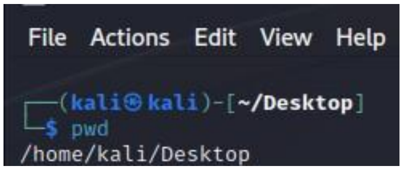
Mid Exam

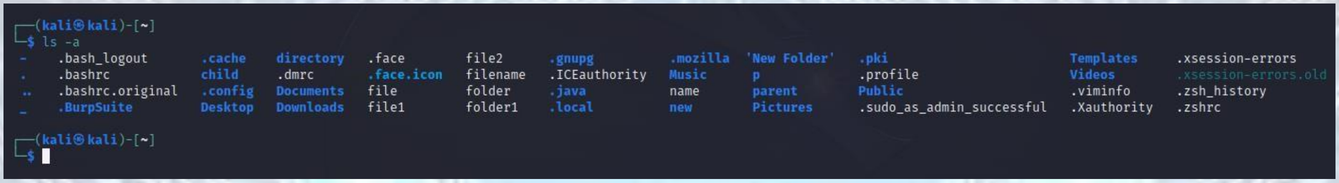
Section 1: File and Directory Management

1. **Display the current working directory.**



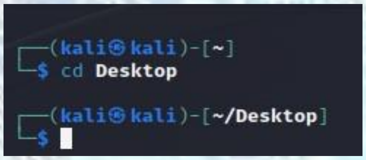
```
┌──(kali㉿kali)-[~/Desktop]
└─$ pwd
/home/kali/Desktop
```

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



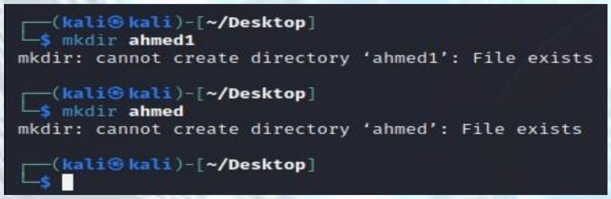
```
┌──(kali㉿kali)-[~]
└─$ ls -a
-    .bash_logout      .cache    directory   .face       file2     .gnupg         .mozilla  'New Folder'   .pki                        Templates    .xsession-errors
.    .bashrc           child     .dmrc       .face.icon  filename  .ICEauthority  Music      p             .profile                    Videos       .xsession-errors.old
..   .bashrc.original  .config   Documents   file        folder    .java          name       parent        Public                      .viminfo     .zsh_history
_    .BurpSuite        Desktop   Downloads   file1       folder1   .local         new        Pictures      .sudo_as_admin_successful   .Xauthority  .zshrc

┌──(kali㉿kali)-[~]
└─$ █
```

3. **Change your directory to the `Desktop`.**



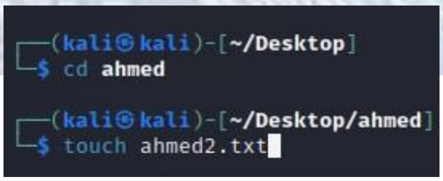
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

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



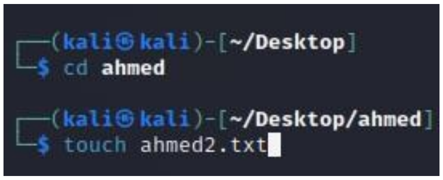
```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir ahmed1
mkdir: cannot create directory ‘ahmed1’: File exists

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir ahmed
mkdir: cannot create directory ‘ahmed’: File exists

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

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



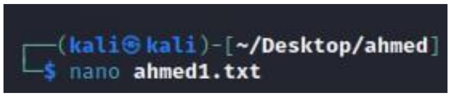
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd ahmed

┌──(kali㉿kali)-[~/Desktop/ahmed]
└─$ touch ahmed2.txt█
```

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



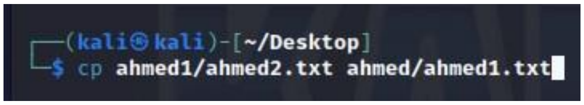
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd ahmed

┌──(kali㉿kali)-[~/Desktop/ahmed]
└─$ touch ahmed2.txt█
```

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



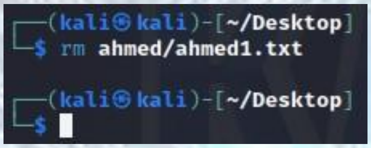
```
┌──(kali㉿kali)-[~/Desktop/ahmed]
└─$ nano ahmed1.txt
```

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



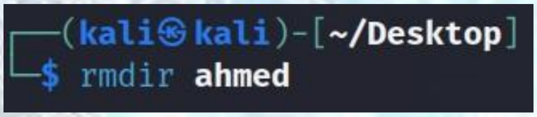
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cp ahmed1/ahmed2.txt ahmed/ahmed1.txt
```

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



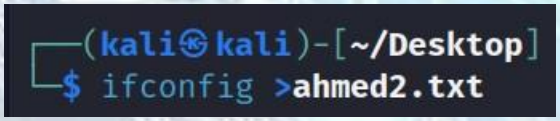
```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm ahmed/ahmed1.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

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



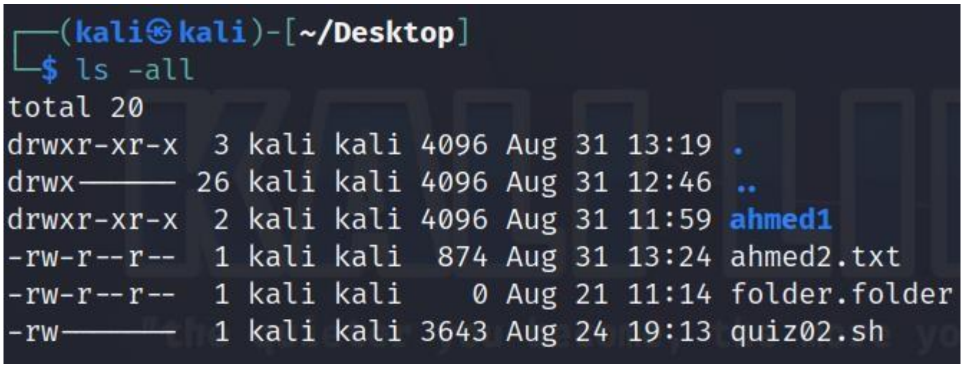
```
┌──(kali㉿kali)-[~/Desktop]
└─$ rmdir ahmed
```

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



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig >ahmed2.txt
```

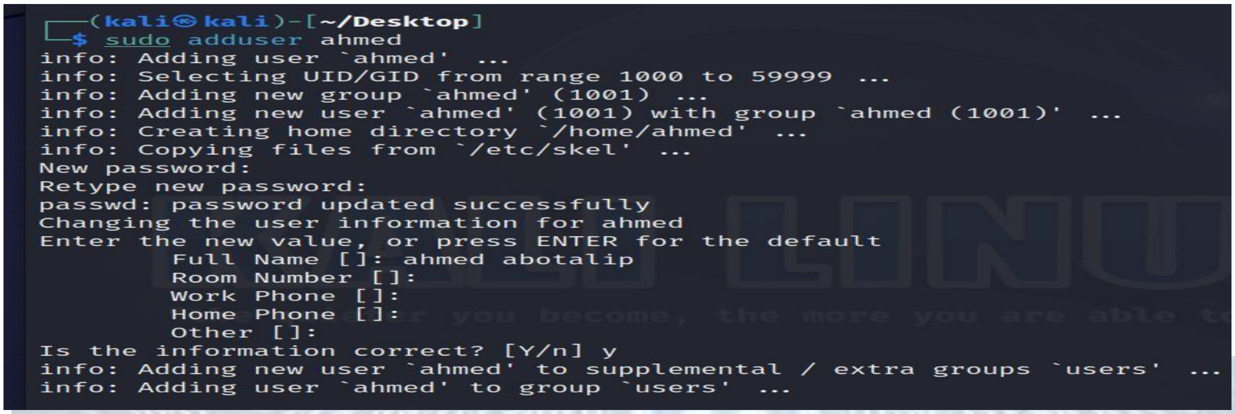
12. Open the Desktop folder and show all files with detailed information.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -all
total 20
drwxr-xr-x  3 kali kali 4096 Aug 31 13:19 .
drwx------ 26 kali kali 4096 Aug 31 12:46 ..
drwxr-xr-x  2 kali kali 4096 Aug 31 11:59 ahmed1
-rw-r--r--  1 kali kali  874 Aug 31 13:24 ahmed2.txt
-rw-r--r--  1 kali kali    0 Aug 21 11:14 folder.folder
-rw-------  1 kali kali 3643 Aug 24 19:13 quiz02.sh
```

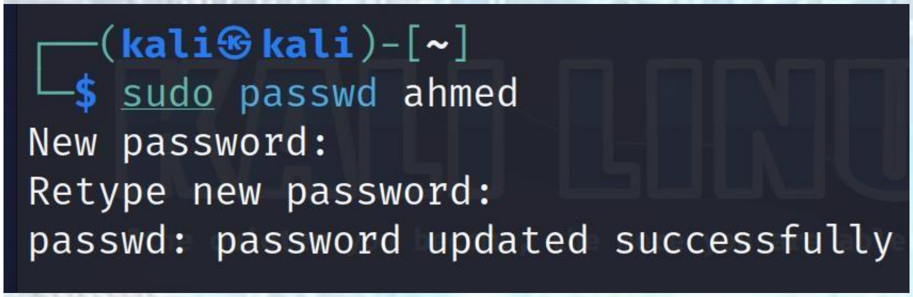
Section 2: Users and Groups Management

13. Create a new user with your name.



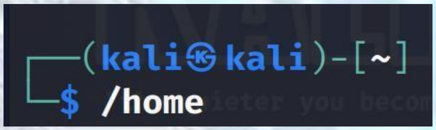
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo adduser ahmed
info: Adding user `ahmed' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `ahmed' (1001) ...
info: Adding new user `ahmed' (1001) with group `ahmed (1001)' ...
info: Creating home directory `/home/ahmed' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ahmed
Enter the new value, or press ENTER for the default
        Full Name []: ahmed abotalip
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `ahmed' to supplemental / extra groups `users' ...
info: Adding user `ahmed' to group `users' ...
```

