MID EXAM

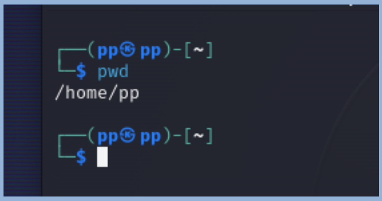
admin2

الدكتور :عبد الرزاق مبروك عبد الولى عبده ثابت امن سيبرانى د(1)

Mid Exam

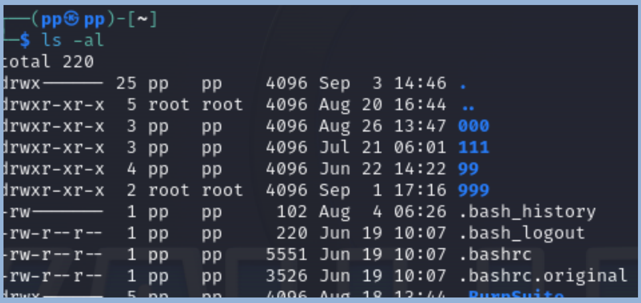
Section 1: File and Directory Management:

1. Display the current working directory.



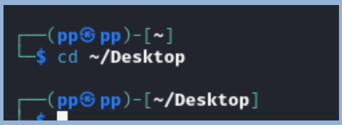
```
┌──(pp㉿pp)-[~]
└─$ pwd
/home/pp

┌──(pp㉿pp)-[~]
└─$ █
```

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



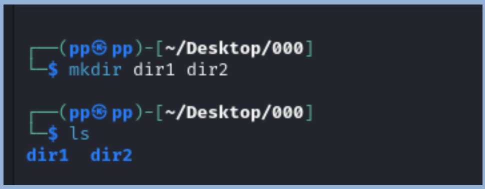
```
──(pp㉿pp)-[~]
─$ ls -al
total 220
drwx------ 25 pp   pp    4096 Sep  3 14:46 .
drwxr-xr-x  5 root root  4096 Aug 20 16:44 ..
drwxr-xr-x  3 pp   pp    4096 Aug 26 13:47 000
drwxr-xr-x  3 pp   pp    4096 Jul 21 06:01 111
drwxr-xr-x  4 pp   pp    4096 Jun 22 14:22 99
drwxr-xr-x  2 root root  4096 Sep  1 17:16 999
-rw-------  1 pp   pp     102 Aug  4 06:26 .bash_history
-rw-r--r--  1 pp   pp     220 Jun 19 10:07 .bash_logout
-rw-r--r--  1 pp   pp    5551 Jun 19 10:07 .bashrc
-rw-r--r--  1 pp   pp    3526 Jun 19 10:07 .bashrc.original
drwx------  5 pp   pp    4096 Aug 18 13:44  BurpSuite
```

3. Change your directory to the `Desktop`.



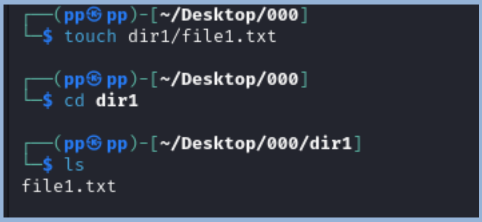
```
┌──(pp㉿pp)-[~]
└─$ cd ~/Desktop

┌──(pp㉿pp)-[~/Desktop]
└─$ █
```

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



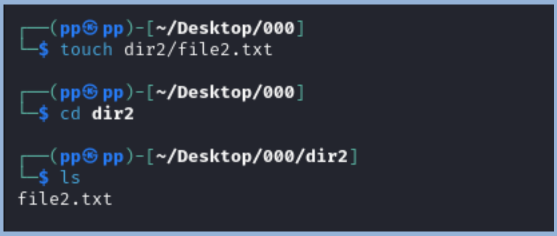
```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ mkdir dir1 dir2

┌──(pp㉿pp)-[~/Desktop/000]
└─$ ls
dir1  dir2
```

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



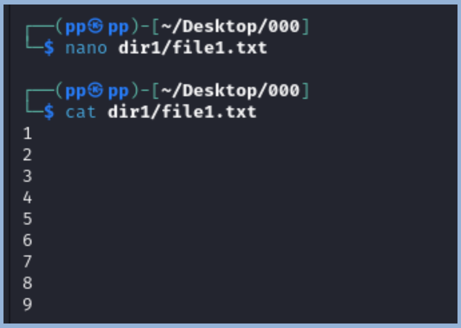
```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ touch dir1/file1.txt

┌──(pp㉿pp)-[~/Desktop/000]
└─$ cd dir1

┌──(pp㉿pp)-[~/Desktop/000/dir1]
└─$ ls
file1.txt
```

