Mid exam

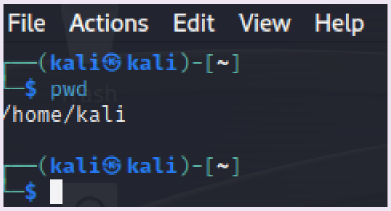
عمل الطالبة/ عُمر خالد الشقلي

م/ عبد الرزاق السماوي

Section 1: File and Directory Management

1. Display the current working directory.

   Pwd

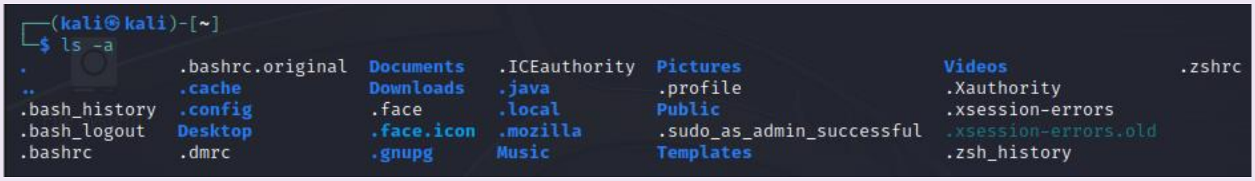


File Actions Edit View Help

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

┌──(kali㉿kali)-[~]
└─$ 
```

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

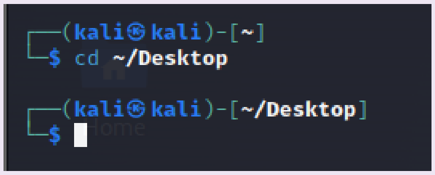
   ls -la



```
┌──(kali㉿kali)-[~]
└─$ ls -a
.              .bashrc.original  Documents   .ICEauthority  Pictures                    Videos                .zshrc
..             .cache            Downloads   .java          .profile                    .Xauthority
.bash_history  .config           .face       .local         Public                      .xsession-errors
.bash_logout   Desktop           .face.icon  .mozilla       .sudo_as_admin_successful   .xsession-errors.old
.bashrc        .dmrc             .gnupg      Music          Templates                   .zsh_history
```

3. Change your directory to the `Desktop`.

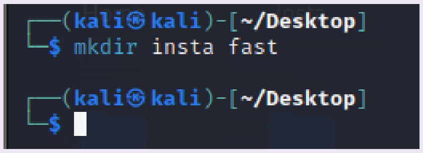
   cd ~/Desktop



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

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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

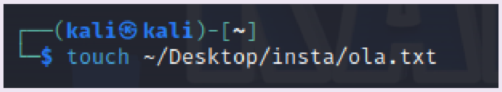
   mkdir dir1 dir2



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

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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

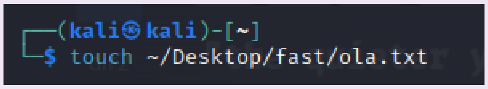
   touch dir1/file1.txt



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

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

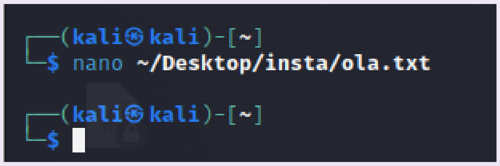
   touch dir2/file2.txt



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

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

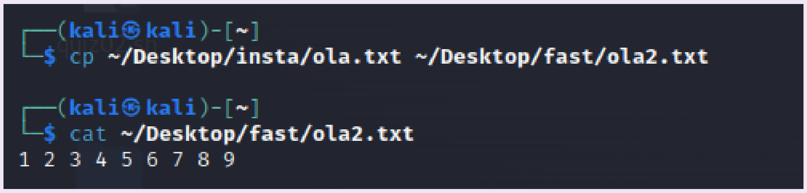
   nano dir1/file1.txt



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

┌──(kali㉿kali)-[~]
└─$ █
```

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

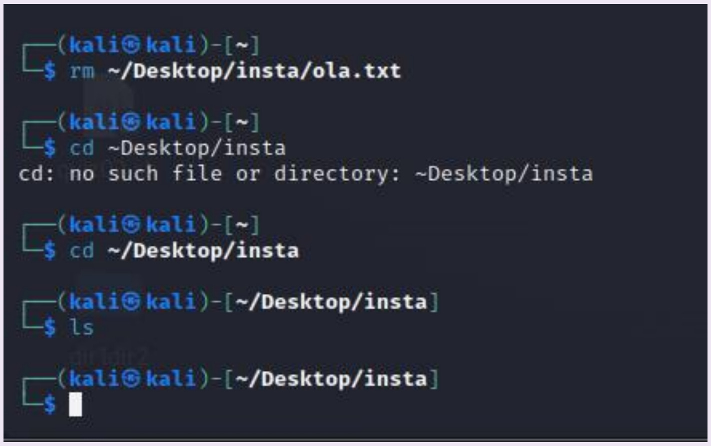
   cp dir1/file1.txt dir2/file2.txt



```
┌──(kali㉿kali)-[~]
└─$ cp ~/Desktop/insta/ola.txt ~/Desktop/fast/ola2.txt

┌──(kali㉿kali)-[~]
└─$ cat ~/Desktop/fast/ola2.txt
1 2 3 4 5 6 7 8 9
```

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

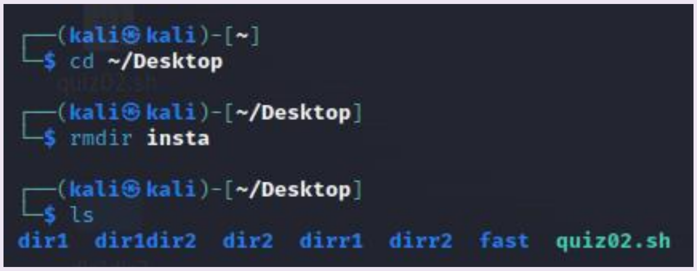
   rm dir1/file.txt



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

┌──(kali㉿kali)-[~]
└─$ cd ~Desktop/insta
cd: no such file or directory: ~Desktop/insta

┌──(kali㉿kali)-[~]
└─$ cd ~/Desktop/insta

┌──(kali㉿kali)-[~/Desktop/insta]
└─$ ls

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

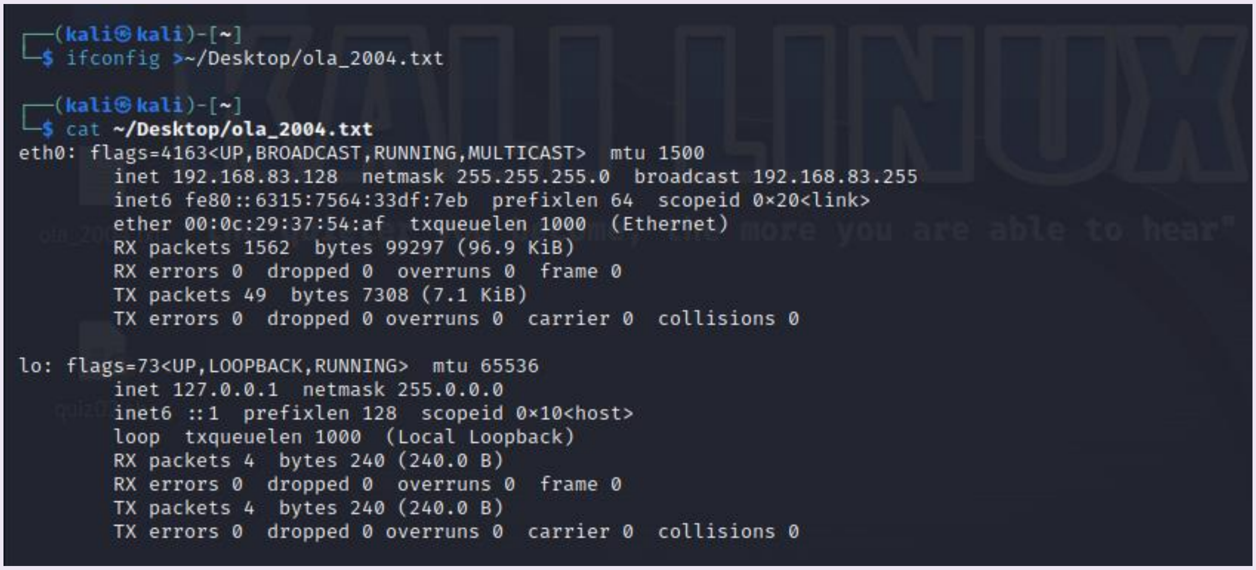
10. Remove the directory `dir1` from the Desktop.

rmdir dir1



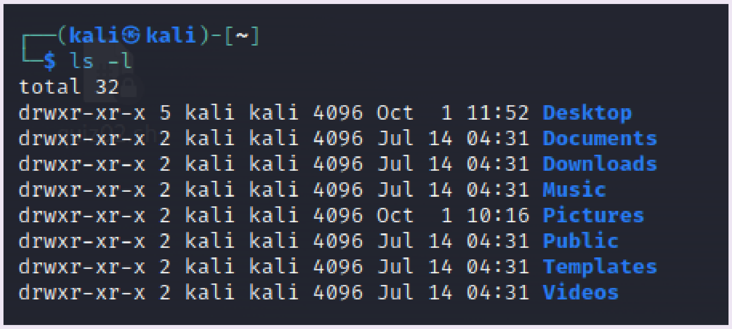
```
┌──(kali㉿kali)-[~]
└─$ cd ~/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ rmdir insta

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
dir1  dir1dir2  dir2  dirr1  dirr2  fast  quiz02.sh
```

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



```
┌──(kali㉿kali)-[~]
└─$ ifconfig >~/Desktop/ola_2004.txt

┌──(kali㉿kali)-[~]
└─$ cat ~/Desktop/ola_2004.txt
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.83.128  netmask 255.255.255.0  broadcast 192.168.83.255
        inet6 fe80::6315:7564:33df:7eb  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:37:54:af  txqueuelen 1000  (Ethernet)
        RX packets 1562  bytes 99297 (96.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49  bytes 7308 (7.1 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 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  collisions 0
```

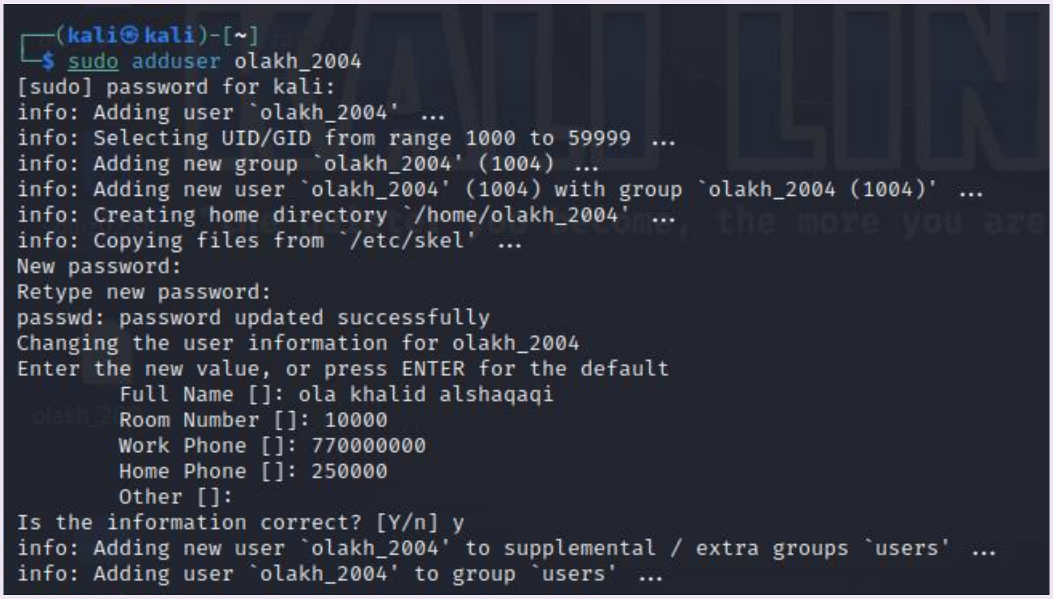
12. Open the Desktop folder and show all files with detailed information.



```
┌──(kali㉿kali)-[~]
└─$ ls -l
total 32
drwxr-xr-x 5 kali kali 4096 Oct  1 11:52 Desktop
drwxr-xr-x 2 kali kali 4096 Jul 14 04:31 Documents
drwxr-xr-x 2 kali kali 4096 Jul 14 04:31 Downloads
drwxr-xr-x 2 kali kali 4096 Jul 14 04:31 Music
drwxr-xr-x 2 kali kali 4096 Oct  1 10:16 Pictures
drwxr-xr-x 2 kali kali 4096 Jul 14 04:31 Public
drwxr-xr-x 2 kali kali 4096 Jul 14 04:31 Templates
drwxr-xr-x 2 kali kali 4096 Jul 14 04:31 Videos
```

