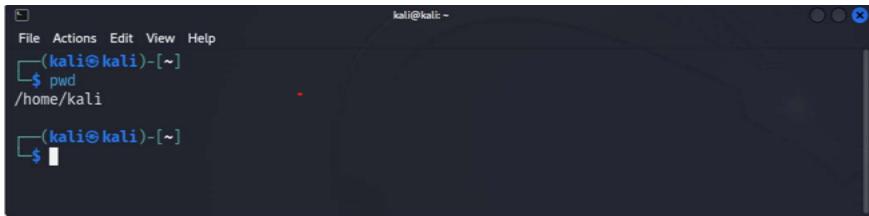


MOHAMMED FAOD.
ALUOSOIFI.

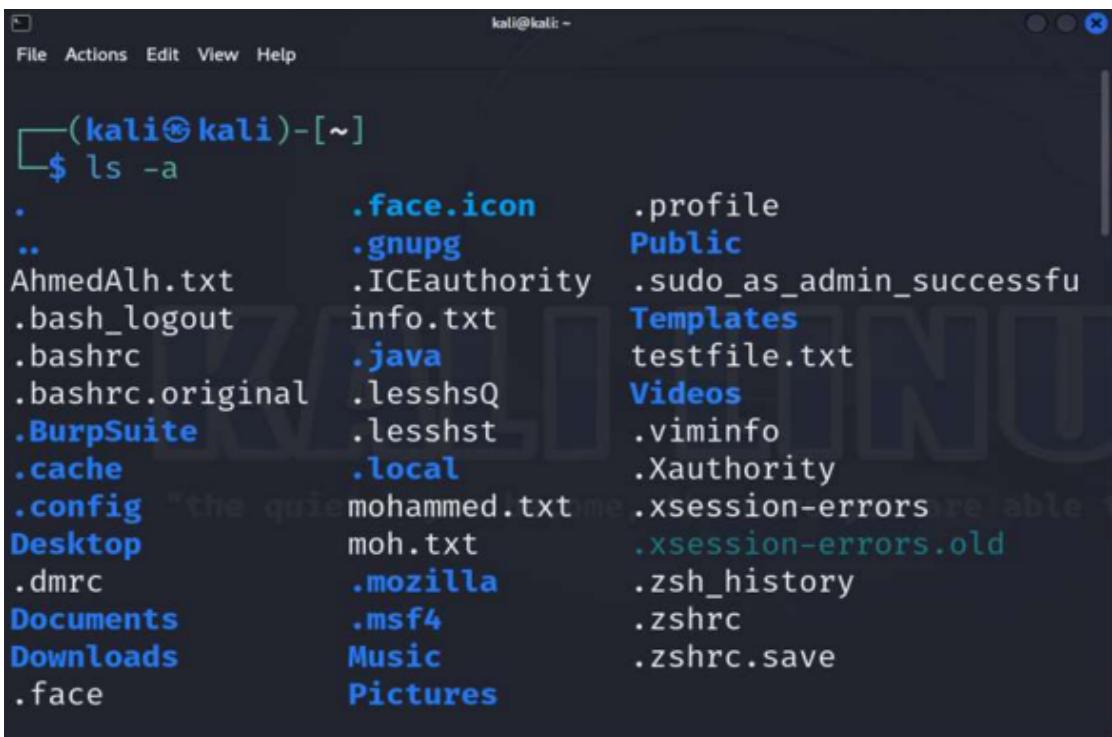
Section 1: File and Directory Management

1. Display the current working directory.



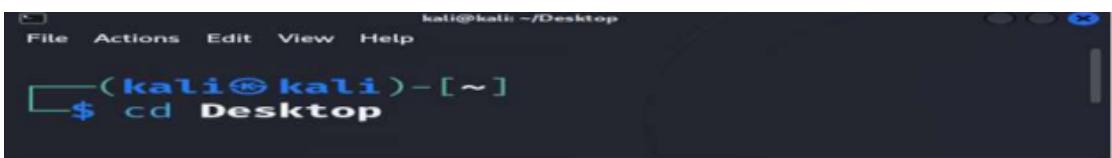
```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]
$ pwd
/home/kali
[(kali㉿kali)-[~]]
$
```

2. List all the contents of your current directory, including hidden files.



```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]
$ ls -a
.
..
AhmedAlh.txt
.bash_logout
.bashrc
.bashrc.original
.BurpSuite
.cache
.config
/Desktop
.dmrc
/Documents
/Downloads
.face
..face.icon
.gnupg
.ICEauthority
.info.txt
.java
.lesshsQ
.lessht
.local
.mohammed.txt
.moh.txt
.mozilla
.msf4
.Music
.Pictures
.profile
.Public
.sudo_as_admin_successfu
.Templates
.testfile.txt
.Videos
.viminfo
.Xauthority
.xsession-errors
.xsession-errors.old
.zsh_history
.zshrc
.zshrc.save
[(kali㉿kali)-[~]]
```

3. Change your directory to the `Desktop`.



```
kali㉿kali: ~/Desktop
File Actions Edit View Help
[(kali㉿kali)-[~]]
$ cd Desktop
```

4. Create two directories named `dir1` and `dir2` on the Desktop.



```
kali㉿kali: ~/Desktop
File Actions Edit View Help
[(kali㉿kali)-[~/Desktop]]
$ mkdir dir1 ,dir2
```

5. Inside `dir1`, create a file named `file1.txt`.



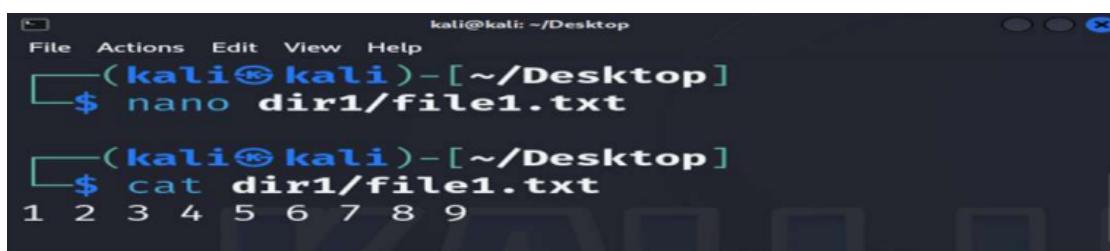
```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ touch dir1/file1.txt
```

6. Inside `dir2`, create a file named `file2.txt`.



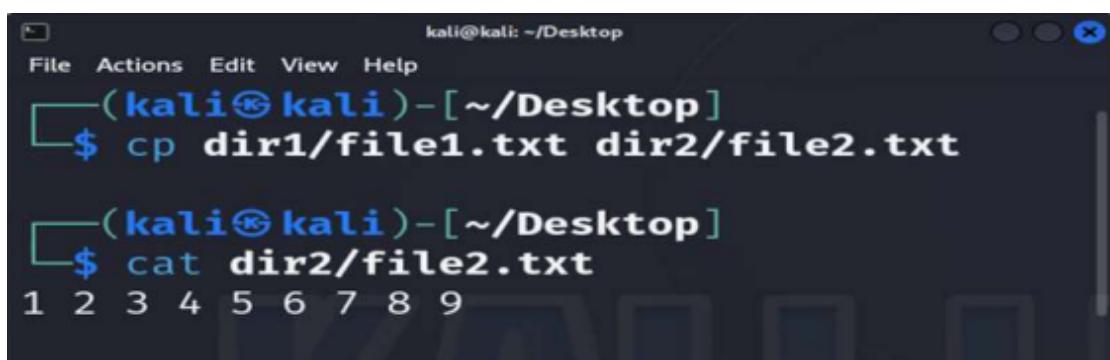
```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ touch dir2/file2.txt
```

7. Using nano or vim Write the numbers 1 to 9 into `file1.txt`.



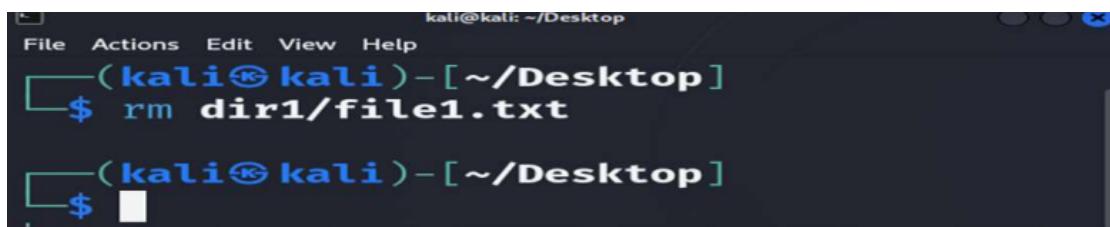
```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ nano dir1/file1.txt
└─(kali㉿kali)-[~/Desktop]
$ cat dir1/file1.txt
1 2 3 4 5 6 7 8 9
```

8. From the home directory Copy the contents of `file1.txt` into `file2.txt`.



```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ cp dir1/file1.txt dir2/file2.txt
└─(kali㉿kali)-[~/Desktop]
$ cat dir2/file2.txt
1 2 3 4 5 6 7 8 9
```