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



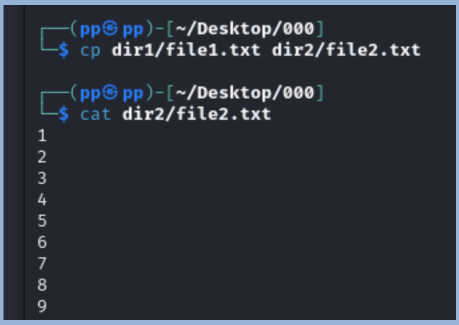
```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ touch dir2/file2.txt

┌──(pp㉿pp)-[~/Desktop/000]
└─$ cd dir2

┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ ls
file2.txt
```

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



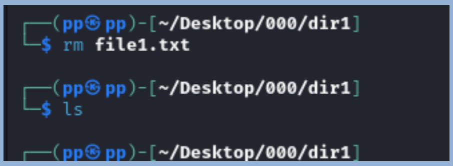
```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ nano dir1/file1.txt

┌──(pp㉿pp)-[~/Desktop/000]
└─$ cat dir1/file1.txt
1
2
3
4
5
6
7
8
9
```

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



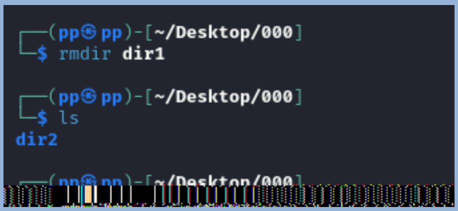
```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ cp dir1/file1.txt dir2/file2.txt

┌──(pp㉿pp)-[~/Desktop/000]
└─$ cat dir2/file2.txt
1
2
3
4
5
6
7
8
9
```

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



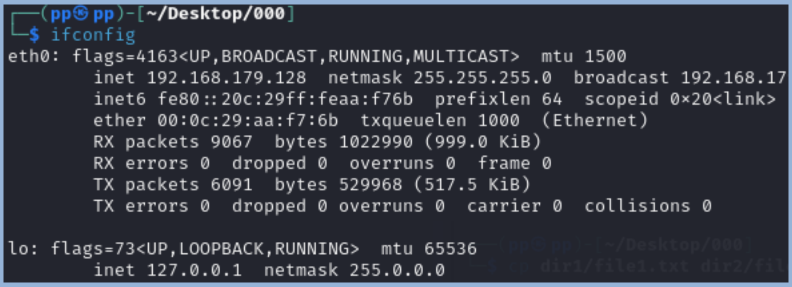
```
┌──(pp㉿pp)-[~/Desktop/000/dir1]
└─$ rm file1.txt

┌──(pp㉿pp)-[~/Desktop/000/dir1]
└─$ ls

┌──(pp㉿pp)-[~/Desktop/000/dir1]
```

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



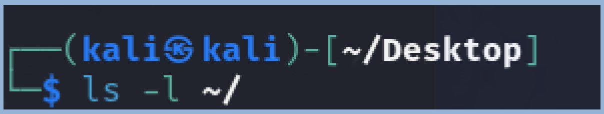
```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ rmdir dir1

┌──(pp㉿pp)-[~/Desktop/000]
└─$ ls
dir2

┌──(pp㉿pp)-[~/Desktop/000]
```

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



```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.179.128  netmask 255.255.255.0  broadcast 192.168.17
        inet6 fe80::20c:29ff:feaa:f76b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:aa:f7:6b  txqueuelen 1000  (Ethernet)
        RX packets 9067  bytes 1022990 (999.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6091  bytes 529968 (517.5 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
```

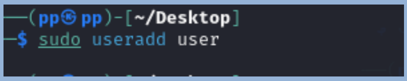
12. Open the Desktop folder and show all files with detailed information.



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

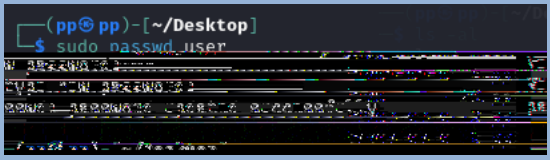
Section 2: Users and Groups Management:

13. Create a new user with your name.



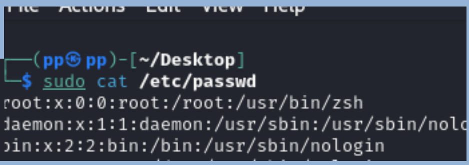
```
┌──(pp㉿pp)-[~/Desktop]
└─$ sudo useradd user
```

14. Set a password for your user.

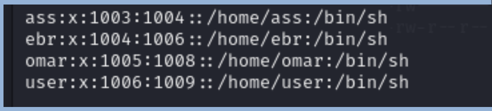


```
┌──(pp㉿pp)-[~/Desktop]
└─$ sudo passwd user
```

