Commands:	What the red-hat!
alias	shortcuts
ACL, getfacl, setfacl	Access Control Lists, allow us to apply a more specific set of permissions to a file or directory without (necessarily) changing the base ownership. getfacl, shows permissions. setfac, change permissions. Ex. "setfac -m o:rwx file1", changes permission for others to read, write and execute.
apt, pacman, yum, rpm	package management
adduser	Add user and will create home directory + skeleton files to that directory
cal	calendar
cat	show file content
cd	navigate through directories
chmod	change file permission - admin, users, others. r(read),w(write),e(execute).
clear	clear terminal
cp	copy files
dd	low level copying of data

deluser	delete user
df	display diskfile info
echo	print text
ifconfig	display network info and ip's
iptables	base firewall (IP based). iptables -L, shows all rules
iptable-persistents	program to save iptabels roles, also after shutdown.
kill / killall	kill active processess (by ID or name)
last	displays information about the last logged-in users
less	display paged output
ln	shortcut to files
ls	list directories
man	display manual page for specific command
mkdir	create directory
mount	mount file systems

mv	move or rename files
passwd	password
ps	display active proccesses
pwd	print working directory
rlogin	Tool for remotely using a computer over a network, clear text
rm	delete files or directory
rsync	(remote sync) is for transferring (synchronizing) files between a computer and ex. server
scp	(secure copy) command in Linux system is used to copy file(s) between servers in a secure way.
service	start/stop service
ssh	secure shell
ss	is used to dump socket statistics. It allows showing information similar to netstat. -lt/-ltn list ports
sudo	super user
telnet	client/server application protocol that allows remote access, clear text

top	task manager
tcpdump	shows tcp packages
touch	create file
traceroute	trace all network hops to destination
tripwire	file integrity monitoring tool that watches for changes to critical files on your system. tripwire --init, installs DB. tripwire --check, generates repports.
ufw	A firewall build upon iptables
unman	get basic information about OS
useradd	add user to system without directory
usermod	used to Modify a User's Linux Settings, usermod -aG sudo "username", adds a user to sudo group.
wget	download files from internet
whatis	gives explanation of what a command actually is
whereis	locates the binary, source, and manual pages for a specific command or program
whoami	Show your user name.

Linux system

Linux 3 layers:	• 1. Hardware, This layer is all the physical components, like RAM, motherboard, Network interface... • 2. Kernel, the kernel is the heart of Linux. It's responsible for low-level tasks and directly interacting with the hardware. • 3. User processes, the User processes include the GUI and Shell, it allows the user to interact with the kernel.
SUID/SGID	SUID allows users to temporarily assume the privileges of the file owner, while SGID enables temporary group ownership
shadow file	"/etc/shadow" is a plain text file that stores information about the passwords of the system's users. The passwords are hashed in the file.
passwd file	"/etc/passwd" contains user info like: user ID, group ID, home directory, shell... and are critical for the login operation.
/etc/	"/etc" is used for configurations files (.conf).
/usr/	"/usr" is used for "user programs". It contains binaries(/usr/bin) and shared files...
/var/	"/var" log files, 'temporary' files (like mail spool), databases, "www" and all other data not tied to a specific user.

Linux - Kail, Metasploit

Metaspliot	Metasploit is designed to help users find, exploit and validate vulnerabilities in system
msfconsole	start Metasploit terminal
exploit	Starts the attack
Metasploitable	Metasploitable is an intentionally vulnerable Linux virtual machine
nmap	Metasploit is designed to help users find, exploit and validate vulnerabilities in system
nmap -sn	search network for IP's - ex nmap -sn 192.168.62.0/24
nmap -A	portscan on specific IP - ex nmap -A 192.168.62.120
nmap -sV	search for open ports to attack