9. From the home directory, delete `file1.txt` inside `dir1`.



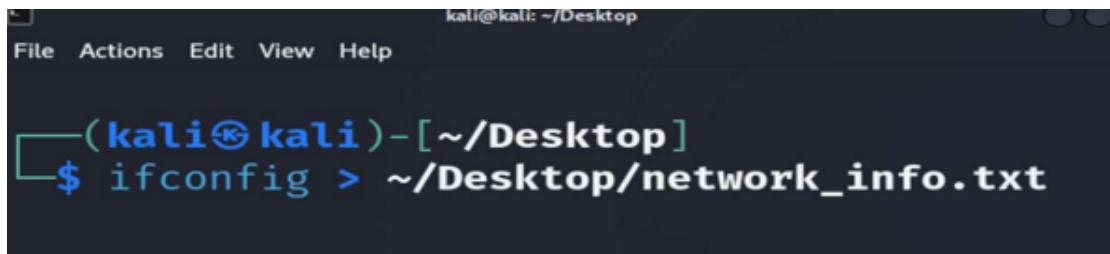
```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ rm dir1/file1.txt
└─(kali㉿kali)-[~/Desktop]
$ █
```

10. Remove the directory `dir1` from the Desktop.



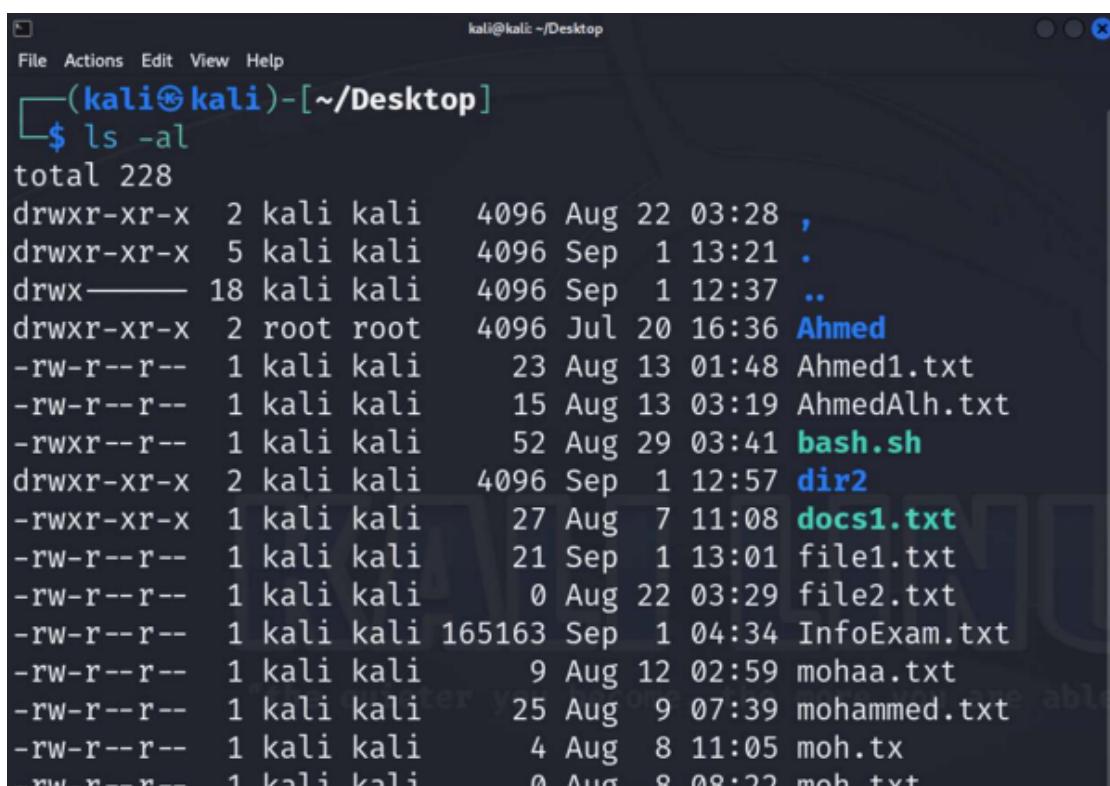
```
kali@kali: ~/Desktop
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ rmdir dir1
```

11. Redirect the output of the network configuration command to a file named `network_info.txt` on the Desktop.



```
kali@kali: ~/Desktop
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ ifconfig > ~/Desktop/network_info.txt
```

12. Open the Desktop folder and show all files with detailed information.



```
kali@kali: ~/Desktop
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop]
$ ls -al
total 228
drwxr-xr-x  2 kali kali  4096 Aug 22  03:28 ,
drwxr-xr-X  5 kali kali  4096 Sep  1 13:21 .
drwx----- 18 kali kali  4096 Sep  1 12:37 ..
drwxr-xr-x  2 root root  4096 Jul 20 16:36 Ahmed
-rw-r--r--  1 kali kali   23 Aug 13 01:48 Ahmed1.txt
-rw-r--r--  1 kali kali   15 Aug 13 03:19 AhmedAlh.txt
-rwxr--r--  1 kali kali   52 Aug 29 03:41 bash.sh
drwxr-xr-x  2 kali kali  4096 Sep  1 12:57 dir2
-rw xr-xr-x  1 kali kali   27 Aug  7 11:08 docs1.txt
-rw-r--r--  1 kali kali   21 Sep  1 13:01 file1.txt
-rw-r--r--  1 kali kali     0 Aug 22 03:29 file2.txt
-rw-r--r--  1 kali kali 165163 Sep  1 04:34 InfoExam.txt
-rw-r--r--  1 kali kali    9 Aug 12 02:59 mohaa.txt
-rw-r--r--  1 kali kali   25 Aug  9 07:39 mohammed.txt
-rw-r--r--  1 kali kali     4 Aug  8 11:05 moh.tx
-rw-r--r--  1 kali kali     0 Aug  8 08:22 moh.txt
```

Section 2: Users and Groups Management

13. Create a new user with your name.
14. Set a password for your user.

```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─$ sudo adduser mohammed
[sudo] password for kali:
[info: Adding user `mohammed' ...
[info: Selecting UID/GID from range 1000 to 59999 ...
[info: Adding new group `mohammed' (1007) ...
[info: Adding new user `mohammed' (1007) with group `mohammed
(1007)' ...
[warn: The home directory `/home/mohammed' already exists. No
t touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mohammed
Enter the new value, or press ENTER for the default
    Full Name []: n
    Room Number []: n
    Work Phone []: n
    Home Phone []: n
    Other []: n
Is the information correct? [Y/n] y
[info: Adding new user `mohammed' to supplemental / extra grou
ps `users' ...
[info: Adding user `mohammed' to group `users' ...


```

15. Open the file that contains user information and verify that your user has been added.

```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─$ cat /etc/passwd | grep mohammed
mohammed:x:1007:1007:n,n,n,n:/home/mohammed:/bin/bash
└─$ █
```

16. Add your user to the file that gives administrative privileges.

```
kali㉿kali:[~/Desktop]
File Actions Edit View Help
└─$ sudo usermod -aG sudo mohammed
└─$ █
```

17. Switch to your user and confirm the user identity.

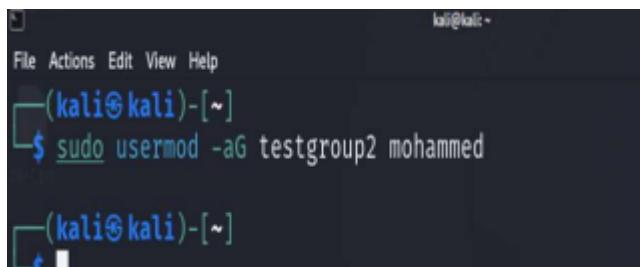
```
mohammed@kali:-
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali:[~])
└─$ su - mohammed
Password:
(mohammed㉿kali:[~])
└─$ █
```

18. Create a new group named `testgroup`.



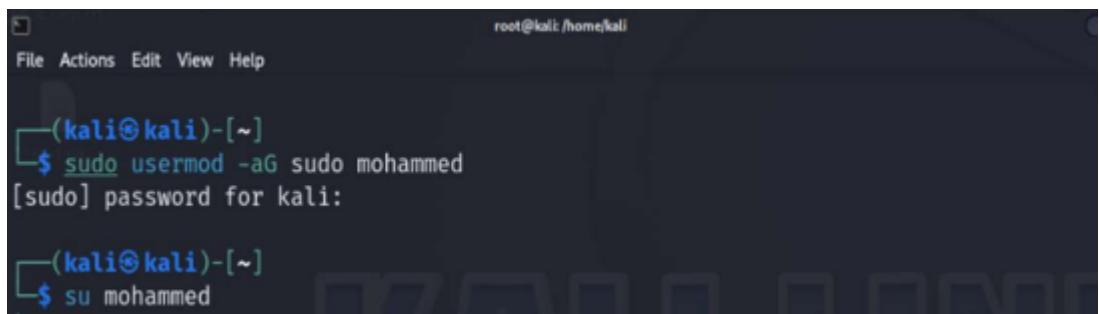
```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo groupadd testgroup2
└─(kali㉿kali)-[~]
$ └─
```

19. Add your user to `testgroup`.



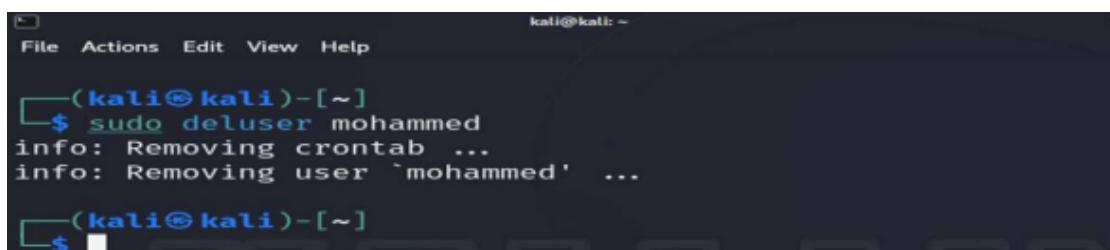
```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo usermod -aG testgroup2 mohammed
└─(kali㉿kali)-[~]
$ └─
```

