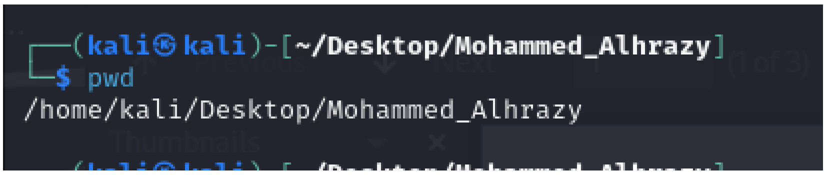
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

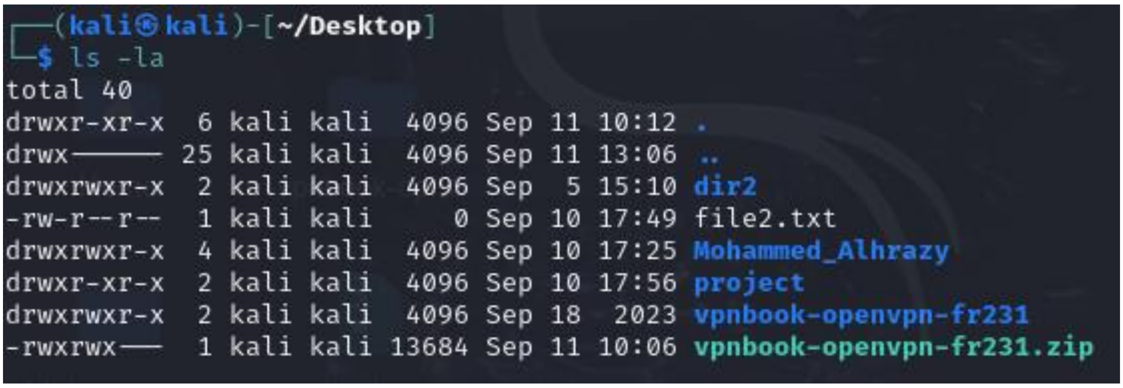
File and Directory Management

1. Display the current working directory.



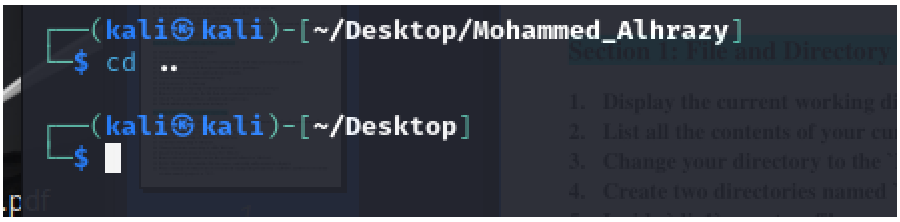
```
┌──(kali㉿kali)-[~/Desktop/Mohammed_Alhrazy]
└─$ pwd
/home/kali/Desktop/Mohammed_Alhrazy
```

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



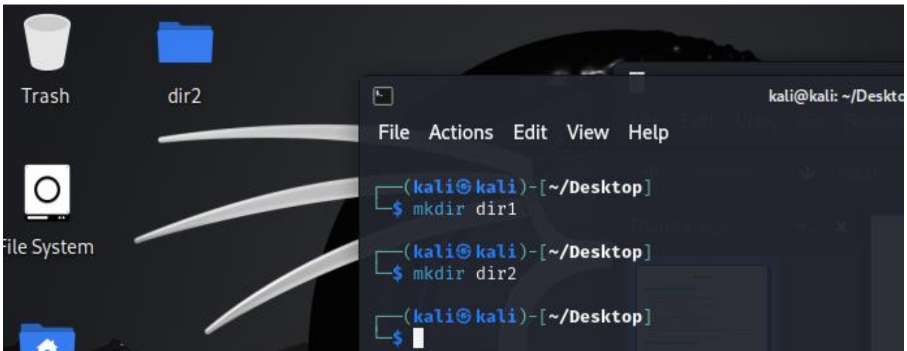
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -la
total 40
drwxr-xr-x  6 kali kali  4096 Sep 11 10:12 .
drwx------ 25 kali kali  4096 Sep 11 13:06 ..
drwxrwxr-x  2 kali kali  4096 Sep  5 15:10 dir2
-rw-r--r--  1 kali kali     0 Sep 10 17:49 file2.txt
drwxrwxr-x  4 kali kali  4096 Sep 10 17:25 Mohammed_Alhrazy
drwxr-xr-x  2 kali kali  4096 Sep 10 17:56 project
drwxrwxr-x  2 kali kali  4096 Sep 18  2023 vpnbook-openvpn-fr231
-rwxrwx---  1 kali kali 13684 Sep 11 10:06 vpnbook-openvpn-fr231.zip
```

3. Change your directory to the `Desktop`.



```
┌──(kali㉿kali)-[~/Desktop/Mohammed_Alhrazy]
└─$ cd ..

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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

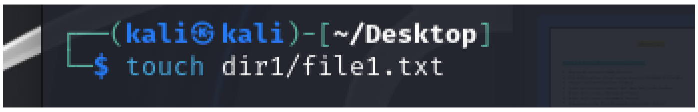


```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir dir1

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir dir2

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

DR:Abdalrzaq Alsmawi

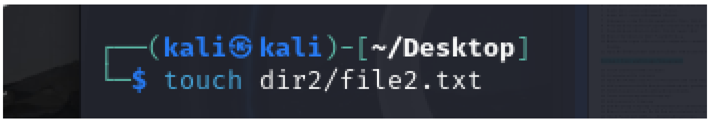
Name:Mohammed Abdalkreem Alhrazy group(2)

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



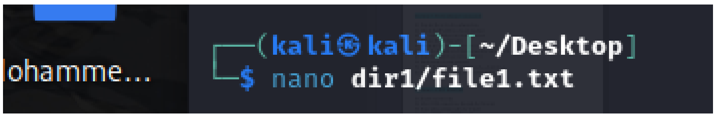
```
┌──(kali㉿kali)-[~/Desktop]
└─$ touch dir1/file1.txt
```

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



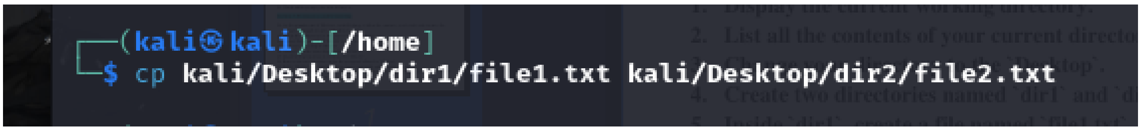
```
┌──(kali㉿kali)-[~/Desktop]
└─$ touch dir2/file2.txt
```

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



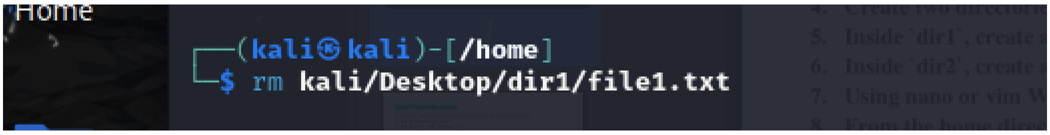
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nano dir1/file1.txt
```

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



```
┌──(kali㉿kali)-[/home]
└─$ cp kali/Desktop/dir1/file1.txt kali/Desktop/dir2/file2.txt
```

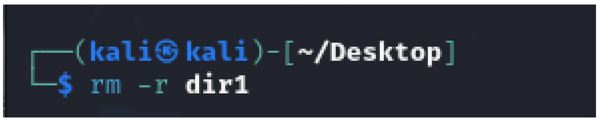
9. From the home directory, delete `file1.txt` inside `dir1`.



```
┌──(kali㉿kali)-[/home]
└─$ rm kali/Desktop/dir1/file1.txt
```

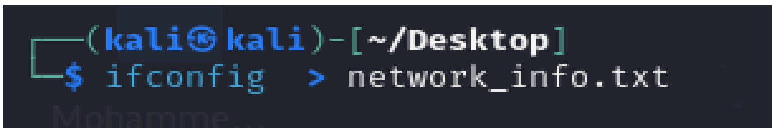
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

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



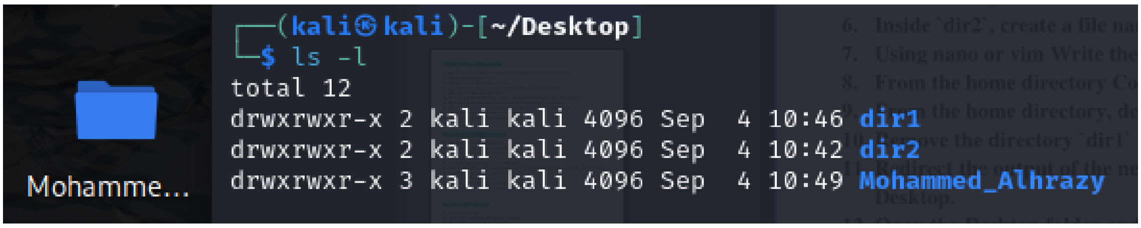
```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm -r dir1
```

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



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig  > network_info.txt
```

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

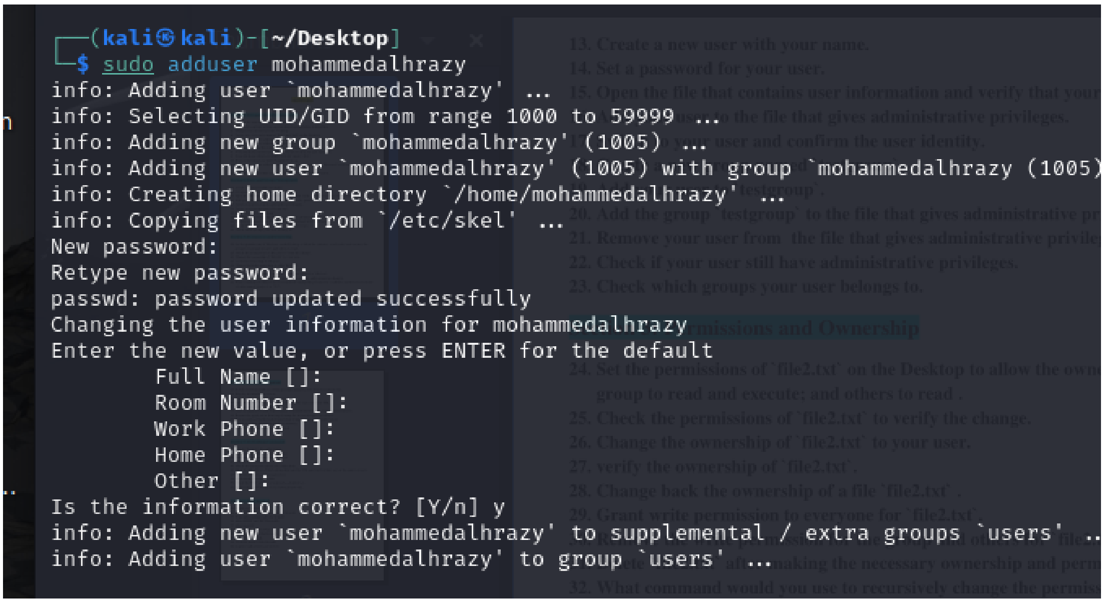


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l
total 12
drwxrwxr-x 2 kali kali 4096 Sep  4 10:46 dir1
drwxrwxr-x 2 kali kali 4096 Sep  4 10:42 dir2
drwxrwxr-x 3 kali kali 4096 Sep  4 10:49 Mohammed_Alhrazy
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

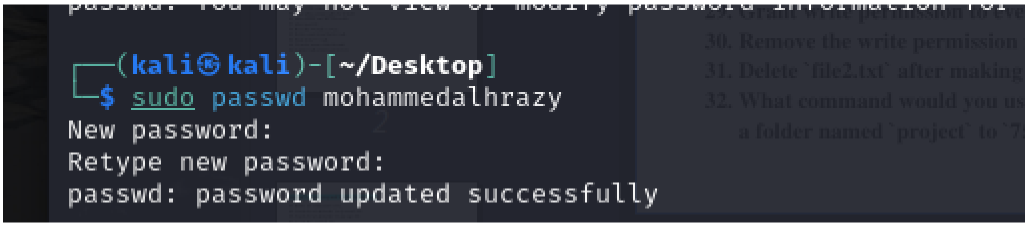
Users and Groups Management

13. Create a new user with your name.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo adduser mohammedalhrazy
info: Adding user `mohammedalhrazy' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `mohammedalhrazy' (1005) ...
info: Adding new user `mohammedalhrazy' (1005) with group `mohammedalhrazy (1005)
info: Creating home directory `/home/mohammedalhrazy' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mohammedalhrazy
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `mohammedalhrazy' to supplemental / extra groups `users' ..
info: Adding user `mohammedalhrazy' to group `users' ...
```

