



Syber Security H.W

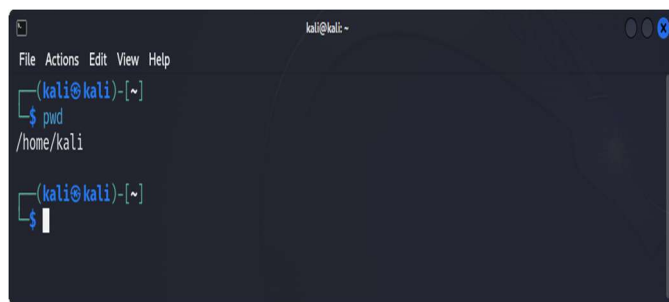
Name: Mohammed Ali Al-Montaser

Groub: First Groub

Subject: Cyber Security

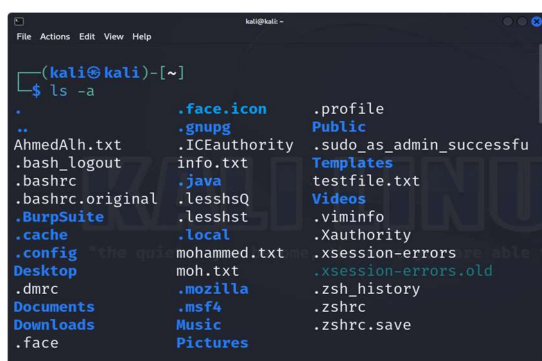
ENG: Abdul Razzaq

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:



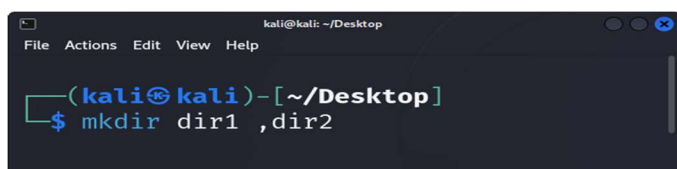
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ls -a  
.  
..  
AhmedAlh.txt  
.bash_logout  
.bashrc  
.bashrc.original  
.BurpSuite  
.cache  
.config  
Desktop  
.dmrc  
Documents  
Downloads  
.face  
.face.icon  
.gnupg  
.ICEauthority  
.info.txt  
.java  
.lesshtqs  
.lesshtst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

3- Change your directory to the Desktop:



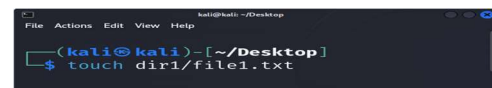
```
kali@kali: ~/Desktop  
File Actions Edit View Help  
(kali@kali)-[~]  
$ cd Desktop
```

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



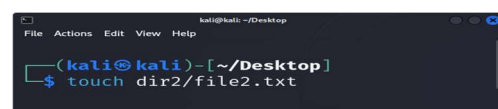
```
kali@kali: ~/Desktop  
File Actions Edit View Help  
(kali@kali)-[~/Desktop]  
$ mkdir dir1 ,dir2
```

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



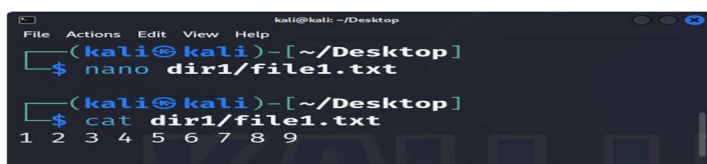
```
kali@kali: ~/Desktop  
File Actions Edit View Help  
(kali@kali)-[~/Desktop]  
$ touch dir1/file1.txt
```

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



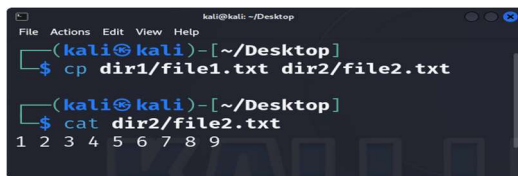
```
kali@kali: ~/Desktop  
File Actions Edit View Help  
(kali@kali)-[~/Desktop]  
$ touch dir2/file2.txt
```

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



```
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
```

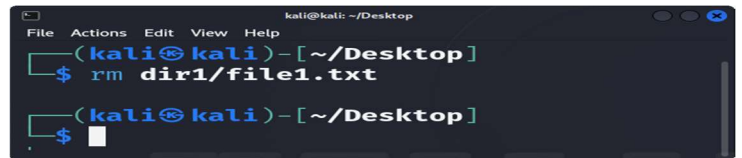
8. Copy the contents of `file1.txt` into `file2.txt`:



```
kali@kali: ~/Desktop
(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
```