14. Set a password for your user.

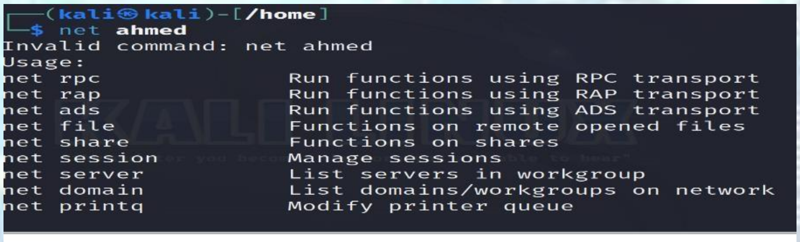


```
┌──(kali㉿kali)-[~]
└─$ sudo passwd ahmed
New password:
Retype new password:
passwd: password updated successfully
```

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

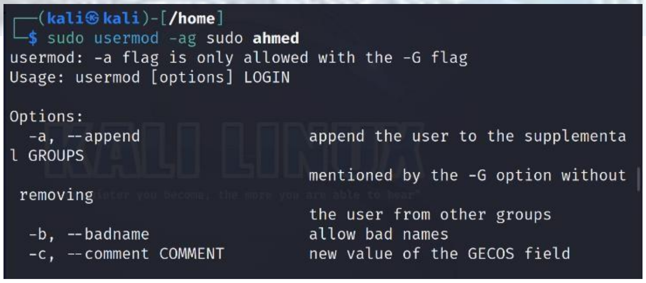


```
┌──(kali㉿kali)-[~]
└─$ /home
```

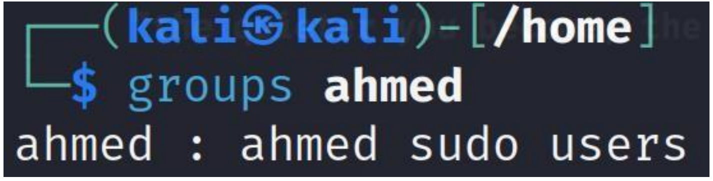


```
┌──(kali㉿kali)-[/home]
└─$ net ahmed
Invalid command: net ahmed
Usage:
net rpc             Run functions using RPC transport
net rap             Run functions using RAP transport
net ads             Run functions using ADS transport
net file            Functions on remote opened files
net share           Functions on shares
net session         Manage sessions
net server          List servers in workgroup
net domain          List domains/workgroups on network
net printq          Modify printer queue
```

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

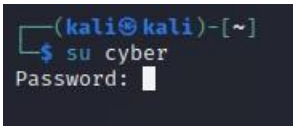


```
┌──(kali㉿kali)-[/home]
└─$ sudo usermod -ag sudo ahmed
usermod: -a flag is only allowed with the -G flag
Usage: usermod [options] LOGIN

Options:
  -a, --append                  append the user to the supplementa
l GROUPS
                                mentioned by the -G option without
 removing
                                the user from other groups
  -b, --badname                 allow bad names
  -c, --comment COMMENT         new value of the GECOS field
```



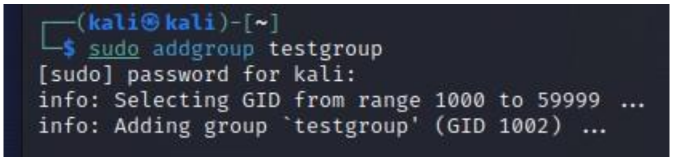
```
┌──(kali㉿kali)-[/home]
└─$ groups ahmed
ahmed : ahmed sudo users
```

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



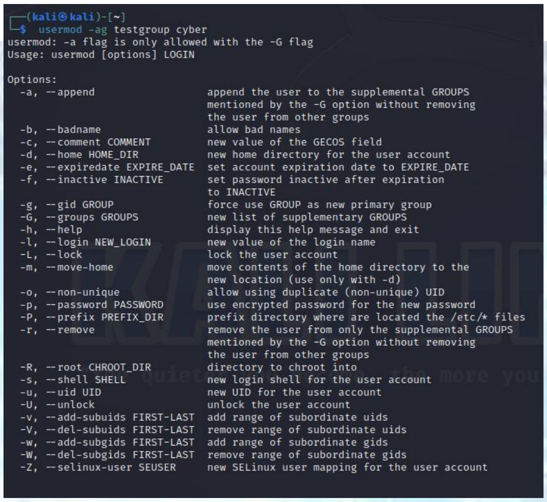
```
┌──(kali㉿kali)-[~]
└─$ su cyber
Password: 
```

18. Create a new group named `testgroup`.



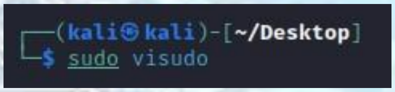
```
┌──(kali㉿kali)-[~]
└─$ sudo addgroup testgroup
[sudo] password for kali:
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `testgroup' (GID 1002) ...
```

19. Add your user to `testgroup`.



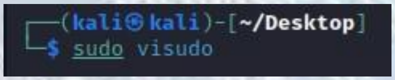
```
┌──(kali㉿kali)-[~]
└─$ usermod -ag testgroup cyber
usermod: -a flag is only allowed with the -G flag
Usage: usermod [options] LOGIN

Options:
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -b, --badname                 allow bad names
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -r, --remove                  remove the user from only the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```

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



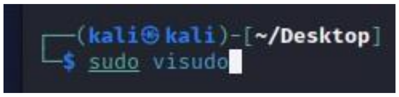
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo visudo
```

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



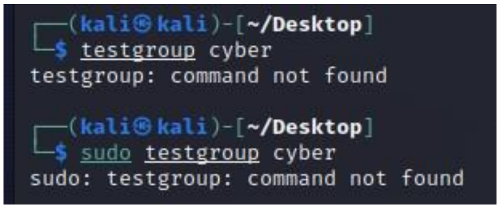
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo visudo
```

22. Check if your user still have administrative privileges.



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

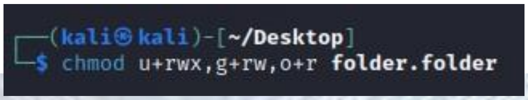
23. Check which groups your user belongs to.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ testgroup cyber
testgroup: command not found

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo testgroup cyber
sudo: testgroup: command not found
```

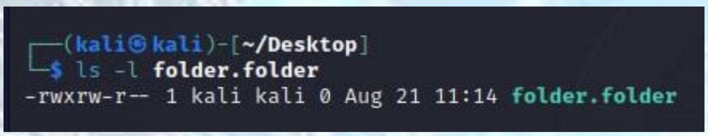
Section 3: Permissions and Ownership

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



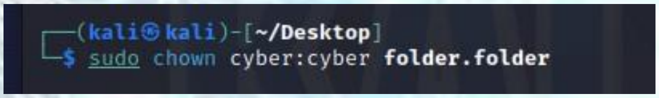
```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod u+rwx,g+rw,o+r folder.folder
```

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



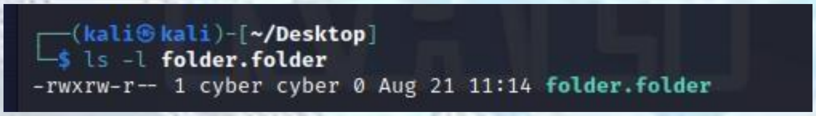
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l folder.folder
-rwxrw-r-- 1 kali kali 0 Aug 21 11:14 folder.folder
```

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



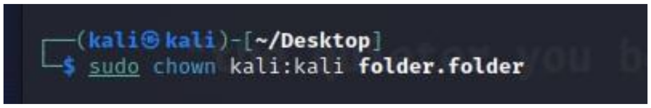
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown cyber:cyber folder.folder
```

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



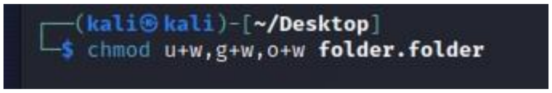
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l folder.folder
-rwxrw-r-- 1 cyber cyber 0 Aug 21 11:14 folder.folder
```

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



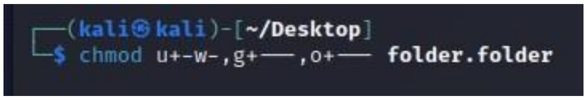
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown kali:kali folder.folder
```