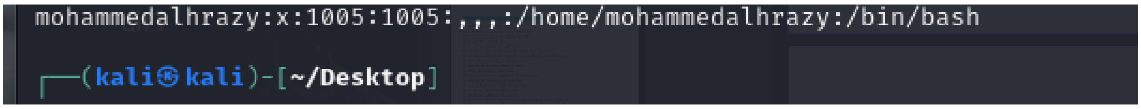
14. Set a password for your user.



```
passwd: You may not view or modify password information for

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo passwd mohammedalhrazy
New password:
Retype new password:
passwd: password updated successfully
```

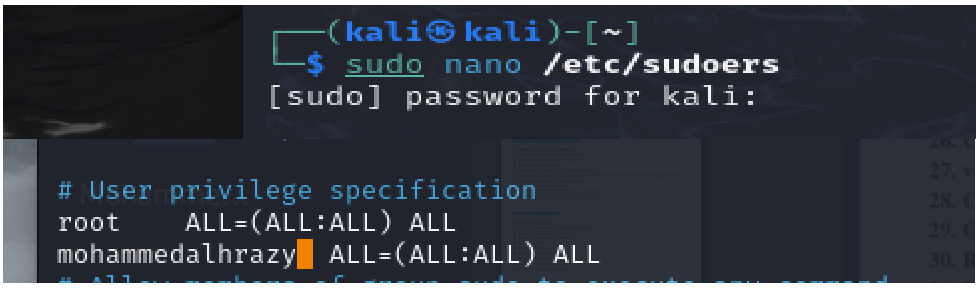
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

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



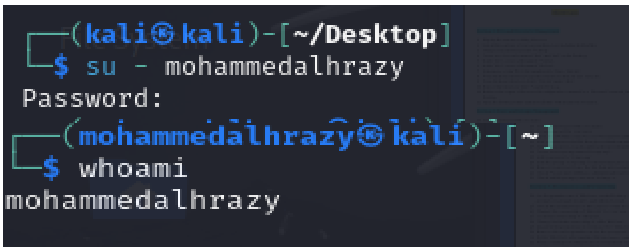
```
mohammedalhrazy:x:1005:1005:,,,:/home/mohammedalhrazy:/bin/bash

┌──(kali㉿kali)-[~/Desktop]
```

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



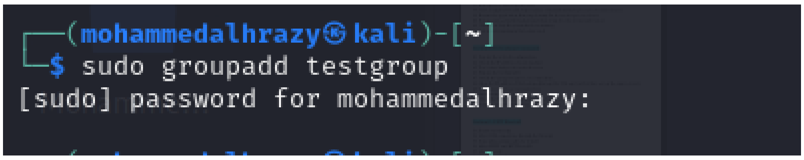
```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/sudoers
[sudo] password for kali:

# User privilege specification
root    ALL=(ALL:ALL) ALL
mohammedalhrazy ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
```

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



```
┌──(kali㉿kali)-[~/Desktop]
└─$ su - mohammedalhrazy
Password:
┌──(mohammedalhrazy㉿kali)-[~]
└─$ whoami
mohammedalhrazy
```

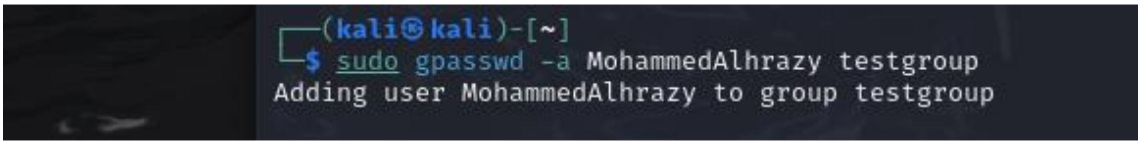
18. Create a new group named `testgroup`.



```
┌──(mohammedalhrazy㉿kali)-[~]
└─$ sudo groupadd testgroup
[sudo] password for mohammedalhrazy:
```

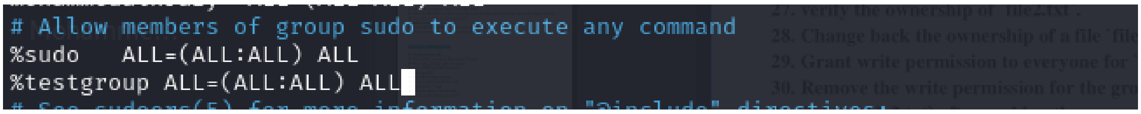
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

19. Add your user to `testgroup`.



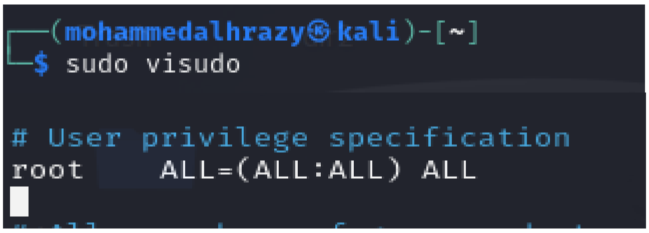
```
┌──(kali㉿kali)-[~]
└─$ sudo gpasswd -a MohammedAlhrazy testgroup
Adding user MohammedAlhrazy to group testgroup
```

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



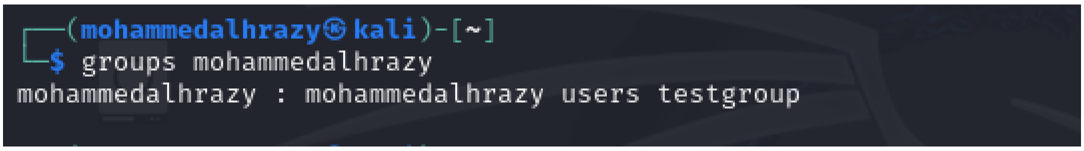
```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%testgroup ALL=(ALL:ALL) ALL
```

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



```
┌──(mohammedalhrazy㉿kali)-[~]
└─$ sudo visudo

# User privilege specification
root    ALL=(ALL:ALL) ALL
```

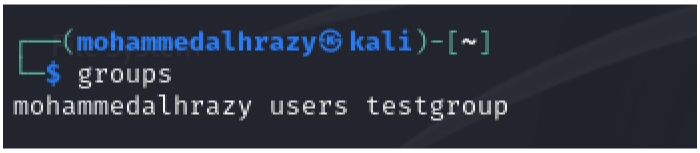
22. Check if your user still have administrative privileges.



```
┌──(mohammedalhrazy㉿kali)-[~]
└─$ groups mohammedalhrazy
mohammedalhrazy : mohammedalhrazy users testgroup
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

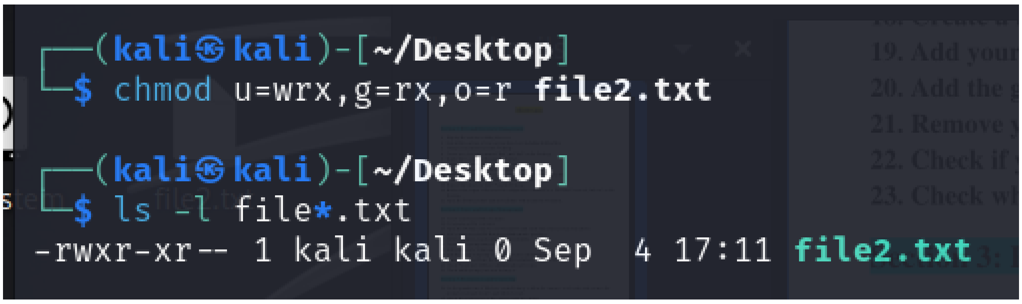
23. Check which groups your user belongs to.



```
┌──(mohammedalhrazy㉿kali)-[~]
└─$ groups
mohammedalhrazy users testgroup
```

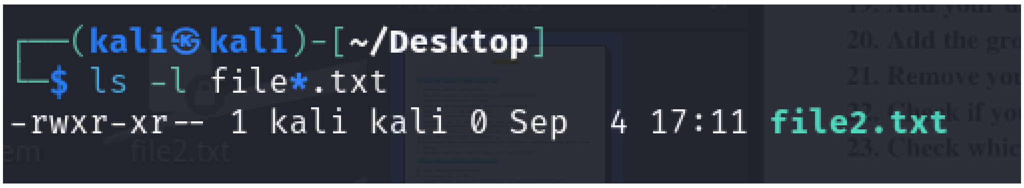
Permissions and Ownership

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 u=wrx,g=rx,o=r file2.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l file*.txt
-rwxr-xr-- 1 kali kali 0 Sep  4 17:11 file2.txt
```

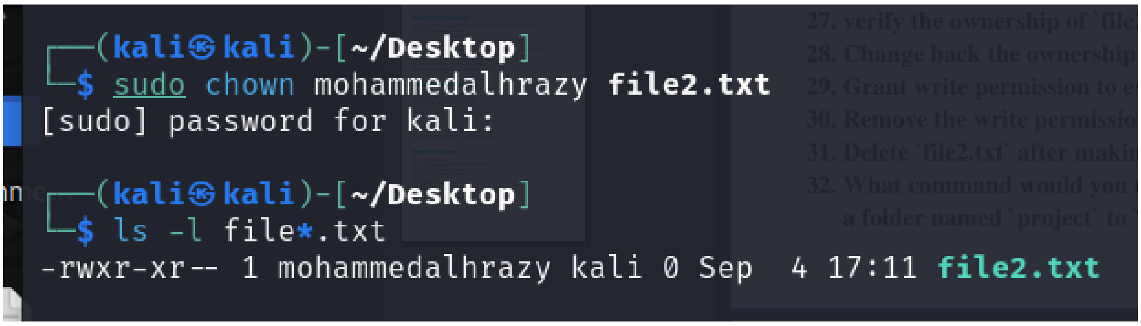
25. Check the permissions of `file2.txt` to verify the change.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l file*.txt
-rwxr-xr-- 1 kali kali 0 Sep  4 17:11 file2.txt
```

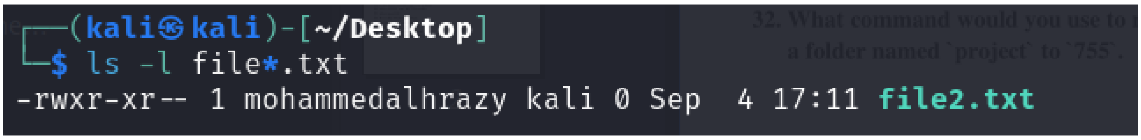
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

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



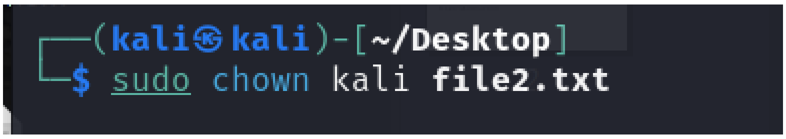
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown mohammedalhrazy file2.txt
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l file*.txt
-rwxr-xr-- 1 mohammedalhrazy kali 0 Sep  4 17:11 file2.txt
```