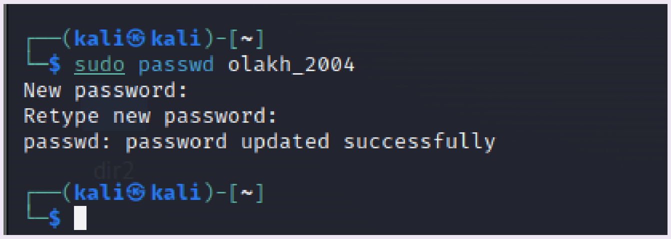
Section 2: Users and Groups Management

13. Create a new user with your name.



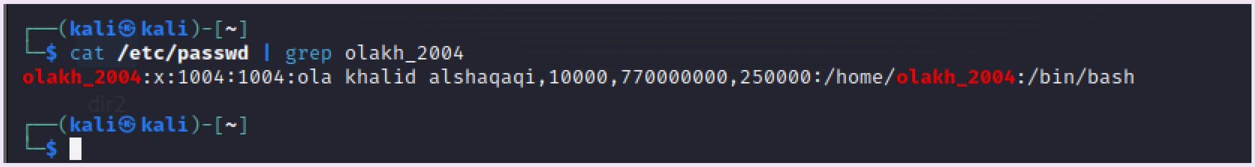
```
┌──(kali㉿kali)-[~]
└─$ sudo adduser olakh_2004
[sudo] password for kali:
info: Adding user `olakh_2004' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `olakh_2004' (1004) ...
info: Adding new user `olakh_2004' (1004) with group `olakh_2004 (1004)' ...
info: Creating home directory `/home/olakh_2004' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for olakh_2004
Enter the new value, or press ENTER for the default
        Full Name []: ola khalid alshaqaqi
        Room Number []: 10000
        Work Phone []: 770000000
        Home Phone []: 250000
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `olakh_2004' to supplemental / extra groups `users' ...
info: Adding user `olakh_2004' to group `users' ...
```

14. Set a password for your user.



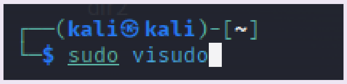
```
┌──(kali㉿kali)-[~]
└─$ sudo passwd olakh_2004
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ 
```

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

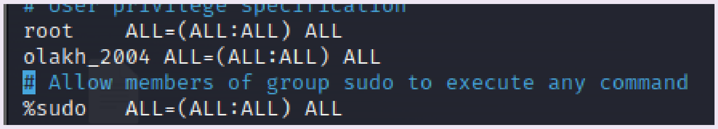


```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd | grep olakh_2004
olakh_2004:x:1004:1004:ola khalid alshaqaqi,10000,770000000,250000:/home/olakh_2004:/bin/bash

┌──(kali㉿kali)-[~]
└─$ 
```

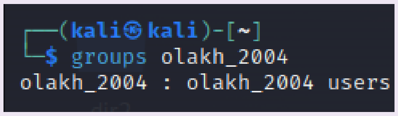
16. Add your user to the file that gives administrative privileges.



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

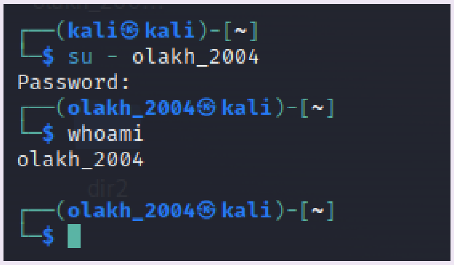


```
# User privilege specification
root    ALL=(ALL:ALL) ALL
olakh_2004 ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```



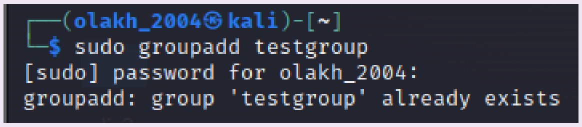
```
┌──(kali㉿kali)-[~]
└─$ groups olakh_2004
olakh_2004 : olakh_2004 users
```

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



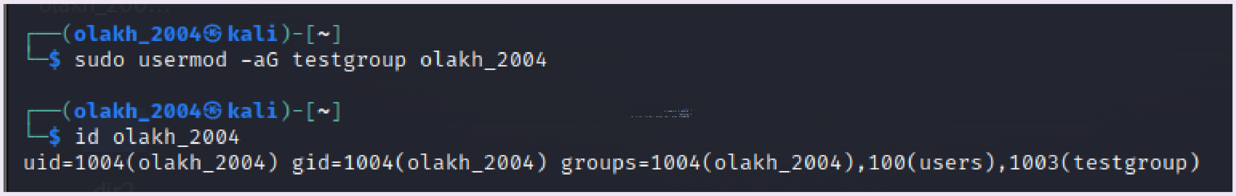
```
┌──(kali㉿kali)-[~]
└─$ su - olakh_2004
Password:
┌──(olakh_2004㉿kali)-[~]
└─$ whoami
olakh_2004

┌──(olakh_2004㉿kali)-[~]
└─$ 
```

18. Create a new group named `testgroup`



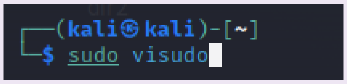
```
┌──(olakh_2004㉿kali)-[~]
└─$ sudo groupadd testgroup
[sudo] password for olakh_2004:
groupadd: group 'testgroup' already exists
```

19. Add your user to `testgroup`.

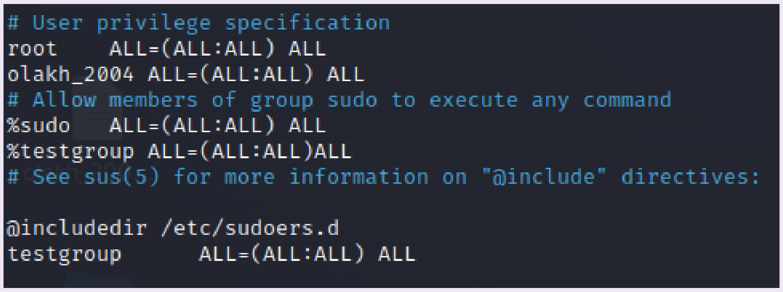


```
┌──(olakh_2004㉿kali)-[~]
└─$ sudo usermod -aG testgroup olakh_2004

┌──(olakh_2004㉿kali)-[~]
└─$ id olakh_2004
uid=1004(olakh_2004) gid=1004(olakh_2004) groups=1004(olakh_2004),100(users),1003(testgroup)
```

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

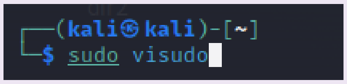


```
┌──(kali㉿kali)-[~]
└─$ sudo visudo
```

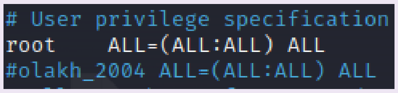


```
# User privilege specification
root    ALL=(ALL:ALL) ALL
olakh_2004 ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%testgroup ALL=(ALL:ALL)ALL
# See sus(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
testgroup      ALL=(ALL:ALL) ALL
```

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

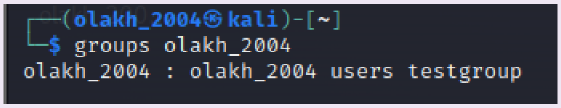


```
┌──(kali㉿kali)-[~]
└─$ sudo visudo
```



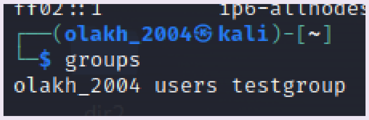
```
# User privilege specification
root    ALL=(ALL:ALL) ALL
#olakh_2004 ALL=(ALL:ALL) ALL
```

22. Check if your user still has administrative privileges.



```
┌──(olakh_2004㉿kali)-[~]
└─$ groups olakh_2004
olakh_2004 : olakh_2004 users testgroup
```

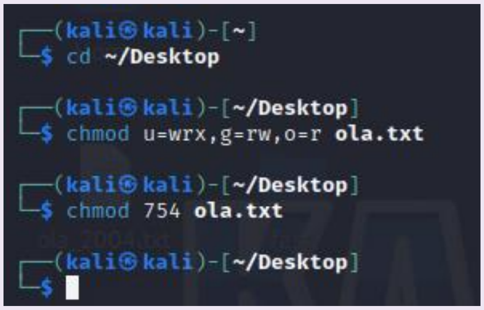
23. Check which groups your user belongs to.



```
ff02::1         ip6-allnodes
┌──(olakh_2004㉿kali)-[~]
└─$ groups
olakh_2004 users testgroup
```

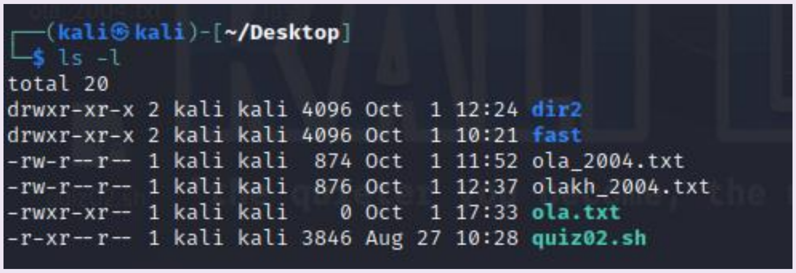
Section 3: Permissions and Ownership

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.



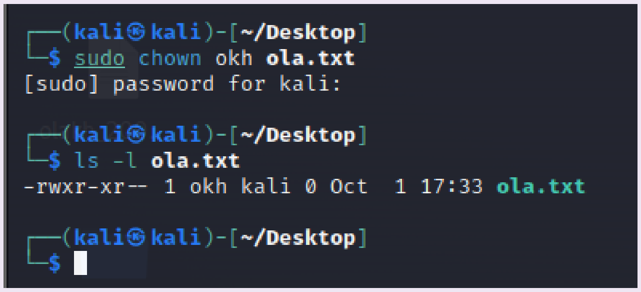
```
┌──(kali㉿kali)-[~]
└─$ cd ~/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ chmod u=wrx,g=rw,o=r ola.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 754 ola.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

