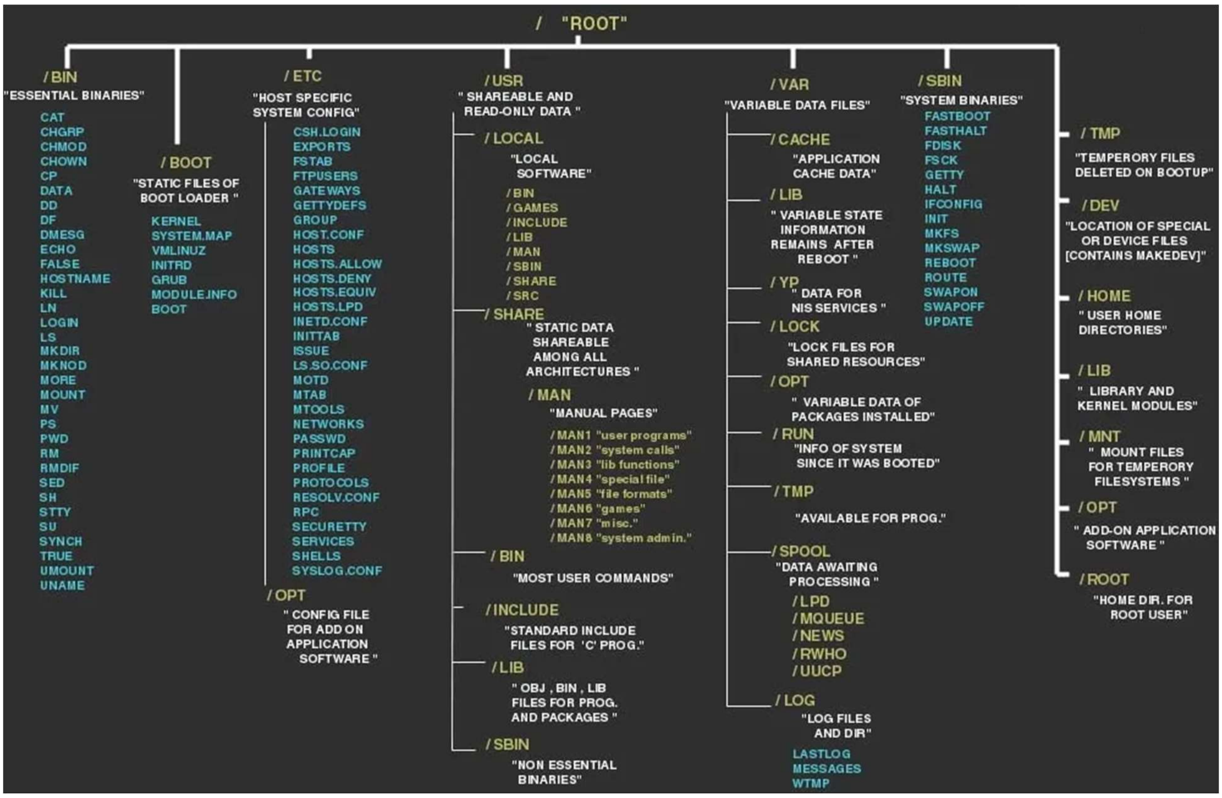
Linux Basics

Filesystem



Basic Linux commands

Command	**Description**
pwd	Show the current working directory
whoami	Show the current user
ls	List then contents of directory
ls -l	Long list of the contents in a directory
ls -la	Long list including hidden files
<command> --help (-h)	Get help for a specific command
man <command>	View manual for a specific command
locate <keyword>	Go through entire file system to locate the specified keyword
whereis	Find binaries (binary file)
which	Return location of the binary in the PATH variable
find <*dir*> -type <*type(dir or file)*> -name <*name to be found*>	Specify the directory and start a search to find the matching query
ps aux	List all running processes
ps	List currently running processes (user)
cat	Display contents of the file or use *redirect* to create a file
touch	Create a file

mkdir	Create a directory
cp *<source file> </dir/newfile>*	Copy file
mv	move file (also used to rename a file)
rm	Remove file
rmdir	Remove directory

Text Manipulation

Command	**Description**
head	Display the first 10 (default) lines in the text
tail	Display the last 10 lines in the text
head -nl	Display numbered lines (nl) in the text
sed	Find and replace text
sed s/mysql/MySQL/g(or #) snort.conf > snort2.conf	*Substitute mysql with MySQL globally (on specific occurrence)*
more	Scroll through text
less	Show less text and use / to search for terms in
grep	