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



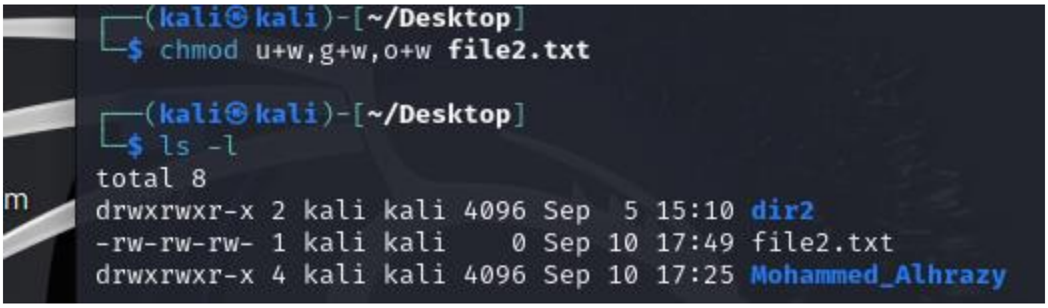
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l file*.txt
-rwxr-xr-- 1 mohammedalhrazy kali 0 Sep  4 17:11 file2.txt
```

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



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

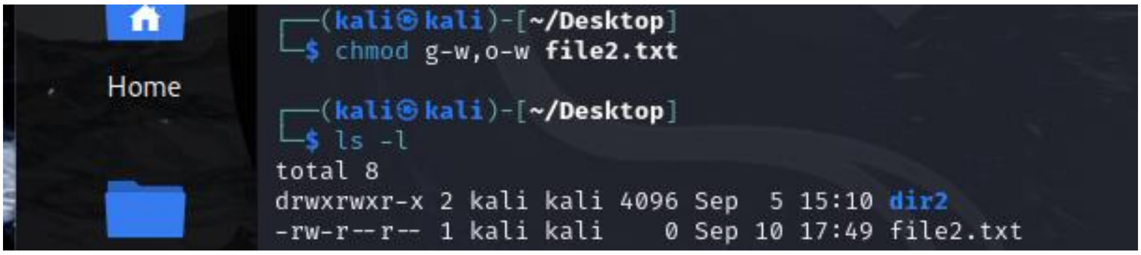
29. Grant write permission to everyone for `file2.txt`.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod u+w,g+w,o+w file2.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l
total 8
drwxrwxr-x 2 kali kali 4096 Sep  5 15:10 dir2
-rw-rw-rw- 1 kali kali    0 Sep 10 17:49 file2.txt
drwxrwxr-x 4 kali kali 4096 Sep 10 17:25 Mohammed_Alhrazy
```

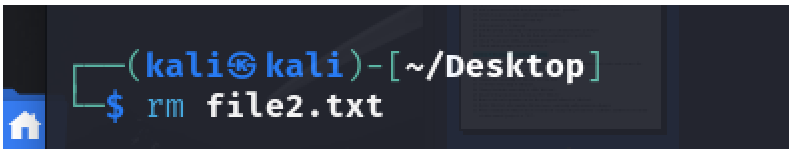
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

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



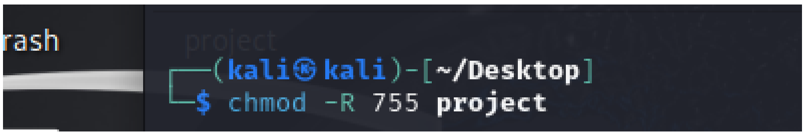
```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod g-w,o-w file2.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l
total 8
drwxrwxr-x 2 kali kali 4096 Sep  5 15:10 dir2
-rw-r--r-- 1 kali kali    0 Sep 10 17:49 file2.txt
```

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



```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm file2.txt
```

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

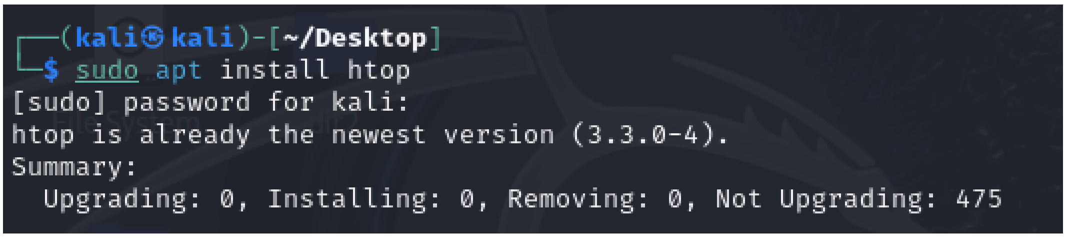


```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod -R 755 project
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy   group(2)

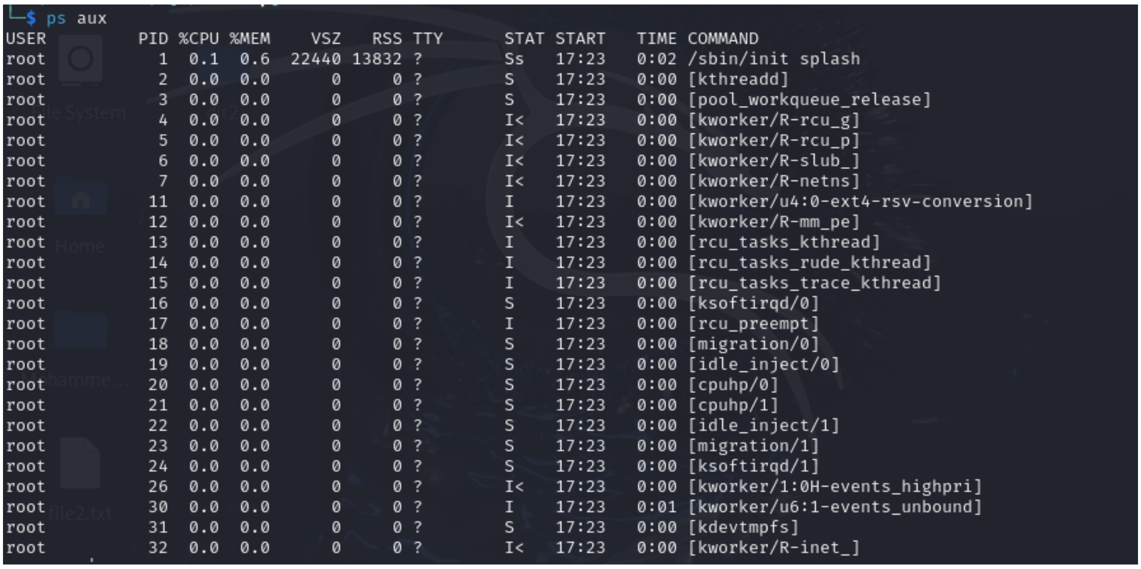
Process Management

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



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install htop
[sudo] password for kali:
htop is already the newest version (3.3.0-4).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 475
```

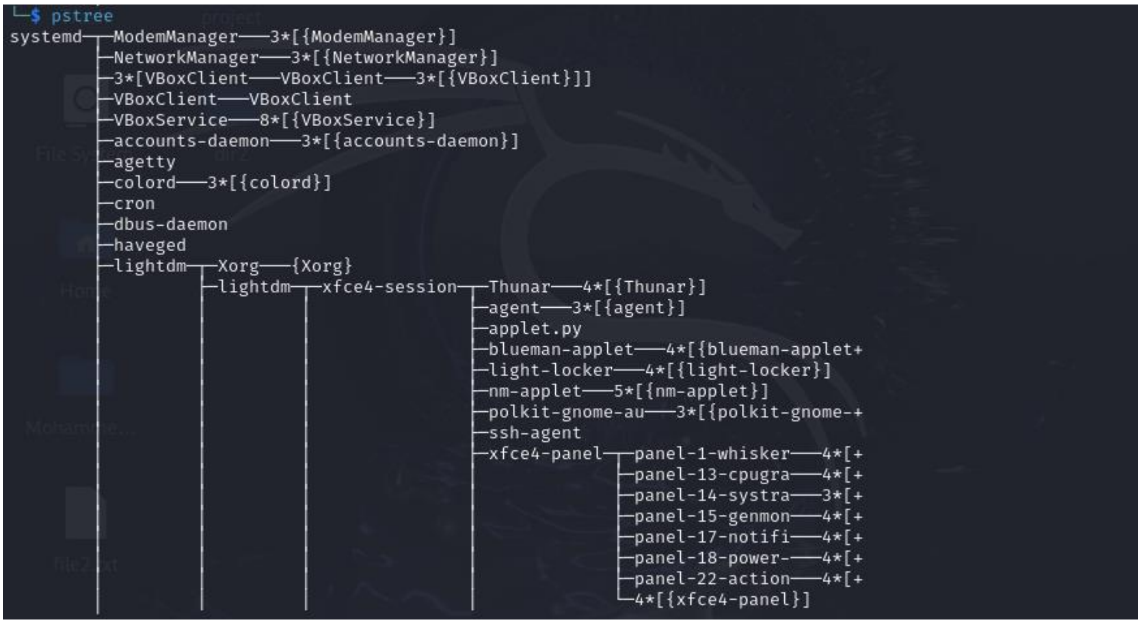
34. Display all running processes.



```
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.6  22440 13832 ?        Ss   17:23   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    17:23   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    17:23   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   17:23   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   17:23   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   17:23   0:00 [kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   17:23   0:00 [kworker/R-netns]
root          11  0.0  0.0      0     0 ?        I    17:23   0:00 [kworker/u4:0-ext4-rsv-conversion]
root          12  0.0  0.0      0     0 ?        I<   17:23   0:00 [kworker/R-mm_pe]
root          13  0.0  0.0      0     0 ?        I    17:23   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    17:23   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    17:23   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    17:23   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    17:23   0:00 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    17:23   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    17:23   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    17:23   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    17:23   0:00 [cpuhp/1]
root          22  0.0  0.0      0     0 ?        S    17:23   0:00 [idle_inject/1]
root          23  0.0  0.0      0     0 ?        S    17:23   0:00 [migration/1]
root          24  0.0  0.0      0     0 ?        S    17:23   0:00 [ksoftirqd/1]
root          26  0.0  0.0      0     0 ?        I<   17:23   0:00 [kworker/1:0H-events_highpri]
root          30  0.0  0.0      0     0 ?        I    17:23   0:01 [kworker/u6:1-events_unbound]
root          31  0.0  0.0      0     0 ?        S    17:23   0:00 [kdevtmpfs]
root          32  0.0  0.0      0     0 ?        I<   17:23   0:00 [kworker/R-inet_]
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

35. Display a tree of all running processes.

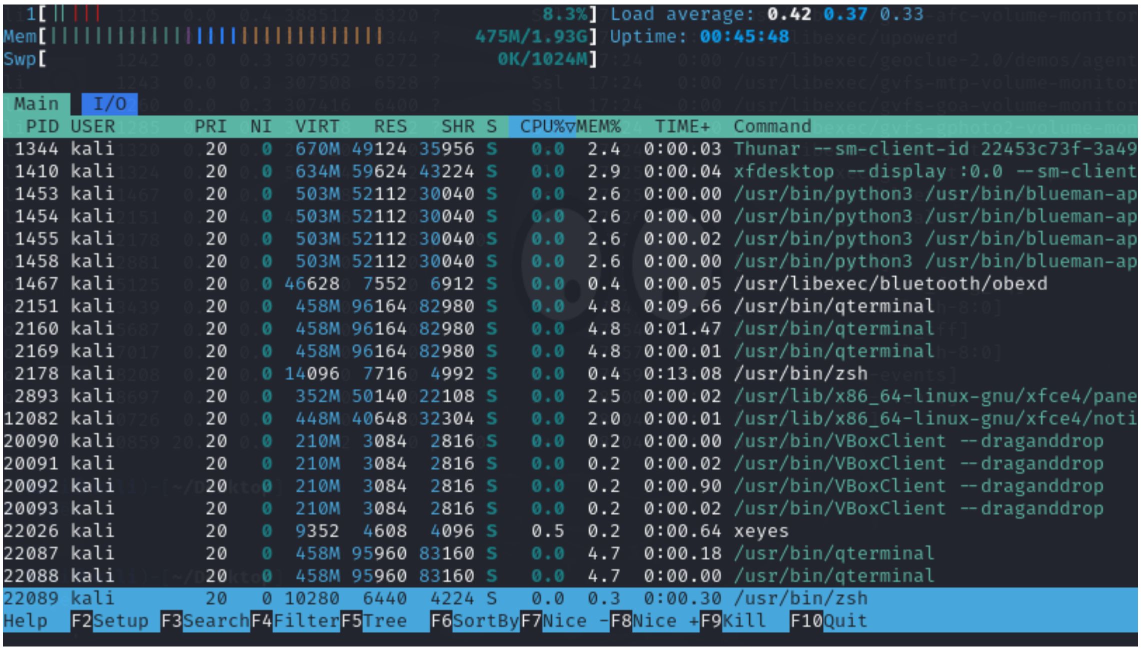