20. Add the group `testgroup` to the file that gives administrative privileges.



```
root@kali: /home/kali
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo usermod -aG sudo mohammed
[sudo] password for kali:
└─(kali㉿kali)-[~]
$ su mohammed
└─(mohammed㉿kali)-[~]
$ └─
```

21. Remove your user from the file that gives administrative privileges.



```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo deluser mohammed
info: Removing crontab ...
info: Removing user 'mohammed' ...
└─(kali㉿kali)-[~]
$ └─
```

22. Check if your user still have administrative privileges.

```
kali@kali: ~
File Actions Edit View Help

└─(kali㉿kali)-[~]
$ groups mohammed
groups: 'mohammed': no such user

└─(kali㉿kali)-[~]
$ █
```

23. Check which groups your user belongs to.

```
kali@kali: ~
File Actions Edit View Help

└─(kali㉿kali)-[~]
$ groups
kali adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth scanner wireshark kaboxer

└─(kali㉿kali)-[~]
$ █
```

Section 3: Permissions and Ownership

24. Set the permissions of `file2.txt` on the Desktop to allow the owner to read, write, and execute; the group to read and execute; and others to read.

```
└─(kali㉿kali)-[~/Desktop]
$ chmod 775 dir2/alshbli2.txt
```

25. Check the permissions of `file2.txt` to verify the change.

```
└─(kali㉿kali)-[~/Desktop]
$ ls -l dir2/alshbli2.txt
-rwxrwxr-x 1 kali kali 18 Sep  3 13:14 dir2/alshbli2.txt
```

26. Change the ownership of `file2.txt` to your user.

```
Ratto@Kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo useradd MohammedAli

└─(kali㉿kali)-[~]
$ sudo chown MohammedAli ~/Desktop/dir2/file2.txt

└─(kali㉿kali)-[~]
$ ┌───
```

27. verify the ownership of `file2.txt` .

```
kali㉿kali: ~
File Actions Edit View Help

└─(kali㉿kali)-[~]
$ ls -l ~/Desktop/dir2/file2.txt
-rwxr-x--x 1 MohammedAli kali 18 Sep 1 13:12 /home/kali/Desktop/di
r2/file2.txt

└─(kali㉿kali)-[~]
$ ┌───
```

28. Change back the ownership of a file `file2.txt` .

```
kali㉿kali: ~
File Actions Edit View Help

└─(kali㉿kali)-[~]
$ sudo chown root ~/Desktop/dir2/file2.txt

└─(kali㉿kali)-[~]
$ ┌───
```

29. Grant write permission to everyone for `file2.txt` .

```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo chmod a+w ~/Desktop/dir2/file2.txt

└─(kali㉿kali)-[~]
```

30. Remove the write permission for the group and others for `file2.txt` .

```
kali㉿kali: ~
File Actions Edit View Help
└$ sudo chmod a+w ~/Desktop/dir2/file2.txt
└(kali㉿kali)-[~]
└$ sudo chmod go-w ~/Desktop/dir2/file2.txt
└(kali㉿kali)-[~]
└$
```

31. Delete `file2.txt` after making the necessary ownership and permission changes.

```
File Actions Edit View Help
└(kali㉿kali)-[~]
└$ rm ~/Desktop/dir2/file2.txt
rm: remove write-protected regular file '/home/kali/Desktop/dir2/file2.txt'?
└(kali㉿kali)-[~]
└$
```

32. What command would you use to recursively change the permissions of all files and directories inside a folder named `project` to `755`.

```
File Actions Edit View Help
└(kali㉿kali)-[~]
└$ mkdir project
└(kali㉿kali)-[~]
└$ sudo chmod -R 755 project
└(kali㉿kali)-[~]
└$
```

Section 4: Process Management:

33. Install a system monitor tool that provides an interactive process viewer(htop).

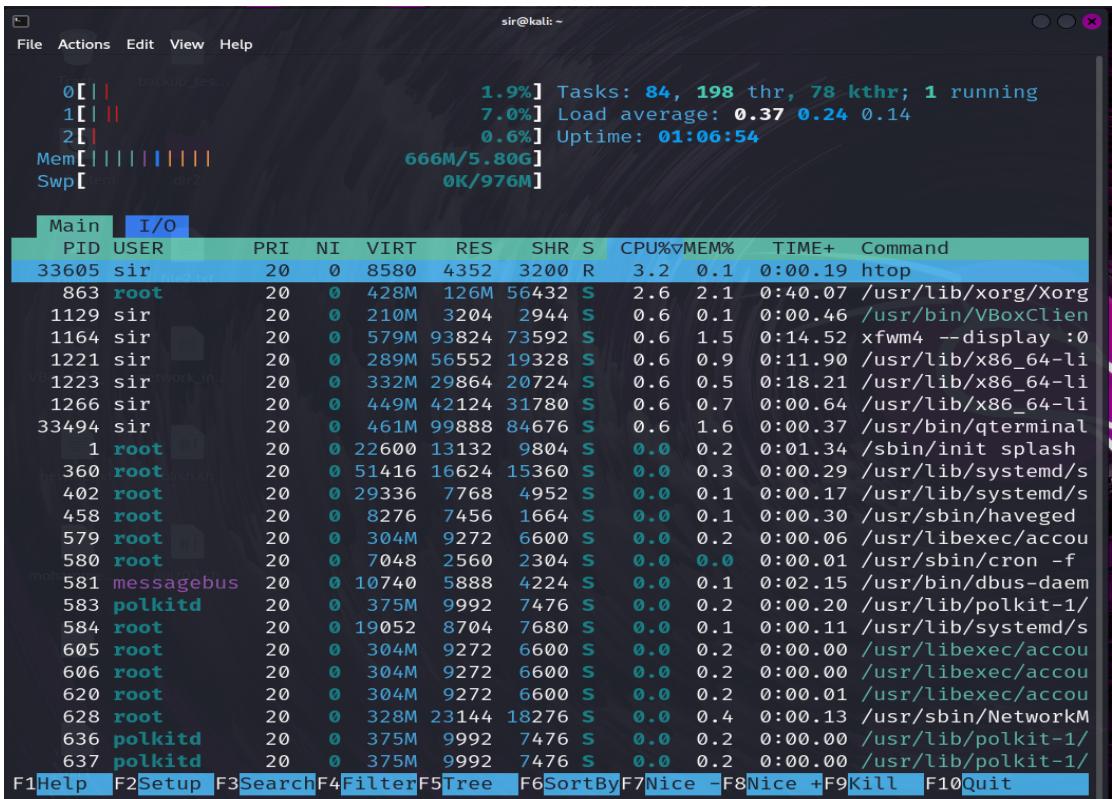


```
sir@kali: ~
File Actions Edit View Help
(sir@kali)-[~]
$ sudo apt install htop
htop is already the newest version (3.3.0-4).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 425
(sir@kali)-[~]
$
```

34. Display all running processes.

There are many ways to display all running processes:

- ps aux
- top
- htop
- pgrep -a
- pstree



htop output showing system stats and process list:

```
Tasks: 84, 198 thr, 78 kthr; 1 running
Load average: 0.37 0.24 0.14
Uptime: 01:06:54
Mem: 666M/5.80G
Swap: 0K/976M
```

Main	I/O	PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%▼MEM%	TIME+	Command
33605	sir	20	0	8580	4352	3200	R	3.2	0.1	0:00.19	htop	
863	root	20	0	428M	126M	56432	S	2.6	2.1	0:40.07	/usr/lib/xorg/Xorg	
1129	sir	20	0	210M	3204	2944	S	0.6	0.1	0:00.46	/usr/bin/VBoxClient	
1164	sir	20	0	579M	93824	73592	S	0.6	1.5	0:14.52	xfwm4 --display :0	
1221	sir	20	0	289M	56552	19328	S	0.6	0.9	0:11.90	/usr/lib/x86_64-li	
1223	sir	20	0	332M	29864	20724	S	0.6	0.5	0:18.21	/usr/lib/x86_64-li	
1266	sir	20	0	449M	42124	31780	S	0.6	0.7	0:00.64	/usr/lib/x86_64-li	
33494	sir	20	0	461M	99888	84676	S	0.6	1.6	0:00.37	/usr/bin/qterminal	
1	root	20	0	22600	13132	9804	S	0.0	0.2	0:01.34	/sbin/init splash	
360	root	20	0	51416	16624	15360	S	0.0	0.3	0:00.29	/usr/lib/systemd/s	
402	root	20	0	29336	7768	4952	S	0.0	0.1	0:00.17	/usr/lib/systemd/s	
458	root	20	0	8276	7456	1664	S	0.0	0.1	0:00.30	/usr/sbin/haveged	
579	root	20	0	304M	9272	6600	S	0.0	0.2	0:00.06	/usr/libexec/accou	
580	root	20	0	7048	2560	2304	S	0.0	0.0	0:00.01	/usr/sbin/cron -f	
581	messagebus	20	0	10740	5888	4224	S	0.0	0.1	0:02.15	/usr/bin/dbus-daem	
583	polkitd	20	0	375M	9992	7476	S	0.0	0.2	0:00.20	/usr/lib/polkit-1/	
584	root	20	0	19052	8704	7680	S	0.0	0.1	0:00.11	/usr/lib/systemd/s	
605	root	20	0	304M	9272	6600	S	0.0	0.2	0:00.00	/usr/libexec/accou	
606	root	20	0	304M	9272	6600	S	0.0	0.2	0:00.00	/usr/libexec/accou	
620	root	20	0	304M	9272	6600	S	0.0	0.2	0:00.01	/usr/libexec/accou	
628	root	20	0	328M	23144	18276	S	0.0	0.4	0:00.13	/usr/sbin/NetworkM	
636	polkitd	20	0	375M	9992	7476	S	0.0	0.2	0:00.00	/usr/lib/polkit-1/	
637	polkitd	20	0	375M	9992	7476	S	0.0	0.2	0:00.00	/usr/lib/polkit-1/	

