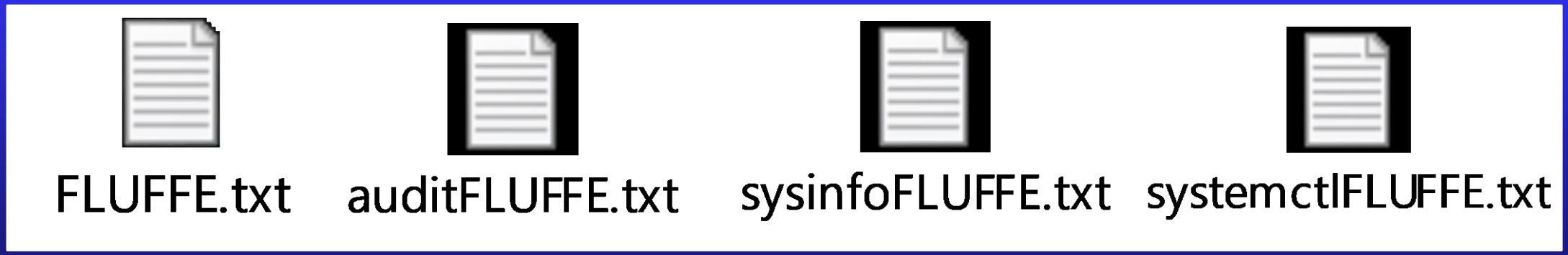
- … just to name a few …
- *Warning: If adversary has root, the binaries may be compromised!*
  - It is best practice to run known good binaries to pull artifacts

System Utilities

- Linux distributions use systemd to initialize and start all services for boot
- Systemd comes with multiple built-in utilities, which can be used to collect artifacts to inform an investigation
- Systemd utilities:
  - Systemctl
  - Networkctl
  - Loginctl
  - Journalctl
  - Notify
  - Analyze
  - Cgls
  - Cgtop

FLUFFE (v1.2)

- First Look Unix Field Forensic Examiner (FLUFFE): Initial forensic analysis tool written in BASH for Linux systems
- *Used for initial incident response to gather artifacts from live hosts, enable initial triage and determine the next best step in the investigation*
  - Leverages known-good binaries of common Linux commands via BusyBox, as well as on disk system utilities to gather artifacts from the potentially infected host
  - *Warning: System utilities leveraged by FLUFFE use on disk binaries*
- Activity: Open FLUFFE and review the BASH script



BusyBox

- Designated as the ‘Swiss Army knife’ for embedded Linux, BusyBox combines tiny versions of many common Unix utilities into a single executable
- 100s of Linux commands are contained in BusyBox
- FLUFFE uses its own BusyBox binaries to ensure known good info is passed back from the target
- To invoke BusyBox:
  - 1. Define absolute path for Linux command to BusyBox each time you call
    - /bin/busybox ls
  - 2. Create a symbolic link for required commands
    - ln –s /bin/busybox ls

Summary

- System hardening
- Software patching
- Integrity checking
- System auditing
- Investigation

Objectives

- List and illustrate the boot sequence for a Linux Operating System
- Describe the daemon start sequence
- Describe why defenders care about patching configuration / events
- List eight native commands that can be used during an investigation
- Describe FLUFFE

Questions?

- Instructor's name: Maj Patrick "Shrink" Vinge
- Instructor's address: USAF Weapons School
  4269 Tyndall Avenue
  Nellis AFB NV 89191-6062
- Instructor's phone: (702) 679-2215
- Instructor's e-mail: patrick.vinge.2@us.af.mil

References

- https://books.google.com/books?id=K7mOQ2CCH-IC&pg=PA219&lpg=PA219&dq=understanding+what+%22right%22+looks+like+on+linux+for+defense&source=bl&ots=o-sYKpjFQP&sig=ACfU3U2Z0yiBoC3i2WhfQDavCuZEk--9NA&hl=en&sa=X&ved=2ahUKEwj43Ymr5tvoAhVRKH0KHWWbAZ4Q6AEwCnoECA0QKQ#v=onepage&q=understanding%20what%20%22right%22%20looks%20like%20on%20linux%20for%20defense&f=false
- https://books.google.com/books?id=PyqjvNNItqYC&pg=PR26&lpg=PR26&dq=understanding+normal+to+defend+linux&source=bl&ots=XFpLbASIfM&sig=ACfU3U2st1ZsegdN3by8UhDiukPY8Z0MEA&hl=en&sa=X&ved=2ahUKEwjB6ra_5tvoAhXKFTQIHd72CbUQ6AEwCXoECAwQKQ#v=onepage&q=understanding%20normal%20to%20defend%20linux&f=false
- https://ftp.kh.edu.tw/Linux/Redhat/en_6.2/doc/ref-guide/s1-sysadmin-boot.htm
- https://github.com/log2timeline/plaso/releases
- https://linux-audit.com/security-defenses-to-fortify-your-linux-systems/
- https://opensource.com/article/17/2/linux-boot-and-startup
- https://plaso.readthedocs.io/en/latest/sources/user/Users-Guide.html#the-tools
- https://vitux.com/secure-ubuntu-with-clamav-antivirus/
- https://www.ossec.net/about/
- https://www.busybox.net/about.html

References

- https://www.dropbox.com/sh/q0w7fy25qyltalh/AAD_VbL27cpa2bKuCtKaCuhaa?dl=0
- https://www.ghacks.net/2009/04/04/get-to-know-linux-the-etcinitd-directory/
- https://www.kali.org/tutorials/configuring-and-tuning-openvas-in-kali-linux/
- https://www.linux.com/training-tutorials/linux-101-updating-your-system/
- https://medium.com/dfclub/how-to-use-log2timeline-54377e24872a
- https://www.tecmint.com/how-to-monitor-user-activity-with-psacct-or-acct-tools/

CWU919KD

Threat Detection: Linux Defensive Capabilities

Instructor: Maj Patrick “Shrink” Vinge

USAF Weapons School • Nellis AFB