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

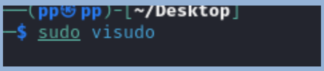


```
┌──(pp㉿pp)-[~/Desktop]
└─$ sudo cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nolo
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

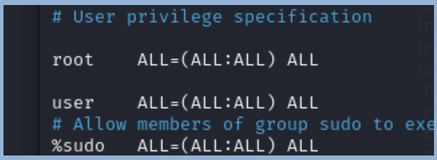


```
ass:x:1003:1004::/home/ass:/bin/sh
ebr:x:1004:1006::/home/ebr:/bin/sh
omar:x:1005:1008::/home/omar:/bin/sh
user:x:1006:1009::/home/user:/bin/sh
```

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

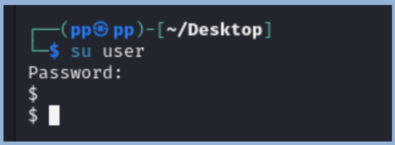


```
┌──(pp㉿pp)-[~/Desktop]
└─$ sudo visudo
```



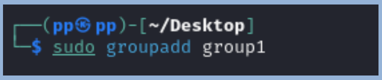
```
# User privilege specification

root    ALL=(ALL:ALL) ALL

user    ALL=(ALL:ALL) ALL
# Allow members of group sudo to exe
%sudo   ALL=(ALL:ALL) ALL
```

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



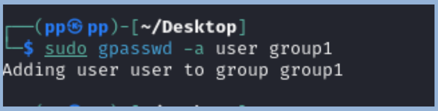
```
┌──(pp㉿pp)-[~/Desktop]
└─$ su user
Password:
$
$ █
```

18. Create a new group named `testgroup`.



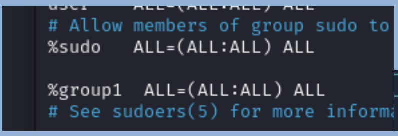
```
┌──(pp㉿pp)-[~/Desktop]
└─$ sudo groupadd group1
```

19. Add your user to `testgroup`.

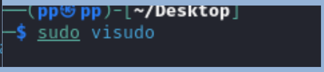


```
┌──(pp㉿pp)-[~/Desktop]
└─$ sudo gpasswd -a user group1
Adding user user to group group1
```

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

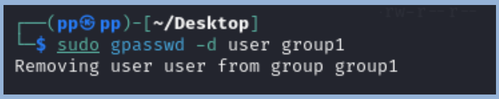


```
# Allow members of group sudo to
%sudo   ALL=(ALL:ALL) ALL

%group1  ALL=(ALL:ALL) ALL
# See sudoers(5) for more informa
```



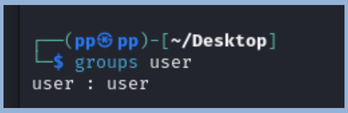
```
──(pp㉿pp)-[~/Desktop]
└─$ sudo visudo
```

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



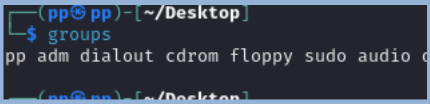
```
┌──(pp㉿pp)-[~/Desktop]
└─$ sudo gpasswd -d user group1
Removing user user from group group1
```

22. Check if your user still have administrative privileges.



```
┌──(pp㉿pp)-[~/Desktop]
└─$ groups user
user : user
```

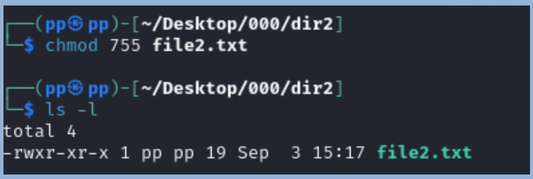
23. Check which groups your user belongs to.



```
┌──(pp㉿pp)-[~/Desktop]
└─$ groups
pp adm dialout cdrom floppy sudo audio d
```

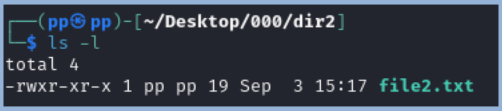
Section 3: Permissions and Ownership:

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 .



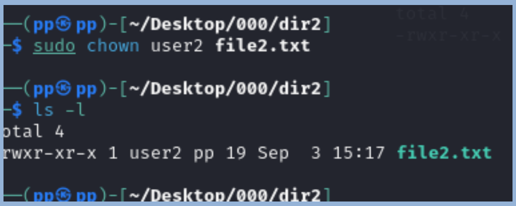
```
┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ chmod 755 file2.txt

┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ ls -l
total 4
-rwxr-xr-x 1 pp pp 19 Sep  3 15:17 file2.txt
```

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



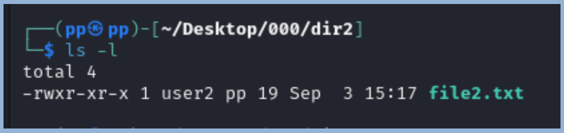
```
┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ ls -l
total 4
-rwxr-xr-x 1 pp pp 19 Sep  3 15:17 file2.txt
```

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



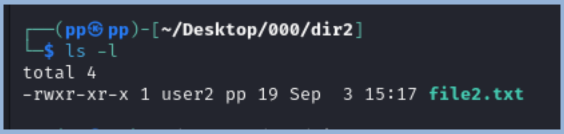
```
─(pp㉿pp)-[~/Desktop/000/dir2]
─$ sudo chown user2 file2.txt

─(pp㉿pp)-[~/Desktop/000/dir2]
─$ ls -l
otal 4
rwxr-xr-x 1 user2 pp 19 Sep  3 15:17 file2.txt

─(pp㉿pp)-[~/Desktop/000/dir2]
```

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



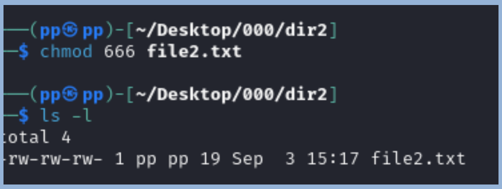
```
┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ ls -l
total 4
-rwxr-xr-x 1 user2 pp 19 Sep  3 15:17 file2.txt
```

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



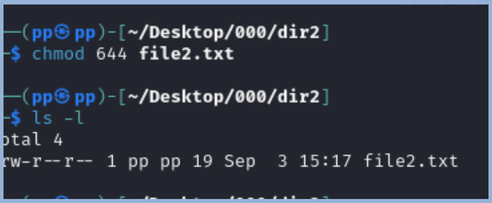
```
┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ ls -l
total 4
-rwxr-xr-x 1 user2 pp 19 Sep  3 15:17 file2.txt
```

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



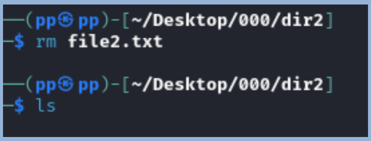
```
─(pp㉿pp)-[~/Desktop/000/dir2]
─$ chmod 666 file2.txt

─(pp㉿pp)-[~/Desktop/000/dir2]
─$ ls -l
otal 4
rw-rw-rw- 1 pp pp 19 Sep  3 15:17 file2.txt
```

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



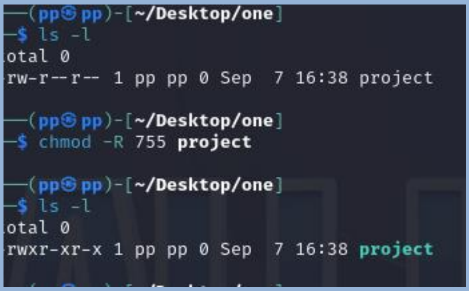
```
─(pp㉿pp)-[~/Desktop/000/dir2]
─$ chmod 644 file2.txt

─(pp㉿pp)-[~/Desktop/000/dir2]
─$ ls -l
otal 4
rw-r--r-- 1 pp pp 19 Sep  3 15:17 file2.txt
```

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



```
──(pp㉿pp)-[~/Desktop/000/dir2]
─$ rm file2.txt

──(pp㉿pp)-[~/Desktop/000/dir2]
─$ ls
```

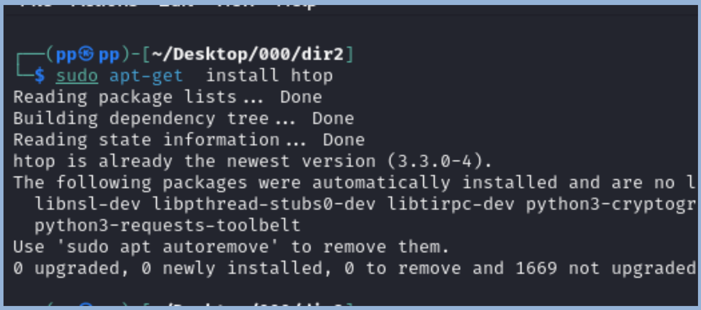
32. What command would you use to recursively change the permissions of all files and directories inside a folder named `project` to `755`.