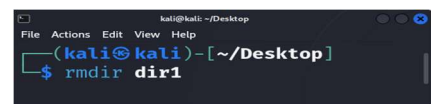
9- Delete `file1.txt` inside `dir1`:



```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
$ rm dir1/file1.txt

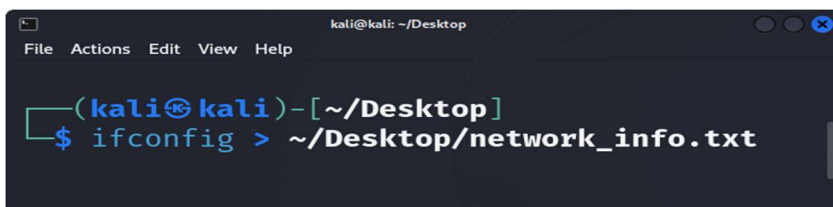
(kali@kali)-[~/Desktop]
$
```

10- Remove the directory `dir1` from the Desktop:



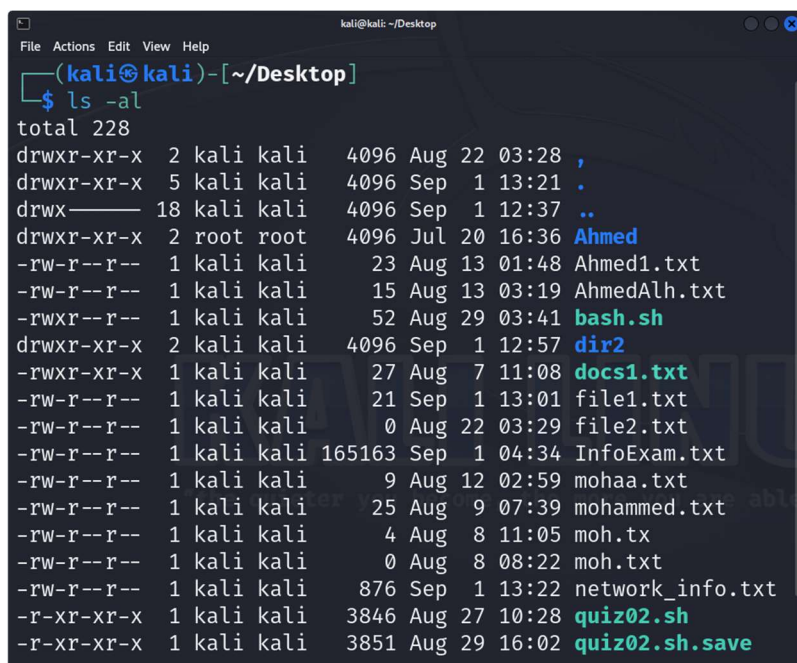
```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
$ rmdir dir1
```

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



```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
$ ifconfig > ~/Desktop/network_info.txt
```

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



```
kali@kali: ~/Desktop
(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
-rwxr-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
-rw-r--r--  1 kali kali    876 Sep  1 13:22 network_info.txt
-r-xr-xr-x  1 kali kali   3846 Aug 27 10:28 quiz02.sh
-r-xr-xr-x  1 kali kali   3851 Aug 29 16:02 quiz02.sh.save
```

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

```
kali@kali: ~/Desktop
(kali@kali)~[~/Desktop]
$ 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. Not 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 groups `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
(kali@kali)~[~/Desktop]
$ cat /etc/passwd | grep mohammed
mohammed:x:1007:1007:n,n,n,n,n:/home/mohammed:/bin/bash
(kali@kali)~[~/Desktop]
$
```

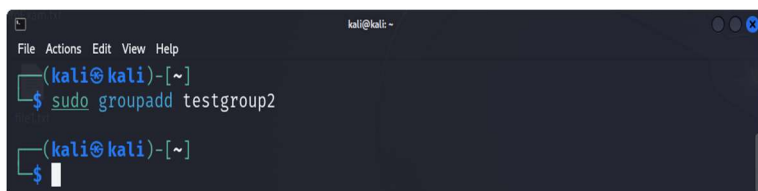
16. Add your user to the file that gives administrative privileges:

```
kali@kali: ~/Desktop
(kali@kali)~[~/Desktop]
$ sudo usermod -aG sudo mohammed
(kali@kali)~[~/Desktop]
$
```

17- Switch to your user and confirm the user identity:

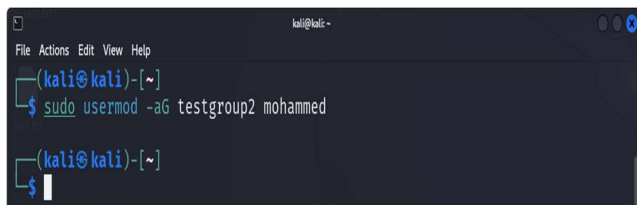
```
mohammed@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~[~]
$ su - mohammed
Password:
(mohammed@kali)~[~]
$
```