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



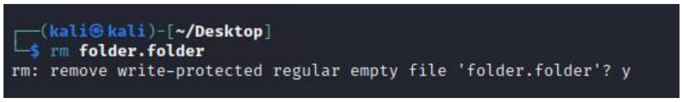
```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod u+w,g+w,o+w folder.folder
```

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



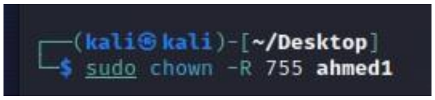
```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod u+-w-,g+——,o+—— folder.folder
```

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



```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm folder.folder
rm: remove write-protected regular empty file 'folder.folder'? y
```

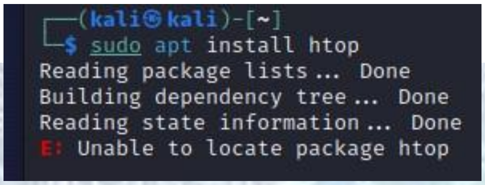
32. **What command would you use to recursively change the permissions of all files and directories inside a folder named `project` to `755`.**



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown -R 755 ahmed1
```

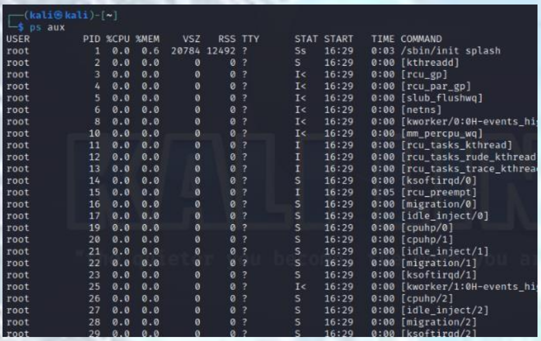
Section 4: Process Management

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



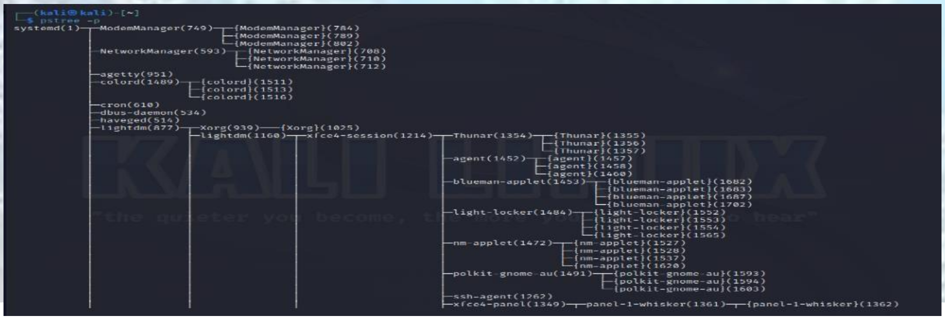
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install htop
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package htop
```

34. **Display all running processes.**



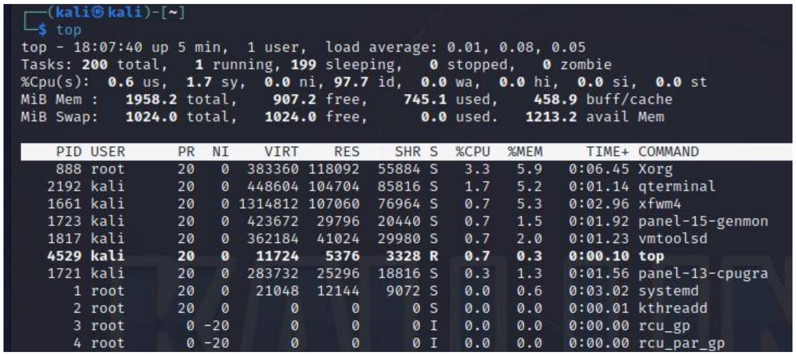
```
┌──(kali㉿kali)-[~]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.6  20784 12492 ?        Ss   16:29   0:03 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    16:29   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   16:29   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   16:29   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   16:29   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   16:29   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   16:29   0:00 [kworker/0:0H-events_hi
root          10  0.0  0.0      0     0 ?        I<   16:29   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    16:29   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    16:29   0:00 [rcu_tasks_rude_kthread
root          13  0.0  0.0      0     0 ?        I    16:29   0:00 [rcu_tasks_trace_kthrea
root          14  0.0  0.0      0     0 ?        S    16:29   0:00 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    16:29   0:05 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    16:29   0:00 [migration/0]
root          17  0.0  0.0      0     0 ?        S    16:29   0:00 [idle_inject/0]
root          19  0.0  0.0      0     0 ?        S    16:29   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    16:29   0:00 [cpuhp/1]
root          21  0.0  0.0      0     0 ?        S    16:29   0:00 [idle_inject/1]
root          22  0.0  0.0      0     0 ?        S    16:29   0:00 [migration/1]
root          23  0.0  0.0      0     0 ?        S    16:29   0:00 [ksoftirqd/1]
root          25  0.0  0.0      0     0 ?        I<   16:29   0:00 [kworker/1:0H-events_hi
root          26  0.0  0.0      0     0 ?        S    16:29   0:00 [cpuhp/2]
root          27  0.0  0.0      0     0 ?        S    16:29   0:00 [idle_inject/2]
root          28  0.0  0.0      0     0 ?        S    16:29   0:00 [migration/2]
root          29  0.0  0.0      0     0 ?        S    16:29   0:00 [ksoftirqd/2]
```

35. **Display a tree of all running processes.**



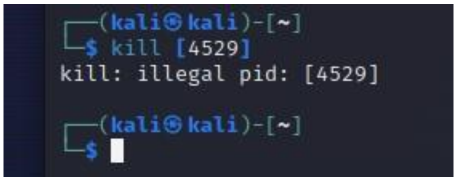
```
┌──(kali㉿kali)-[~]
└─$ pstree -p
systemd(1)─┬─ModemManager(749)─┬─{ModemManager}(784)
           │                   ├─{ModemManager}(789)
           │                   └─{ModemManager}(802)
           ├─NetworkManager(593)─┬─{NetworkManager}(708)
           │                     ├─{NetworkManager}(710)
           │                     └─{NetworkManager}(712)
           ├─agetty(951)
           ├─colord(1489)─┬─{colord}(1511)
           │              ├─{colord}(1513)
           │              └─{colord}(1516)
           ├─cron(610)
           ├─dbus-daemon(534)
           ├─haveged(514)
           ├─lightdm(877)─┬─Xorg(939)───{Xorg}(1025)
           │              └─lightdm(1160)─┬─xfce4-session(1214)─┬─Thunar(1354)─┬─{Thunar}(1355)
           │                              │                     │              ├─{Thunar}(1356)
           │                              │                     │              └─{Thunar}(1357)
           │                              │                     ├─agent(1452)─┬─{agent}(1457)
           │                              │                     │             ├─{agent}(1458)
           │                              │                     │             └─{agent}(1460)
           │                              │                     ├─blueman-applet(1453)─┬─{blueman-applet}(1682)
           │                              │                     │                      ├─{blueman-applet}(1683)
           │                              │                     │                      ├─{blueman-applet}(1687)
           │                              │                     │                      └─{blueman-applet}(1702)
           │                              │                     ├─light-locker(1484)─┬─{light-locker}(1552)
           │                              │                     │                    ├─{light-locker}(1553)
           │                              │                     │                    ├─{light-locker}(1554)
           │                              │                     │                    └─{light-locker}(1565)
           │                              │                     ├─nm-applet(1472)─┬─{nm-applet}(1527)
           │                              │                     │                 ├─{nm-applet}(1528)
           │                              │                     │                 ├─{nm-applet}(1537)
           │                              │                     │                 └─{nm-applet}(1620)
           │                              │                     ├─polkit-gnome-au(1491)─┬─{polkit-gnome-au}(1593)
           │                              │                     │                       ├─{polkit-gnome-au}(1594)
           │                              │                     │                       └─{polkit-gnome-au}(1603)
           │                              │                     ├─ssh-agent(1262)
           │                              │                     ├─xfce4-panel(1349)─┬─panel-1-whisker(1361)─┬─{panel-1-whisker}(1362)
```