```
└─$ pstree
systemd─┬─ModemManager───3*[{ModemManager}]
        ├─NetworkManager───3*[{NetworkManager}]
        ├─3*[VBoxClient───VBoxClient───3*[{VBoxClient}]]
        ├─VBoxClient───VBoxClient
        ├─VBoxService───8*[{VBoxService}]
        ├─accounts-daemon───3*[{accounts-daemon}]
        ├─agetty
        ├─colord───3*[{colord}]
        ├─cron
        ├─dbus-daemon
        ├─haveged
        ├─lightdm─┬─Xorg───{Xorg}
        │         └─lightdm─┬─xfce4-session─┬─Thunar───4*[{Thunar}]
        │         │         │               ├─agent───3*[{agent}]
        │         │         │               ├─applet.py
        │         │         │               ├─blueman-applet───4*[{blueman-applet+
        │         │         │               ├─light-locker───4*[{light-locker}]
        │         │         │               ├─nm-applet───5*[{nm-applet}]
        │         │         │               ├─polkit-gnome-au───3*[{polkit-gnome-+
        │         │         │               ├─ssh-agent
        │         │         │               ├─xfce4-panel─┬─panel-1-whisker───4*[+
        │         │         │               │             ├─panel-13-cpugra───4*[+
        │         │         │               │             ├─panel-14-systra───3*[+
        │         │         │               │             ├─panel-15-genmon───4*[+
        │         │         │               │             ├─panel-17-notifi───4*[+
        │         │         │               │             ├─panel-18-power-───4*[+
        │         │         │               │             ├─panel-22-action───4*[+
        │         │         │               │             └─4*[{xfce4-panel}]
        │         │         │               │
```

DR:Abdalrzaq Alsmawi

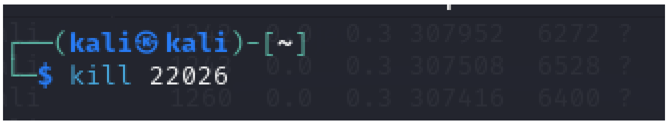
Name:Mohammed Abdalkreem Alhrazy group(2)

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



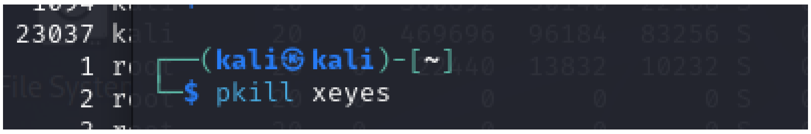
```
  1[||||                          8.3%] Load average: 0.42 0.37 0.33
Mem[||||||||||||||||||||||||||||||475M/1.93G] Uptime: 00:45:48
Swp[                              0K/1024M]

 Main  I/O
  PID USER      PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
 1344 kali       20   0  670M 49124 35956 S   0.0  2.4  0:00.03 Thunar --sm-client-id 22453c73f-3a49
 1410 kali       20   0  634M 59624 43224 S   0.0  2.9  0:00.04 xfdesktop --display :0.0 --sm-client
 1453 kali       20   0  503M 52112 30040 S   0.0  2.6  0:00.00 /usr/bin/python3 /usr/bin/blueman-ap
 1454 kali       20   0  503M 52112 30040 S   0.0  2.6  0:00.00 /usr/bin/python3 /usr/bin/blueman-ap
 1455 kali       20   0  503M 52112 30040 S   0.0  2.6  0:00.02 /usr/bin/python3 /usr/bin/blueman-ap
 1458 kali       20   0  503M 52112 30040 S   0.0  2.6  0:00.00 /usr/bin/python3 /usr/bin/blueman-ap
 1467 kali       20   0 46628  7552  6912 S   0.0  0.4  0:00.05 /usr/libexec/bluetooth/obexd
 2151 kali       20   0  458M 96164 82980 S   0.0  4.8  0:09.66 /usr/bin/qterminal
 2160 kali       20   0  458M 96164 82980 S   0.0  4.8  0:01.47 /usr/bin/qterminal
 2169 kali       20   0  458M 96164 82980 S   0.0  4.8  0:00.01 /usr/bin/qterminal
 2178 kali       20   0 14096  7716  4992 S   0.0  0.4  0:13.08 /usr/bin/zsh
 2893 kali       20   0  352M 50140 22108 S   0.0  2.5  0:00.02 /usr/lib/x86_64-linux-gnu/xfce4/pane
12082 kali       20   0  448M 40648 32304 S   0.0  2.0  0:00.01 /usr/lib/x86_64-linux-gnu/xfce4/noti
20090 kali       20   0  210M  3084  2816 S   0.0  0.2  0:00.00 /usr/bin/VBoxClient --draganddrop
20091 kali       20   0  210M  3084  2816 S   0.0  0.2  0:00.02 /usr/bin/VBoxClient --draganddrop
20092 kali       20   0  210M  3084  2816 S   0.0  0.2  0:00.90 /usr/bin/VBoxClient --draganddrop
20093 kali       20   0  210M  3084  2816 S   0.0  0.2  0:00.02 /usr/bin/VBoxClient --draganddrop
22026 kali       20   0  9352  4608  4096 S   0.5  0.2  0:00.64 xeyes
22087 kali       20   0  458M 95960 83160 S   0.0  4.7  0:00.18 /usr/bin/qterminal
22088 kali       20   0  458M 95960 83160 S   0.0  4.7  0:00.00 /usr/bin/qterminal
22089 kali       20   0 10280  6440  4224 S   0.0  0.3  0:00.30 /usr/bin/zsh
Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

37. Kill a process with a specific PID.



```
┌──(kali㉿kali)-[~]
└─$ kill 22026
```

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

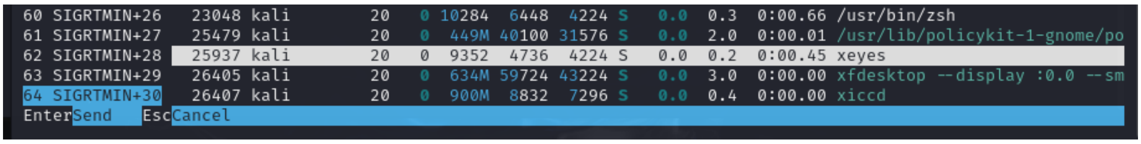


```
23037 k
    1 r   ┌──(kali㉿kali)-[~]
    2 r   └─$ pkill xeyes
```

DR:Abdalrzaq Alsmawi

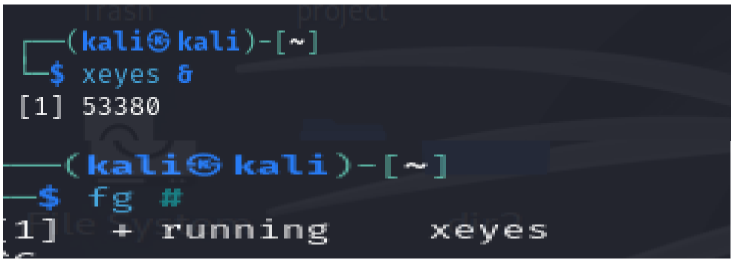
Name:Mohammed Abdalkreem Alhrazy   group(2)

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



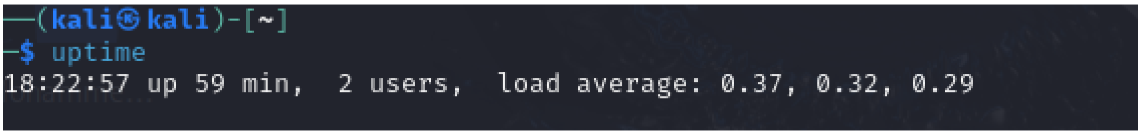
```
60 SIGRTMIN+26   23048 kali        20   0 10284   6448   4224 S   0.0  0.3  0:00.66 /usr/bin/zsh
61 SIGRTMIN+27   25479 kali        20   0  449M 40100 31576 S   0.0  2.0  0:00.01 /usr/lib/policykit-1-gnome/po
62 SIGRTMIN+28   25937 kali        20   0  9352  4736  4224 S   0.0  0.2  0:00.45 xeyes
63 SIGRTMIN+29   26405 kali        20   0  634M 59724 43224 S   0.0  3.0  0:00.00 xfdesktop --display :0.0 --sm
64 SIGRTMIN+30   26407 kali        20   0  900M  8832  7296 S   0.0  0.4  0:00.00 xiccd
EnterSend    EscCancel
```

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



```
┌──(kali㉿kali)-[~]
└─$ xeyes &
[1] 53380

──(kali㉿kali)-[~]
─$ fg #
[1]  + running    xeyes
```

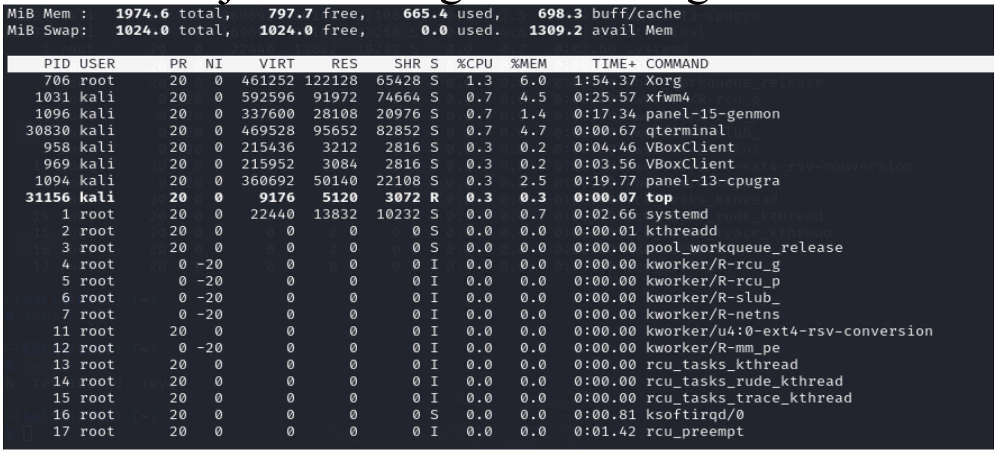
41. Check how long the system has been running.



```
─(kali㉿kali)-[~]
─$ uptime
18:22:57 up 59 min,  2 users,  load average: 0.37, 0.32, 0.29
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

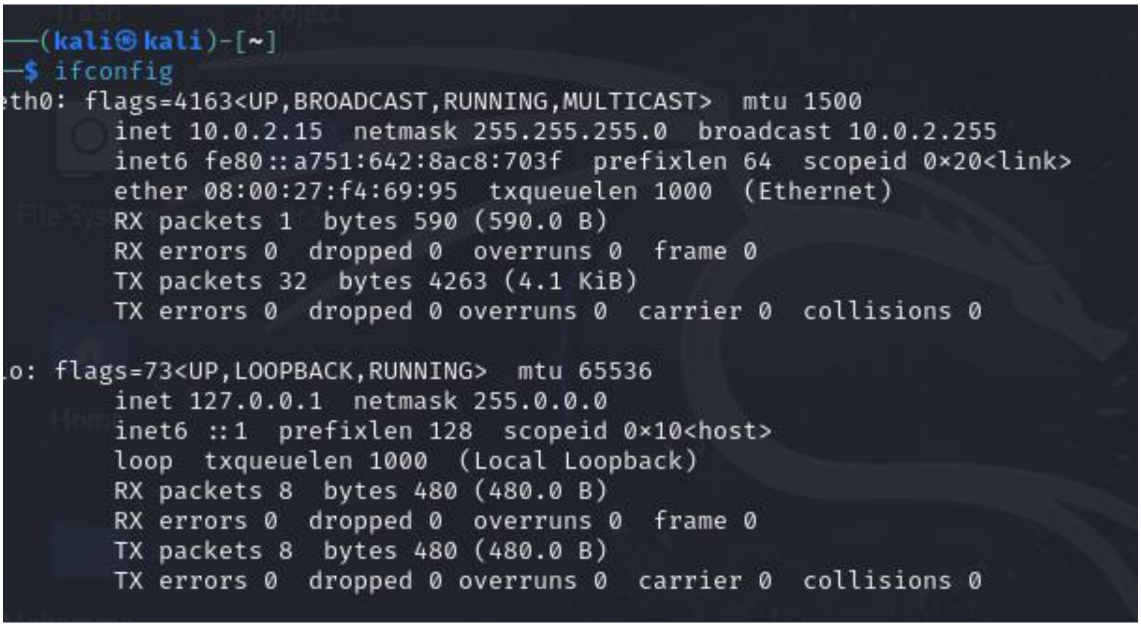
42. List all jobs running in the background.