18. Create a new group named `testgroup`:



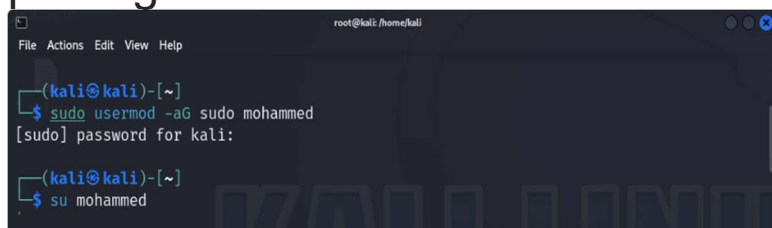
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo groupadd testgroup2  
(kali@kali)-[~]  
$
```

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:



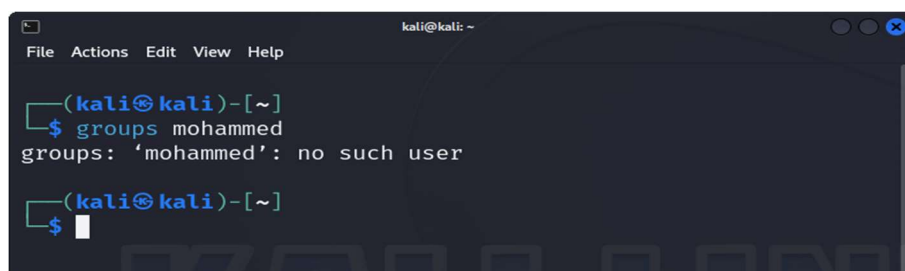
```
root@kali: /home/kali  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo usermod -aG sudo mohammed  
[sudo] password for kali:  
(kali@kali)-[~]  
$ su mohammed
```

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 has 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 user  
s netdev bluetooth scanner wireshark kaboxer  
(kali@kali)-[~]  
$
```

24-Set the permissions of `file2.txt`:

2



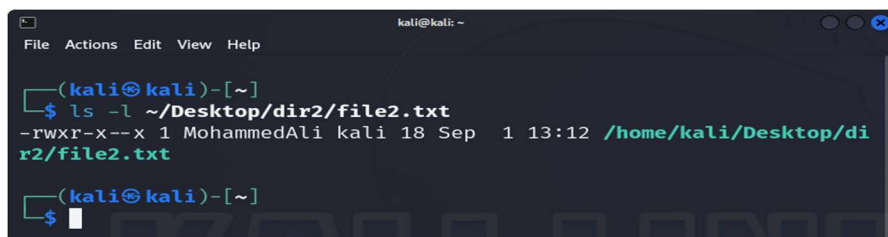
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ chmod 751 ~/Desktop/dir2/file2.txt  
(kali@kali)-[~]  
$
```

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



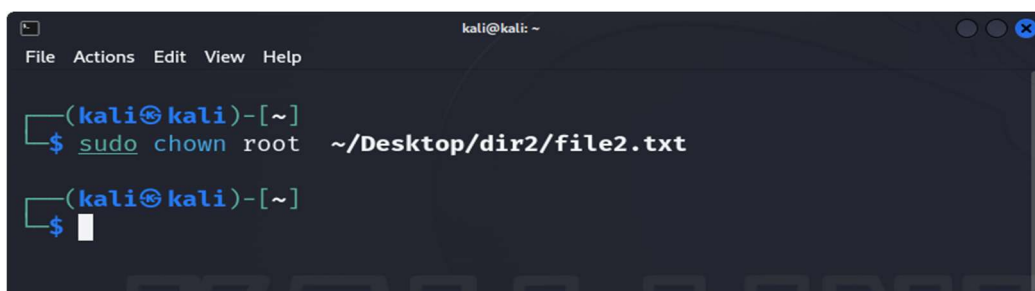
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo useradd MohammedAli  
(kali@kali)-[~]  
$ sudo chown MohammedAli ~/Desktop/dir2/file2.txt  
(kali@kali)-[~]  
$
```

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/dir2/file2.txt  
(kali@kali)-[~]  
$
```

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



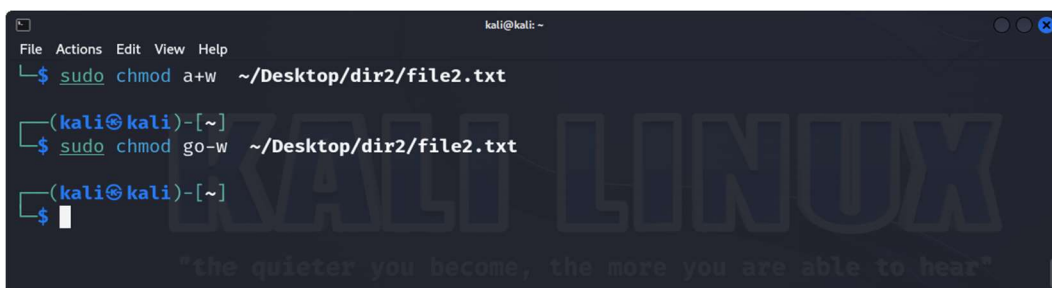
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo chown root ~/Desktop/dir2/file2.txt  
(kali@kali)-[~]  
$
```

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



```
kali@kali: ~  
File Actions Edit View Help  
$ sudo chmod a+w ~/Desktop/dir2/file2.txt  
$
```