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



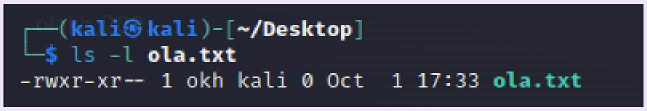
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l
total 20
drwxr-xr-x 2 kali kali 4096 Oct  1 12:24 dir2
drwxr-xr-x 2 kali kali 4096 Oct  1 10:21 fast
-rw-r--r-- 1 kali kali  874 Oct  1 11:52 ola_2004.txt
-rw-r--r-- 1 kali kali  876 Oct  1 12:37 olakh_2004.txt
-rwxr-xr-- 1 kali kali    0 Oct  1 17:33 ola.txt
-r-xr--r-- 1 kali kali 3846 Aug 27 10:28 quiz02.sh
```

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



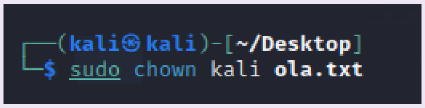
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown okh ola.txt
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ola.txt
-rwxr-xr-- 1 okh kali 0 Oct  1 17:33 ola.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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



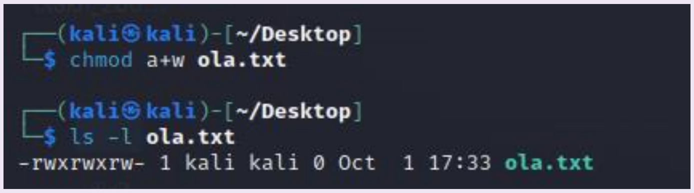
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ola.txt
-rwxr-xr-- 1 okh kali 0 Oct  1 17:33 ola.txt
```

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



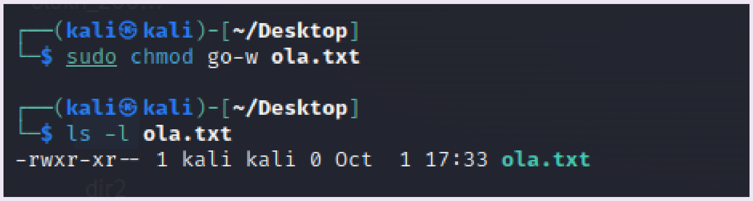
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown kali ola.txt
```

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



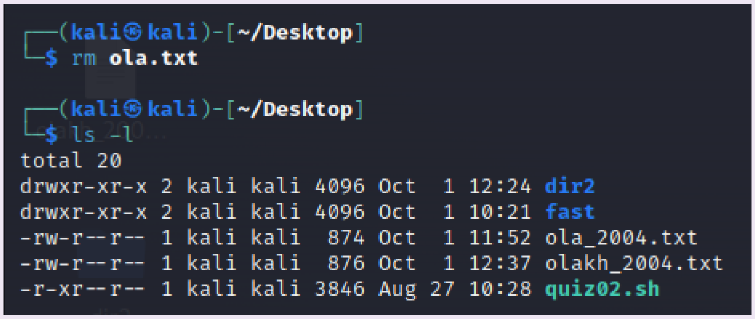
```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod a+w ola.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ola.txt
-rwxrwxrw- 1 kali kali 0 Oct  1 17:33 ola.txt
```

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



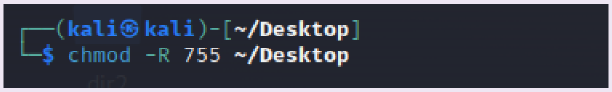
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chmod go-w ola.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ola.txt
-rwxr-xr-- 1 kali kali 0 Oct  1 17:33 ola.txt
```

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



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

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l
total 20
drwxr-xr-x 2 kali kali 4096 Oct  1 12:24 dir2
drwxr-xr-x 2 kali kali 4096 Oct  1 10:21 fast
-rw-r--r-- 1 kali kali  874 Oct  1 11:52 ola_2004.txt
-rw-r--r-- 1 kali kali  876 Oct  1 12:37 olakh_2004.txt
-r-xr--r-- 1 kali kali 3846 Aug 27 10:28 quiz02.sh
```

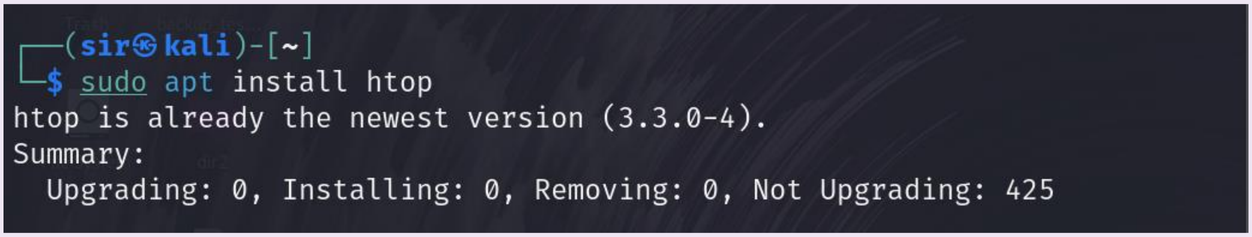
32. What command would you use to recursively change the permissions of all files and directories inside a folder named `project` to `755`.



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

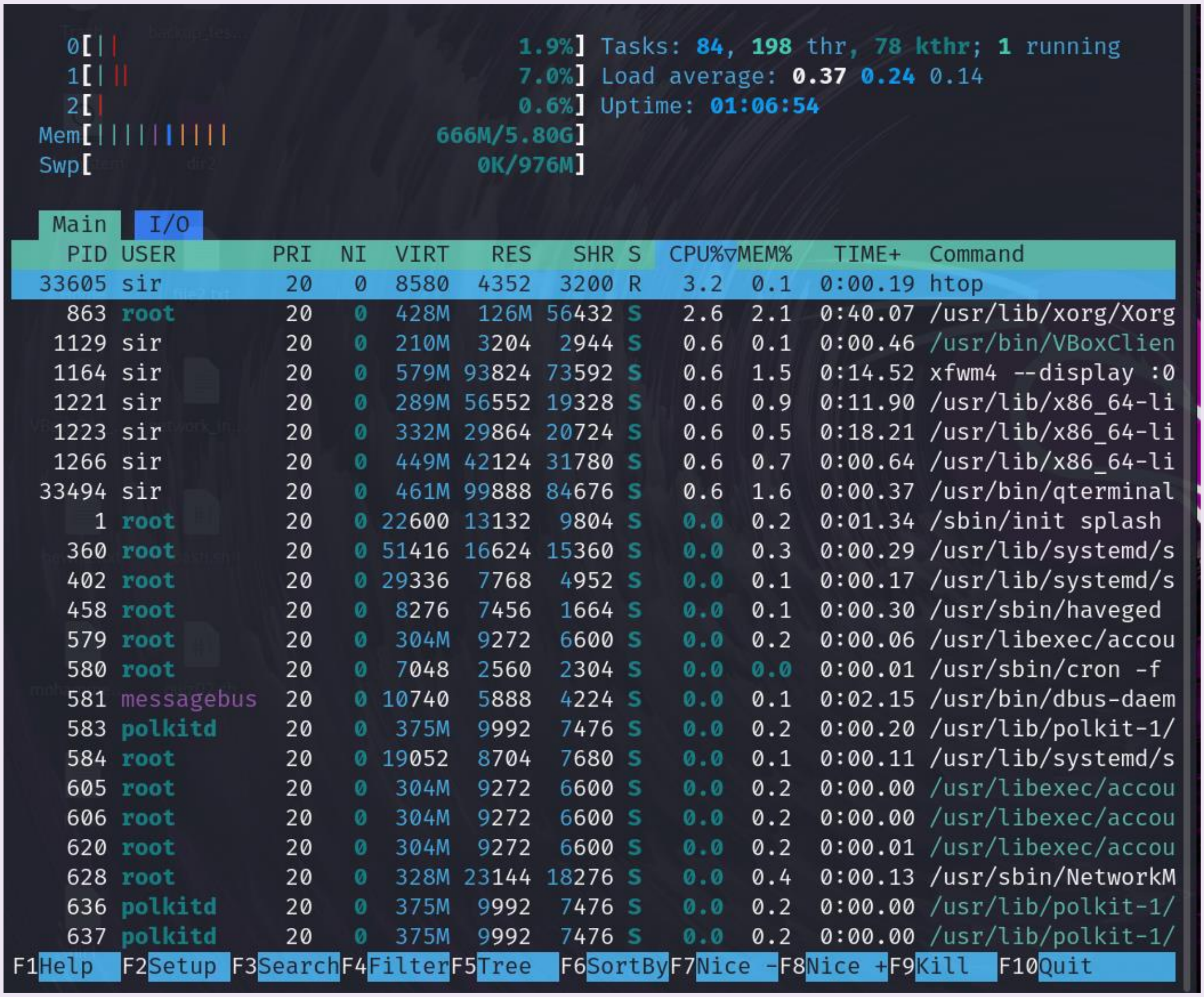
Section 4: Process Management

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



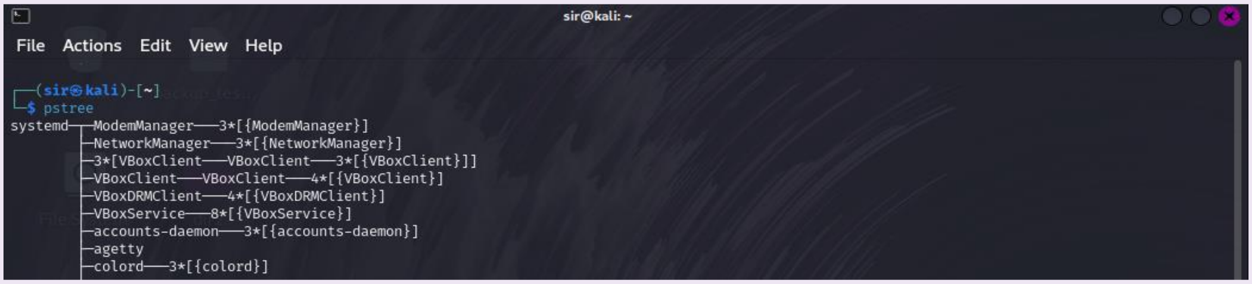
```
┌──(sir㉿kali)-[~]
└─$ sudo apt install htop
htop is already the newest version (3.3.0-4).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 425
```

Display all running processes.



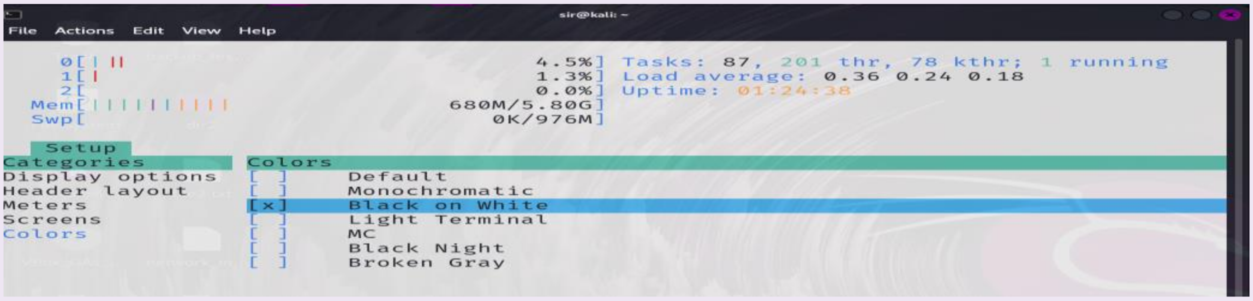
```
    0[||                          1.9%] Tasks: 84, 198 thr, 78 kthr; 1 running
    1[|||                         7.0%] Load average: 0.37 0.24 0.14
    2[|                           0.6%] Uptime: 01:06:54
  Mem[||||||||||            666M/5.80G]
  Swp[                         0K/976M]

  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/VBoxClien
   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 F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