```
MiB Mem :   1974.6 total,    797.7 free,    665.4 used,    698.3 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   1309.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    706 root      20   0  461252 122128  65428 S   1.3   6.0   1:54.37 Xorg
   1031 kali      20   0  592596  91972  74664 S   0.7   4.5   0:25.57 xfwm4
   1096 kali      20   0  337600  28108  20976 S   0.7   1.4   0:17.34 panel-15-genmon
  30830 kali      20   0  469528  95652  82852 S   0.7   4.7   0:00.67 qterminal
    958 kali      20   0  215436   3212   2816 S   0.3   0.2   0:04.46 VBoxClient
    969 kali      20   0  215952   3084   2816 S   0.3   0.2   0:03.56 VBoxClient
   1094 kali      20   0  360692  50140  22108 S   0.3   2.5   0:19.77 panel-13-cpugra
  31156 kali      20   0    9176   5120   3072 R   0.3   0.3   0:00.07 top
      1 root      20   0   22440  13832  10232 S   0.0   0.7   0:02.66 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_g
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_p
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-slub_
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-netns
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/u4:0-ext4-rsv-conversion
     12 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-mm_pe
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     14 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.81 ksoftirqd/0
     17 root      20   0       0      0      0 I   0.0   0.0   0:01.42 rcu_preempt
```

Networking Commands

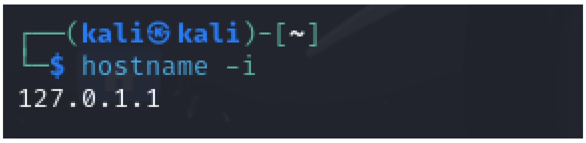
43. Display the network configuration.



```
—(kali㉿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::a751:642:8ac8:703f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f4:69:95  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 4263 (4.1 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

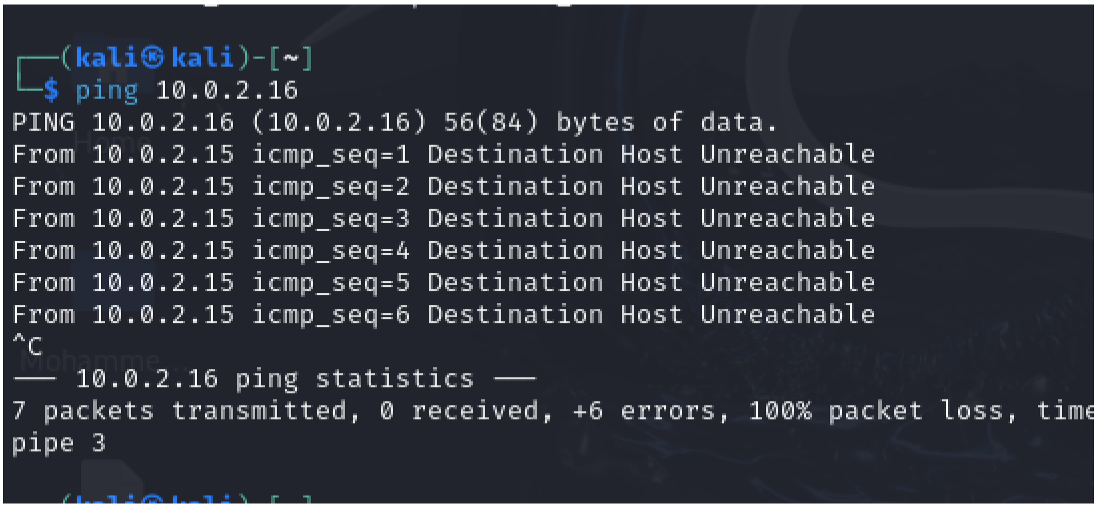
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

44. Check the IP address of your machine.



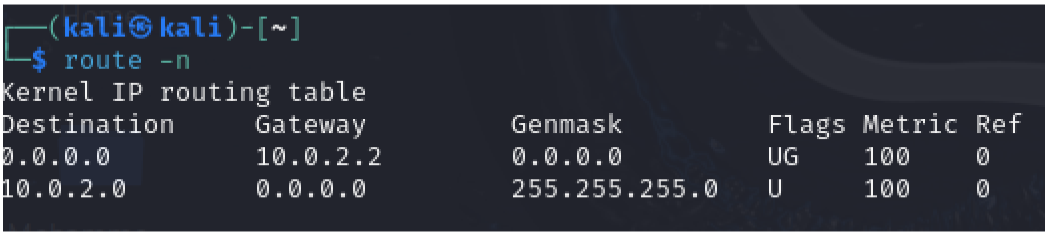
```
┌──(kali㉿kali)-[~]
└─$ hostname -i
127.0.1.1
```

45. Test connectivity to an external server.



```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.16
PING 10.0.2.16 (10.0.2.16) 56(84) bytes of data.
From 10.0.2.15 icmp_seq=1 Destination Host Unreachable
From 10.0.2.15 icmp_seq=2 Destination Host Unreachable
From 10.0.2.15 icmp_seq=3 Destination Host Unreachable
From 10.0.2.15 icmp_seq=4 Destination Host Unreachable
From 10.0.2.15 icmp_seq=5 Destination Host Unreachable
From 10.0.2.15 icmp_seq=6 Destination Host Unreachable
^C
── 10.0.2.16 ping statistics ──
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time
pipe 3
```

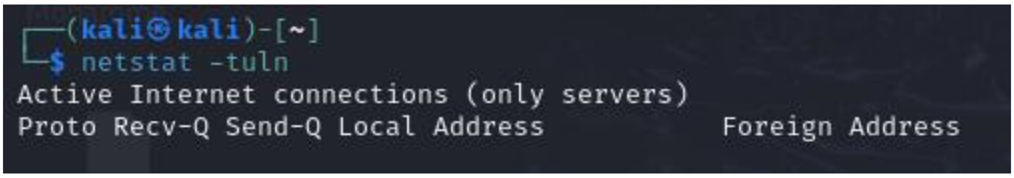
46. Display the routing table.



```
┌──(kali㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0
```

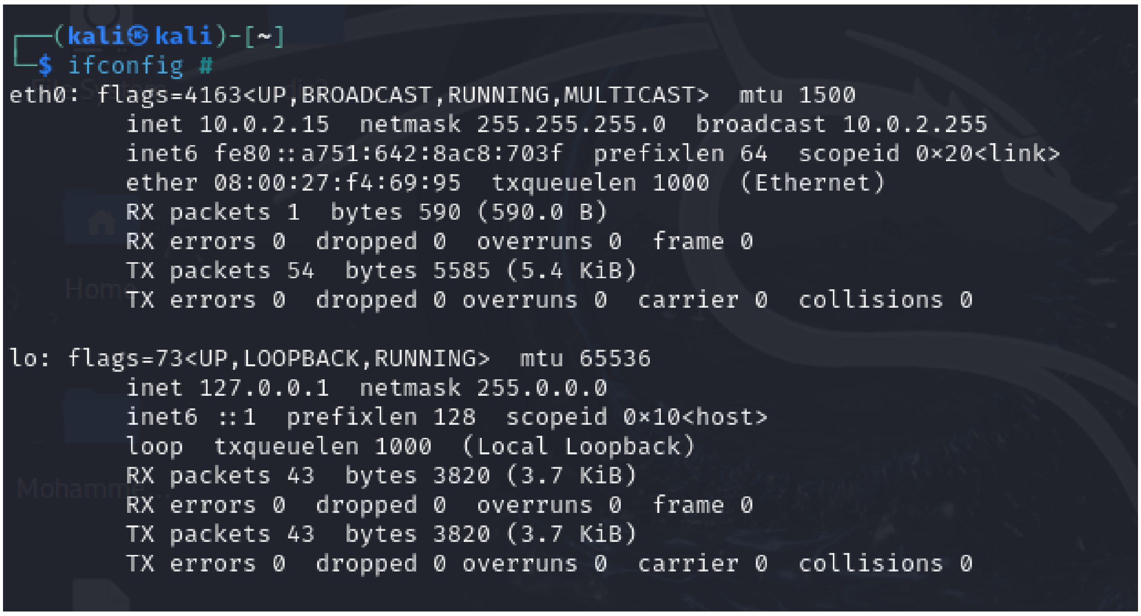
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

47. Check the open ports and active connections.



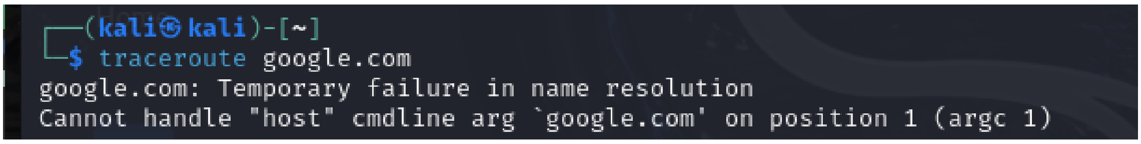
```
┌──(kali㉿kali)-[~]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
```

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



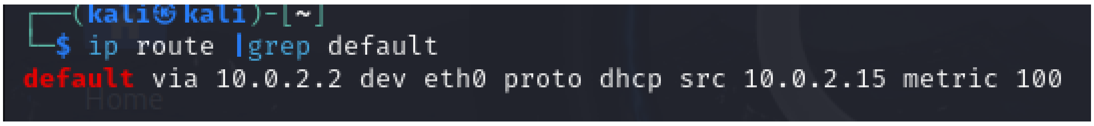
```
┌──(kali㉿kali)-[~]
└─$ ifconfig #
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a751:642:8ac8:703f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f4:69:95  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 5585 (5.4 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 43  bytes 3820 (3.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43  bytes 3820 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

49. Trace the route to an external server.



```
┌──(kali㉿kali)-[~]
└─$ traceroute google.com
google.com: Temporary failure in name resolution
Cannot handle "host" cmdline arg `google.com' on position 1 (argc 1)
```

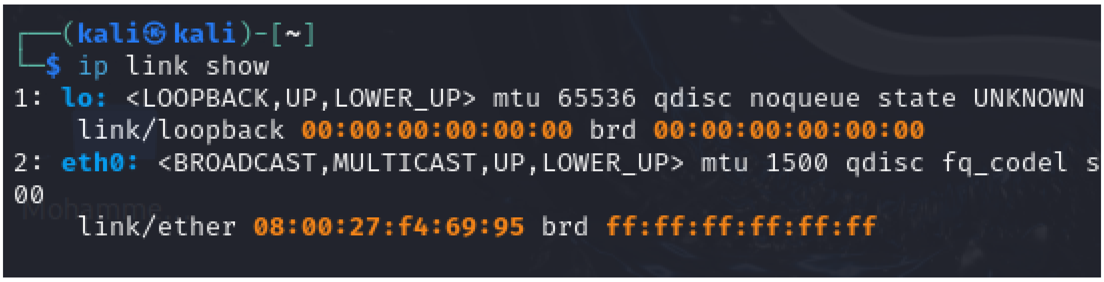
50. Find out the default gateway.