```
──(pp㉿pp)-[~/Desktop/one]
─$ ls -l
otal 0
rw-r--r-- 1 pp pp 0 Sep  7 16:38 project

──(pp㉿pp)-[~/Desktop/one]
─$ chmod -R 755 project

──(pp㉿pp)-[~/Desktop/one]
─$ ls -l
otal 0
rwxr-xr-x 1 pp pp 0 Sep  7 16:38 project
```

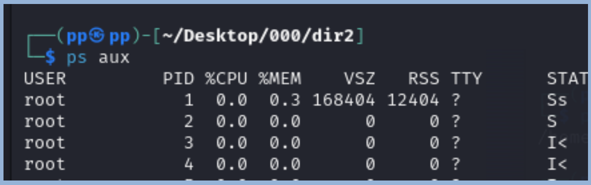
Section 4: Process Management:

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



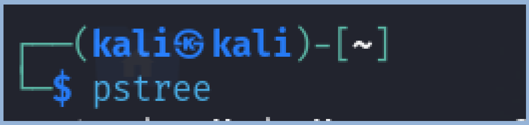
```
┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ sudo apt-get  install htop
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
htop is already the newest version (3.3.0-4).
The following packages were automatically installed and are no l
  libnsl-dev libpthread-stubs0-dev libtirpc-dev python3-cryptogr
  python3-requests-toolbelt
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1669 not upgraded
```

34. Display all running processes.



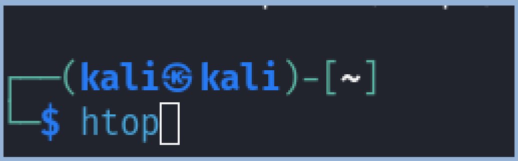
```
┌──(pp㉿pp)-[~/Desktop/000/dir2]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT
root           1  0.0  0.3 168404 12404 ?        Ss
root           2  0.0  0.0      0     0 ?        S
root           3  0.0  0.0      0     0 ?        I<
root           4  0.0  0.0      0     0 ?        I<
```

35. Display a tree of all running processes.



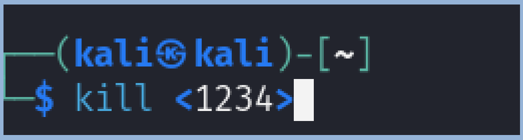
```
┌──(kali㉿kali)-[~]
└─$ pstree
```

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



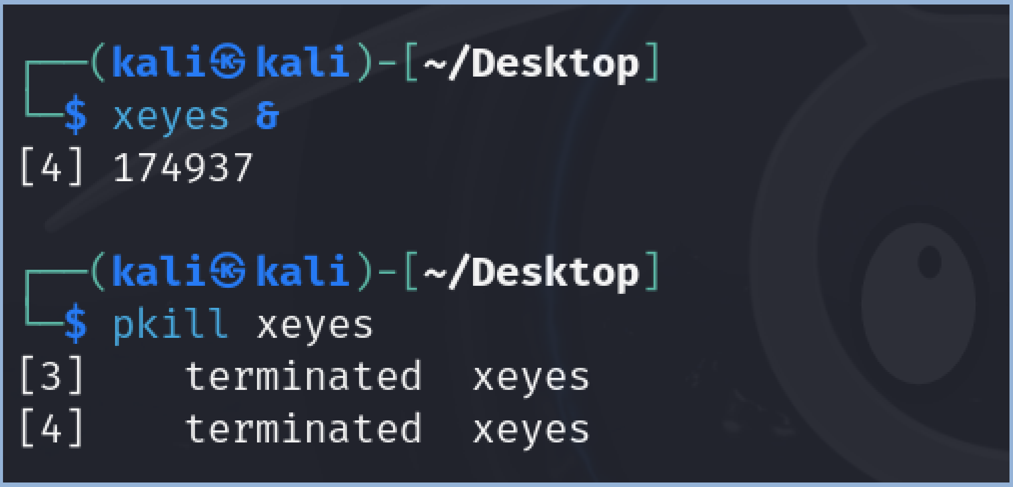
```
┌──(kali㉿kali)-[~]
└─$ htop
```

37. Kill a process with a specific PID.



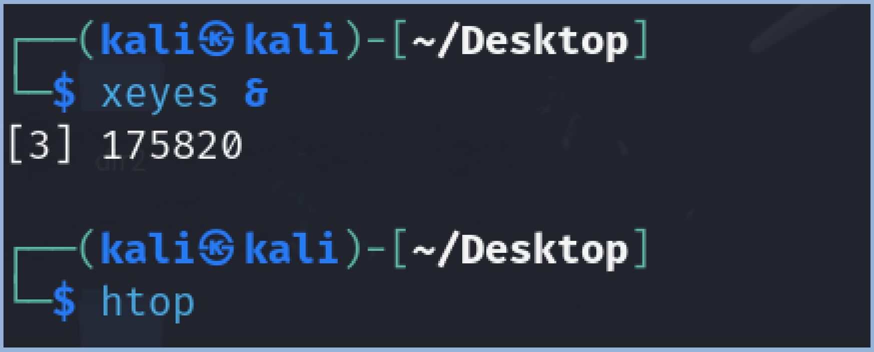
```
──(kali㉿kali)-[~]
─$ kill <1234>
```

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