34. Display a tree of all running processes.



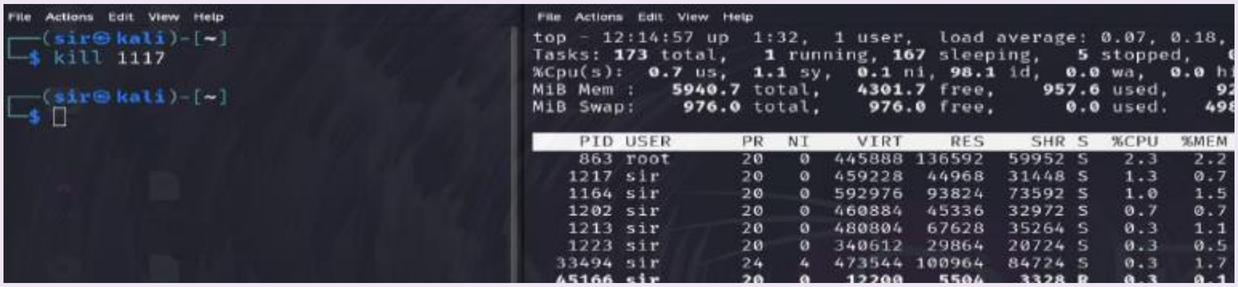
```
┌──(sir㉿kali)-[~]
└─$ pstree
systemd─┬─ModemManager───3*[{ModemManager}]
        ├─NetworkManager───3*[{NetworkManager}]
        ├─3*[VBoxClient───VBoxClient───3*[{VBoxClient}]]
        ├─VBoxClient───VBoxClient───4*[{VBoxClient}]
        ├─VBoxDRMClient───4*[{VBoxDRMClient}]
        ├─VBoxService───8*[{VBoxService}]
        ├─accounts-daemon───3*[{accounts-daemon}]
        ├─agetty
        ├─colord───3*[{colord}]
```

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



```
    0[| ||                          4.5%]  Tasks: 87, 201 thr, 78 kthr; 1 running
    1[|                             1.3%]  Load average: 0.36 0.24 0.18
    2[                              0.0%]  Uptime: 01:24:38
  Mem[||||||||||            680M/5.80G]
  Swp[                         0K/976M]

   Setup
Categories          Colors
Display options     [ ]     Default
Header layout       [ ]     Monochromatic
Meters              [x]     Black on White
Screens             [ ]     Light Terminal
Colors              [ ]     MC
                    [ ]     Black Night
                    [ ]     Broken Gray
```

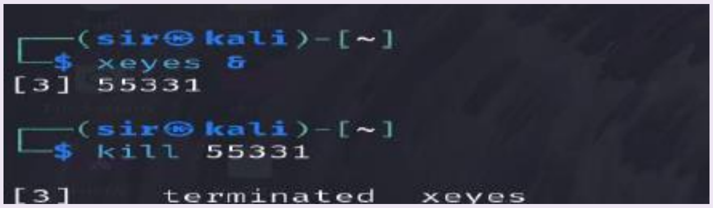
36. Kill a process with a specific PID.



```
┌──(sir㉿kali)-[~]
└─$ kill 1117

┌──(sir㉿kali)-[~]
└─$ 
```

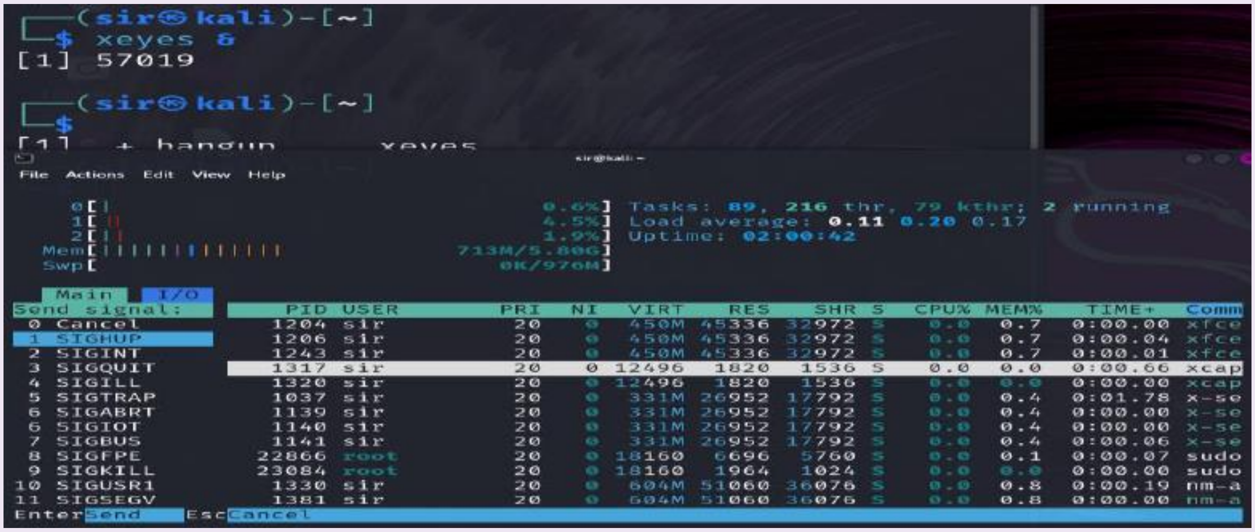
```
top - 12:14:57 up  1:32,  1 user,  load average: 0.07, 0.18,
Tasks: 173 total,   1 running, 167 sleeping,   5 stopped,
%Cpu(s):  0.7 us,  1.1 sy,  0.1 ni, 98.1 id,  0.0 wa,  0.0 hi
MiB Mem :   5940.7 total,   4301.7 free,    957.6 used,    92
MiB Swap:    976.0 total,    976.0 free,      0.0 used.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

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM
    863 root      20   0  445888 136592  59952 S   2.3   2.2
   1217 sir       20   0  459228  44968  31448 S   1.3   0.7
   1164 sir       20   0  592976  93824  73592 S   1.0   1.5
   1202 sir       20   0  460884  45336  32972 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
```

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



```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[3] 55331

┌──(sir㉿kali)-[~]
└─$ kill 55331

[3]    terminated  xeyes
```

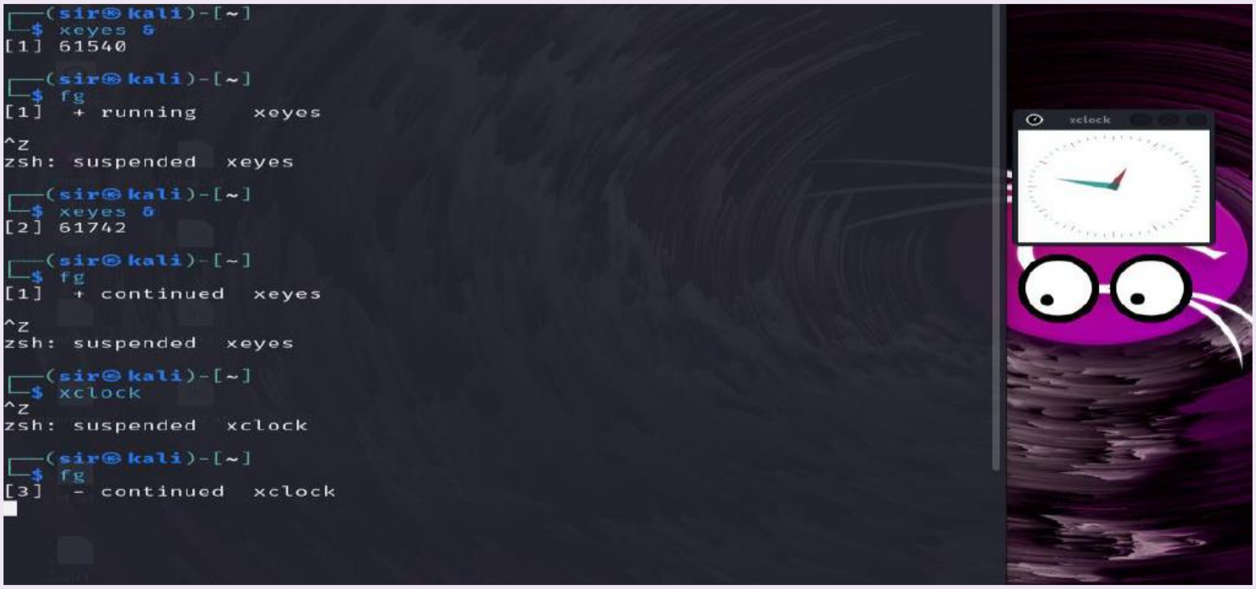
38. Restart the application, then stop it using the interactive process viewer.



```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[1] 57019

┌──(sir㉿kali)-[~]
└─$
[1]  + hangup       xeyes
```

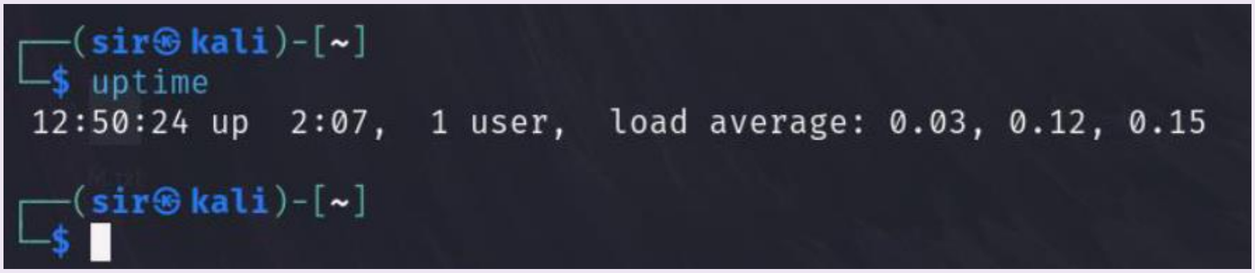
```
    0[|                                 0.6%]  Tasks: 89, 216 thr, 79 kthr; 2 running
    1[||                                4.5%]  Load average: 0.11 0.20 0.17
    2[||                                1.9%]  Uptime: 02:00:42
  Mem[||||||||||||||               713M/5.80G]
  Swp[                                0K/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
 6 SIGIOT         1140 sir         20   0  331M 26952 17792 S   0.0  0.4  0:00.00 x-se
 7 SIGBUS         1141 sir         20   0  331M 26952 17792 S   0.0  0.4  0:00.06 x-se
 8 SIGFPE        22866 root        20   0 18160  6696  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
```

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



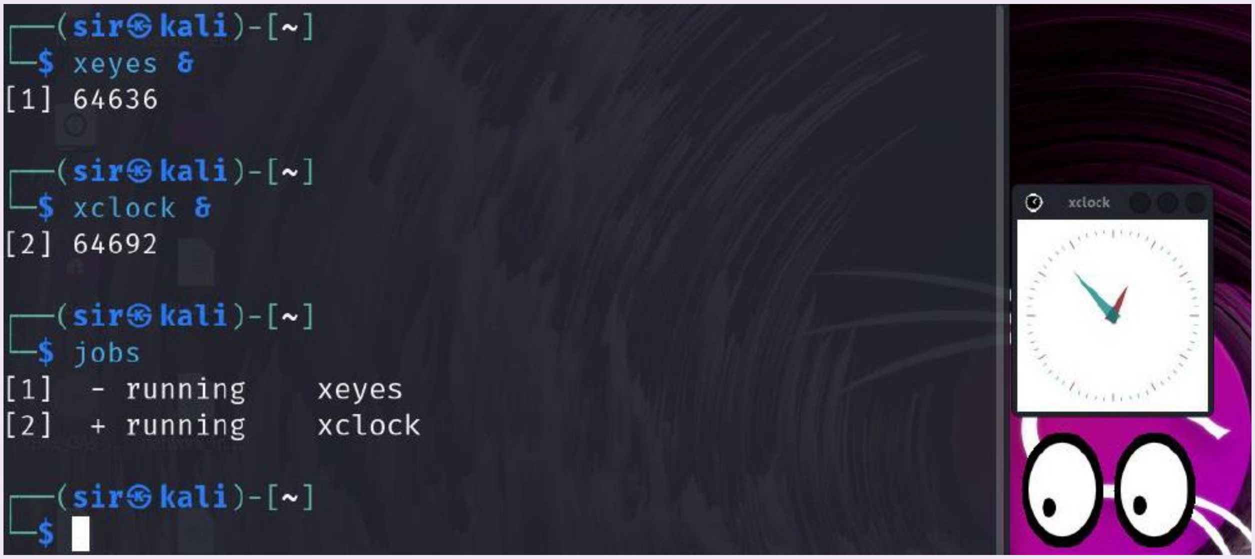
```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[1] 61540

┌──(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
```