```
┌──(kali㉿kali)-[~]
└─$ ip route |grep default
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
```

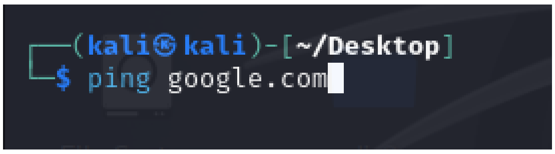
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

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
    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 s
00
    link/ether 08:00:27:f4:69:95 brd ff:ff:ff:ff:ff:ff
```

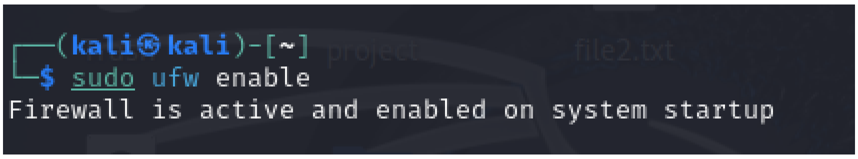
52. Ensure that the VM can access external networks.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping google.com
```

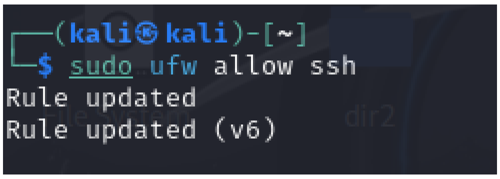
UFW Firewall

53. Enable the firewall.



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

54. Allow SSH connections through the firewall.

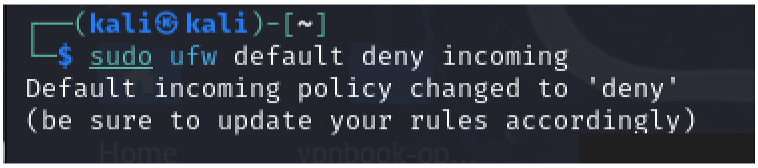


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule updated
Rule updated (v6)
```

DR:Abdalrzaq Alsmawi

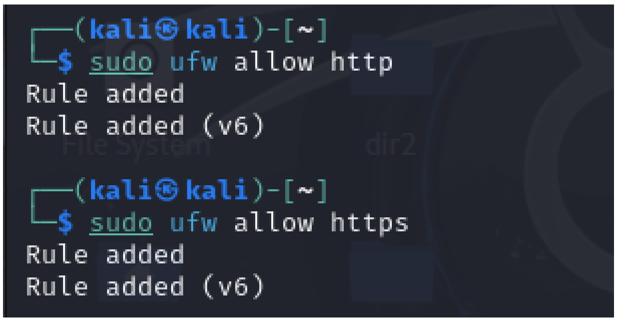
Name:Mohammed Abdalkreem Alhrazy group(2)

55. Deny all incoming traffic by default.



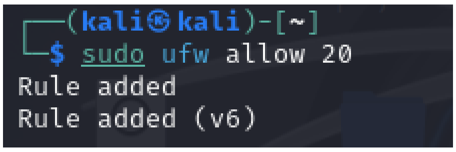
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

56. Allow HTTP and HTTPS traffic.



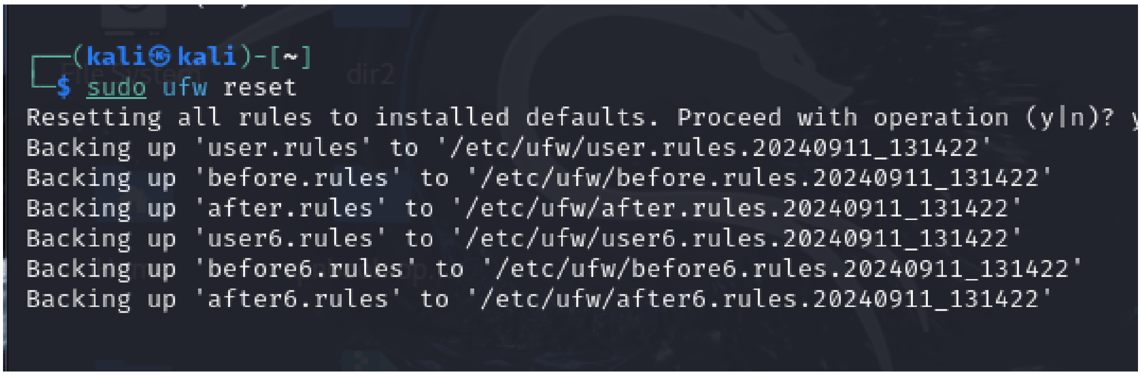
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow http
Rule added
Rule added (v6)

┌──(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)
```

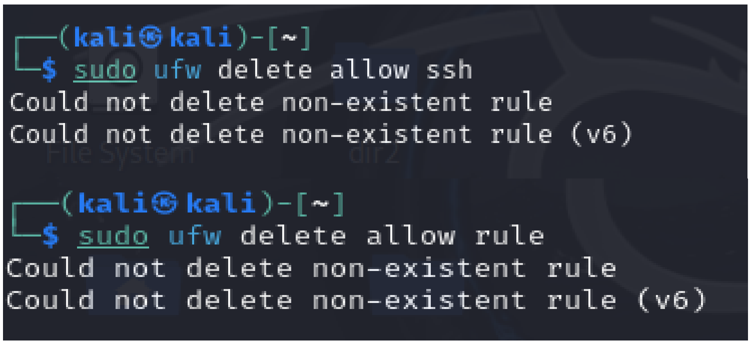
58. Reset the firewall settings.



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20240911_131422'
Backing up 'before.rules' to '/etc/ufw/before.rules.20240911_131422'
Backing up 'after.rules' to '/etc/ufw/after.rules.20240911_131422'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20240911_131422'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20240911_131422'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20240911_131422'
```

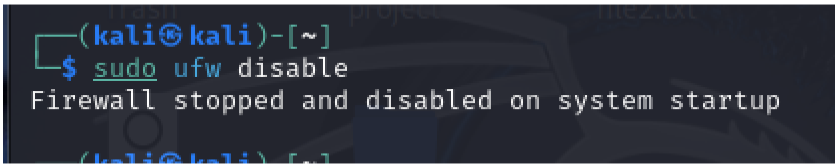
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

59. Delete a rule from the firewall.



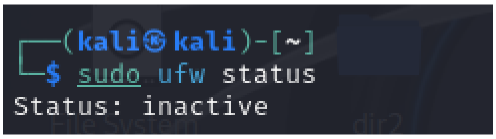
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw delete allow ssh
Could not delete non-existent rule
Could not delete non-existent rule (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw delete allow rule
Could not delete non-existent rule
Could not delete non-existent rule (v6)
```

60. Disable the firewall.



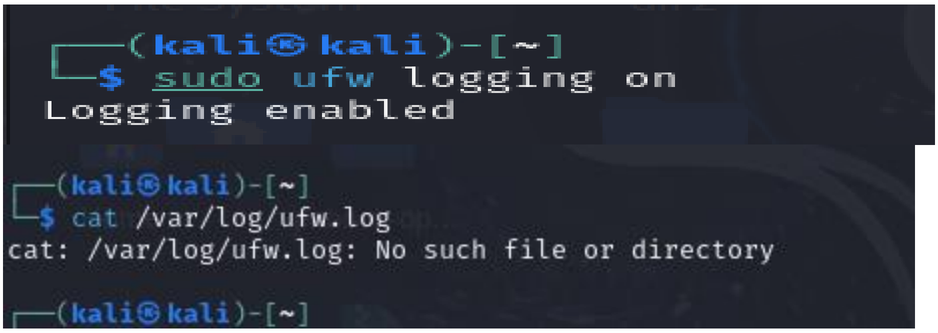
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw disable
Firewall stopped and disabled on system startup

┌──(kali㉿kali)-[~]
```

61. View the status of the firewall.



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: inactive
```

62. Log firewall activity and view it.



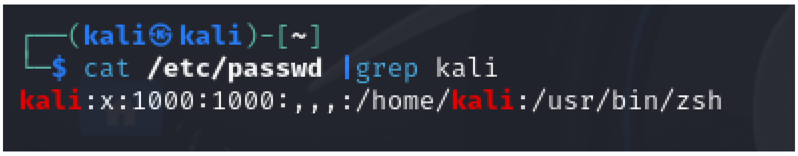
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw logging on
Logging enabled

┌──(kali㉿kali)-[~]
└─$ cat /var/log/ufw.log
cat: /var/log/ufw.log: No such file or directory

┌──(kali㉿kali)-[~]
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

Searching and System Information

63. Delete the command history.

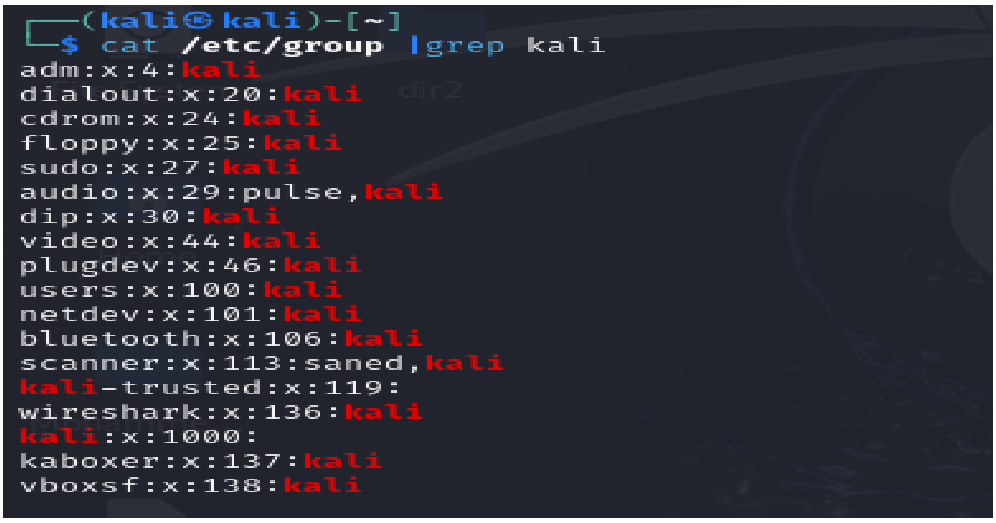
64. Search for a kali in the `/etc/passwd` file.



```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd |grep kali
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
```

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

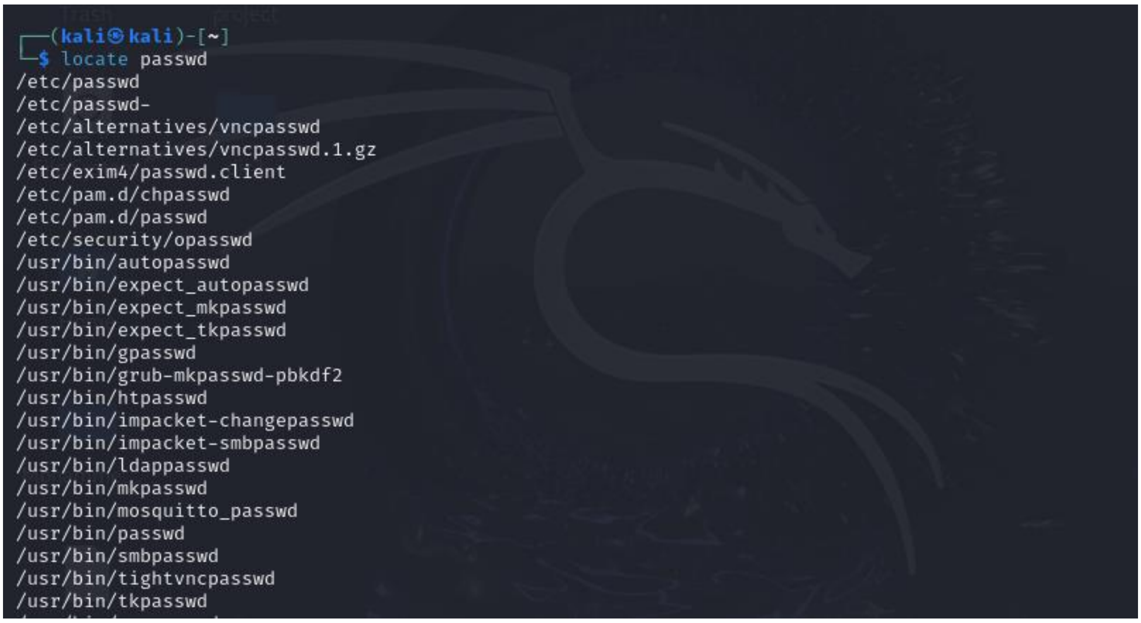
.