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit

35. Display a tree of all running processes.

- `pstree`

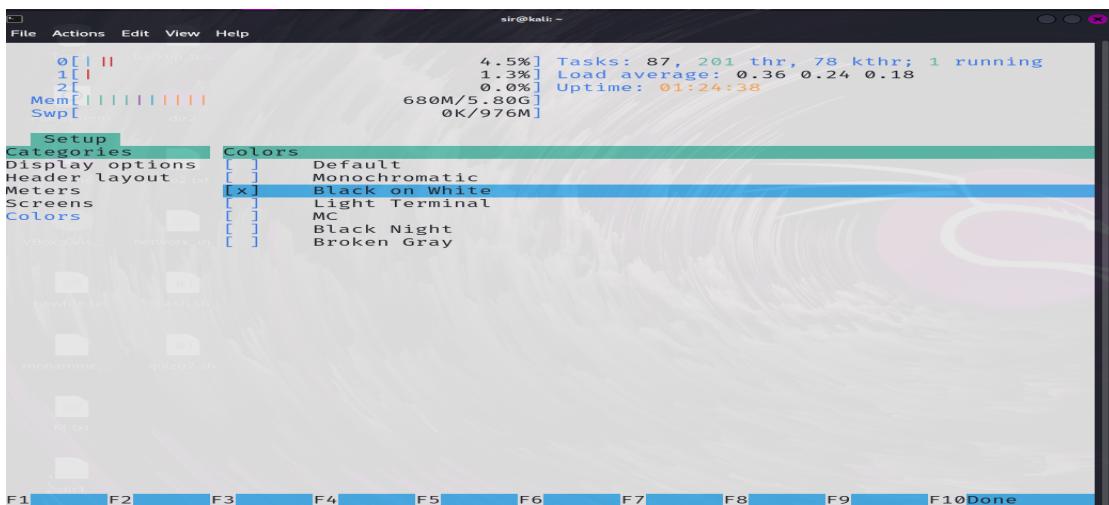
```
sir@kali: ~
$ pstree
systemd--ModemManager---3*[{ModemManager}]
systemd--NetworkManager---1*[{NetworkManager}]
  -3*[VBoxClient---VBoxClient---3*[{VBoxClient}]}
  -VBoxClient---VBoxClient---4*[{VBoxClient}]
  -VBoxClient---4*[{VBoxClient}]
  -VBoxService---8*[{VBoxService}]
accounts-daemon---3*[{accounts-daemon}]
agetty
cron
dbus-daemon
haveged
lightdm---Xorg---x-session-manag---Thunar---3*[{Thunar}]
  -agent---3*[{agent}]
  -apilet-p
  -blue-man-applet---4*[{blue-man-applet}]
  -light-locker---4*[{light-locker}]
  -nm-applet---5*[{nm-applet}]
  -polkit-mate-aut---3*[{polkit-mate-aut}]
  -polkit-agent
  -xfce4-panel---panel-1-whisker---4*[{panel-1-whisker}]
    -panel-13-cpugra---3*[{panel-13-cpugra}]
    -panel-14-cpugra---3*[{panel-14-cpugra}]
    -panel-15-genmon---4*[{panel-15-genmon}]
    -panel-16-pulsea---4*[{panel-16-pulsea}]
    -panel-17-notifii---4*[{panel-17-notifii}]
    -panel-18-power---4*[{panel-18-power}]
    -panel-22-action---4*[{panel-22-action}]
    -4*[{xfce4-panel}]
  -xfce4-power-man---4*[{xfce4-power-man}]
  -xfdesktop---4*[{xfdesktop}]
  -xfsettingsd---3*[{xfsettingsd}]
  -xfwm4---4*[{xfwm4}]
  -xkb-dm---1*[{xkb-dm}]
  -3*[{x-session-manag}]

  -polkitd---3*[{lightdm}]
  -qterminal---zsh---htop
  -2*[{qterminal}]
  -rtkit-daemon---2*[{rtkit-daemon}]
  -sudo---sudo---apt---http
systemd---(sd-pam)
  -at-spi1-bus-laun---dbus-daemon
  -at-spi2-registr---3*[{at-spi2-registr}]
  -dbus-daemon
  -dconf-service---3*[{dconf-service}]
  -gnome-keyring-d---4*[{gnome-keyring-d}]
```

36. Open the interactive process viewer and identify a process by its PID.

- The steps to do it:

1. Do the command (`htop`).
2. To identify a process by its PID: press (F3 or /) to open a search function.
3. Finally type the PID that you want.



37. Kill a process with a specific PID.

The terminal window shows the output of the 'top' command followed by the execution of the 'kill' command. The 'top' command displays system load averages and a list of processes. The 'kill' command is used to terminate a process with PID 1117.

```
File Actions Edit View Help
(sir㉿kali)-[~]
$ kill 1117
(sir㉿kali)-[~]
$
```

```
File Actions Edit View Help
top - 12:14:57 up 1:32, 1 user, load average: 0.07, 0.18,
Tasks: 173 total, 1 running, 167 sleeping, 5 stopped, 0
%Cpu(s): 0.7 us, 1.1 sy, 0.1 ni, 98.1 id, 0.0 wa, 0.0 hi
MiB Mem : 5940.7 total, 4301.7 free, 957.6 used, 92
MiB Swap: 976.0 total, 976.0 free, 0.0 used, 498

```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM
863	root	20	0	445888	136592	59952	S	2.3	2.2
45166	sir	20	0	45928	4468	31448	S	1.3	0.7
1164	sir	20	0	52976	9187	52972	S	1.0	1.5
1202	sir	20	0	460884	45336	52972	S	0.7	0.7
1213	sir	20	0	480804	67628	35264	S	0.3	1.1
1223	sir	20	0	340612	29864	20724	S	0.3	0.5
33494	sir	24	4	473544	100964	84724	S	0.3	1.7
45166	sir	20	0	12200	5504	3328	R	0.3	0.1
45430	sir	20	0	472296	99912	84836	S	0.3	1.6
1	root	20	0	22600	13132	9804	S	0.0	0.2
2	root	20	0	0	0	0	S	0.0	0.0
3	root	20	0	0	0	0	S	0.0	0.0
4	root	0	-20	0	0	0	I	0.0	0.0
5	root	0	-20	0	0	0	I	0.0	0.0
6	root	0	-20	0	0	0	I	0.0	0.0
7	root	0	-20	0	0	0	I	0.0	0.0
10	root	0	-20	0	0	0	I	0.0	0.0
12	root	0	-20	0	0	0	I	0.0	0.0
13	root	20	0	0	0	0	I	0.0	0.0
14	root	20	0	0	0	0	I	0.0	0.0
15	root	20	0	0	0	0	I	0.0	0.0
16	root	20	0	0	0	0	S	0.0	0.0
17	root	20	0	0	0	0	I	0.0	0.0
18	root	rt	0	0	0	0	S	0.0	0.0
19	root	-51	0	0	0	0	S	0.0	0.0
20	root	0	0	0	0	0	S	0.0	0.0
21	root	20	0	0	0	0	S	0.0	0.0
22	root	-51	0	0	0	0	S	0.0	0.0
23	root	rt	0	0	0	0	S	0.0	0.0

38. Start an application and stop it using a command that kills processes by name(exeyes).

The terminal window shows the execution of the 'xeyes' command, which starts the Xeyes application. The application is then terminated using the 'kill' command with the process ID 55331.

```
File Actions Edit View Help
(sir㉿kali)-[~]
$ xeyes &
[3] 55331
[3] terminated xeyes
(sir㉿kali)-[~]
$
```

39. Restart the application, then stop it using the interactive process viewer.

```
sir@kali:~
└─$ xeyes &
[1] 57019

(sir@kali)-[~]
└─$ top
   0.6% Tasks: 89, 216 thr, 79 kthr; 2 running
   4.5% Load average: 0.11 0.20 0.17
   1.9% Uptime: 02:00:42
Mem[ 713M/5.80G ] OK/976M

Main I/O
Send signal: PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Comm
0 Cancel 1204 sir 20 0 450M 45336 32972 S 0.0 0.7 0:00.00 xfce
1 SIGHUP 1206 sir 20 0 450M 45336 32972 S 0.0 0.7 0:00.04 xfce
2 SIGINT 1243 sir 20 0 450M 45336 32972 S 0.0 0.7 0:00.01 xfce
3 SIGQUIT 1317 sir 20 0 12496 1820 1536 S 0.0 0.0 0:00.66 xcap
4 SIGILL 1320 sir 20 0 12496 1820 1536 S 0.0 0.0 0:00.00 xcap
5 SIGTRAP 1037 sir 20 0 331M 26952 17792 S 0.0 0.4 0:01.78 x-se
6 SIGABRT 1139 sir 20 0 331M 26952 17792 S 0.0 0.4 0:00.00 x-se
7 SIGFPE 1141 sir 20 0 331M 26952 17792 S 0.0 0.4 0:00.00 x-se
8 SIGPIPE 22866 root 20 0 18160 1960 5760 S 0.0 0.1 0:00.07 sudo
9 SIGKILL 23084 root 20 0 18160 1964 1024 S 0.0 0.0 0:00.00 sudo
10 SIGUSR1 1330 sir 20 0 604M 51060 36076 S 0.0 0.8 0:00.19 nm-a
11 SIGSEGV 1381 sir 20 0 604M 51060 36076 S 0.0 0.8 0:00.00 nm-a

EnterSend EscCancel
```