```
┌──(kali㉿kali)-[~/Desktop]
└─$ xeyes &
[4] 174937

┌──(kali㉿kali)-[~/Desktop]
└─$ pkill xeyes
[3]    terminated  xeyes
[4]    terminated  xeyes
```

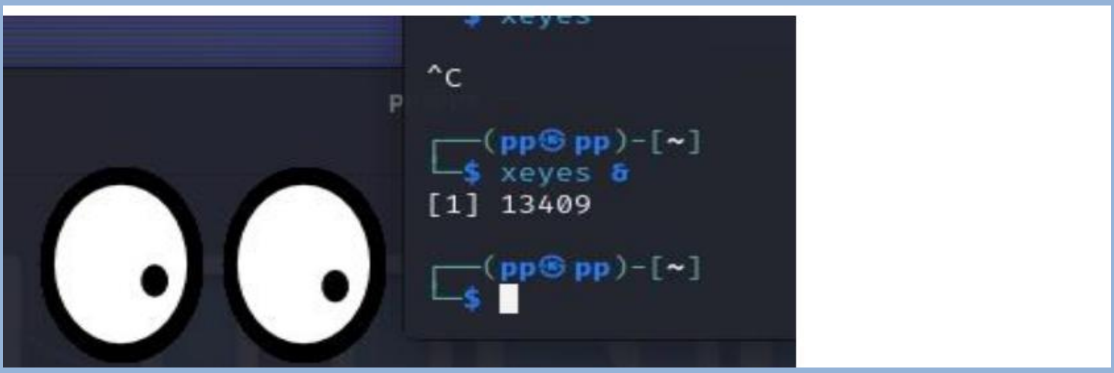
39. Restart the application, then stop it using the interactive process viewer.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ xeyes &
[3] 175820

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

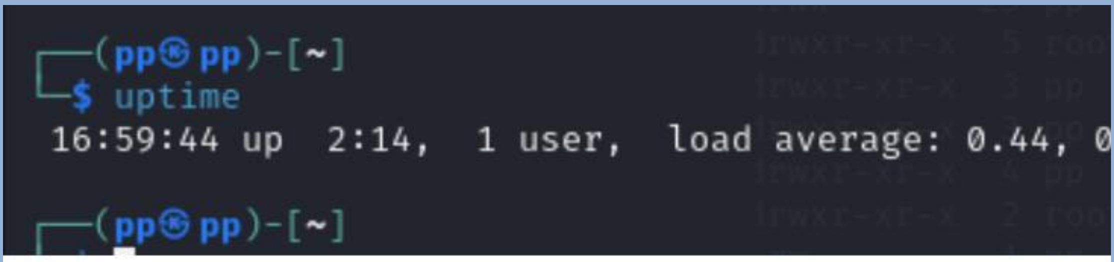
نحدد على العملية الذي نريد ايقافها ونقوم بضغط على F9

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



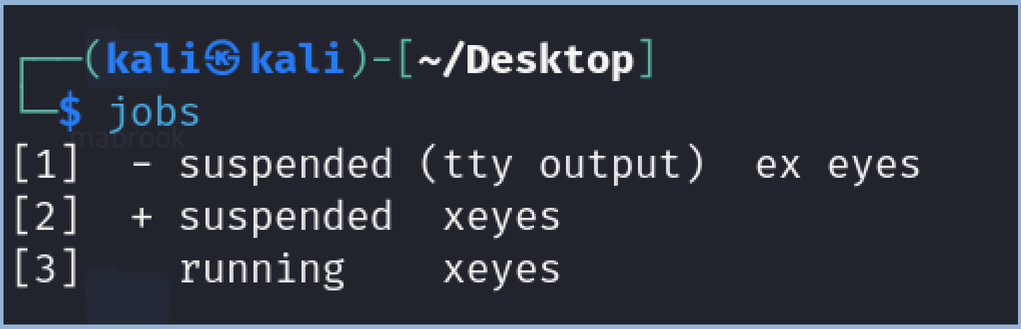
```
  $ xeyes

^C

┌──(pp㉿pp)-[~]
└─$ xeyes &
[1] 13409

┌──(pp㉿pp)-[~]
└─$ █
```

41. Check how long the system has been running.