```
┌──(kali㉿kali)-[~]
└─$ cat /etc/group |grep kali
adm:x:4:kali
dialout:x:20:kali
cdrom:x:24:kali
floppy:x:25:kali
sudo:x:27:kali
audio:x:29:pulse,kali
dip:x:30:kali
video:x:44:kali
plugdev:x:46:kali
users:x:100:kali
netdev:x:101:kali
bluetooth:x:106:kali
scanner:x:113:saned,kali
kali-trusted:x:119:
wireshark:x:136:kali
kali:x:1000:
kaboxer:x:137:kali
vboxsf:x:138:kali
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

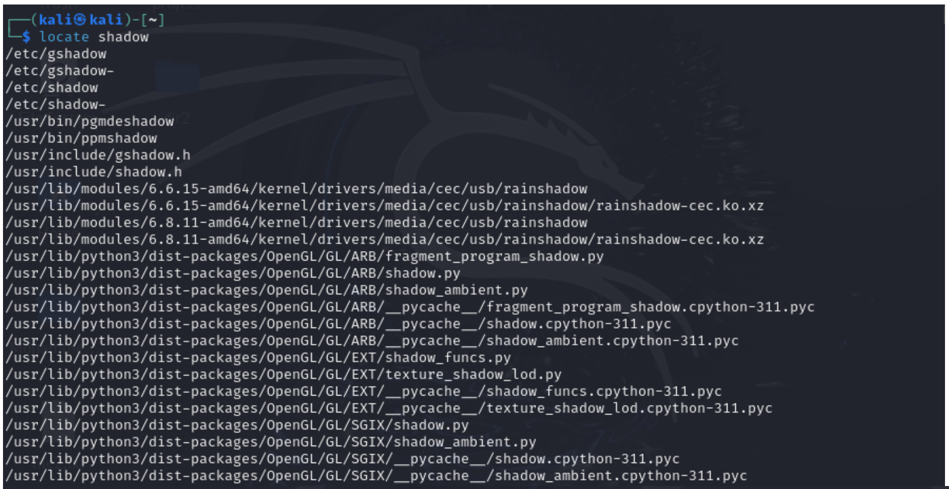
66. Locate the `passwd` file.



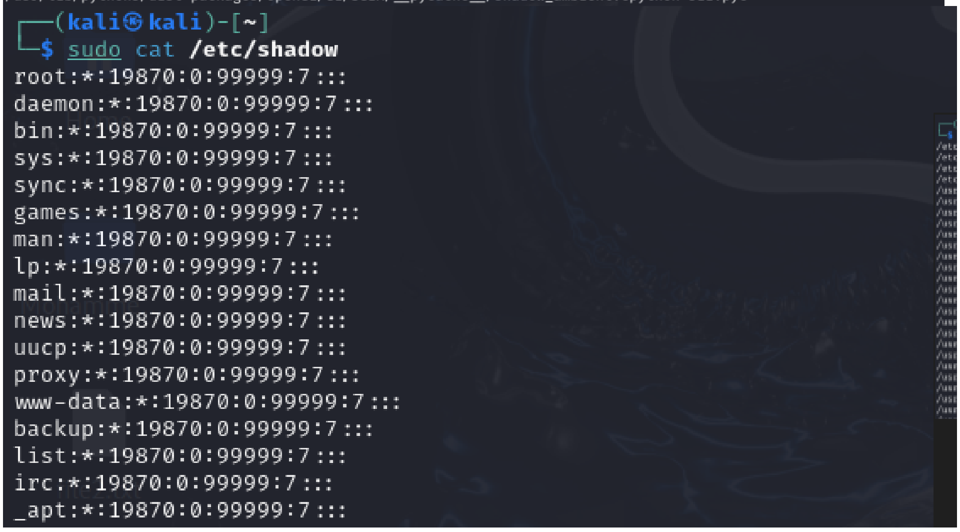
```
┌──(kali㉿kali)-[~]
└─$ locate passwd
/etc/passwd
/etc/passwd-
/etc/alternatives/vncpasswd
/etc/alternatives/vncpasswd.1.gz
/etc/exim4/passwd.client
/etc/pam.d/chpasswd
/etc/pam.d/passwd
/etc/security/opasswd
/usr/bin/autopasswd
/usr/bin/expect_autopasswd
/usr/bin/expect_mkpasswd
/usr/bin/expect_tkpasswd
/usr/bin/gpasswd
/usr/bin/grub-mkpasswd-pbkdf2
/usr/bin/htpasswd
/usr/bin/impacket-changepasswd
/usr/bin/impacket-smbpasswd
/usr/bin/ldappasswd
/usr/bin/mkpasswd
/usr/bin/mosquitto_passwd
/usr/bin/passwd
/usr/bin/smbpasswd
/usr/bin/tightvncpasswd
/usr/bin/tkpasswd
```

DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

67. Locate the shadow file and open it.



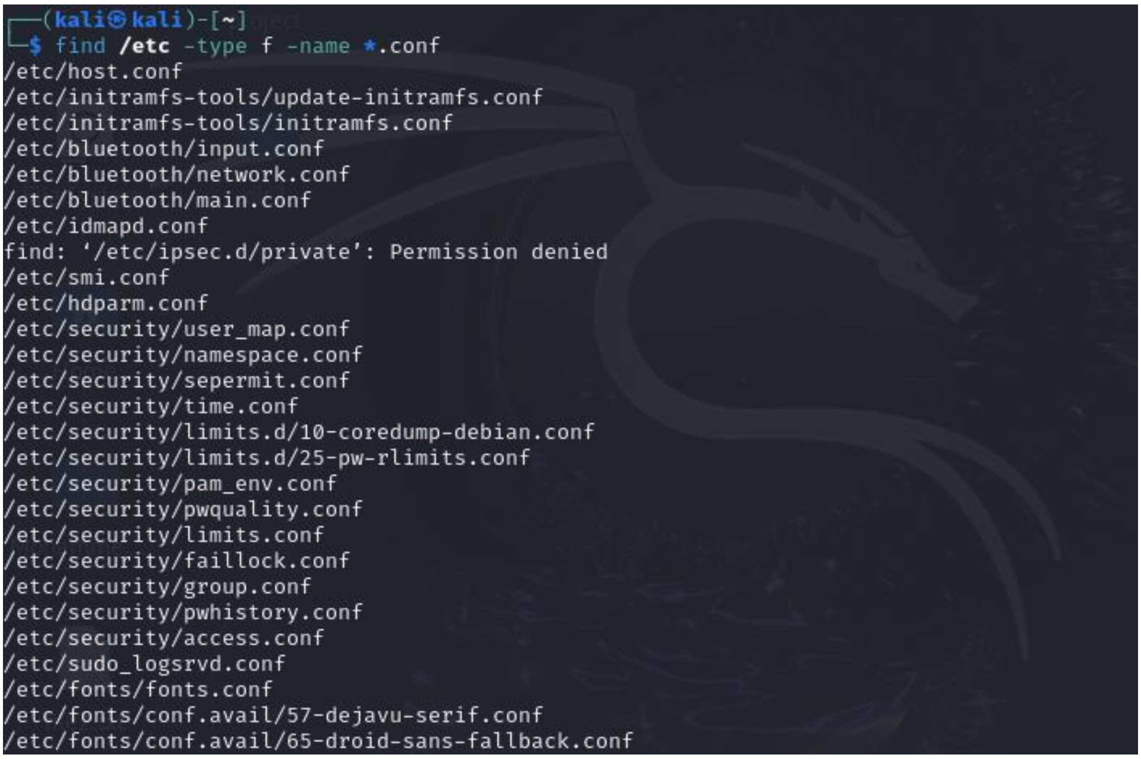
```
┌──(kali㉿kali)-[~]
└─$ locate shadow
/etc/gshadow
/etc/gshadow-
/etc/shadow
/etc/shadow-
/usr/bin/pgmdeshadow
/usr/bin/ppmshadow
/usr/include/gshadow.h
/usr/include/shadow.h
/usr/lib/modules/6.6.15-amd64/kernel/drivers/media/cec/usb/rainshadow
/usr/lib/modules/6.6.15-amd64/kernel/drivers/media/cec/usb/rainshadow/rainshadow-cec.ko.xz
/usr/lib/modules/6.8.11-amd64/kernel/drivers/media/cec/usb/rainshadow
/usr/lib/modules/6.8.11-amd64/kernel/drivers/media/cec/usb/rainshadow/rainshadow-cec.ko.xz
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/fragment_program_shadow.py
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/shadow.py
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/shadow_ambient.py
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/__pycache__/fragment_program_shadow.cpython-311.pyc
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/__pycache__/shadow.cpython-311.pyc
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/__pycache__/shadow_ambient.cpython-311.pyc
/usr/lib/python3/dist-packages/OpenGL/GL/EXT/shadow_funcs.py
/usr/lib/python3/dist-packages/OpenGL/GL/EXT/texture_shadow_lod.py
/usr/lib/python3/dist-packages/OpenGL/GL/EXT/__pycache__/shadow_funcs.cpython-311.pyc
/usr/lib/python3/dist-packages/OpenGL/GL/EXT/__pycache__/texture_shadow_lod.cpython-311.pyc
/usr/lib/python3/dist-packages/OpenGL/GL/SGIX/shadow.py
/usr/lib/python3/dist-packages/OpenGL/GL/SGIX/shadow_ambient.py
/usr/lib/python3/dist-packages/OpenGL/GL/SGIX/__pycache__/shadow.cpython-311.pyc
/usr/lib/python3/dist-packages/OpenGL/GL/SGIX/__pycache__/shadow_ambient.cpython-311.pyc
```



```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow
root:*:19870:0:99999:7:::
daemon:*:19870:0:99999:7:::
bin:*:19870:0:99999:7:::
sys:*:19870:0:99999:7:::
sync:*:19870:0:99999:7:::
games:*:19870:0:99999:7:::
man:*:19870:0:99999:7:::
lp:*:19870:0:99999:7:::
mail:*:19870:0:99999:7:::
news:*:19870:0:99999:7:::
uucp:*:19870:0:99999:7:::
proxy:*:19870:0:99999:7:::
www-data:*:19870:0:99999:7:::
backup:*:19870:0:99999:7:::
list:*:19870:0:99999:7:::
irc:*:19870:0:99999:7:::
_apt:*:19870:0:99999:7:::
```

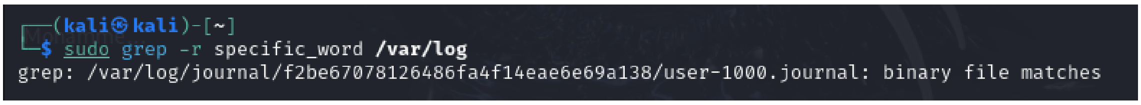
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

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



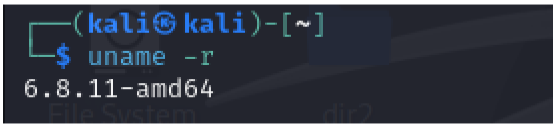
```
┌──(kali㉿kali)-[~]
└─$ find /etc -type f -name *.conf
/etc/host.conf
/etc/initramfs-tools/update-initramfs.conf
/etc/initramfs-tools/initramfs.conf
/etc/bluetooth/input.conf
/etc/bluetooth/network.conf
/etc/bluetooth/main.conf
/etc/idmapd.conf
find: '/etc/ipsec.d/private': Permission denied
/etc/smi.conf
/etc/hdparm.conf
/etc/security/user_map.conf
/etc/security/namespace.conf
/etc/security/sepermit.conf
/etc/security/time.conf
/etc/security/limits.d/10-coredump-debian.conf
/etc/security/limits.d/25-pw-rlimits.conf
/etc/security/pam_env.conf
/etc/security/pwquality.conf
/etc/security/limits.conf
/etc/security/faillock.conf
/etc/security/group.conf
/etc/security/pwhistory.conf
/etc/security/access.conf
/etc/sudo_logsrvd.conf
/etc/fonts/fonts.conf
/etc/fonts/conf.avail/57-dejavu-serif.conf
/etc/fonts/conf.avail/65-droid-sans-fallback.conf
```

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



```
┌──(kali㉿kali)-[~]
└─$ sudo grep -r specific_word /var/log
grep: /var/log/journal/f2be67078126486fa4f14eae6e69a138/user-1000.journal: binary file matches
```