40. Run a command in the background, then bring it to the foreground(exeyes).

```
sir@kali:~
└─$ xeyes &
[1] 61540

(sir@kali)-[~]
└─$ fg
[1] + running xeyes
^Z
zsh: suspended xeyes
(sir@kali)-[~]
└─$ xeyes &
[2] 61742

(sir@kali)-[~]
└─$ fg
[1] + continued xeyes
^Z
zsh: suspended xeyes
(sir@kali)-[~]
└─$ xclock
^Z
zsh: suspended xclock
(sir@kali)-[~]
└─$ fg
[3] - continued xclock
```

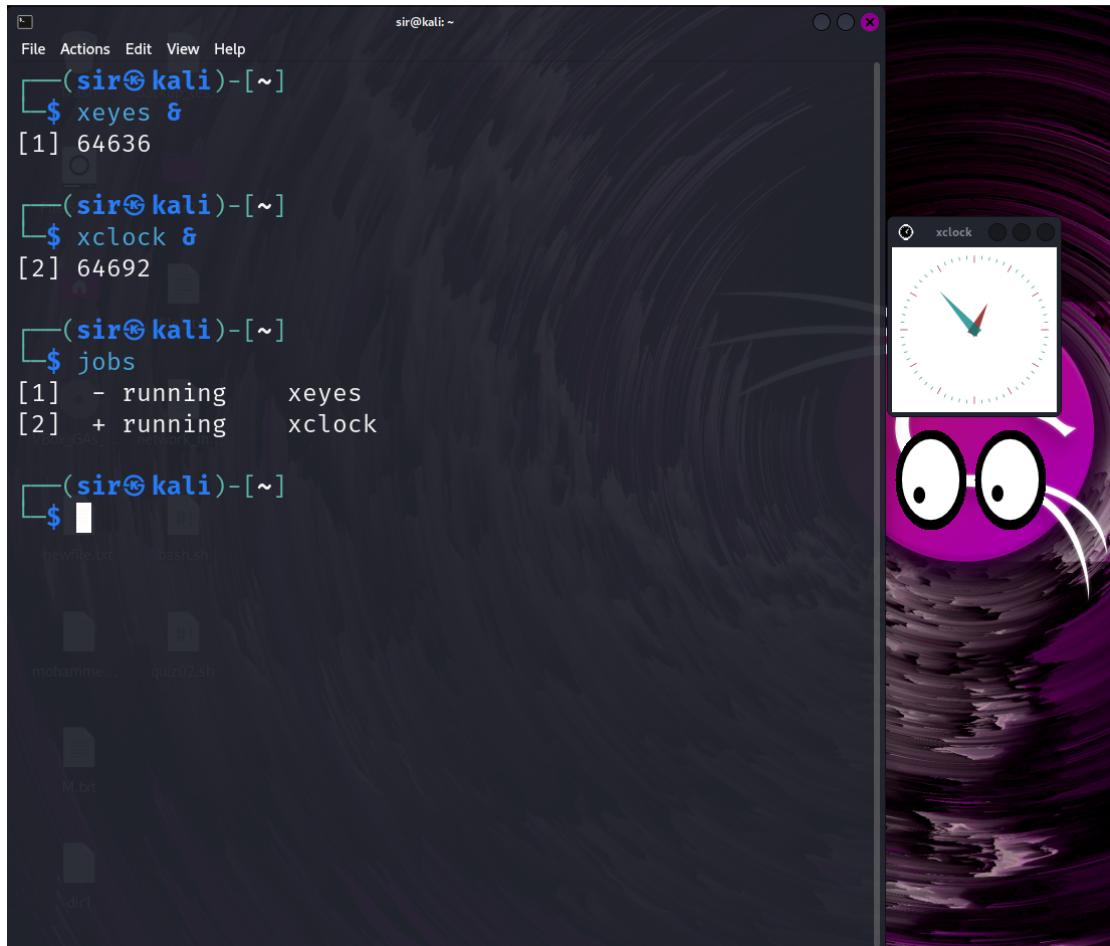
41. Check how long the system has been running.

- Using uptime command

```
(sir@kali)-[~]
└─$ uptime
12:50:24 up 2:07, 1 user, load average: 0.03, 0.12, 0.15

(sir@kali)-[~]
└─$
```

42. List all jobs running in the background.



The image shows a terminal window titled '(sir@sir-kali)-[~]' with the command '\$ jobs' entered. The output shows two background jobs: [1] 64636 (xeyes) and [2] 64692 (xclock). To the right of the terminal is a desktop environment with a purple background featuring a cartoon cat face. A window titled 'xclock' is open, displaying a digital clock.

```
sir@sir-kali: ~
(sir@sir-kali)-[~]
$ xeyes &
[1] 64636

(sir@sir-kali)-[~]
$ xclock &
[2] 64692

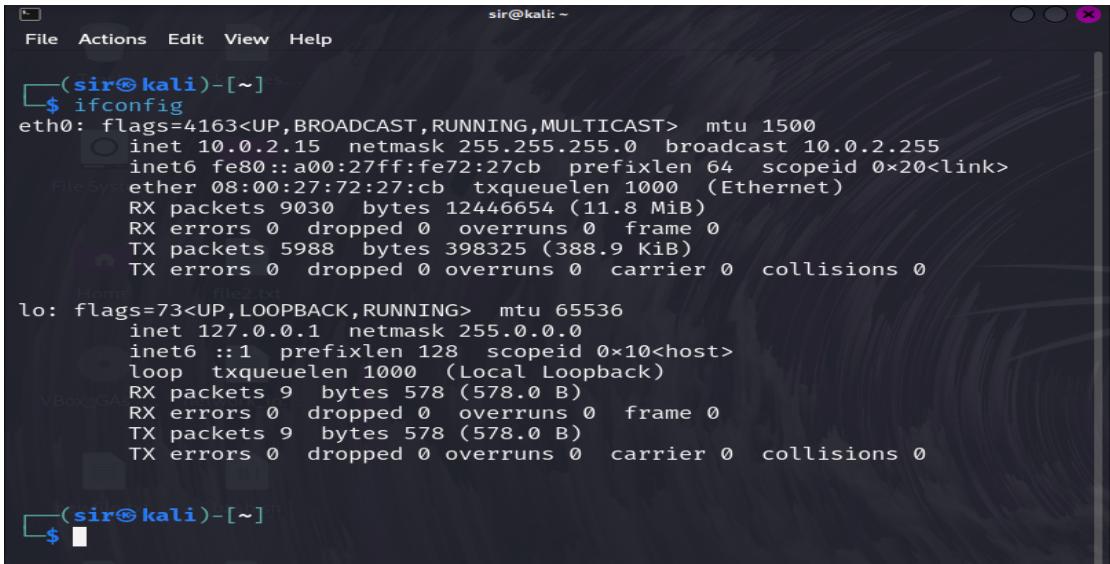
(sir@sir-kali)-[~]
$ jobs
[1] - running      xeyes
[2] + running      xclock

(sir@sir-kali)-[~]
$
```

Section 5: Networking Commands:

43. Display the network configuration.

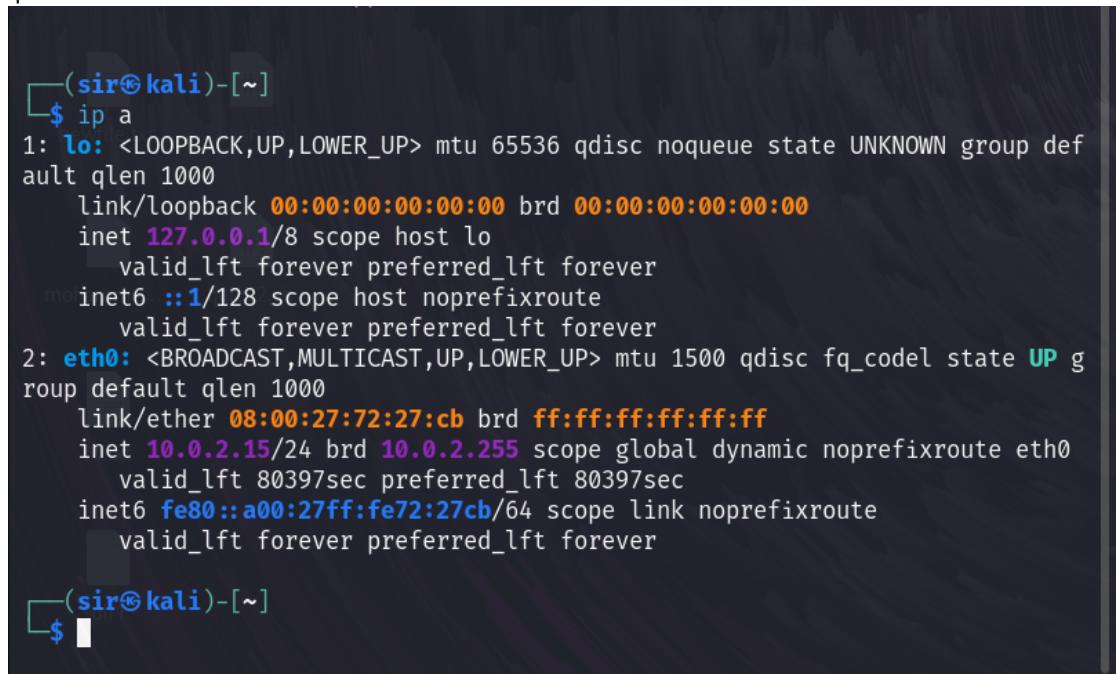
- Ifconfig



A terminal window titled "sir@kali: ~" showing the output of the "ifconfig" command. The output lists two interfaces: eth0 and lo. eth0 has an IP of 10.0.2.15 and MAC address 08:00:27:72:27:cb. lo has an IP of 127.0.0.1 and MAC address ::1. Both interfaces show high activity with many RX and TX packets.

```
sir@kali: ~
File Actions Edit View Help
[sir@kali] ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
                inet6 fe80::a00:27ff:fe72:27cb prefixlen 64 scopeid 0x20<link>
                    ether 08:00:27:72:27:cb txqueuelen 1000 (Ethernet)
                    RX packets 9030 bytes 12446654 (11.8 MiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 5988 bytes 398325 (388.9 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 9 bytes 578 (578.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 9 bytes 578 (578.0 B)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[sir@kali] ~]$
```

- ip a



A terminal window titled "sir@kali: ~" showing the output of the "ip a" command. It lists two interfaces: lo and eth0. The lo interface is a loopback interface with IP 127.0.0.1. The eth0 interface is an Ethernet interface with IP 10.0.2.15 and MAC address 08:00:27:72:27:cb. Both interfaces have their link layer information displayed.

```
sir@kali: ~
[sir@kali] ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:72:27:cb brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 80397sec preferred_lft 80397sec
        inet6 fe80::a00:27ff:fe72:27cb/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[sir@kali] ~]$
```

44. Check the IP address of your machine.

- hostname -l
- ip addr show

```
(sir@sir@kali)-[~]
$ hostname -I
10.0.2.15

(sir@sir@kali)-[~]
$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
    mmo 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
        link/ether 08:00:27:72:27:cb brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
            valid_lft 80235sec preferred_lft 80235sec
        inet6 fe80::a00:27ff:fe72:27cb/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

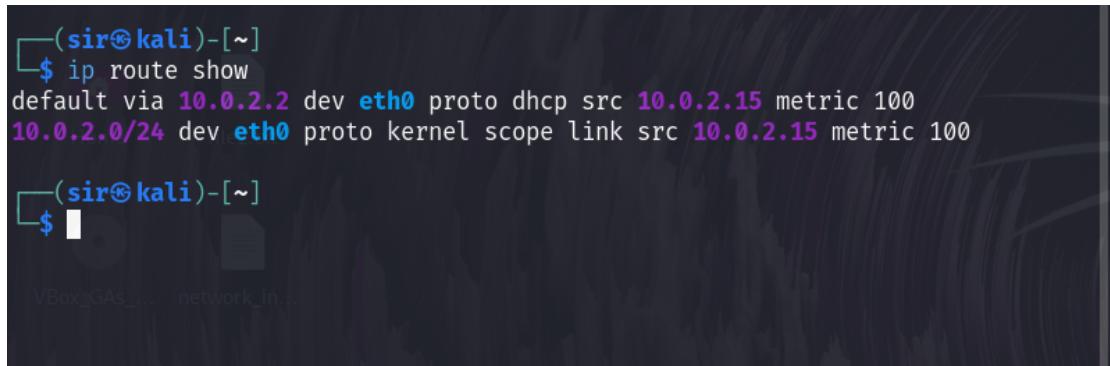
(sir@sir@kali)-[~]
$
```

45. Test connectivity to an external server.

```
(sir@sir@kali)-[~]
$ ping example.com
PING example.com (93.184.215.14) 56(84) bytes of data.
64 bytes from 93.184.215.14: icmp_seq=1 ttl=53 time=808 ms
64 bytes from 93.184.215.14: icmp_seq=2 ttl=53 time=301 ms
64 bytes from 93.184.215.14: icmp_seq=3 ttl=53 time=210 ms
64 bytes from 93.184.215.14: icmp_seq=4 ttl=53 time=233 ms
64 bytes from 93.184.215.14: icmp_seq=5 ttl=53 time=253 ms
64 bytes from 93.184.215.14: icmp_seq=6 ttl=53 time=302 ms
64 bytes from 93.184.215.14: icmp_seq=7 ttl=53 time=277 ms
64 bytes from 93.184.215.14: icmp_seq=8 ttl=53 time=195 ms
64 bytes from 93.184.215.14: icmp_seq=9 ttl=53 time=233 ms
64 bytes from 93.184.215.14: icmp_seq=10 ttl=53 time=248 ms
64 bytes from 93.184.215.14: icmp_seq=11 ttl=53 time=284 ms
64 bytes from 93.184.215.14: icmp_seq=12 ttl=53 time=295 ms
64 bytes from 93.184.215.14: icmp_seq=13 ttl=53 time=211 ms
64 bytes from 93.184.215.14: icmp_seq=14 ttl=53 time=233 ms
64 bytes from 93.184.215.14: icmp_seq=15 ttl=53 time=383 ms
64 bytes from 93.184.215.14: icmp_seq=16 ttl=53 time=272 ms
64 bytes from 93.184.215.14: icmp_seq=17 ttl=53 time=223 ms
64 bytes from 93.184.215.14: icmp_seq=18 ttl=53 time=245 ms
64 bytes from 93.184.215.14: icmp_seq=19 ttl=53 time=268 ms
64 bytes from 93.184.215.14: icmp_seq=20 ttl=53 time=216 ms
64 bytes from 93.184.215.14: icmp_seq=21 ttl=53 time=240 ms
64 bytes from 93.184.215.14: icmp_seq=22 ttl=53 time=259 ms
64 bytes from 93.184.215.14: icmp_seq=23 ttl=53 time=283 ms
64 bytes from 93.184.215.14: icmp_seq=24 ttl=53 time=203 ms
64 bytes from 93.184.215.14: icmp_seq=25 ttl=53 time=228 ms
64 bytes from 93.184.215.14: icmp_seq=26 ttl=53 time=247 ms
64 bytes from 93.184.215.14: icmp_seq=27 ttl=53 time=265 ms
64 bytes from 93.184.215.14: icmp_seq=28 ttl=53 time=290 ms
64 bytes from 93.184.215.14: icmp_seq=29 ttl=53 time=212 ms
64 bytes from 93.184.215.14: icmp_seq=30 ttl=53 time=296 ms
64 bytes from 93.184.215.14: icmp_seq=31 ttl=53 time=278 ms
64 bytes from 93.184.215.14: icmp_seq=32 ttl=53 time=199 ms
64 bytes from 93.184.215.14: icmp_seq=33 ttl=53 time=221 ms
64 bytes from 93.184.215.14: icmp_seq=34 ttl=53 time=239 ms
64 bytes from 93.184.215.14: icmp_seq=35 ttl=53 time=258 ms
```

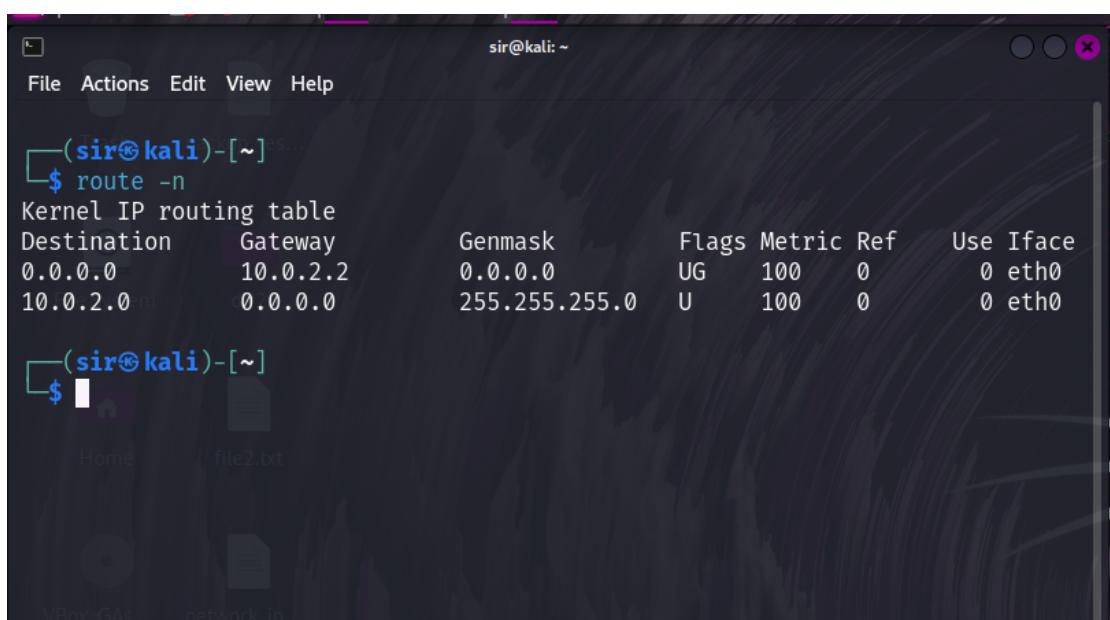
46. Display the routing table.