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:



```
kali@kali: ~  
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- Command to recursively change the permissions of all files and directories inside a folder named `project` to `755`:



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


33. Install `htop`:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo apt install htop  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
htop is already the newest version (3.3.0-4).  
The following packages were automatically installed and are no longer required:  
  fonts-noto-color-emoji libnsl-dev libtirpc-dev  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 1978 not upgraded.
```

34.-Display all running processes:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ps aux  
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root           1  0.0  0.1 21108 12368 ?        Ss   15:06   0:05 /sbin/init splash  
root           2  0.0  0.0      0     0 ?        S    15:06   0:00 [kthreadd]  
root           3  0.0  0.0      0     0 ?        I<   15:06   0:00 [rcu_gp]  
root           4  0.0  0.0      0     0 ?        I<   15:06   0:00 [rcu_par_gp]  
root           5  0.0  0.0      0     0 ?        I<   15:06   0:00 [slub_flushwq]  
root           6  0.0  0.0      0     0 ?        I<   15:06   0:00 [netns]  
root          11  0.0  0.0      0     0 ?        I<   15:06   0:00 [mm_percpu_wq]  
root          12  0.0  0.0      0     0 ?        I    15:06   0:00 [rcu_tasks_kthread]  
root          13  0.0  0.0      0     0 ?        I    15:06   0:00 [rcu_tasks_rude_kthread]  
root          14  0.0  0.0      0     0 ?        I    15:06   0:00 [rcu_tasks_trace_kthread]  
root          15  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/0]  
root          16  0.0  0.0      0     0 ?        I    15:06   0:03 [rcu_preempt]  
root          17  0.0  0.0      0     0 ?        S    15:06   0:00 [migration/0]  
root          18  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/0]  
root          19  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/0]  
root          20  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/1]  
root          21  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/1]  
root          22  0.0  0.0      0     0 ?        S    15:06   0:01 [migration/1]  
root          23  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/1]  
root          25  0.0  0.0      0     0 ?        I<   15:06   0:00 [kworker/1:0H-events_high]  
root          26  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/2]  
root          27  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/2]  
root          28  0.0  0.0      0     0 ?        S    15:06   0:01 [migration/2]  
root          29  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/2]  
root          31  0.0  0.0      0     0 ?        I<   15:06   0:00 [kworker/2:0H-events_high]  
root          32  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/3]  
root          33  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/3]  
root          34  0.0  0.0      0     0 ?        S    15:06   0:01 [migration/3]  
root          35  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/3]  
root          44  0.0  0.0      0     0 ?        S    15:06   0:00 [kdevtmpfs]  
root          45  0.0  0.0      0     0 ?        I<   15:06   0:00 [inet_frag_wq]  
root          46  0.0  0.0      0     0 ?        S    15:06   0:00 [kauditd]  
root          48  0.0  0.0      0     0 ?        S    15:06   0:00 [khungtaskd]
```


35-Display a tree of all running processes:

```
kali@kali: ~  
$ ps aux  
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root           1  0.0  0.1 21108 12368 ?        Ss   15:06   0:05 /sbin/init splash  
root           2  0.0  0.0      0     0 ?        S    15:06   0:00 [kthreadd]  
root           3  0.0  0.0      0     0 ?        I<   15:06   0:00 [rcu_gp]  
root           4  0.0  0.0      0     0 ?        I<   15:06   0:00 [rcu_par_gp]  
root           5  0.0  0.0      0     0 ?        I<   15:06   0:00 [slub_flushwq]  
root           6  0.0  0.0      0     0 ?        I<   15:06   0:00 [netns]  
root          11  0.0  0.0      0     0 ?        I<   15:06   0:00 [mm_percpu_wq]  
root          12  0.0  0.0      0     0 ?        I    15:06   0:00 [rcu_tasks_kthread]  
root          13  0.0  0.0      0     0 ?        I    15:06   0:00 [rcu_tasks_rude_kthread]  
root          14  0.0  0.0      0     0 ?        I    15:06   0:00 [rcu_tasks_trace_kthread]  
root          15  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/0]  
root          16  0.0  0.0      0     0 ?        I    15:06   0:03 [rcu_preempt]  
root          17  0.0  0.0      0     0 ?        S    15:06   0:00 [migration/0]  
root          18  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/0]  
root          19  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/0]  
root          20  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/1]  
root          21  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/1]  
root          22  0.0  0.0      0     0 ?        S    15:06   0:01 [migration/1]  
root          23  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/1]  
root          25  0.0  0.0      0     0 ?        I<   15:06   0:00 [kworker/1:0H-events_high]  
root          26  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/2]  
root          27  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/2]  
root          28  0.0  0.0      0     0 ?        S    15:06   0:01 [migration/2]  
root          29  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/2]  
root          31  0.0  0.0      0     0 ?        I<   15:06   0:00 [kworker/2:0H-events_high]  
root          32  0.0  0.0      0     0 ?        S    15:06   0:00 [cpuhp/3]  
root          33  0.0  0.0      0     0 ?        S    15:06   0:00 [idle_inject/3]  
root          34  0.0  0.0      0     0 ?        S    15:06   0:01 [migration/3]  
root          35  0.0  0.0      0     0 ?        S    15:06   0:00 [ksoftirqd/3]  
root          44  0.0  0.0      0     0 ?        S    15:06   0:00 [kdevtmpfs]  
root          45  0.0  0.0      0     0 ?        I<   15:06   0:00 [inet_frag_wq]  
root          46  0.0  0.0      0     0 ?        S    15:06   0:00 [kauditd]  
root          48  0.0  0.0      0     0 ?        S    15:06   0:00 [khungtaskd]
```

36. Open the interactive process viewer:

```
Tasks: 78, 190 thr: 124 kthr: 1 running  
Load average: 0.10 0.17 0.13  
Uptime: 01:59:24  
Mem: 803M/7.74G 3.7%  
Swp: 0K/1024M  
Main 1/0  
PID USER PRI NI VIRT RES SHR S CPU%MEM% TIME+ Command  
60804 kali 20 0 8188 4352 3328 R 6.8 0.1 0:01.99 htop  
941 root 20 0 880M 169M 8192 S 4.3 2.1 2:39.11 /usr/lib/xorg/Xorg :0 --seat seat  
600 messagebus 20 0 10612 1504 4224 S 1.2 0.1 0:05.14 /usr/bin/dbus-daemon --system --  
1323 kali 20 0 390M 4732 3328 S 1.2 0.6 0:04.49 /usr/lib/x86_64-linux-gnu/xfce4/  
1344 kali 20 0 390M 4732 3328 S 1.2 0.6 0:05.97 /usr/lib/x86_64-linux-gnu/xfce4/  
59586 kali 20 0 449M 107M 90328 S 1.2 1.4 0:01.58 /usr/bin/qterminal  
583 root 20 0 235M 1672 7848 S 0.6 0.2 0:14.95 /usr/bin/vmtoolsd  
1255 kali 20 0 1292M 109M 78272 S 0.6 1.4 1:02.42 xfwm4 --display :0.0 --sm-client  
1293 root 20 0 306M 13420 7424 S 0.6 0.2 0:02.28 /usr/libexec/upowerd  
1297 root 20 0 306M 13420 7424 S 0.6 0.2 0:01.42 /usr/libexec/upowerd  
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice F9Kill F10Quit
```

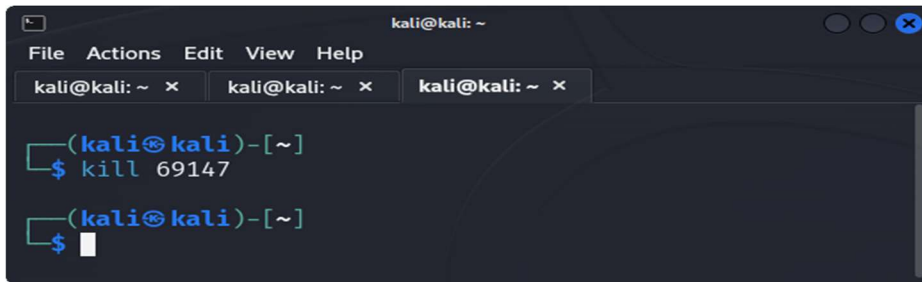
37-Kill a process with a specific PID:

```
kali@kali: ~  
$ kill 63960
```

38- Start an application and stop it using a command that kills processes by name:

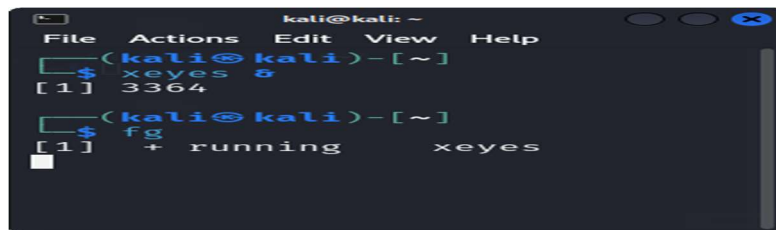
```
kali@kali: ~  
$ pkill xeyes
```

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



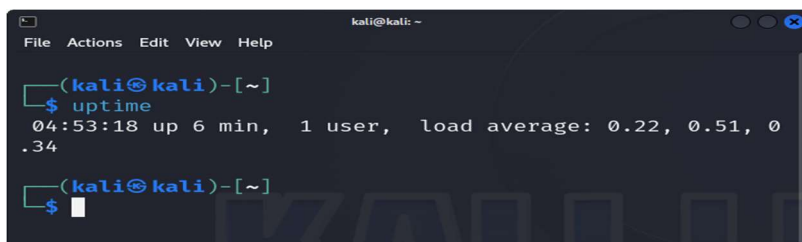
```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x  
(kali@kali)-[~]  
$ kill 69147  
(kali@kali)-[~]  
$
```

40. Run a command in the background, then bring it to the foreground:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ xeyes &  
[1] 3364  
(kali@kali)-[~]  
$ fg  
[1] + running xeyes
```