40. Check how long the system has been running.



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

┌──(sir㉿kali)-[~]
└─$ 
```

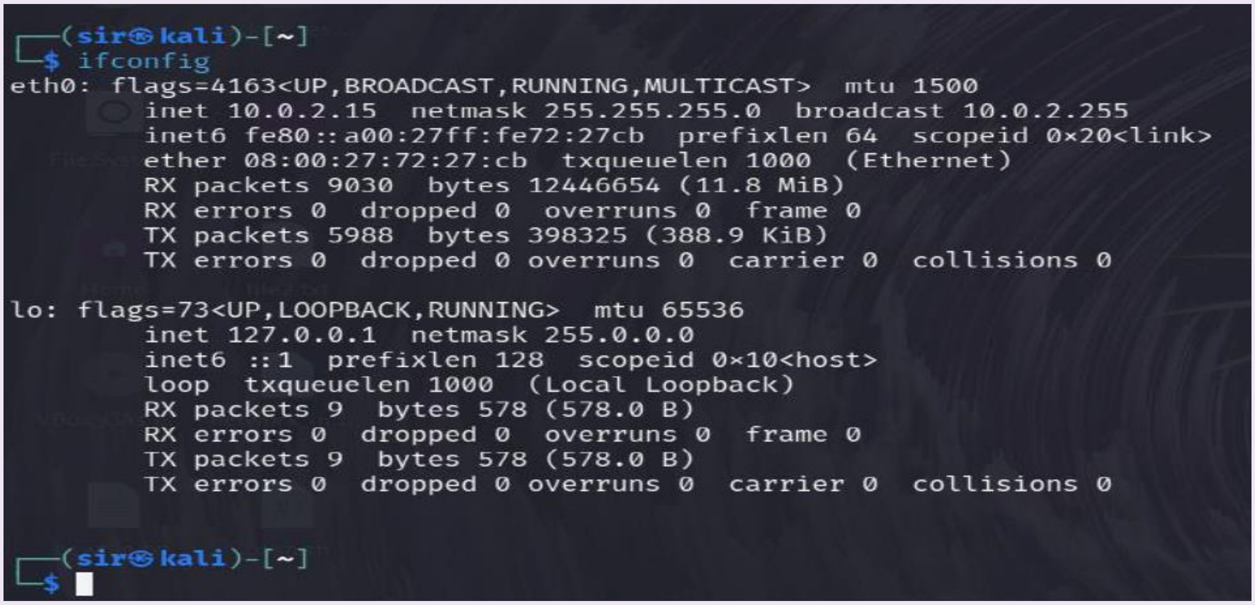
41. List all jobs running in the background.



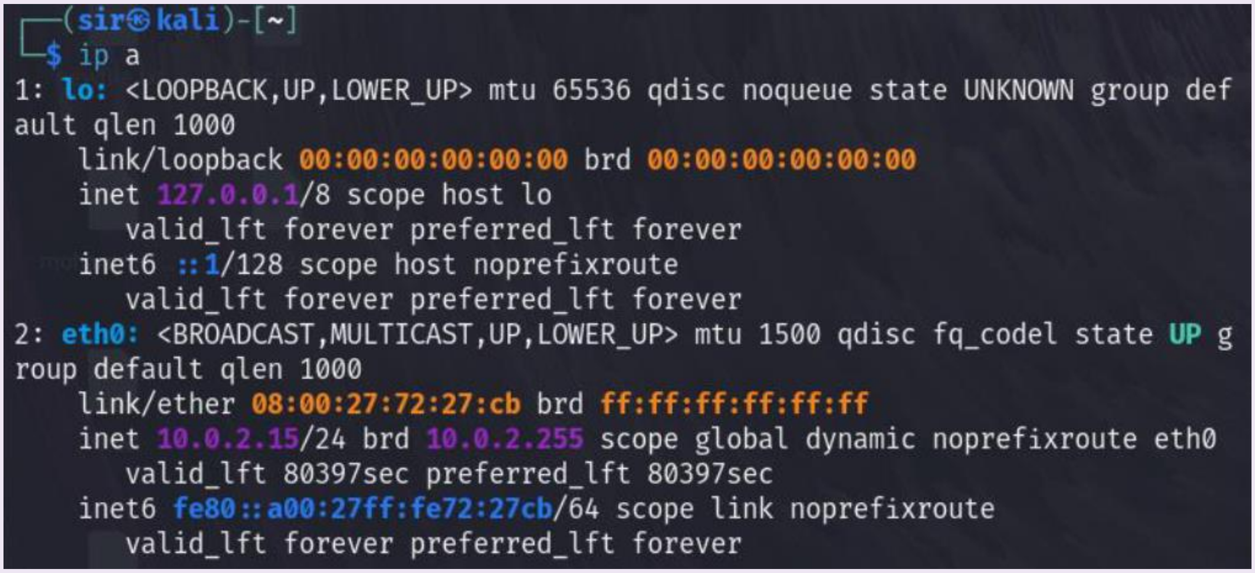
```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[1] 64636

┌──(sir㉿kali)-[~]
└─$ xclock &
[2] 64692

┌──(sir㉿kali)-[~]
└─$ jobs
[1]  - running    xeyes
[2]  + running    xclock

┌──(sir㉿kali)-[~]
└─$ 
```

Section 5: Networking Commands

42. Display the network configuration.

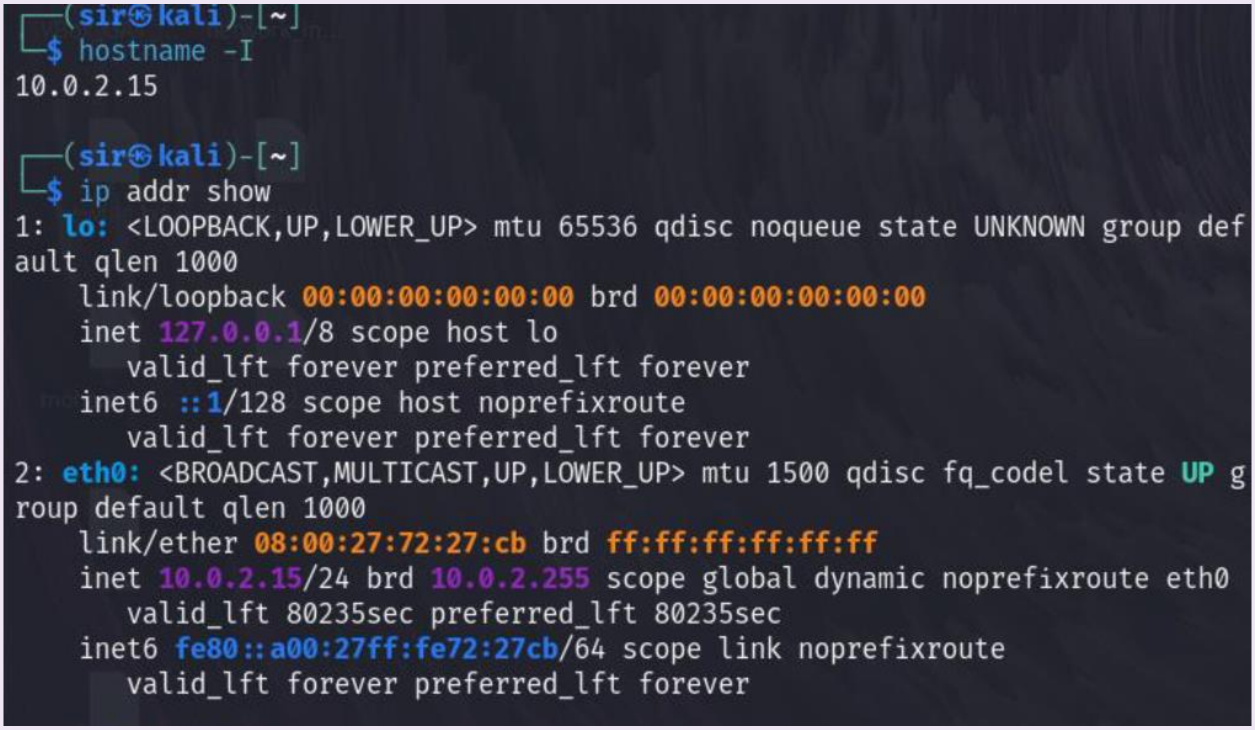


```
┌──(sir㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe72:27cb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:72:27:cb  txqueuelen 1000  (Ethernet)
        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)-[~]
└─$ █
```



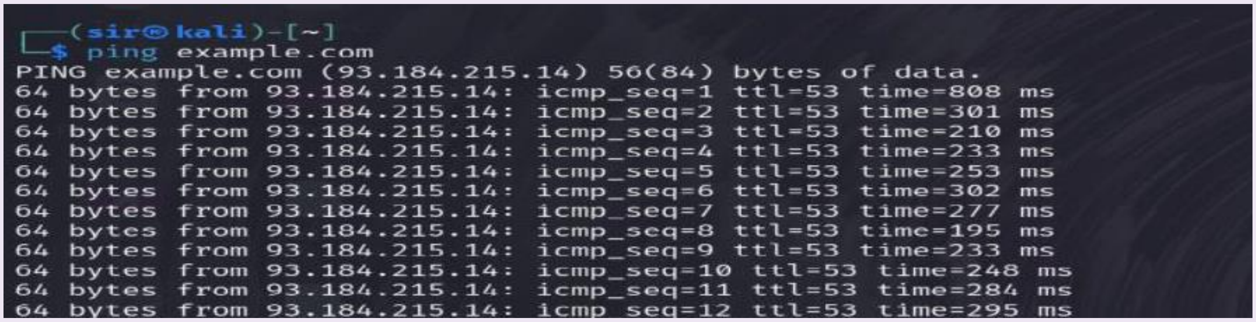
```
┌──(sir㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup 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
```

43. Check the IP address of your machine.



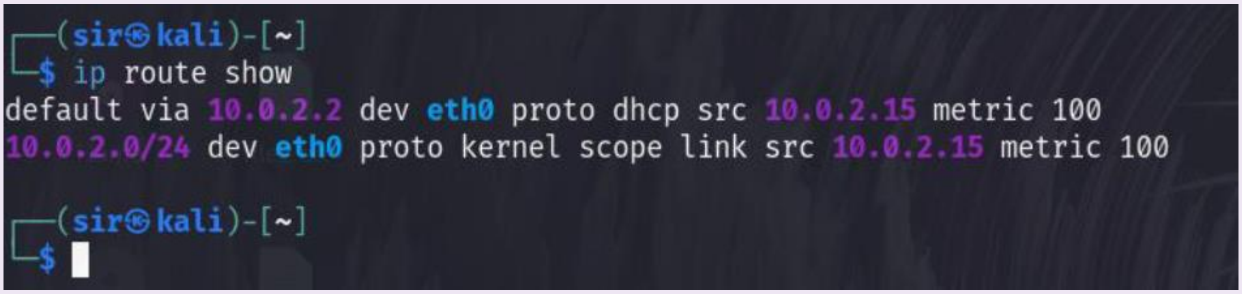
```
┌──(sir㉿kali)-[~]
└─$ hostname -I
10.0.2.15