Networking

Command	Description
ifconfig	Display physical int ip configuration
iwconfig	Display wireless int ip config
ifconfig eth <IP> netmask <subnet> broadcast <gateway>	Change the interface ip configuration
dhclient eht0	Reassigned IP via dhcp on eth0
dig <address> ns/nx	Find specific domain name servers/mail servers
vm /etc/hosts	Change local DNS entry
vm /etc/resolv.conf	Change DNS server

Adding and Removing Software

Command	**Description**
apt-cache search <*package*>	Search for software in the repository (local)
apt-get install <*package*>	Install software stored locally
apt-get remove (*package*>	Remove installed software
apt-get purge <*package*>	Remove installed software and the configuration files
apt autoremove <*package*>	Remove all the dependencies
apt-get update	Check and download available updates
apt-get upgrade	Install the downloaded updates
vm /etc/apt/sources.list	Add repositories to query for software
apt-get synaptic	Run *synaptic* from shell (GUI based installer)

File and Directory Permissions

Command	Description
chown *<user> <dir/file>*	Change ownership for user on specific file
chgrp *<group> <dir>*	Change ownership for group on specific files
ls -l *</dir/file>*	Check current permissions

Octal and Binary Representation of Permissions

Binary	Octal	rwx
000	0	---
001	1	--x
010	2	-w-
011	3	-wx
100	4	r--
101	5	r-x
110	6	rw-
111	7	rwx

chmod 774 *<file>*	Change permissions on file for *owner/group/other* to *rwxrwxr*
chmod u-w *<file>*	Remove write permissions for user from specific file
chmod u+x,o+x *<file>*	Grant permissions for users and others to specific file
umask	Subtract permissions from a file using binary table (can be set default in *.profile*). Change default permissions to a file
suid	Grant temporary root permissions

Process Management

Command	Description
ps	Show active processes
ps aux	Show active processes for all users
top	List the top running processes
nice -n -10/10 *<process>*	Increase/decrease priority (Allocate resources)
renice 19 *<pid>*	Take an absolute value and re-set the priority
kill -1 *<pid>*	Kill a process
bg *<pid>*	Run the process in the background
fg *<pid>*	Bring the process to foreground
jobs	List jobs running in the background

Kill signals

Signal name	Option Number	Description
SIGHUP	1	Hangup (HUP) signal – stop and restart with the PID
SIGNIT	2	Interrupt (INT) signal – weak kill signal (not guaranteed to work)
SIGQUIT	3	Core dump – terminates the process and save the process info in memory, and then saves the information in the current working directory to a file named *core.*
SIGTERM	15	Termination (TERM) – kill commands default kill signal
SIGKILL	9	Absoulute kill signal – forces the process to stop by sending the process resources to special device, */dev/null*

Managing User Environment Variables

Command	Description
env	Manage user set variables
set	Manage all variables (local, shell functions, user-defined variables, command aliases)
unset	Delete values from variable or function
<variable>=*<value>* E.g. HISTSIZE=0	Set environmental variable value for session only
export *<variable>*	Export the variable from the current session to make be re-used in later session
export/set> ~/*<exportedvalues.txt>*	Export single or all the environmental values to user home directory before making changes
PATH=$PATH:/root/newtool	Add new directory to PATH variable (will be queried for commands)
MYNEWVARIABLE="*<value>*"	Set new variable for later use

Compressing and Archiving

Command	Description
tar • -c (create) • -v (verbose) • -f (write) *tar -xvf <archive.tar> <file1> <file2> <file3>* • -t (display) • -x (extract)	Archive many files into one file with .tar extension • Creates the .tar file • List the files that are being worker with • Write to the following file • Display the contents without extracting • Extract the files
gzip (.tar.gz / .tgz)	Most common – falls between compress and bzip2
bzip2 (.tar.bz2)	Slowest – resultant files are the smallest
compress (.tar.z)	Fastest – resultant files are the largest
uncompress	Un-compress the compressed files
bunzip2	Un-compress the compressed files
dd *<if=inputfile of=outputfile>*	Create a bit-by-bit or physical copies of storage devices, including deleted files