41. Check how long the system has been running:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ uptime  
04:53:18 up 6 min, 1 user, load average: 0.22, 0.51, 0.34  
(kali@kali)-[~]  
$
```

42-List all jobs running in the background:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ xeyes &  
[1] 16329  
(kali@kali)-[~]  
$ xclock &  
[2] 16407  
(kali@kali)-[~]  
$ jobs  
[1] - running xeyes  
[2] + running xclock
```

43. Display the network configuration:

```
kali@kali: ~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.159.132 netmask 255.255.255.0 broad-  
    dcast 192.168.159.255  
    inet6 fe80::e4db:5726:c3d4:bced prefixlen 64 sc-  
    opeid 0<link>  
    ether 00:0c:29:cc:d2:6b txqueuelen 1000 (Ethern-  
    et)  
    RX packets 373 bytes 24200 (23.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 43 bytes 5996 (4.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 col-  
    lisions 0  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 col-  
    lisions 0
```

44-Check the IP address of your machine:

```
kali@kali: ~  
$ hostname -I  
192.168.159.132
```

45. Test connectivity to an external server:

```
kali@kali: ~  
$ ping google.com  
PING google.com (216.58.204.142) 56(84) bytes of data:  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=1 ttl=128 time=246 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=2 ttl=128 time=166 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=3 ttl=128 time=188 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=4 ttl=128 time=211 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=5 ttl=128 time=233 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=6 ttl=128 time=154 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=8 ttl=128 time=191 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=9 ttl=128 time=212 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=10 ttl=128 time=146 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=11 ttl=128 time=257 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=12 ttl=128 time=278 ms  
64 bytes from par21s05-in-f142.1e100.net (216.58.204.142): icmp_seq=13 ttl=128 time=300 ms
```

46. Display the routing table:

```
kali@kali: ~  
$ ip route show  
default via 192.168.159.2 dev eth0 proto dhcp src 192.168.159.132 metric 100  
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.132 metric 100
```

47. Check the open ports and active connections:

```
kali@kali:~$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

48. Show the IP address of the host machine and the VM, and verify if they are on the same network:

```
C:\Users\pc>ipconfig
Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . : 
   Link-local IPv6 Address . . . . . : fe80::4afe:15af:f58e:89fe%10
   IPv4 Address. . . . . : 192.168.159.1
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : 
   . . . . .

Wireless LAN adapter Ethernet:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : 
   . . . . .

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . : 
   Link-local IPv6 Address . . . . . : fe80::112a:4be6:a56e:b8aa%9
   IPv4 Address. . . . . : 192.168.247.1
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . : 
   Link-local IPv6 Address . . . . . : fe80::1576:bdd2:f315:3647%28
   IPv4 Address. . . . . : 192.168.159.1
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 

Ethernet adapter Bluetooth:

   Media State . . . . . : Media disconnected
   . . . . .
```

```
kali@kali:~$ hostname -i
192.168.159.132
```

```
C:\Users\pc>ping 192.168.159.132
Pinging 192.168.159.132 with 32 bytes of data:
Reply from 192.168.159.132: bytes=32 time<1ms TTL=64
Reply from 192.168.159.132: bytes=32 time<1ms TTL=64
Reply from 192.168.159.132: bytes=32 time<1ms TTL=64
Reply from 192.168.159.132: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.159.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

49-Trace the route to an external server:

```
kali@kali:~$ traceroute google.com
traceroute to google.com (216.58.204.142), 30 hops max, 60 byte packets
 1 192.168.159.2 (192.168.159.2) 0.476 ms 0.287 ms 0.668 ms
 2 * * *
```

50- Find out the default gateway:

```
kali@kali:~$ ip route | grep default
default via 192.168.159.2 dev eth0 proto dhcp src 192.168.159.132 metric 100
```

51- Check the MAC address of your network interface:

```
kali@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 00:0c:29:cc:d2:6b brd ff:ff:ff:ff:ff:ff  
kali@kali: ~
```

52- Ensure that the VM can access external networks:

```
kali@kali: ~  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
From 192.168.43.31 icmp_seq=3 Destination Host Unreachable  
From 192.168.43.31 icmp_seq=6 Destination Host Unreachable  
From 192.168.43.31 icmp_seq=9 Destination Host Unreachable  
From 192.168.43.31 icmp_seq=12 Destination Host Unreachable  
From 192.168.43.31 icmp_seq=15 Destination Host Unreachable  
From 192.168.43.31 icmp_seq=18 Destination Host Unreachable  
From 192.168.43.31 icmp_seq=21 Destination Host Unreachable  
From 192.168.43.31 icmp_seq=24 Destination Host Unreachable
```

53. Enable the firewall:

```
kali@kali: ~  
$ ufw --version  
ufw 0.36.2  
Copyright 2008-2023 Canonical Ltd.  
kali@kali: ~  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
kali@kali: ~  
$
```

54. Allow SSH connections through the firewall:

```
kali@kali: ~  
$ sudo ufw allow ssh  
Rule added  
Rule added (v6)
```

55-Deny all incoming traffic by default:

```
kali@kali: ~  
$ sudo ufw default deny incoming  
Default incoming policy changed to 'deny'  
(be sure to update your rules accordingly)  
kali@kali: ~  
$
```