┌──(sir㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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 g
roup 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
```

44. Test connectivity to an external server.



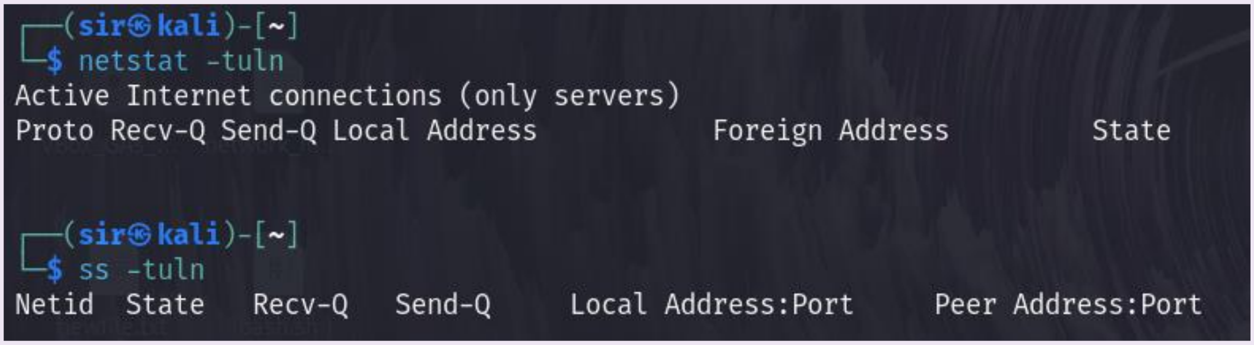
```
┌──(sir㉿kali)-[~]
└─$ ping example.com
PING example.com (93.184.215.14) 56(84) bytes of data.
64 bytes from 93.184.215.14: icmp_seq=1 ttl=53 time=808 ms
64 bytes from 93.184.215.14: icmp_seq=2 ttl=53 time=301 ms
64 bytes from 93.184.215.14: icmp_seq=3 ttl=53 time=210 ms
64 bytes from 93.184.215.14: 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
```

45. Display the routing table.



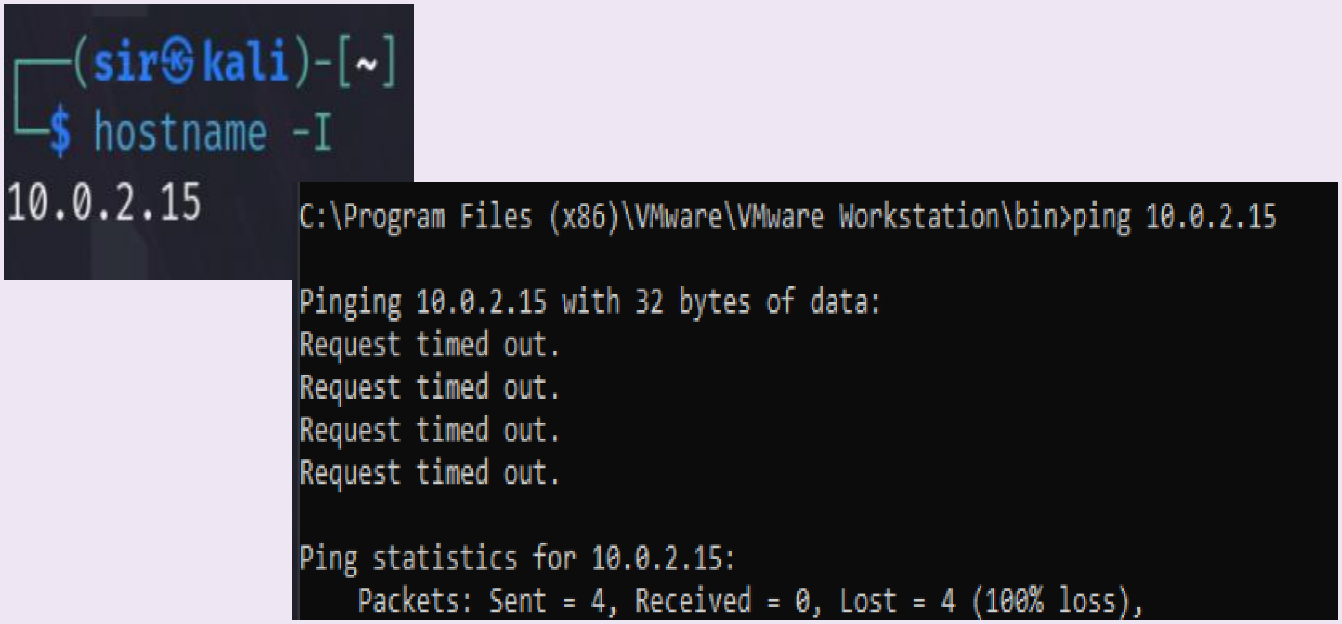
```
┌──(sir㉿kali)-[~]
└─$ ip route show
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100

┌──(sir㉿kali)-[~]
└─$ █
```

46. Check the open ports and active connections.



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


┌──(sir㉿kali)-[~]
└─$ ss -tuln
Netid  State   Recv-Q   Send-Q     Local Address:Port     Peer Address:Port
```

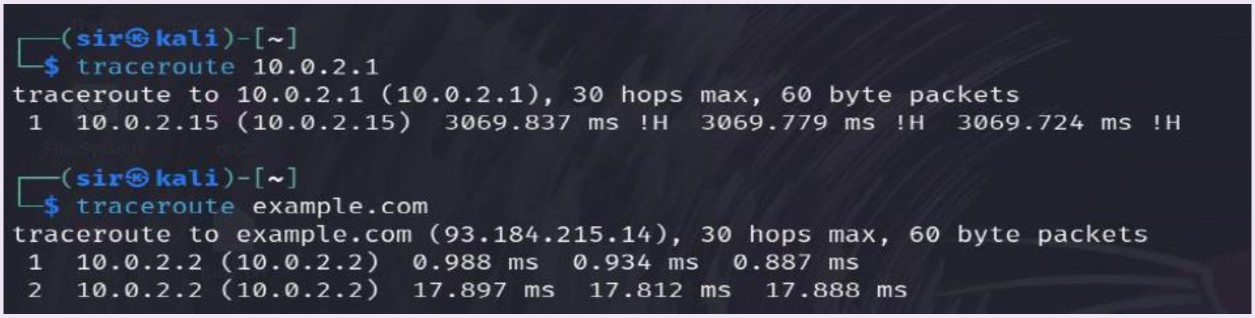
47. Show the IP address of the host machine and the VM, and verify if they are on the same network.



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

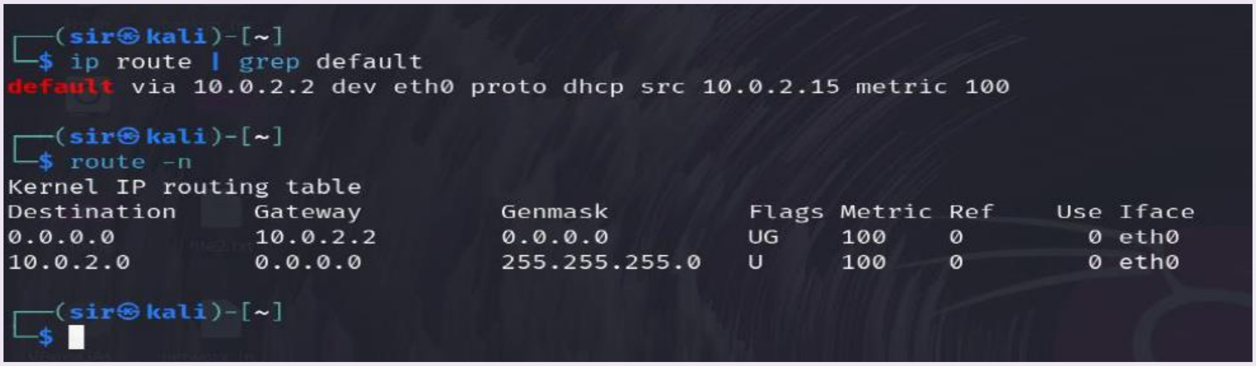
```
C:\Program Files (x86)\VMware\VMware Workstation\bin>ping 10.0.2.15

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),
```

48. Trace the route to an external server.



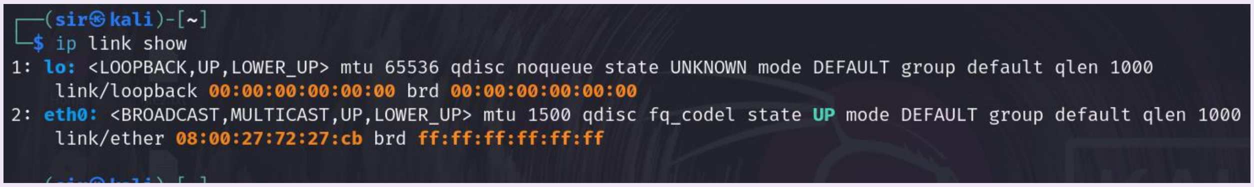
```
┌──(sir㉿kali)-[~]
└─$ traceroute 10.0.2.1
traceroute to 10.0.2.1 (10.0.2.1), 30 hops max, 60 byte packets
 1  10.0.2.15 (10.0.2.15)  3069.837 ms !H  3069.779 ms !H  3069.724 ms !H

┌──(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
```

49. Find out the default gateway



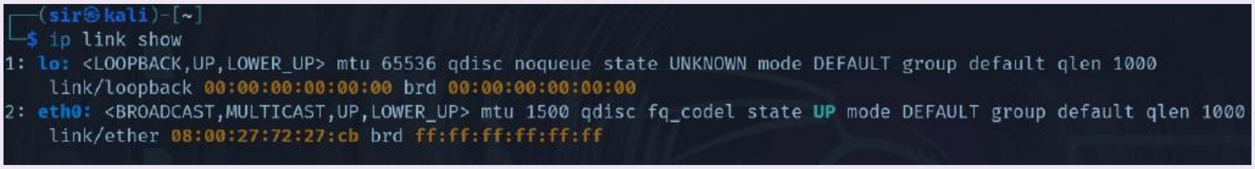
```
┌──(sir㉿kali)-[~]
└─$ ip route | grep default
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100

┌──(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)-[~]
└─$ 
```

50. Check the MAC address of your network interface.



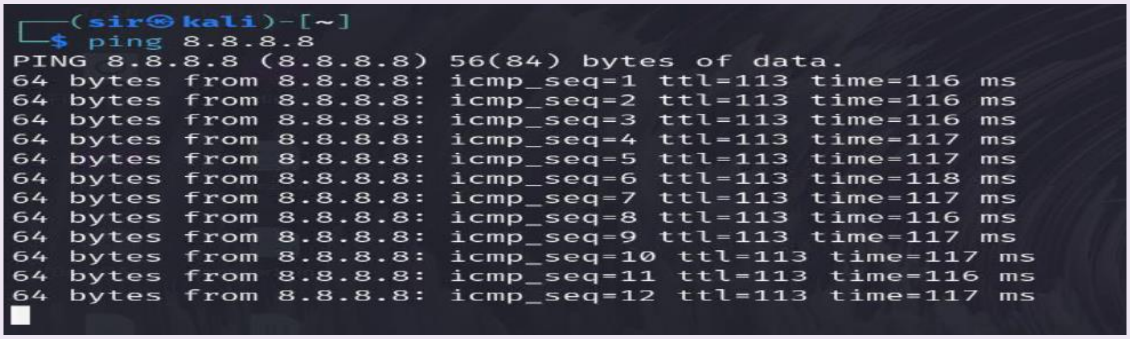
```
┌──(sir㉿kali)-[~]
└─$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default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

51. Ensure that the VM can access external networks.