File System and Storage Device Management

Command	**Description**
/dev	Directory containing files for each attached device
fdisk -l	List all the partitions and see how much capacity is available
c (*character*)	External devices (mice, keyboard)
b (*block*)	Block devices (hard drives, DVD drives) – high speed data throughput
lsblk	List block devices
mount *dev/sdb1 /mnt (/media)*	Mount drive manually to access the contents
umount */dev/sdb1*	Unmount the drive
df *(disk free)*	Acquire information on mounted disks
fsck *(file system check)*	Check for errors
dd	Copy all the contents, for example, from flash drive to hard drive

Device naming system

Device File	**Description**
sda	First SATA drive
sdb	Second SATA drive
sdc	Third SATA drive
sdd	Fourth SATA Drive

Partition labeling system

Partition	**Description**
sda1	The first partition (1) of the SATA (a) drive
sda2	The second (2) partition of the SATA (a) drive
sda3	The third (3) partition of the SATA (a) drive

The Logging System

Command	**Description**
rsyslog.conf	Configuration file containing rules of what to log
logrotate.conf	Automatically cleans up log files (archiving)
shred *shred -f -n /var/log/auth.log** • -f • -n	Shred the log files by generating random symbols making them indecipherable • Give permission to shred file • Desired number of times to overwrite
service <*servicename*> *start|restart|stop*	Start or stop rsyslog service

Using and Abusing Services

Command	**Description**
proxychains <*the command to proxy*> <*argument*>	Send a give command through a proxy to maintain anonymity
vim */etc/proxychains.conf*	Set proxies in a config file

Inspecting Wireless Networks

Wireless (Wi-Fi)

Command	**Description**
ifconfig	List activated network interfaces
iwconfig	View wireless network interface
iwlist <*interface*> scan	Scan for all AP's that the network card can reach
nmcli *(network manager command line interface)* *ncmli dev <network type>*	View wifi AP's nearby and their key data
nmcli dev *wifi* connect <*AP-SSID*> password <*password*>	Connect to AP within range
airmon-ng *start|restart|stop <interface>*	Put the network card in monitor mode to see all the passing through traffic
airodump-ng *wlan0mon*	Capture and display key data from broadcasting AP's
airodump-ng -c 10 –bssid <*mac-address*> -w <ESSID> wlan0mon	Capture all the packets traversing the found AP on channel (-c) 10
aireplay-ng –deauth 100 -a <*mac-address*> -c <*man-address*> wlan0mon	Force all the AP clients to re-authenticate in order to capture the password hash
aircrack-ng -w wordlist.cap -b <*mac-address*> <*filename*>	Find the captured password from the list

Bluetooth

Command	Description
hciconfig	Look at the Bluetooth interfaces (works like ifconfig)
hcitool	Inquiry tool: provides device name, device ID, device class, device clock information (enables the device to work synchronously)
hcidump	Sniff the Bluetooth communications (capture data sent over Bluetooth signal)
hciconfig <*name*> up	Check that the connection is enabled
hcitool scan	Check for Bluetooth devices sending out them discover beacons (discovery mode)
hcitool inq	Gather information about the detected devices
sdptool browse <*mac-address*>	Search for Bluetooth services (device does not need to be in discovery mode)
l2ping <*mac-address*> -c <*number-of-packets*>	Send out ping to see if the device is within reach

Managing the Linux Kernel and Loadable Kernel Modules

Command	Description
uname -a	Check the kernel that the system is running
cat /proc/version	Check the kernel that the system is running (alternative way)
systl	Tune the kernel (memory allocation, networking modules etc.)
ksmod	Manage kernel modules
modinfo <*module name*>	Find more information about a specific module
modprobe -a <*module name*>	Add a module to the kernel
modprobe -r <*module name*>	Remove a module from the kernel
dsmeg	Print out a message buffer from the kernel to see if the module has loaded successfully or returned any errors

Job Scheduling

Time representation for Use in the crontab

Field	Time unit	Representation
1	Minute	0-59
2	Hour	0-23
3	DOM (Day of the month)	1-31
4	MON (Month)	1-12
5	DOW (Day of the week)	0-7

Command	Description
crontab -e	Edit the crontab by providing the -*e* switch
vim /etc/crontab	Open the crontab
<date & time> <user> bin/<backup-script.sh>	*Add the line to crontab to schedule a job to execute backup script in the bin directory*
update-rc.d <*name of the script or service*> remove|defaults|disable|enable	Add services or scripts to run at startup