```
┌──(pp㉿pp)-[~]
└─$ uptime
 16:59:44 up  2:14,  1 user,  load average: 0.44, 0

┌──(pp㉿pp)-[~]
```

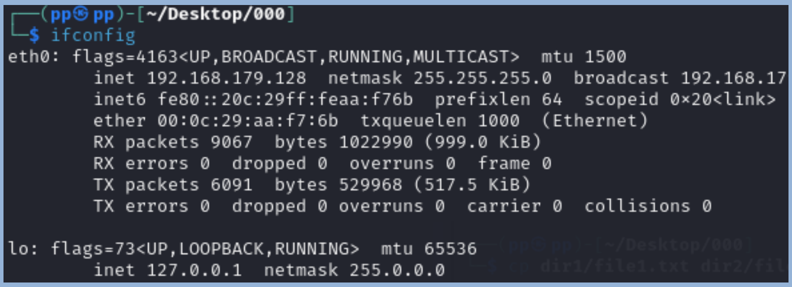
42. List all jobs running in the background.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ jobs
[1]  - suspended (tty output)  ex eyes
[2]  + suspended  xeyes
[3]    running    xeyes
```

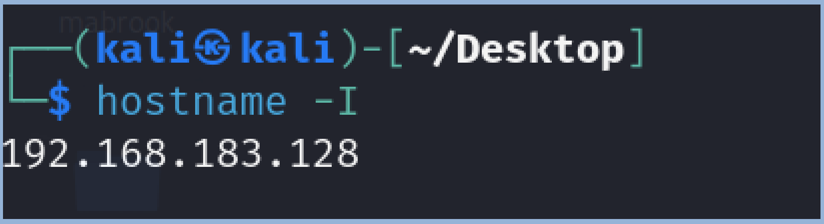
Section 5: Networking Commands:

43. Display the network configuration.



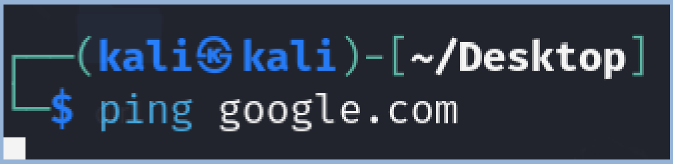
```
┌──(pp㉿pp)-[~/Desktop/000]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.179.128  netmask 255.255.255.0  broadcast 192.168.17
        inet6 fe80::20c:29ff:feaa:f76b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:aa:f7:6b  txqueuelen 1000  (Ethernet)
        RX packets 9067  bytes 1022990 (999.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6091  bytes 529968 (517.5 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
```

44. Check the IP address of your machine.



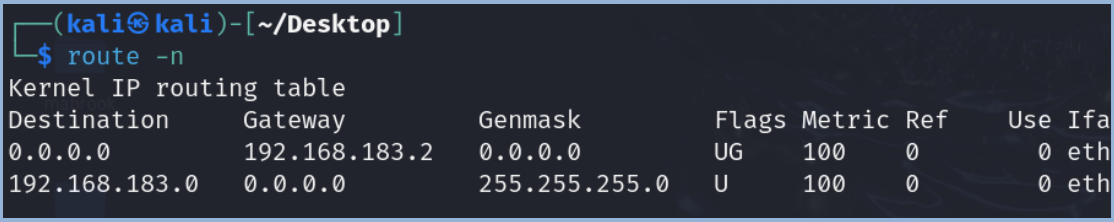
```
┌──(kali㉿kali)-[~/Desktop]
└─$ hostname -I
192.168.183.128
```

45. Test connectivity to an external server.



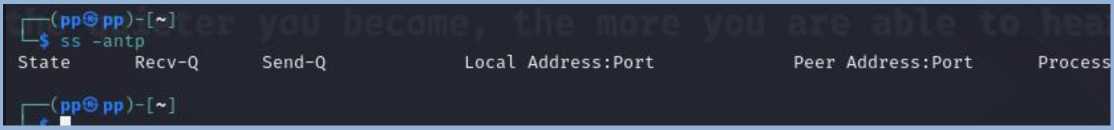
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping google.com
```

46. Display the routing table.



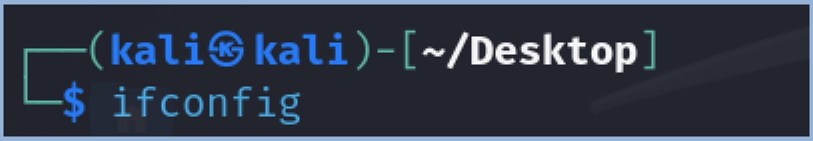
```
┌──(kali㉿kali)-[~/Desktop]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Ifa
0.0.0.0         192.168.183.2   0.0.0.0         UG    100    0        0 eth
192.168.183.0   0.0.0.0         255.255.255.0   U     100    0        0 eth
```

47. Check the open ports and active connections.



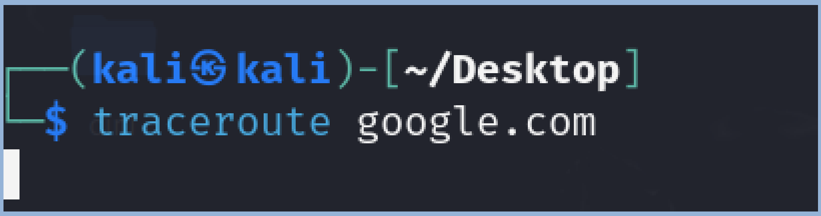
```
┌──(pp㉿pp)-[~]
└─$ ss -antp
State      Recv-Q     Send-Q          Local Address:Port          Peer Address:Port     Process