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



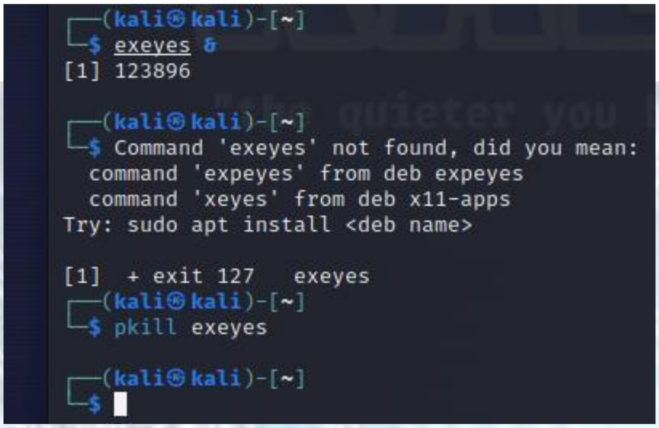
```
┌──(kali㉿kali)-[~]
└─$ top
top - 18:07:40 up 5 min,  1 user,  load average: 0.01, 0.08, 0.05
Tasks: 200 total,   1 running, 199 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.6 us,  1.7 sy,  0.0 ni, 97.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   1958.2 total,    907.2 free,    745.1 used,    458.9 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   1213.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    888 root      20   0  383360 118092  55884 S   3.3   5.9   0:06.45 Xorg
   2192 kali      20   0  448604 104704  85816 S   1.7   5.2   0:01.14 qterminal
   1661 kali      20   0 1314812 107060  76964 S   0.7   5.3   0:02.96 xfwm4
   1723 kali      20   0  423672  29796  20440 S   0.7   1.5   0:01.92 panel-15-genmon
   1817 kali      20   0  362184  41024  29980 S   0.7   2.0   0:01.23 vmtoolsd
   4529 kali      20   0   11724   5376   3328 R   0.7   0.3   0:00.10 top
   1721 kali      20   0  283732  25296  18816 S   0.3   1.3   0:01.56 panel-13-cpugra
      1 root      20   0   21048  12144   9072 S   0.0   0.6   0:03.02 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
```

37. Kill a process with a specific PID.



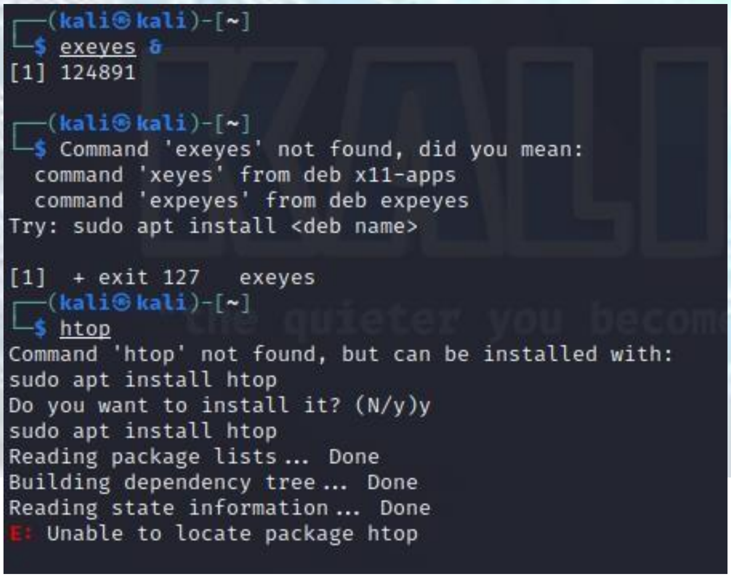
```
┌──(kali㉿kali)-[~]
└─$ kill [4529]
kill: illegal pid: [4529]

┌──(kali㉿kali)-[~]
└─$ 
```

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



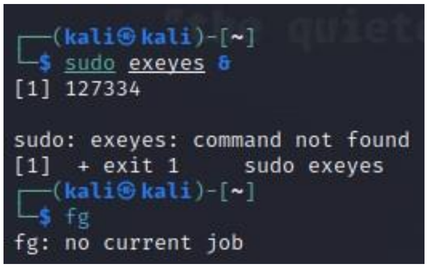
```
┌──(kali㉿kali)-[~]
└─$ exeyes &
[1] 123896

┌──(kali㉿kali)-[~]
└─$ Command 'exeyes' not found, did you mean:
  command 'expeyes' from deb expeyes
  command 'xeyes' from deb x11-apps
Try: sudo apt install <deb name>

[1]  + exit 127   exeyes
┌──(kali㉿kali)-[~]
└─$ pkill exeyes

┌──(kali㉿kali)-[~]
└─$ 
```

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



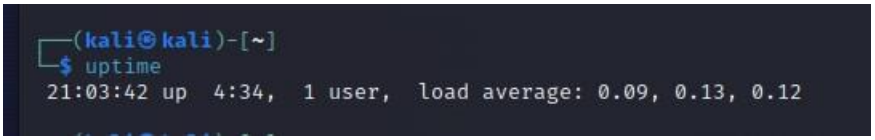
```
┌──(kali㉿kali)-[~]
└─$ exeyes &
[1] 124891

┌──(kali㉿kali)-[~]
└─$ Command 'exeyes' not found, did you mean:
  command 'xeyes' from deb x11-apps
  command 'expeyes' from deb expeyes
Try: sudo apt install <deb name>

[1]  + exit 127   exeyes
┌──(kali㉿kali)-[~]
└─$ htop
Command 'htop' not found, but can be installed with:
sudo apt install htop
Do you want to install it? (N/y)y
sudo apt install htop
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package htop
```

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



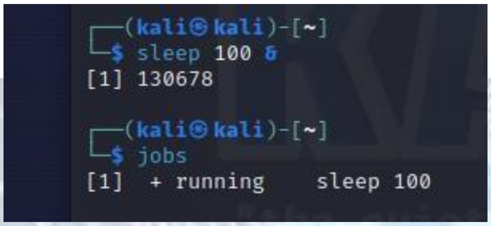
```
┌──(kali㉿kali)-[~]
└─$ sudo exeyes &
[1] 127334

sudo: exeyes: command not found
[1]  + exit 1     sudo exeyes
┌──(kali㉿kali)-[~]
└─$ fg
fg: no current job
```

41. Check how long the system has been running.



```
┌──(kali㉿kali)-[~]
└─$ uptime
 21:03:42 up  4:34,  1 user,  load average: 0.09, 0.13, 0.12
```

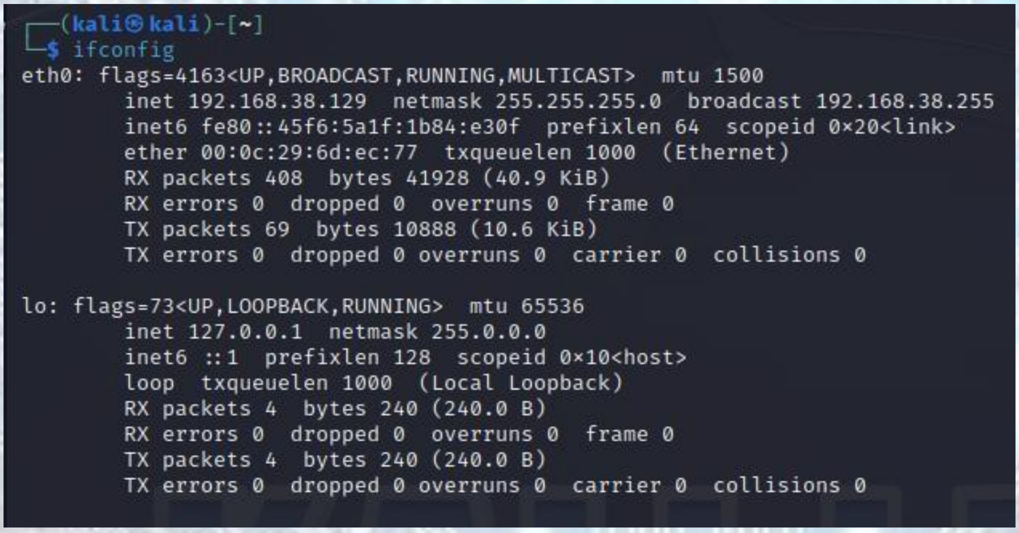
42. List all jobs running in the background.



```
┌──(kali㉿kali)-[~]
└─$ sleep 100 &
[1] 130678

┌──(kali㉿kali)-[~]
└─$ jobs
[1]  + running    sleep 100
```