- ip route show
- route -n



```
(sir@sir@sir)-[~]
$ ip route show
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100

(sir@sir@sir)-[~]
$
```

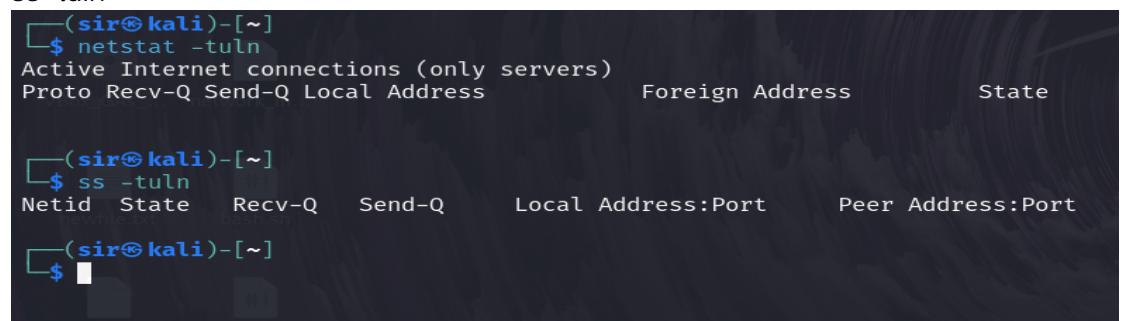


```
(sir@sir@sir)-[~]
$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2      0.0.0.0       UG    100    0        0 eth0
10.0.2.0        0.0.0.0       255.255.255.0 U     100    0        0 eth0

(sir@sir@sir)-[~]
$
```

47. Check the open ports and active connections.

- netstat -tuln
- ss -tuln



```
(sir@sir@sir)-[~]
$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
          Proto Recv-Q Send-Q Local Address:Port          Peer Address:Port
          Netid State      Recv-Q   Send-Q      Local Address:Port      Peer Address:Port

(sir@sir@sir)-[~]
$ ss -tuln
          Proto Recv-Q Send-Q Local Address:Port          Peer Address:Port
          Netid State      Recv-Q   Send-Q      Local Address:Port      Peer Address:Port

(sir@sir@sir)-[~]
$
```

48. Show the IP address of the host machine and the VM, and

verify if they are on the same network.

```
C:\Program Files (x86)\VMware\VMware Workstation\bin>ipconfig

Windows IP Configuration

Ethernet adapter [1] Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
Unknown adapter [2] XXXXXXXX XXXXXX:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
Ethernet adapter [3] Ethernet 2:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address . . . . . : fe80::b950:326:bcec:6157%6
  IPv4 Address. . . . . : 192.168.9.246
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.9.10
Wireless LAN adapter [4] XXXXXXXX XXXXXX* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
Wireless LAN adapter [5] XXXXXXXX XXXXXX* 10:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
Ethernet adapter VMware Network Adapter VMnet1:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address . . . . . : fe80::cd3f:1f08:bb4c:ce83%24
  IPv4 Address. . . . . : 192.168.58.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address . . . . . : fe80::bc6:9623:aa24:de2b%11
  IPv4 Address. . . . . : 192.168.152.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
Wireless LAN adapter [6] XXXXX Wi-Fi:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address . . . . . : fe80::caee:b808:e021:489a%23
  IPv4 Address. . . . . : 192.168.1.104
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
Ethernet adapter [7] XXXXX XXXXXX Bluetooth:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
```

```
(sir㉿kali)-[~]
$ hostname -I
10.0.2.15

(sir㉿kali)-[~]
$ ping 10.0.2.15
Pinging 10.0.2.15 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

49. Trace the route to an external server.

- tracert 10.0.2.1 (used in Window)

```
:\\Program Files (x86)\\VMware\\VMware Workstation\\bin>tracert example.com

Tracing route to example.com [93.184.215.14]
over a maximum of 30 hops:

 1    7 ms      2 ms      2 ms  192.168.1.1
 2   42 ms     914 ms     46 ms  82.114.163.112
 3  1178 ms     514 ms    305 ms  82.114.160.6
 4   818 ms    220 ms     87 ms  82.114.164.18
 5  1056 ms    433 ms    287 ms  mei-b5-link.ip.twelve99.net [62.115.148.118]
 6   600 ms    206 ms      *     prs-bb1-link.ip.twelve99.net [62.115.124.54]
 7     *        *       686 ms  ash-bb2-link.ip.twelve99.net [62.115.112.242]
 8   396 ms    310 ms    243 ms
```

- traceroute 10.0.2.1

```
sir@kali: ~
File Actions Edit View Help
(sir@kali)-[~]
$ traceroute 10.0.2.1
traceroute to 10.0.2.1 (10.0.2.1), 30 hops max, 60 byte packets
1 10.0.2.15 (10.0.2.15) 3069.837 ms !H 3069.779 ms !H 3069.724 ms !H
File System Network ...
(sir@kali)-[~]
$ traceroute example.com
traceroute to example.com (93.184.215.14), 30 hops max, 60 byte packets
1 10.0.2.2 (10.0.2.2) 0.988 ms 0.934 ms 0.887 ms
2 10.0.2.2 (10.0.2.2) 17.897 ms 17.812 ms 17.888 ms
(sir@kali)-[~]
$
```

The terminal window shows two traceroute commands. The first command, `traceroute 10.0.2.1`, traces the path to a local host (10.0.2.1). The second command, `traceroute example.com`, traces the path to an external website (example.com). Both commands show the path through various routers and hosts, with their respective round-trip times.

50. Find out the default gateway.

```
sir@kali: ~
File Actions Edit View Help
(sir@kali)-[~]
$ ip route | grep default
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
(sir@kali)-[~]
$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2      0.0.0.0       UG    100    0        0 eth0
10.0.2.0        0.0.0.0       255.255.255.0 U     100    0        0 eth0
(sir@kali)-[~]
$
```

The terminal window displays the output of `ip route` and `route -n`. The `ip route` command shows a default route via interface `eth0` with a metric of 100. The `route -n` command shows the kernel's IP routing table, listing the default gateway (10.0.2.2) and another route for 10.0.2.0.

51. Check the MAC address of your network interface.

```
(sir@kali)-[~]
$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:72:27:cb brd ff:ff:ff:ff:ff:ff
(sir@kali)-[~]
```

The terminal window shows the output of `ip link show`. It lists two interfaces: `lo` (loopback) and `eth0` (ethernet). The `eth0` interface has a MAC address of `08:00:27:72:27:cb`.

52. Ensure that the VM can access external networks.

```
(sir@kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=113 time=118 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=113 time=117 ms
```

The terminal window shows the output of `ping 8.8.8.8`. It sends 12 ICMP echo requests to the Google DNS server at 8.8.8.8, receiving responses back from the target host.

Section 6: UFW Firewall:

53. Enable the firewall.

```
(sir㉿kali)-[~]
└─$ ufw --version
ufw 0.36.2
Copyright 2008-2023 Canonical Ltd.

(sir㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

(sir㉿kali)-[~]
└─$
```

54. Allow SSH connections through the firewall.

```
(sir㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)
```

55. Deny all incoming traffic by default.

```
sir@kali: ~
File Actions Edit View Help

(sir㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(sir㉿kali)-[~]
└─$
```

56. Allow HTTP and HTTPS traffic.

```
(sir㉿kali)-[~]
└─$ sudo ufw allow http
Rule added
Rule added (v6)

(sir㉿kali)-[~]
└─$ sudo ufw allow https
Rule added
Rule added (v6)

(sir㉿kali)-[~]
└─$
```

57. Allow port 20

```
└─(sir㉿kali)-[~]
└─$ sudo ufw allow 20
Rule added
Rule added (v6)
```

58. Reset the firewall settings.

```
└─(sir㉿kali)-[~]
└─$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with
operation (y|n)? █
```

59. Delete a rule from the firewall.

```
└─(sir㉿kali)-[~]
└─$ sudo ufw delete 1
█
```

60. Disable the firewall.

```
└─(sir㉿kali)-[~]
└─$ sudo ufw disable
```

61. View the status of the firewall.

```
└─(sir㉿kali)-[~]
└─$ sudo ufw status
```

62. Log firewall activity and view it.

```
└─(sir㉿kali)-[~]
└─$ sudo ufw logging on
```

Section 7: Searching and System Information:

63. Delete the command history.

```
[sir@kali:~/Desktop]$ history -c  
fc: event not found: -c
```

64. Search for a kali in the `/etc/passwd` file.

```
[sir@kali:~/Desktop]$ grep kali /etc/passwd  
[sir@kali:~/Desktop]$
```

65. Search for a kali in the `/etc/group` file.

```
[sir@kali:~/Desktop]$ grep kali /etc/group  
kali-trusted:x:135:
```

66. Locate the `passwd` file.

```
[sir@kali:~/Desktop]$ which passwd  
/usr/bin/passwd
```

67. Locate the shadow file and open it.