56-Allow HTTP and HTTPS traffic:

```
kali@kali: ~  
$ sudo ufw allow http  
Rule added  
Rule added (v6)  
kali@kali: ~  
$ sudo ufw allow https  
Rule added  
Rule added (v6)
```


57- Allow port 20:

```
kali@kali: ~  
$ sudo ufw allow 20  
Rule added  
Rule added (v6)  
$
```

58- Reset the firewall settings:

```
kali@kali: ~  
$ sudo ufw reset  
Resetting all rules to installed defaults. Proceed with operation (y/n)?
```

59- Delete a rule from the firewall:

```
kali@kali: ~  
$ sudo ufw delete allow ssh  
Rule deleted  
Rule deleted (v6)  
$
```

60- Disable the firewall:

```
kali@kali: ~  
$ sudo ufw disable  
Firewall stopped and disabled on system startup  
$
```

61- View the status of the firewall:

```
kali@kali: ~  
$ sudo ufw status  
Status: inactive  
$
```

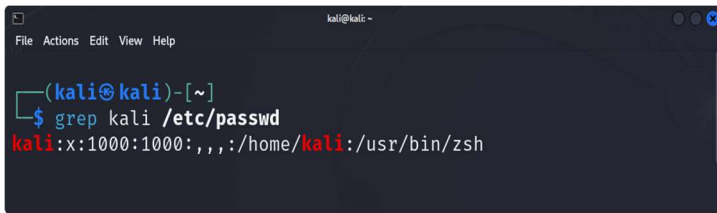
62- Log firewall activity and view it:

```
kali@kali: ~  
$ sudo ufw logging on  
ERROR: Invalid syntax  
Usage: ufw COMMAND  
  
Commands:  
enable          enables the firewall  
disable         disables the firewall  
default ARG     set default policy  
logging LEVEL   set logging to LEVEL  
allow ARGS      add allow rule  
deny ARGS       add deny rule  
reject ARGS     add reject rule  
limit ARGS      add limit rule  
delete RULE|NUM delete RULE  
insert NUM RULE insert RULE at NUM  
prepend RULE    prepend RULE  
route RULE      add route RULE  
route delete RULE|NUM delete route RULE  
route insert NUM RULE insert route RULE at NUM  
reload          reload firewall  
reset           reset firewall  
status          show firewall status  
status numbered show firewall status as n  
status verbose  show verbose firewall status  
show ARG        show firewall report  
version         display version information
```

63- Delete the command history:

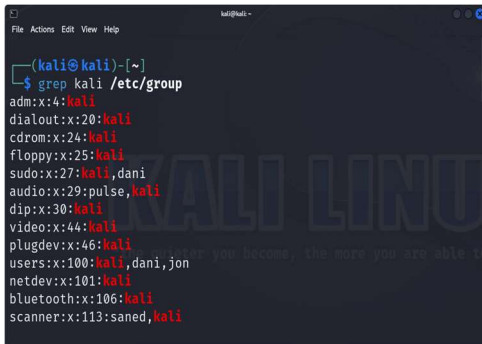
```
kali@kali: ~  
$ history -c  
fc: event not found: -c
```

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



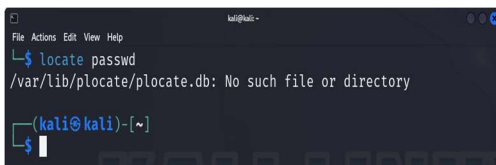
```
kali@kali:~$ grep kali /etc/passwd
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
```

65-Search for `kali` in the `/etc/group` file:



```
kali@kali:~$ grep kali /etc/group
adm:x:4:kali
dialout:x:20:kali
cdrom:x:24:kali
floppy:x:25:kali
sudo:x:27:kali,dani
audio:x:29:pulse,kali
dip:x:30:kali
video:x:44:kali
plugdev:x:46:kali
users:x:100:kali,dani,jon
netdev:x:101:kali
bluetooth:x:106:kali
scanner:x:113:saned,kali
```

66. Locate the `passwd` file:



```
kali@kali:~$ locate passwd
/var/lib/plocate/plocate.db: No such file or directory
```

67. Locate the shadow file and open it:



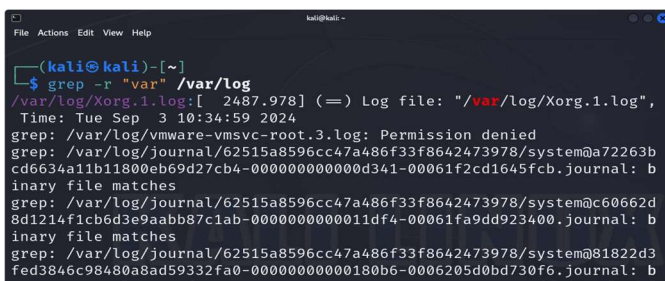
```
kali@kali:~$ sudo cat /etc/shadow
root:$y$j9T$1/h1.hgr6VAkcsdS3vwqA1$qVDNFTTy1z1lhRgZBZXEgJa091tPb
54g.PwUHiasI9:19931:0:99999:7:::
daemon:*:19691:0:99999:7:::
bin:*:19691:0:99999:7:::
sys:*:19691:0:99999:7:::
sync:*:19691:0:99999:7:::
games:*:19691:0:99999:7:::
man:*:19691:0:99999:7:::
lp:*:19691:0:99999:7:::
mail:*:19691:0:99999:7:::
news:*:19691:0:99999:7:::
```