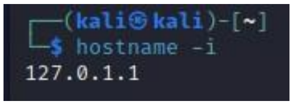
Section 5: Networking Commands

43. Display the network configuration



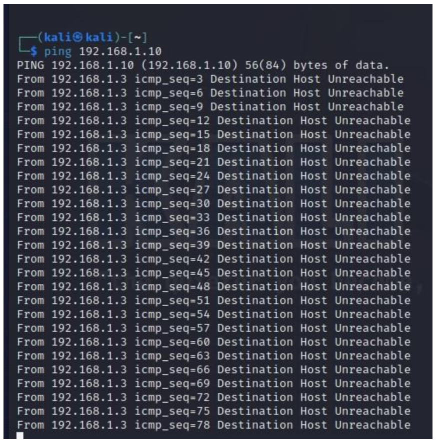
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.38.129  netmask 255.255.255.0  broadcast 192.168.38.255
        inet6 fe80::45f6:5a1f:1b84:e30f  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:6d:ec:77  txqueuelen 1000  (Ethernet)
        RX packets 408  bytes 41928 (40.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 69  bytes 10888 (10.6 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 0×10<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
```

44. Check the IP address of your machine.



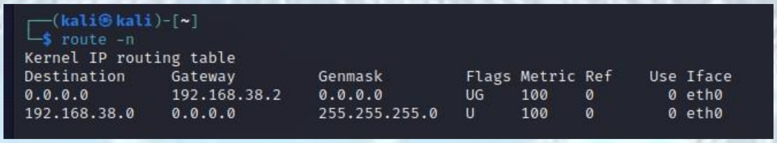
```
┌──(kali㉿kali)-[~]
└─$ hostname -i
127.0.1.1
```

45. Test connectivity to an external server.



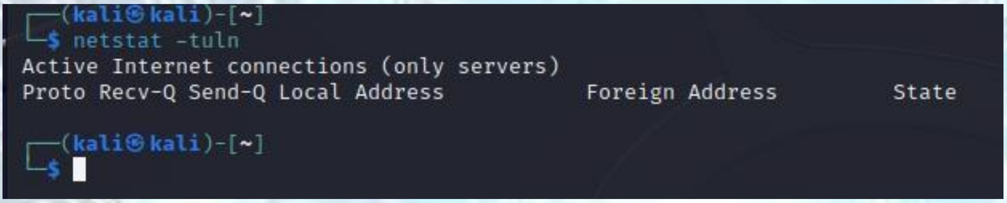
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
From 192.168.1.3 icmp_seq=3 Destination Host Unreachable
From 192.168.1.3 icmp_seq=6 Destination Host Unreachable
From 192.168.1.3 icmp_seq=9 Destination Host Unreachable
From 192.168.1.3 icmp_seq=12 Destination Host Unreachable
From 192.168.1.3 icmp_seq=15 Destination Host Unreachable
From 192.168.1.3 icmp_seq=18 Destination Host Unreachable
From 192.168.1.3 icmp_seq=21 Destination Host Unreachable
From 192.168.1.3 icmp_seq=24 Destination Host Unreachable
From 192.168.1.3 icmp_seq=27 Destination Host Unreachable
From 192.168.1.3 icmp_seq=30 Destination Host Unreachable
From 192.168.1.3 icmp_seq=33 Destination Host Unreachable
From 192.168.1.3 icmp_seq=36 Destination Host Unreachable
From 192.168.1.3 icmp_seq=39 Destination Host Unreachable
From 192.168.1.3 icmp_seq=42 Destination Host Unreachable
From 192.168.1.3 icmp_seq=45 Destination Host Unreachable
From 192.168.1.3 icmp_seq=48 Destination Host Unreachable
From 192.168.1.3 icmp_seq=51 Destination Host Unreachable
From 192.168.1.3 icmp_seq=54 Destination Host Unreachable
From 192.168.1.3 icmp_seq=57 Destination Host Unreachable
From 192.168.1.3 icmp_seq=60 Destination Host Unreachable
From 192.168.1.3 icmp_seq=63 Destination Host Unreachable
From 192.168.1.3 icmp_seq=66 Destination Host Unreachable
From 192.168.1.3 icmp_seq=69 Destination Host Unreachable
From 192.168.1.3 icmp_seq=72 Destination Host Unreachable
From 192.168.1.3 icmp_seq=75 Destination Host Unreachable
From 192.168.1.3 icmp_seq=78 Destination Host Unreachable
```

46. Display the routing table.



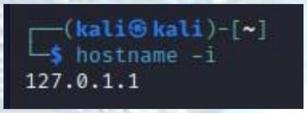
```
┌──(kali㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.38.2    0.0.0.0         UG    100    0        0 eth0
192.168.38.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

47. Check the open ports and active connections.



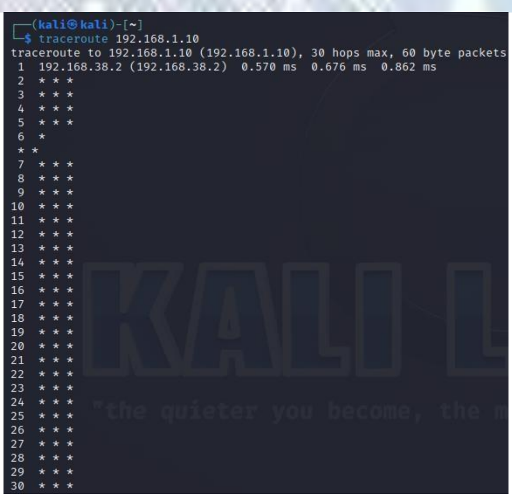
```
┌──(kali㉿kali)-[~]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(kali㉿kali)-[~]
└─$ 
```

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



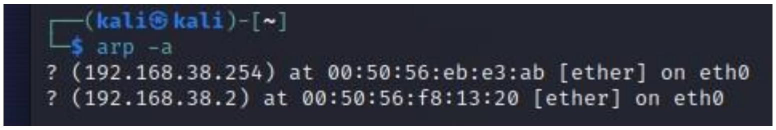
```
┌──(kali㉿kali)-[~]
└─$ hostname -i
127.0.1.1
```

49. Trace the route to an external server.



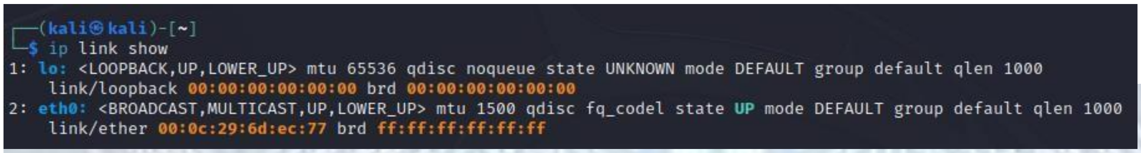
```
┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.1.10
traceroute to 192.168.1.10 (192.168.1.10), 30 hops max, 60 byte packets
 1  192.168.38.2 (192.168.38.2)  0.570 ms  0.676 ms  0.862 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  *
 * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

50. **Find out the default gateway.**



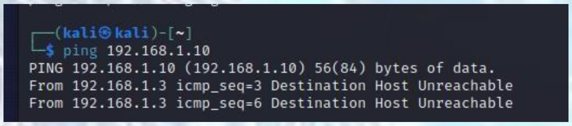
```
┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.38.254) at 00:50:56:eb:e3:ab [ether] on eth0
? (192.168.38.2) at 00:50:56:f8:13:20 [ether] on eth0
```

51. **Check the MAC address of your network interface.**



```
┌──(kali㉿kali)-[~]
└─$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:6d:ec:77 brd ff:ff:ff:ff:ff:ff
```

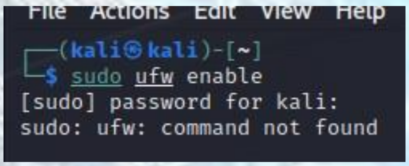
52. **Ensure that the VM can access external networks.**



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
From 192.168.1.3 icmp_seq=3 Destination Host Unreachable
From 192.168.1.3 icmp_seq=6 Destination Host Unreachable
```

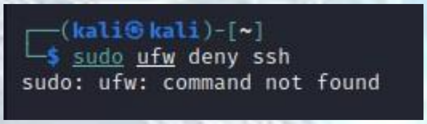
Section 6: UFW Firewall

53. **Enable the firewall.**



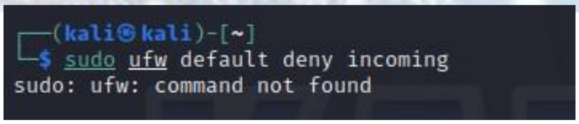
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
[sudo] password for kali:
sudo: ufw: command not found
```

54. **Allow SSH connections through the firewall.**



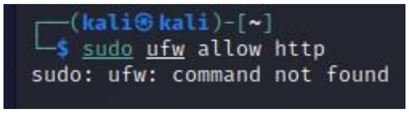
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw deny ssh
sudo: ufw: command not found
```

55. **Deny all incoming traffic by default.**



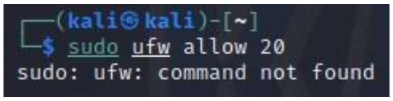
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default deny incoming
sudo: ufw: command not found
```

56. **Allow HTTP and HTTPS traffic.**



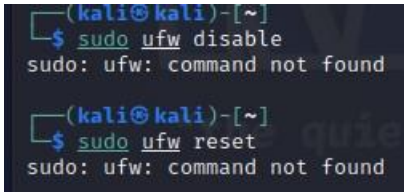
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow http
sudo: ufw: command not found
```

57. **Allow port 20**



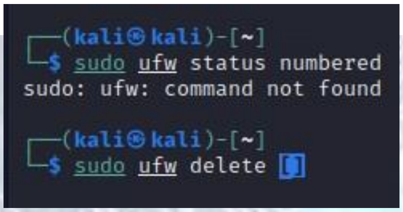
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 20
sudo: ufw: command not found
```

58. Reset the firewall settings.



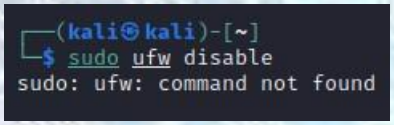
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw disable
sudo: ufw: command not found

┌──(kali㉿kali)-[~]
└─$ sudo ufw reset
sudo: ufw: command not found
```

59. Delete a rule from the firewall.



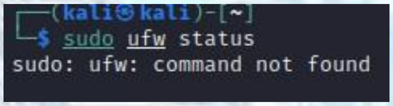
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered
sudo: ufw: command not found

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

60. Disable the firewall.



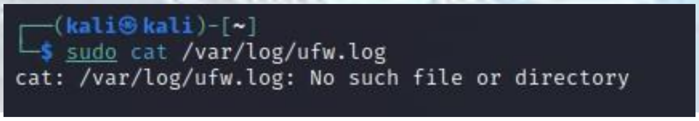
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw disable
sudo: ufw: command not found
```