```
┌──(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
```

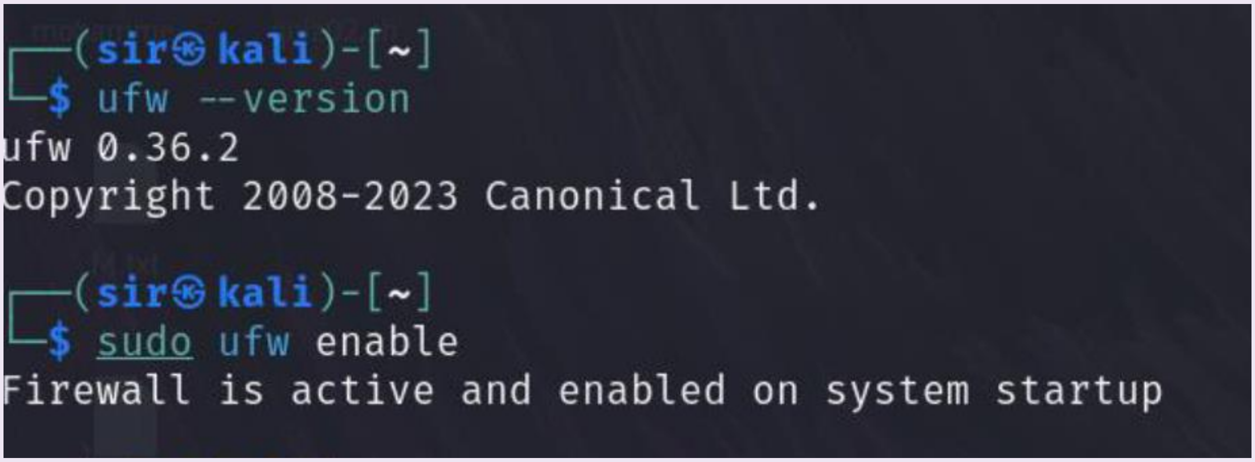
52. Ensure that the VM can access external networks.



```
┌──(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
```

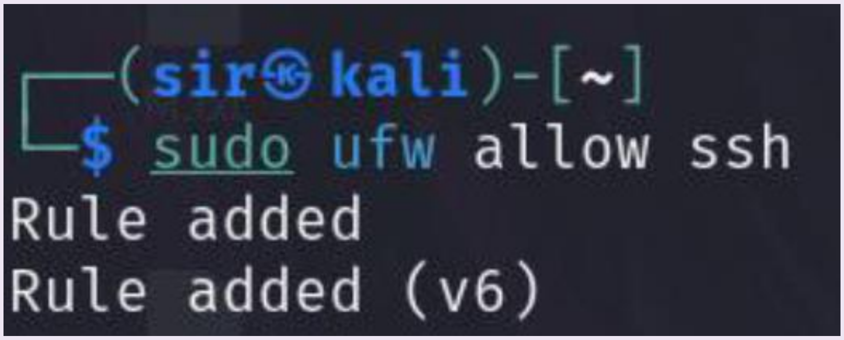
Section 6: UFW Firewall

53. Enable the firewall.



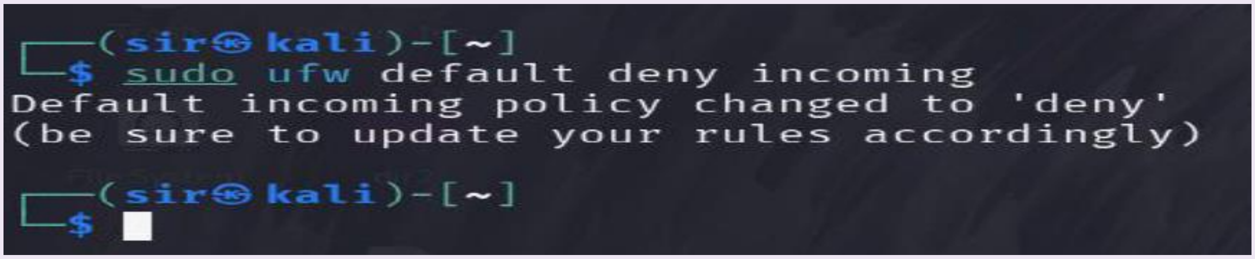
```
┌──(sir㉿kali)-[~]
└─$ ufw --version
ufw 0.36.2
Copyright 2008-2023 Canonical Ltd.

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

54. Allow SSH connections through the firewall.



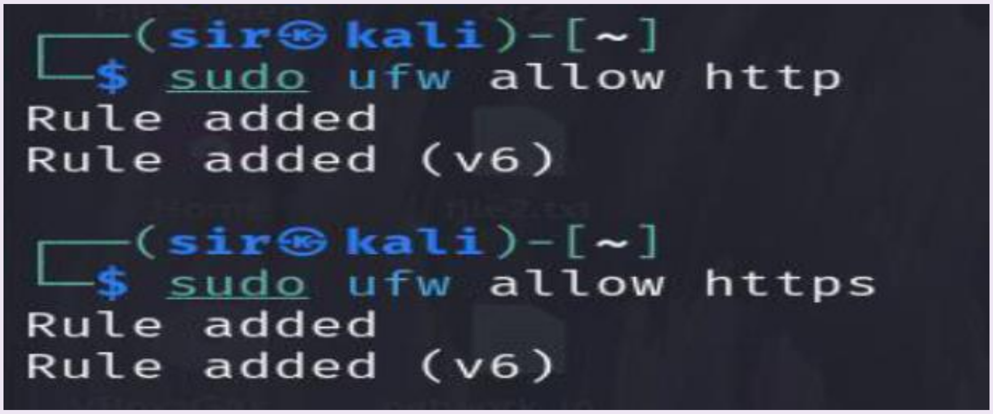
```
┌──(sir㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)
```

55. Deny all incoming traffic by default.



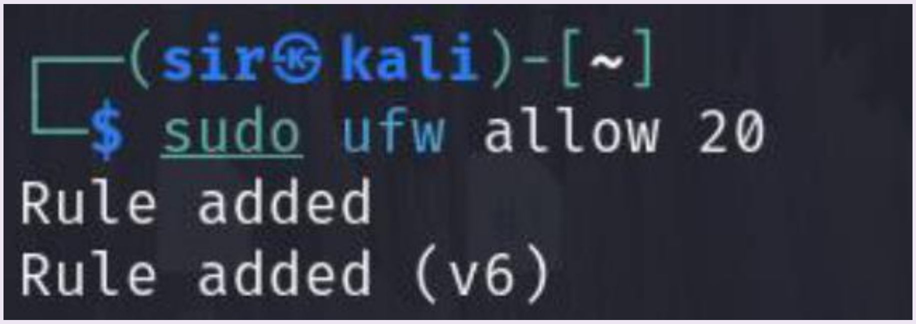
```
┌──(sir㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

┌──(sir㉿kali)-[~]
└─$ █
```

56. Allow HTTP and HTTPS traffic.



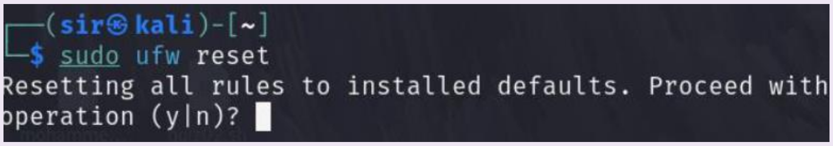
```
┌──(sir㉿kali)-[~]
└─$ sudo ufw allow http
Rule added
Rule added (v6)

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

57. Allow port 20



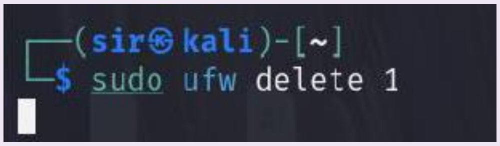
```
┌──(sir㉿kali)-[~]
└─$ sudo ufw allow 20
Rule added
Rule added (v6)
```

58. Reset the firewall settings.



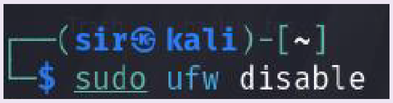
```
┌──(sir㉿kali)-[~]
└─$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with
operation (y|n)? █
```

59. Delete a rule from the firewall.



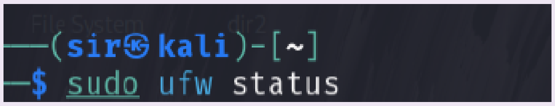
```
┌──(sir㉿kali)-[~]
└─$ sudo ufw delete 1
█
```

60. Disable the firewall.



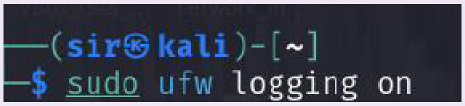
```
┌──(sir㉿kali)-[~]
└─$ sudo ufw disable
```

61. View the status of the firewall.



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

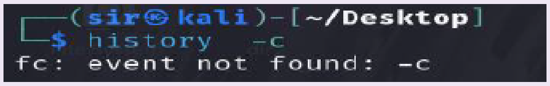
62. Log firewall activity and view it.



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

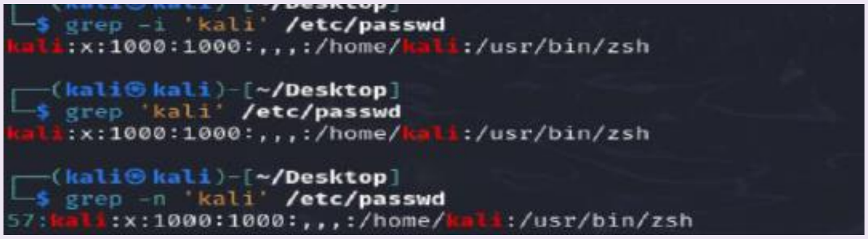
Section 7: Searching and System Information

63. Delete the command history.



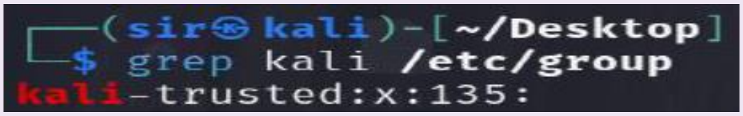
```
┌──(sir㉿kali)-[~/Desktop]
└─$ history -c
fc: event not found: -c
```

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



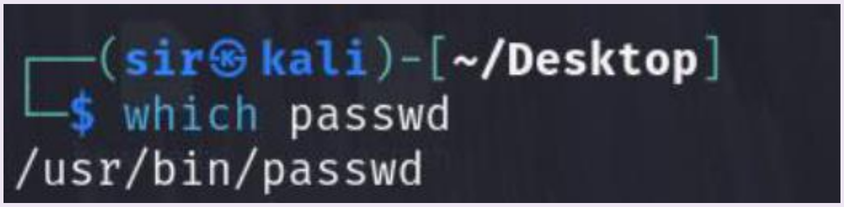
```
└─$ grep -i 'kali' /etc/passwd
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh

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

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

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



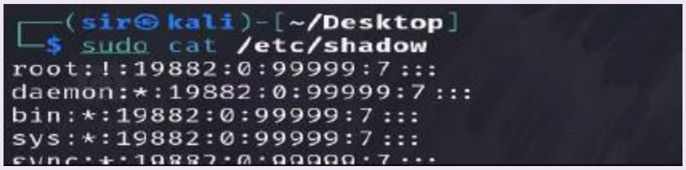
```
┌──(sir㉿kali)-[~/Desktop]
└─$ grep kali /etc/group
kali-trusted:x:135:
```

66. Locate the `passwd` file.



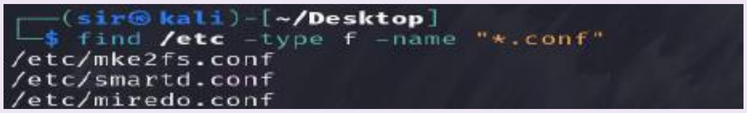
```
┌──(sir㉿kali)-[~/Desktop]
└─$ which passwd
/usr/bin/passwd
```

67. Locate the shadow file and open it.



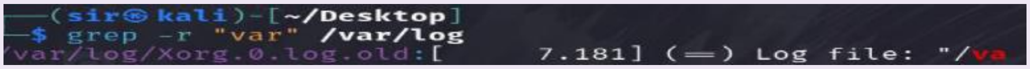
```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo cat /etc/shadow
root:!:19882:0:99999:7:::
daemon:*:19882:0:99999:7:::
bin:*:19882:0:99999:7:::
sys:*:19882:0:99999:7:::
sync:*:19882:0:99999:7:::
```