```
[sir@kali:~/Desktop]$ sudo cat /etc/shadow  
root:!$19882:0:99999:7:::  
daemon:*$19882:0:99999:7:::  
bin:*$19882:0:99999:7:::  
sys:*$19882:0:99999:7:::  
sync:*$19882:0:99999:7:::  
games:*$19882:0:99999:7:::  
man:*$19882:0:99999:7:::  
lp:*$19882:0:99999:7:::  
mail:*$19882:0:99999:7:::  
news:*$19882:0:99999:7:::  
uucp:*$19882:0:99999:7:::  
proxy:*$19882:0:99999:7:::  
www-data:*$19882:0:99999:7:::  
backup:*$19882:0:99999:7:::  
list:*$19882:0:99999:7:::  
irc:*$19882:0:99999:7:::  
_apt:*$19882:0:99999:7:::  
nobody:*$19882:0:99999:7:::  
systemd-network:!$19882:::::  
_galera:!$19882:::::  
mysql:!$19882:::::  
tss:!$19882:::::  
strongswan:!$19882:::::  
systemd-timesync:!$19882:::::  
rwhod:!$19882:::::  
_gophish:!$19882:::::  
iodine:!$19882:::::  
messagebus:!$19882:::::  
tcpdump:!$19882:::::  
miredo:!$19882:::::  
_rpc:!$19882:::::  
Debian-snmp:!$19882:::::  
redis:!$19882:::::
```

68. Search for all configuration files in the `/etc` directory.

```
[sir@sir-kali:~/Desktop]$ find /etc -type f -name "*.conf"
/etc/mke2fs.conf
/etcSMARTD.conf
/etc/miredo.conf
/etcUPower/UPower.conf
/etcselinux/semanage.conf
/etclibao.conf
/etcmosquitto/mosquitto.conf
/etcpam.conf
find: '/etcvpnc': Permission denied
/etcpostgresql-common/createcluster.conf
/etchdparm.conf
/etcgtk-2.0/im-multipress.conf
find: '/etcredis': Permission denied
/etccracklib/cracklib.conf
/etcavahi/avahi-daemon.conf
/etcjohn/john-mail.conf
/etcjohn/john.conf
/etcSAMBA/smb.conf
/etclightdm/keys.conf
/etclightdm/lightdm.conf
/etclightdm/lightdm-gtk-greeter.conf
/etclightdm/users.conf
/etcstrongswan.conf
/etcstrongswan3.conf
/etcresponder/Responder.conf
/etcusb_modeswitch.conf
/etcnginx/fastcgi.conf
/etcnginx/nginx.conf
/etcnginx/snippets/snakeoil.conf
/etcnginx/snippets/fastcgi-php.conf
/etcstrongswan.conf
/etcstrongswan.d/starter.conf
/etcstrongswan.d/charon.conf
```

69. Search recursively for a specific word in the `/var/log` directory.

```
[sir@sir-kali:~/Desktop]$ grep -r "var" /var/log
/varlog/Xorg.0.log.old:[ 7.181] (==) Log file: "/varlog/Xorg.0.log", Time: Sat Aug 31 23:42:38 2024
grep: /varlog/boot.log.4: Permission denied
grep: /varlog/lightdm: Permission denied
grep: /varlog/boot.log.1: Permission denied
grep: /varlog/boot.log.2: Permission denied
grep: /varlog/speech-dispatcher: Permission denied
grep: /varlog/boot.log: Permission denied
grep: /varlog/inetsim: Permission denied
grep: /varlog/vboxadd-install.log: Permission denied
/varlog/Xorg.1.log.old:[ 2383.961] (==) Log file: "/varlog/Xorg.1.log", Time: Wed Aug 7 18:28:01 2024
grep: /varlog/installer/partman: Permission denied
/varlog/installer/hardware-summary:lsmod: efivarfs
24576 0
grep: /varlog/installer/Xorg.0.log: Permission denied
grep: /varlog/installer/syslog: Permission denied
/varlog/installer/status:Description: debconf preseedin
g via environment variables
/varlog/installer/status: The library provides an inter
face for raw netlink messaging and various
/varlog/installer/status: The library provides an inter
face for raw netlink messaging and various
grep: /varlog/installer/cdebconf/questions.dat: Permiss
ion denied
grep: /varlog/installer/cdebconf/templates.dat: Permiss
ion denied
grep: /varlog/private: Permission denied
/varlog/Xorg.0.log:[ 5.478] (==) Log file: "/varlog/Xorg.0.log", Time: Sun Sep 1 10:42:54 2024
grep: /varlog/btmp.1: Permission denied
grep: /varlog/boot.log.5: Permission denied
/varlog/fontconfig.log:/var/cache/fontconfig: cleaning
```

70. View the system's kernel version.

```
(sir㉿kali)-[~/Desktop]
$ uname -r
6.6.15-amd64
```

71. Display the system's memory usage.

```
(sir㉿kali)-[~/Desktop]
$ free -h
              total        used        free      shared  buff/cache   available
Mem:       5.8Gi       1.0Gi      3.9Gi     9.4Mi      1.2Gi      4.8Gi
Swap:    975Mi          0B      975Mi
```

72. Show the system's disk usage.

```
(sir㉿kali)-[~/Desktop]
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            2.9G   0    2.9G  0% /dev
tmpfs           595M  1.1M  594M  1% /run
/dev/sda1        49G   15G   32G  32% /
tmpfs           3.0G   0    3.0G  0% /dev/shm
tmpfs           5.0M   0    5.0M  0% /run/lock
Transfer         43G   23G   20G  54% /media/sf_Transfer
tmpfs           595M  124K  594M  1% /run/user/1000
```

73. Check the system's uptime and load average.

```
(sir㉿kali)-[~/Desktop]
$ uptime
14:54:32 up  4:11,  1 user,  load average: 0.00, 0.03, 0.01
```

74. Display the current logged-in users.

```
(sir㉿kali)-[~/Desktop]
$ who
sir      tty7          2024-09-01 10:43 (:0)
sir      pts/1          2024-09-01 11:28
sir      pts/3          2024-09-01 14:18
sir      pts/4          2024-09-01 14:20
sir      pts/5          2024-09-01 14:22
sir      pts/6          2024-09-01 14:29
sir      pts/7          2024-09-01 14:30
sir      pts/8          2024-09-01 14:31
sir      pts/9          2024-09-01 14:33
sir      pts/10         2024-09-01 14:34
```

75. Check the identity of the current user.

```
└─(sir㉿kali)-[~/Desktop]
└$ whoami
sir
```

76. View the `/var/log/auth.log` file.

```
└─(sir㉿kali)-[~/Desktop]
└$ sudo less /var/log/auth.log
/var/log/auth.log: No such file or directory
```

77. Shred the `auth.log` file securely.

```
└─(sir㉿kali)-[~/Desktop]
└$ sudo shred -u /var/log/auth.log
shred: /var/log/auth.log: failed to open for writing: No such file or directory
```

78. How do you lock a user account to prevent them from logging in.

```
└─(sir㉿kali)-[~/Desktop]
└$ sudo usermod -L sir
```

79. What command would you use to change a user's default shell.

```
└─(sir㉿kali)-[~/Desktop]
└$ sudo chsh -s /bin/bash sir
```

80. Display the system's boot messages.

```
sir@kali: ~/Desktop
```

```
File Actions Edit View Help
[ 0.00000] Linux version 6.6.15-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-24) 13.2.0, GNU ld (GNU Binutils for Debian) 2.42) #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17)
[ 0.00000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-amd64 root=UUID=87d2f760-2ba2-47f1-965c-12ab19f8ce3c ro quiet splash
[ 0.00000] [Firmware Bug]: TSC doesn't count with P0 frequency!
[ 0.00000] BIOS-provided physical RAM map:
[ 0.00000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[ 0.00000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[ 0.00000] BIOS-e820: [mem 0x000000000000f000-0x00000000000ffff] reserved
[ 0.00000] BIOS-e820: [mem 0x00000000000100000-0x000000000dffefff] usable
[ 0.00000] BIOS-e820: [mem 0x000000000dff0000-0x000000000dffffff] ACPI data
[ 0.00000] BIOS-e820: [mem 0x000000000fec0000-0x000000000fec00ff] reserved
[ 0.00000] BIOS-e820: [mem 0x000000000fee0000-0x000000000fee00ff] reserved
[ 0.00000] BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffff] reserved
[ 0.00000] BIOS-e820: [mem 0x00000000100000000-0x000000001a07ffff] usable
[ 0.00000] NX (Execute Disable) protection: active
[ 0.00000] APIC: Static calls initialized
[ 0.00000] SMBIOS 2.5 present.
[ 0.00000] DMI: innotech GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[ 0.00000] newfile.btrw: mounted
[ 0.00000] Hypervisor detected: KVM
[ 0.00000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[ 0.00002] kvm-clock: using sched offset of 9922726103 cycles
[ 0.00005] clocksource: kvm-clock: mask: 0xfffffffffffffff max_cycles: 0x1cd42e4dfffb, max_idle_ns: 881590591483 ns
[ 0.00007] tsc: Detected 2295.686 MHz processor
[ 0.001263] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[ 0.001266] e820: remove [mem 0x000a0000-0x000fffff] usable
[ 0.001271] last_pfn = 0x1a0800 max_arch_pfn = 0x400000000
[ 0.001281] MTRRs disabled by BIOS
[ 0.001283] x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
[ 0.001304] last_pfn = 0xdfff0 max_arch_pfn = 0x400000000
[ 0.001327] found SMP MP-table at [mem 0x0009ff0-0x0009ffff]
[ 0.001620] RAMDISK: [mem 0x2e8a3000-0x33448fff]

log file: S
```