61. View the status of the firewall.



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status
sudo: ufw: command not found
```

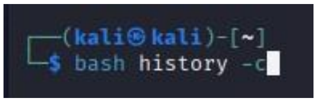
62. Log firewall activity and view it.



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

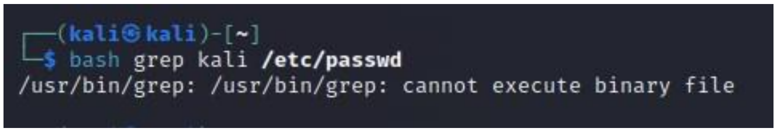
Section 7: Searching and System Information

63. Delete the command history.



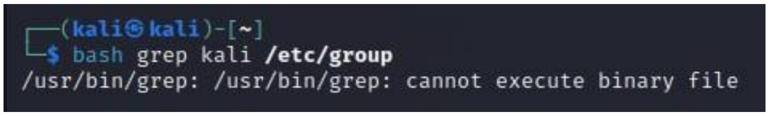
```
┌──(kali㉿kali)-[~]
└─$ bash history -c
```

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



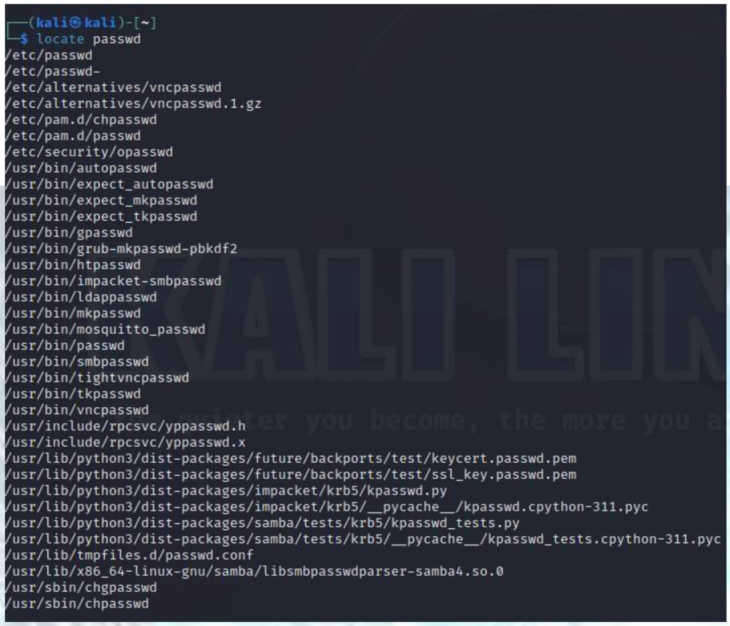
```
┌──(kali㉿kali)-[~]
└─$ bash grep kali /etc/passwd
/usr/bin/grep: /usr/bin/grep: cannot execute binary file
```

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



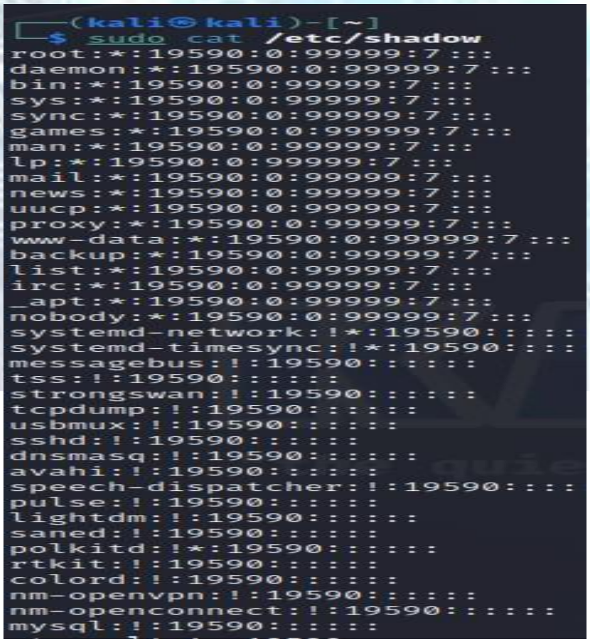
```
┌──(kali㉿kali)-[~]
└─$ bash grep kali /etc/group
/usr/bin/grep: /usr/bin/grep: cannot execute binary file
```

66. **Locate the `passwd` file.**



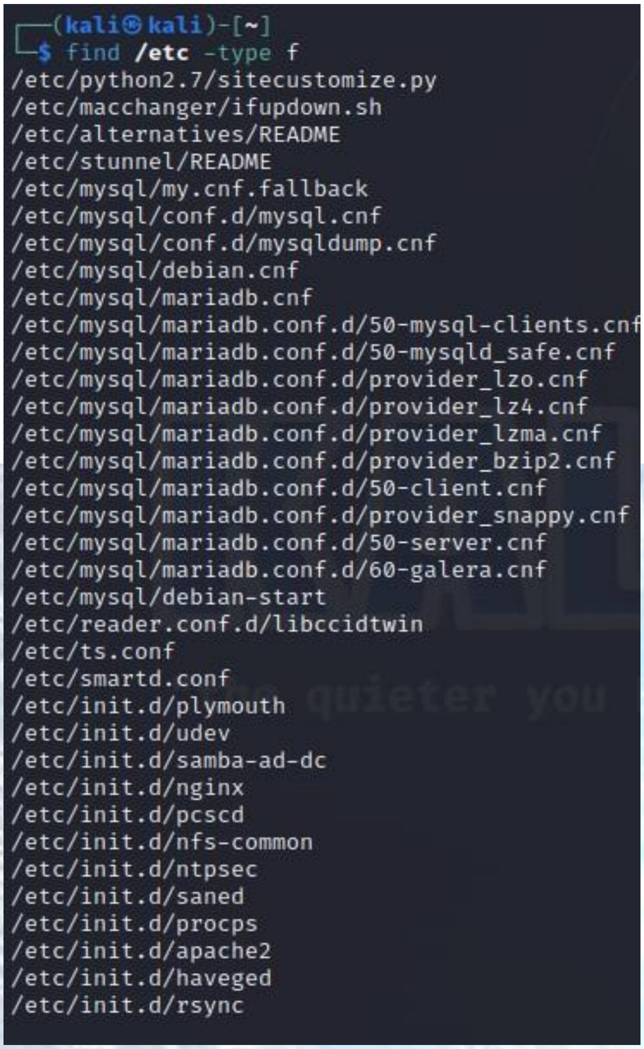
```
┌──(kali㉿kali)-[~]
└─$ locate passwd
/etc/passwd
/etc/passwd-
/etc/alternatives/vncpasswd
/etc/alternatives/vncpasswd.1.gz
/etc/pam.d/chpasswd
/etc/pam.d/passwd
/etc/security/opasswd
/usr/bin/autopasswd
/usr/bin/expect_autopasswd
/usr/bin/expect_mkpasswd
/usr/bin/expect_tkpasswd
/usr/bin/gpasswd
/usr/bin/grub-mkpasswd-pbkdf2
/usr/bin/htpasswd
/usr/bin/impacket-smbpasswd
/usr/bin/ldappasswd
/usr/bin/mkpasswd
/usr/bin/mosquitto_passwd
/usr/bin/passwd
/usr/bin/smbpasswd
/usr/bin/tightvncpasswd
/usr/bin/tkpasswd
/usr/bin/vncpasswd
/usr/include/rpcsvc/yppasswd.h
/usr/include/rpcsvc/yppasswd.x
/usr/lib/python3/dist-packages/future/backports/test/keycert.passwd.pem
/usr/lib/python3/dist-packages/future/backports/test/ssl_key.passwd.pem
/usr/lib/python3/dist-packages/impacket/krb5/kpasswd.py
/usr/lib/python3/dist-packages/impacket/krb5/__pycache__/kpasswd.cpython-311.pyc
/usr/lib/python3/dist-packages/samba/tests/krb5/kpasswd_tests.py
/usr/lib/python3/dist-packages/samba/tests/krb5/__pycache__/kpasswd_tests.cpython-311.pyc
/usr/lib/tmpfiles.d/passwd.conf
/usr/lib/x86_64-linux-gnu/samba/libsmbpasswdparser-samba4.so.0
/usr/sbin/chgpasswd
/usr/sbin/chpasswd
```

67. **Locate the shadow file and open it.**



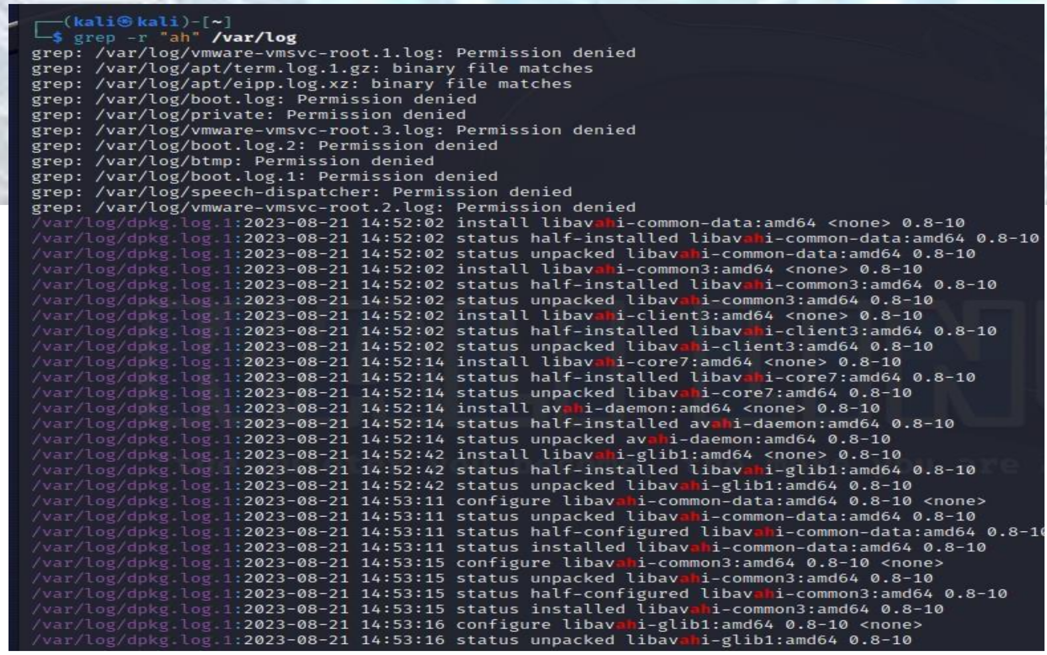
```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow
root:*:19590:0:99999:7:::
daemon:*:19590:0:99999:7:::
bin:*:19590:0:99999:7:::
sys:*:19590:0:99999:7:::
sync:*:19590:0:99999:7:::
games:*:19590:0:99999:7:::
man:*:19590:0:99999:7:::
lp:*:19590:0:99999:7:::
mail:*:19590:0:99999:7:::
news:*:19590:0:99999:7:::
uucp:*:19590:0:99999:7:::
proxy:*:19590:0:99999:7:::
www-data:*:19590:0:99999:7:::
backup:*:19590:0:99999:7:::
list:*:19590:0:99999:7:::
irc:*:19590:0:99999:7:::
_apt:*:19590:0:99999:7:::
nobody:*:19590:0:99999:7:::
systemd-network:!*:19590::::::
systemd-timesync:!*:19590::::::
messagebus:!:19590::::::
tss:!:19590::::::
strongswan:!:19590::::::
tcpdump:!:19590::::::
usbmux:!:19590::::::
sshd:!:19590::::::
dnsmasq:!:19590::::::
avahi:!:19590::::::
speech-dispatcher:!:19590::::::
pulse:!:19590::::::
lightdm:!:19590::::::
saned:!:19590::::::
polkitd:!*:19590::::::
rtkit:!:19590::::::
colord:!:19590::::::
nm-openvpn:!:19590::::::
nm-openconnect:!:19590::::::
mysql:!:19590::::::
```

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



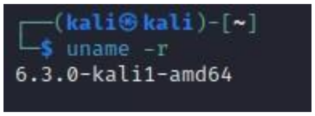
```
┌──(kali㉿kali)-[~]
└─$ find /etc -type f
/etc/python2.7/sitecustomize.py
/etc/macchanger/ifupdown.sh
/etc/alternatives/README
/etc/stunnel/README
/etc/mysql/my.cnf.fallback
/etc/mysql/conf.d/mysql.cnf
/etc/mysql/conf.d/mysqldump.cnf
/etc/mysql/debian.cnf
/etc/mysql/mariadb.cnf