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



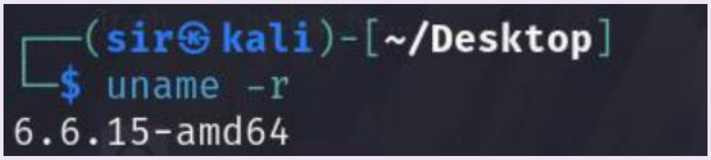
```
┌──(sir㉿kali)-[~/Desktop]
└─$ find /etc -type f -name "*.conf"
/etc/mke2fs.conf
/etc/smartd.conf
/etc/miredo.conf
```

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



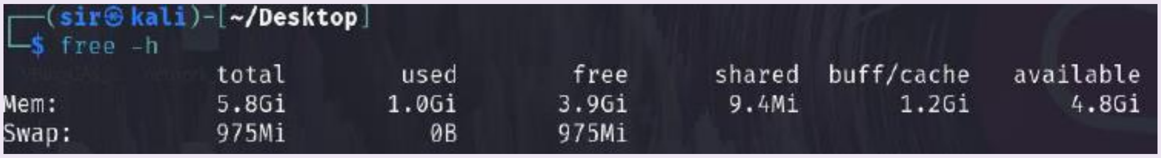
```
──(sir㉿kali)-[~/Desktop]
─$ grep -r "var" /var/log
/var/log/Xorg.0.log.old:[     7.181] (==) Log file: "/va
```

70. View the system's kernel version.



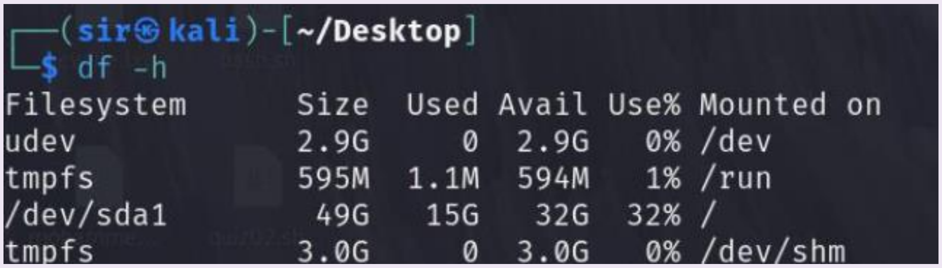
```
┌──(sir㉿kali)-[~/Desktop]
└─$ uname -r
6.6.15-amd64
```

71. Display the system's memory usage.



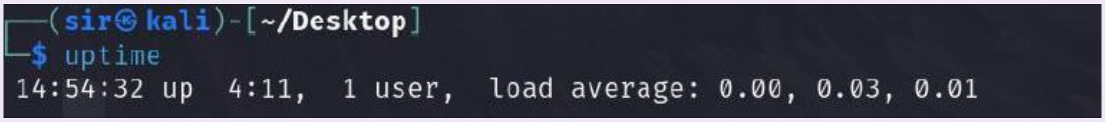
```
┌──(sir㉿kali)-[~/Desktop]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           5.8Gi       1.0Gi       3.9Gi       9.4Mi       1.2Gi       4.8Gi
Swap:          975Mi          0B       975Mi
```

72. Show the system’s disk usage.



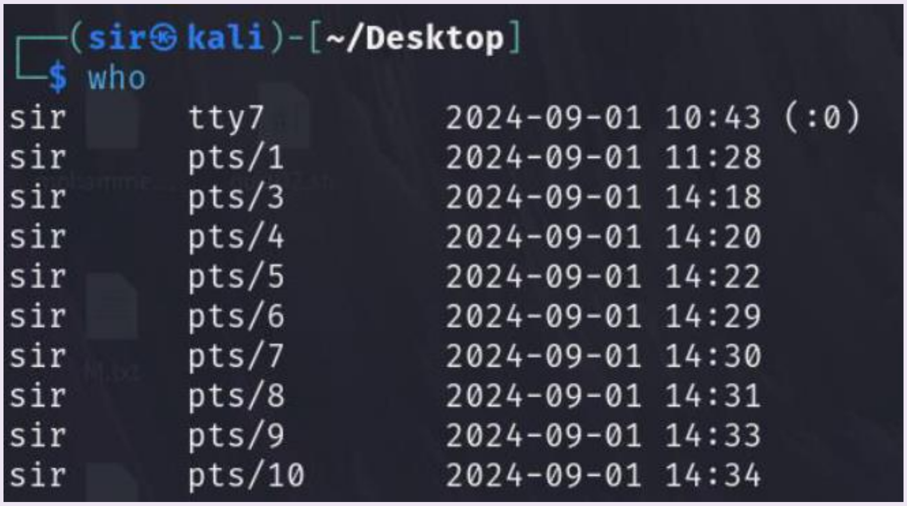
```
┌──(sir㉿kali)-[~/Desktop]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            2.9G     0  2.9G   0% /dev
tmpfs           595M  1.1M  594M   1% /run
/dev/sda1        49G   15G   32G  32% /
tmpfs           3.0G     0  3.0G   0% /dev/shm
```

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



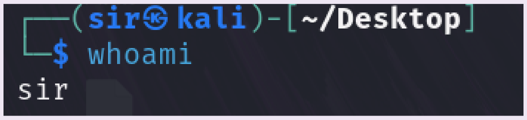
```
┌──(sir㉿kali)-[~/Desktop]
└─$ uptime
 14:54:32 up  4:11,  1 user,  load average: 0.00, 0.03, 0.01
```

74. Display the current logged-in users.



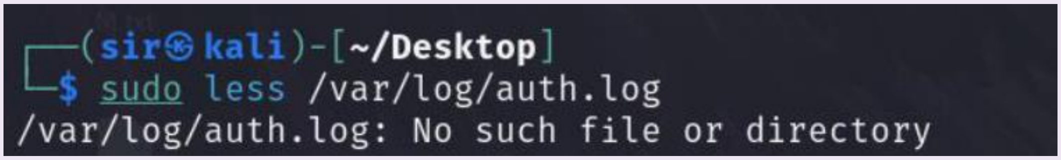
```
┌──(sir㉿kali)-[~/Desktop]
└─$ who
sir      tty7         2024-09-01 10:43 (:0)
sir      pts/1        2024-09-01 11:28
sir      pts/3        2024-09-01 14:18
sir      pts/4        2024-09-01 14:20
sir      pts/5        2024-09-01 14:22
sir      pts/6        2024-09-01 14:29
sir      pts/7        2024-09-01 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.



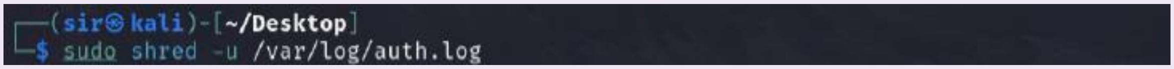
```
┌──(sir㉿kali)-[~/Desktop]
└─$ whoami
sir
```

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



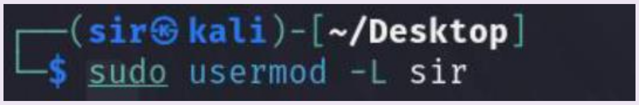
```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo less /var/log/auth.log
/var/log/auth.log: No such file or directory
```

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



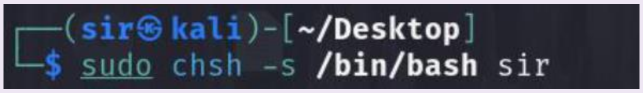
```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo shred -u /var/log/auth.log
```

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



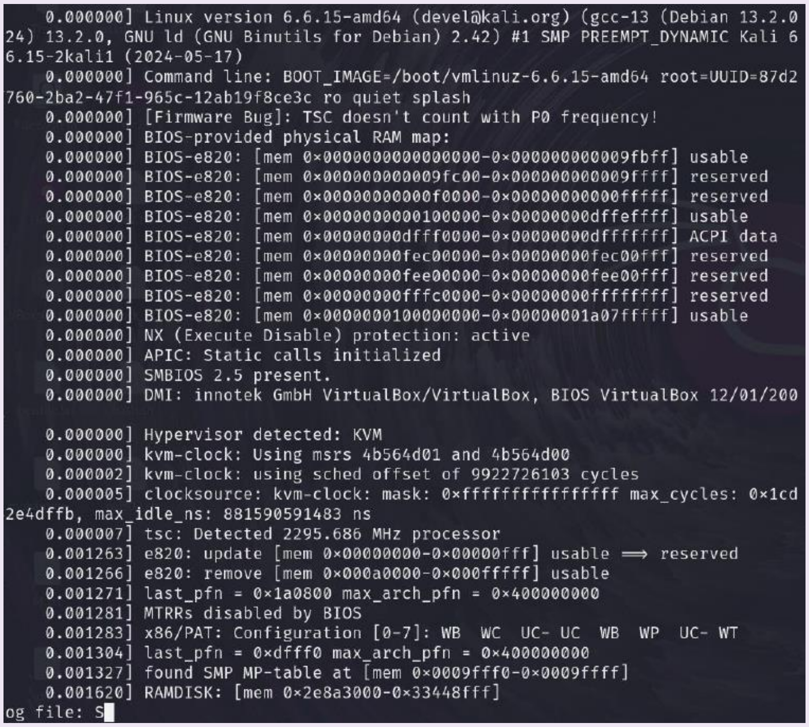
```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo usermod -L sir
```

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.



```
    0.000000] 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)
    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-amd64 root=UUID=87d2
760-2ba2-47f1-965c-12ab19f8ce3c ro quiet splash
    0.000000] [Firmware Bug]: TSC doesn't count with P0 frequency!
    0.000000] BIOS-provided physical RAM map:
    0.000000] BIOS-e820: [mem 0×0000000000000000-0×000000000009fbff] usable
    0.000000] BIOS-e820: [mem 0×000000000009fc00-0×000000000009ffff] reserved
    0.000000] BIOS-e820: [mem 0×00000000000f0000-0×00000000000fffff] reserved
    0.000000] BIOS-e820: [mem 0×0000000000100000-0×00000000dffeffff] usable
    0.000000] BIOS-e820: [mem 0×00000000dfff0000-0×00000000dfffffff] ACPI data
    0.000000] BIOS-e820: [mem 0×00000000fec00000-0×00000000fec00fff] reserved
    0.000000] BIOS-e820: [mem 0×00000000fee00000-0×00000000fee00fff] reserved
    0.000000] BIOS-e820: [mem 0×00000000fffc0000-0×00000000ffffffff] reserved
    0.000000] BIOS-e820: [mem 0×0000000100000000-0×00000001a07fffff] usable
    0.000000] NX (Execute Disable) protection: active
    0.000000] APIC: Static calls initialized
    0.000000] SMBIOS 2.5 present.
    0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/200

    0.000000] Hypervisor detected: KVM
    0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
    0.000002] kvm-clock: using sched offset of 9922726103 cycles
    0.000005] clocksource: kvm-clock: mask: 0×ffffffffffffffff max_cycles: 0×1cd
2e4dffb, max_idle_ns: 881590591483 ns
    0.000007] tsc: Detected 2295.686 MHz processor
    0.001263] e820: update [mem 0×00000000-0×00000fff] usable ⟹ reserved
    0.001266] e820: remove [mem 0×000a0000-0×000fffff] usable
    0.001271] last_pfn = 0×1a0800 max_arch_pfn = 0×400000000
    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 = 0×dfff0 max_arch_pfn = 0×400000000
    0.001327] found SMP MP-table at [mem 0×0009fff0-0×0009ffff]
    0.001620] RAMDISK: [mem 0×2e8a3000-0×33448fff]
og file: S█
```

عمل الطالبة/ علّا خالد عبد الوهاب الشقاقي التخصص/الامن السيبراني

المجموعة/الخامسة عملي

م/عبد الرزاق السماوي