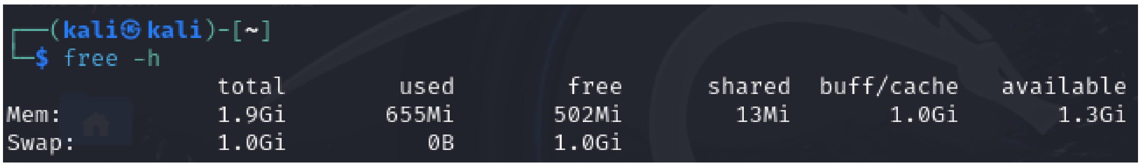
70. View the system's kernel version.



```
┌──(kali㉿kali)-[~]
└─$ uname -r
6.8.11-amd64
```

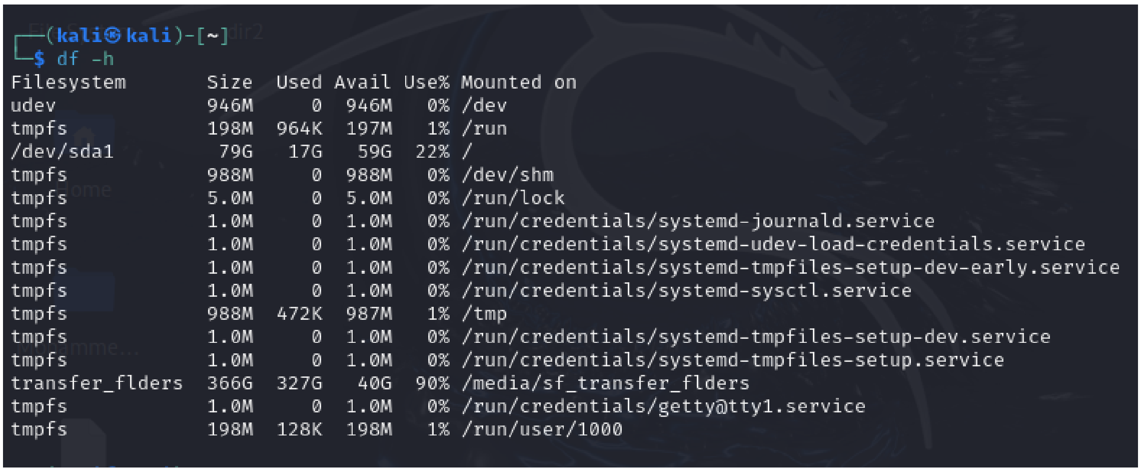
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

71. Display the system’s memory usage.



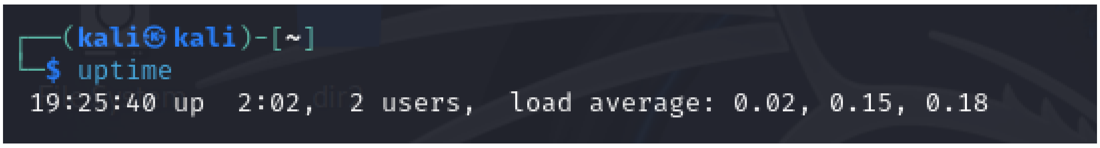
```
┌──(kali㉿kali)-[~]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       655Mi       502Mi        13Mi       1.0Gi       1.3Gi
Swap:          1.0Gi          0B       1.0Gi
```

72. Show the system’s disk usage.



```
┌──(kali㉿kali)-[~]
└─$ df -h
Filesystem       Size  Used Avail Use% Mounted on
udev             946M     0  946M   0% /dev
tmpfs            198M  964K  197M   1% /run
/dev/sda1         79G   17G   59G  22% /
tmpfs            988M     0  988M   0% /dev/shm
tmpfs            5.0M     0  5.0M   0% /run/lock
tmpfs            1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs            1.0M     0  1.0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs            1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs            1.0M     0  1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs            988M  472K  987M   1% /tmp
tmpfs            1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs            1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup.service
transfer_flders  366G  327G   40G  90% /media/sf_transfer_flders
tmpfs            1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs            198M  128K  198M   1% /run/user/1000
```

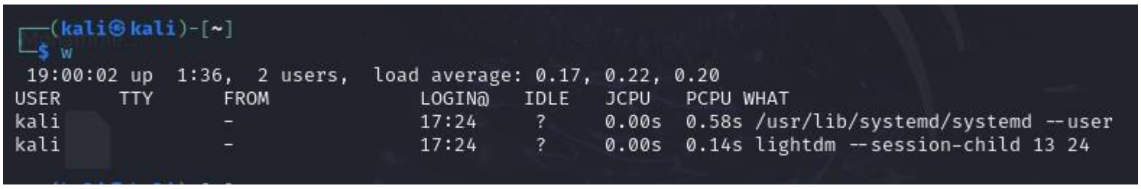
73. Check the system's uptime and load average.



```
┌──(kali㉿kali)-[~]
└─$ uptime
 19:25:40 up  2:02,  2 users,  load average: 0.02, 0.15, 0.18
```

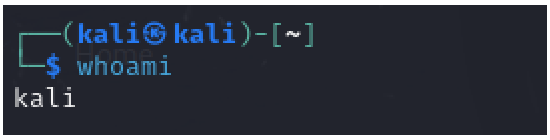
DR:Abdalrzaq Alsmawi
Name:Mohammed Abdalkreem Alhrazy group(2)

74. Display the current logged-in users.



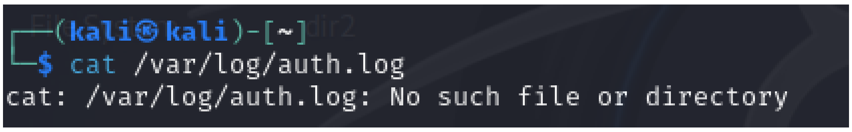
```
┌──(kali㉿kali)-[~]
└─$ w
 19:00:02 up  1:36,  2 users,  load average: 0.17, 0.22, 0.20
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
kali              -                17:24     ?     0.00s  0.58s /usr/lib/systemd/systemd --user
kali              -                17:24     ?     0.00s  0.14s lightdm --session-child 13 24
```

75. Check the identity of the current user.



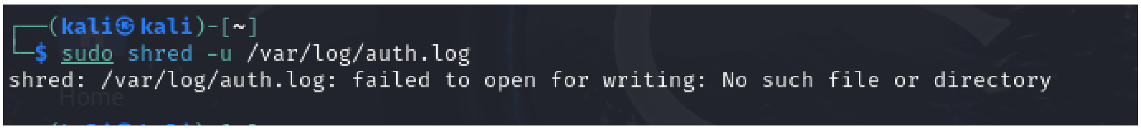
```
┌──(kali㉿kali)-[~]
└─$ whoami
kali
```

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



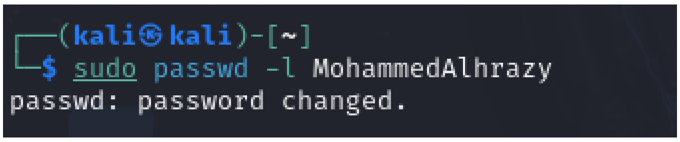
```
┌──(kali㉿kali)-[~]
└─$ cat /var/log/auth.log
cat: /var/log/auth.log: No such file or directory
```

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



```
┌──(kali㉿kali)-[~]
└─$ 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.

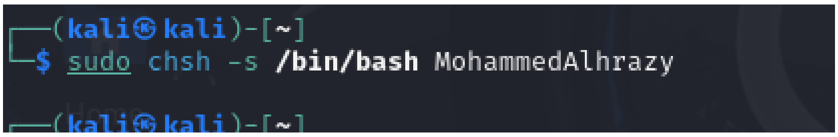


```
┌──(kali㉿kali)-[~]
└─$ sudo passwd -l MohammedAlhrazy
passwd: password changed.
```

DR:Abdalrzaq Alsmawi

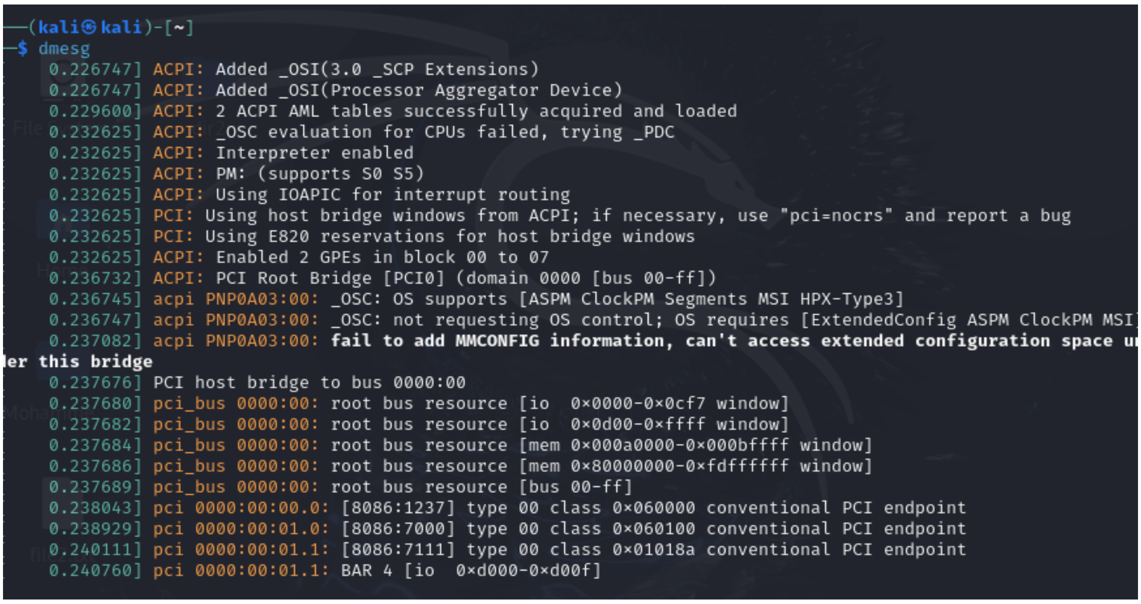
Name:Mohammed Abdalkreem Alhrazy group(2)

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



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

┌──(kali㉿kali)-[~]
```

80. Display the system's boot messages



```
──(kali㉿kali)-[~]
─$ dmesg
    0.226747] ACPI: Added _OSI(3.0 _SCP Extensions)
    0.226747] ACPI: Added _OSI(Processor Aggregator Device)
    0.229600] ACPI: 2 ACPI AML tables successfully acquired and loaded
    0.232625] ACPI: _OSC evaluation for CPUs failed, trying _PDC
    0.232625] ACPI: Interpreter enabled
    0.232625] ACPI: PM: (supports S0 S5)
    0.232625] ACPI: Using IOAPIC for interrupt routing
    0.232625] PCI: Using host bridge windows from ACPI; if necessary, use "pci=nocrs" and report a bug
    0.232625] PCI: Using E820 reservations for host bridge windows
    0.232625] ACPI: Enabled 2 GPEs in block 00 to 07
    0.236732] ACPI: PCI Root Bridge [PCI0] (domain 0000 [bus 00-ff])
    0.236745] acpi PNP0A03:00: _OSC: OS supports [ASPM ClockPM Segments MSI HPX-Type3]
    0.236747] acpi PNP0A03:00: _OSC: not requesting OS control; OS requires [ExtendedConfig ASPM ClockPM MSI]
    0.237082] acpi PNP0A03:00: fail to add MMCONFIG information, can't access extended configuration space un
der this bridge
    0.237676] PCI host bridge to bus 0000:00
    0.237680] pci_bus 0000:00: root bus resource [io  0×0000-0×0cf7 window]
    0.237682] pci_bus 0000:00: root bus resource [io  0×0d00-0×ffff window]
    0.237684] pci_bus 0000:00: root bus resource [mem 0×000a0000-0×000bffff window]
    0.237686] pci_bus 0000:00: root bus resource [mem 0×80000000-0×fdffffff window]
    0.237689] pci_bus 0000:00: root bus resource [bus 00-ff]
    0.238043] pci 0000:00:00.0: [8086:1237] type 00 class 0×060000 conventional PCI endpoint
    0.238929] pci 0000:00:01.0: [8086:7000] type 00 class 0×060100 conventional PCI endpoint
    0.240111] pci 0000:00:01.1: [8086:7111] type 00 class 0×01018a conventional PCI endpoint
    0.240760] pci 0000:00:01.1: BAR 4 [io  0×d000-0×d00f]
```