/etc/mysql/mariadb.conf.d/50-mysql-clients.cnf
/etc/mysql/mariadb.conf.d/50-mysqld_safe.cnf
/etc/mysql/mariadb.conf.d/provider_lzo.cnf
/etc/mysql/mariadb.conf.d/provider_lz4.cnf
/etc/mysql/mariadb.conf.d/provider_lzma.cnf
/etc/mysql/mariadb.conf.d/provider_bzip2.cnf
/etc/mysql/mariadb.conf.d/50-client.cnf
/etc/mysql/mariadb.conf.d/provider_snappy.cnf
/etc/mysql/mariadb.conf.d/50-server.cnf
/etc/mysql/mariadb.conf.d/60-galera.cnf
/etc/mysql/debian-start
/etc/reader.conf.d/libccidtwin
/etc/ts.conf
/etc/smartd.conf
/etc/init.d/plymouth
/etc/init.d/udev
/etc/init.d/samba-ad-dc
/etc/init.d/nginx
/etc/init.d/pcscd
/etc/init.d/nfs-common
/etc/init.d/ntpsec
/etc/init.d/saned
/etc/init.d/procps
/etc/init.d/apache2
/etc/init.d/haveged
/etc/init.d/rsync
```

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



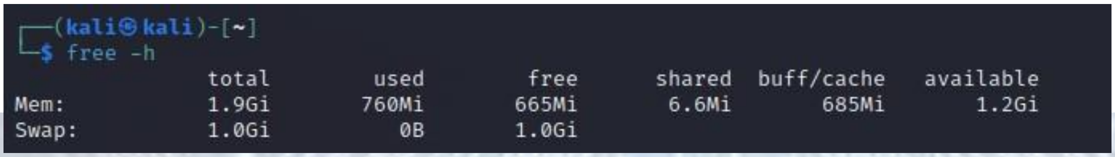
```
┌──(kali㉿kali)-[~]
└─$ grep -r "ah" /var/log
grep: /var/log/vmware-vmsvc-root.1.log: Permission denied
grep: /var/log/apt/term.log.1.gz: binary file matches
grep: /var/log/apt/eipp.log.xz: binary file matches
grep: /var/log/boot.log: Permission denied
grep: /var/log/private: Permission denied
grep: /var/log/vmware-vmsvc-root.3.log: Permission denied
grep: /var/log/boot.log.2: Permission denied
grep: /var/log/btmp: Permission denied
grep: /var/log/boot.log.1: Permission denied
grep: /var/log/speech-dispatcher: Permission denied
grep: /var/log/vmware-vmsvc-root.2.log: Permission denied
/var/log/dpkg.log.1:2023-08-21 14:52:02 install libavahi-common-data:amd64 <none> 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 status half-installed libavahi-common-data:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 status unpacked libavahi-common-data:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 install libavahi-common3:amd64 <none> 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 status half-installed libavahi-common3:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 status unpacked libavahi-common3:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 install libavahi-client3:amd64 <none> 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 status half-installed libavahi-client3:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:02 status unpacked libavahi-client3:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:14 install libavahi-core7:amd64 <none> 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:14 status half-installed libavahi-core7:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:14 status unpacked libavahi-core7:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:14 install avahi-daemon:amd64 <none> 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:14 status half-installed avahi-daemon:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:14 status unpacked avahi-daemon:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:42 install libavahi-glib1:amd64 <none> 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:42 status half-installed libavahi-glib1:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:52:42 status unpacked libavahi-glib1:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:53:11 configure libavahi-common-data:amd64 0.8-10 <none>
/var/log/dpkg.log.1:2023-08-21 14:53:11 status unpacked libavahi-common-data:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:53:11 status half-configured libavahi-common-data:amd64 0.8-1
/var/log/dpkg.log.1:2023-08-21 14:53:11 status installed libavahi-common-data:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:53:15 configure libavahi-common3:amd64 0.8-10 <none>