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



```
kali@kali:~$ find /etc -type f -name "*.conf"
/etc/xdg/compton.conf
/etc/xdg/qt6ct/qt6ct.conf
/etc/xdg/picom.conf
/etc/xdg/user-dirs.conf
/etc/xdg/qt5ct/qt5ct.conf
/etc/plymouth/plymouthd.conf
/etc/bluetooth/input.conf
/etc/bluetooth/main.conf
/etc/bluetooth/network.conf
/etc/dhcp/dhclient.conf
/etc/request-key.conf
```

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



```
kali@kali:~$ grep -r "var" /var/log
/var/log/Xorg.1.log:[ 2487.978] (==) Log file: "/var/log/Xorg.1.log",
Time: Tue Sep 3 10:34:59 2024
grep: /var/log/vmware-vmxvc-root.3.log: Permission denied
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/system@a72263b
cd6634a11b1800eb69d27cb4-000000000000d341-00061f2cd1645fcb.journal: b
inary file matches
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/system@c06662d
8d1214f1cb6d3e9aabb87c1ab-0000000000011df4-00061fa9dd923400.journal: b
inary file matches
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/system@81822d3
fed3846c98480ad59332fa0-00000000000180b6-0006205d0bd730f6.journal: b
```


70- View the system's kernel version:

```
kali@kali: ~  
$ uname -r  
6.5.0-kali3-amd64  
kali@kali: ~  
$
```

71- Display the system's memory usage:

```
kali@kali: ~  
$ free -h  
              total        used        free      shared  bu  
ff/cache available  
Mem:          7.7Gi          912Mi        6.6Gi         5.4Mi  
474Mi  
Swap:         1.0Gi           0B         1.0Gi  
kali@kali: ~  
$
```

72. Show the system's disk usage:

```
kali@kali: ~  
$ df -h  
Filesystem      Size  Used Avail Use% Mounted on  
udev            3.9G   0    3.9G   0% /dev  
tmpfs           794M  1.3M  792M   1% /run  
/dev/sda1       79G   16G   59G  22% /  
tmpfs           3.9G   0    3.9G   0% /dev/shm  
tmpfs           5.0M   0    5.0M   0% /run/lock  
tmpfs           794M  120K  793M   1% /run/user/1000  
kali@kali: ~  
$
```

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

```
kali@kali: ~  
$ uptime  
12:59:43 up 6 min,  1 user,  load average: 0.05, 0.27, 0.17  
kali@kali: ~  
$
```

74. Display the current logged-in users:

```
kali@kali: ~  
$ who  
kali    tty7      2024-09-03 12:54 (:0)  
kali@kali: ~  
$
```

75. Check the identity of the current user:

```
kali@kali: ~  
$ whoami  
kali  
kali@kali: ~  
$
```

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

```
kali@kali: ~  
$ sudo less /var/log/auth.log  
[sudo] password for kali:  
/var/log/auth.log: No such file or directory  
kali@kali: ~  
$
```



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo shred -u /var/log/auth.log
shred: /var/log/auth.log: failed to open for writing: No such
file or directory
(kali@kali)-[~]
$

```

[illegible]

```
kali@kali ~  
File Actions Edit View Help  
(kali㉿kali)-[~]  
$ sudo chsh -s /bin/bash sir
```

```
kali@kali ~  
File Actions Edit View Help  
[kali@kali]~  
$ dmesg  
[ 0.000000] Linux version 6.5.0-kali3-amd64 (devel@kali.org) (gc  
c-13 (Debian 13.2.0-4) 13.2.0, GNU ld (GNU Binutils for Debian) 2.4  
1) #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09)  
[ 0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.5.0-kali3-a  
md64 root=UUID=c300d76e-fff31-4ba0-9526-ba4b2e4282af ro quiet splash  
[ 0.000000] Disabled fast string operations  
[ 0.000000] BIOS-provided physical RAM map:  
[ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009f3f  
f] usable  
[ 0.000000] BIOS-e820: [mem 0x000000000009f400-0x000000000009fff  
f] reserved  
[ 0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000ffff  
f] reserved  
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000bfbfdfff  
f] usable  
[ 0.000000] BIOS-e820: [mem 0x00000000bfbfee000-0x00000000bfbfefff  
f] ACPI data  
[ 0.000000] BIOS-e820: [mem 0x00000000bfbfeff00-0x00000000bfbfefff  
f] ACPI NVS  
[ 0.000000] BIOS-e820: [mem 0x00000000bffb00000-0x00000000bfbfffff
```