/var/log/dpkg.log.1:2023-08-21 14:53:15 status unpacked libavahi-common3:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:53:15 status half-configured libavahi-common3:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:53:15 status installed libavahi-common3:amd64 0.8-10
/var/log/dpkg.log.1:2023-08-21 14:53:16 configure libavahi-glib1:amd64 0.8-10 <none>
/var/log/dpkg.log.1:2023-08-21 14:53:16 status unpacked libavahi-glib1:amd64 0.8-10
```

70. View the system’s kernel version.



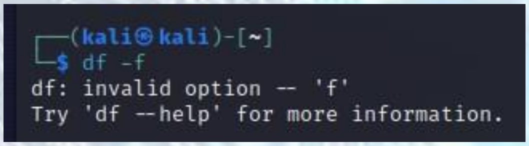
```
┌──(kali㉿kali)-[~]
└─$ uname -r
6.3.0-kali1-amd64
```

71. Display the system’s memory usage.



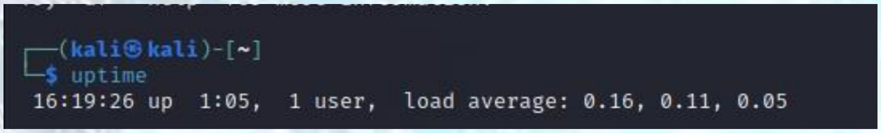
```
┌──(kali㉿kali)-[~]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       760Mi       665Mi       6.6Mi       685Mi       1.2Gi
Swap:          1.0Gi          0B       1.0Gi
```

72. Show the system’s disk usage.



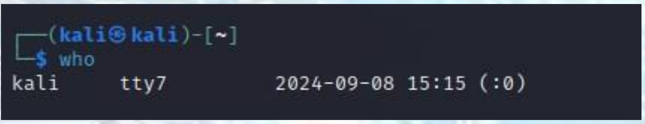
```
┌──(kali㉿kali)-[~]
└─$ df -f
df: invalid option -- 'f'
Try 'df --help' for more information.
```

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



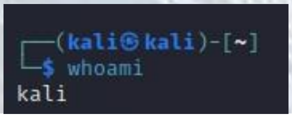
```
┌──(kali㉿kali)-[~]
└─$ uptime
 16:19:26 up  1:05,  1 user,  load average: 0.16, 0.11, 0.05
```

74. Display the current logged-in users.



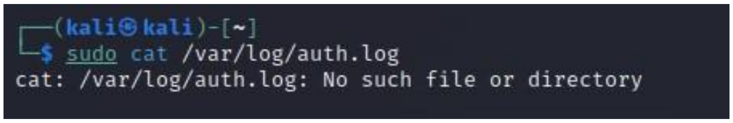
```
┌──(kali㉿kali)-[~]
└─$ who
kali     tty7         2024-09-08 15:15 (:0)
```

75. Check the identity of the current user.



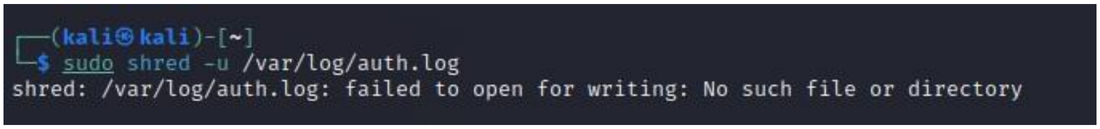
```
┌──(kali㉿kali)-[~]
└─$ whoami
kali
```

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



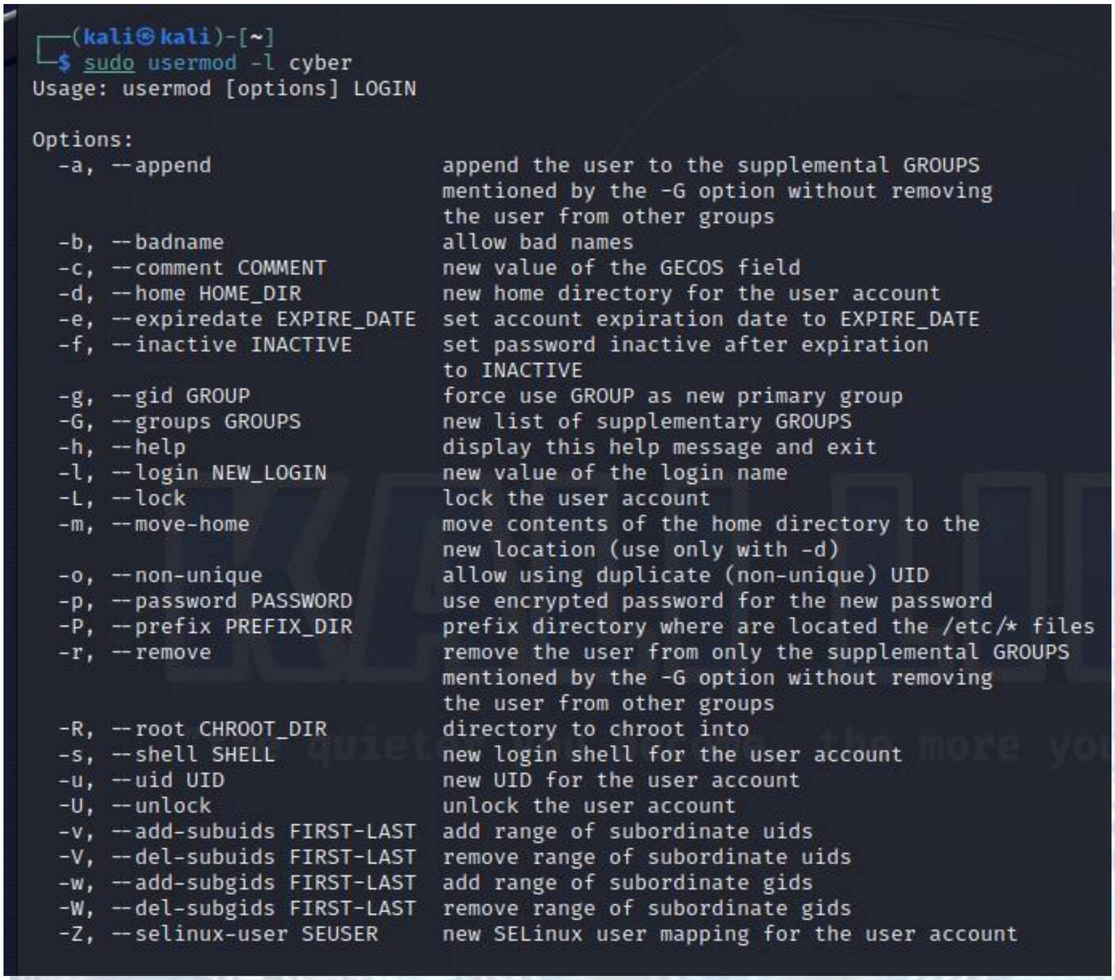
```
┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log
cat: /var/log/auth.log: No such file or directory
```

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



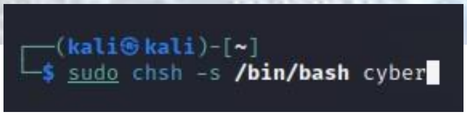
```
┌──(kali㉿kali)-[~]
└─$ sudo shred -u /var/log/auth.log
shred: /var/log/auth.log: failed to open for writing: No such file or directory
```

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



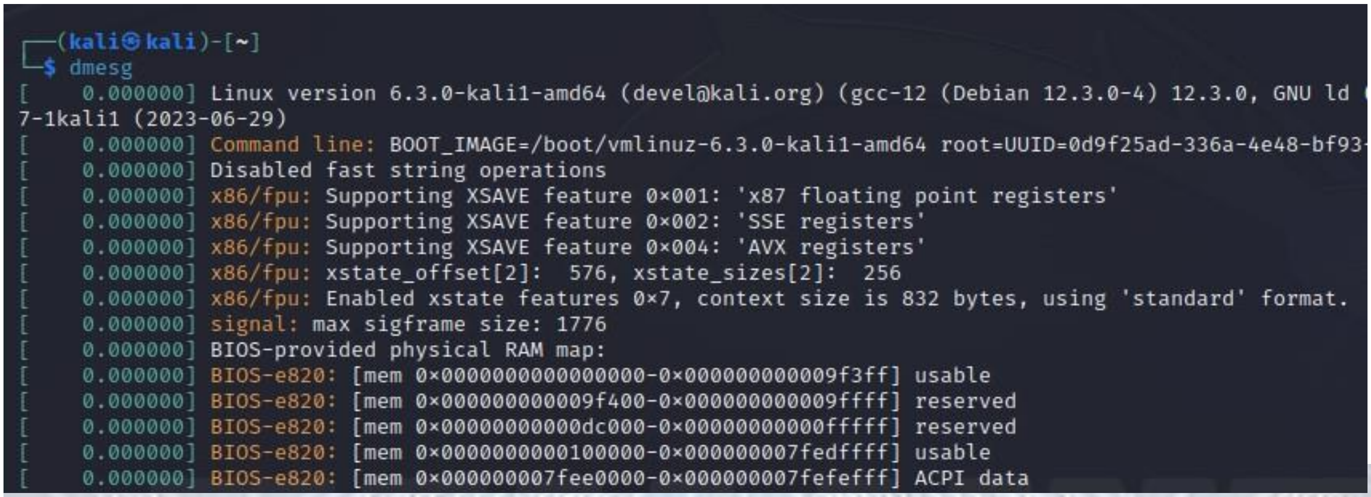
```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -l cyber
Usage: usermod [options] LOGIN

Options:
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -b, --badname                 allow bad names
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -r, --remove                  remove the user from only the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```

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



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

80. **Display the system's boot messages.**



```
┌──(kali㉿kali)-[~]
└─$ dmesg
[    0.000000] Linux version 6.3.0-kali1-amd64 (devel@kali.org) (gcc-12 (Debian 12.3.0-4) 12.3.0, GNU ld (
7-1kali1 (2023-06-29)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.3.0-kali1-amd64 root=UUID=0d9f25ad-336a-4e48-bf93-
[    0.000000] Disabled fast string operations
[    0.000000] x86/fpu: Supporting XSAVE feature 0×001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0×002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0×004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0×7, context size is 832 bytes, using 'standard' format.
[    0.000000] signal: max sigframe size: 1776
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0×0000000000000000-0×000000000009f3ff] usable
[    0.000000] BIOS-e820: [mem 0×000000000009f400-0×000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0×00000000000dc000-0×00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0×0000000000100000-0×000000007fedffff] usable
[    0.000000] BIOS-e820: [mem 0×000000007fee0000-0×000000007fefefff] ACPI data
```

اعداد الطالب: اصيل بدري العزي حفيظ

تم بحمد اللة وفضلة ومعونته