┌──(pp㉿pp)-[~]
└─$
```

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



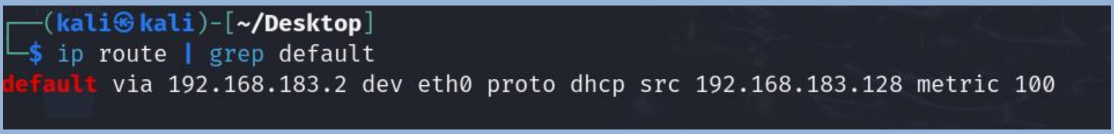
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
```

49. Trace the route to an external server.



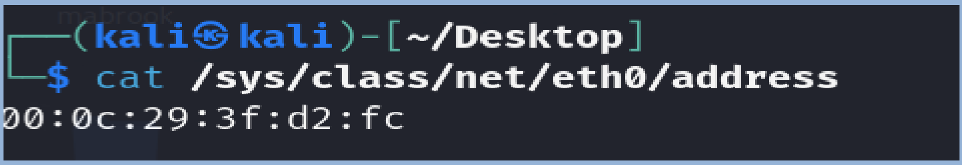
```
┌──(kali㉿kali)-[~/Desktop]
└─$ traceroute google.com
```

50. Find out the default gateway.



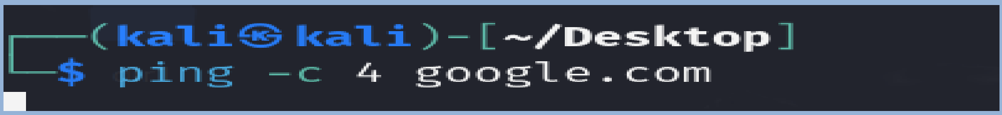
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ip route | grep default
default via 192.168.183.2 dev eth0 proto dhcp src 192.168.183.128 metric 100
```

51. Check the MAC address of your network interface.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat /sys/class/net/eth0/address
00:0c:29:3f:d2:fc
```

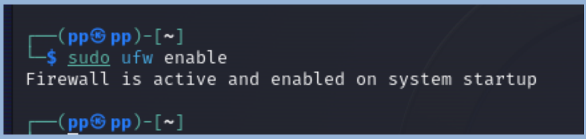
52. Ensure that the VM can access external networks.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -c 4 google.com
```

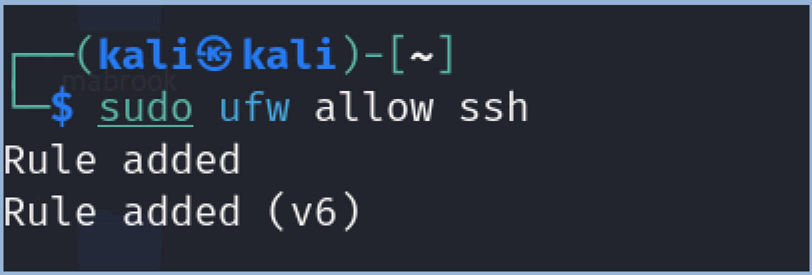
Section 6: UFW Firewall:

53. Enable the firewall.



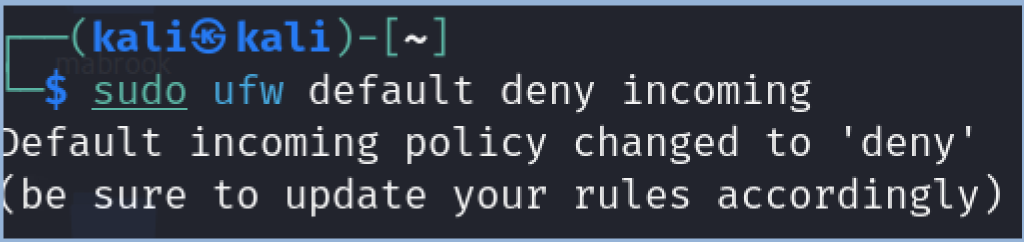
```
┌──(pp㉿pp)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(pp㉿pp)-[~]
```

54. Allow SSH connections through the firewall



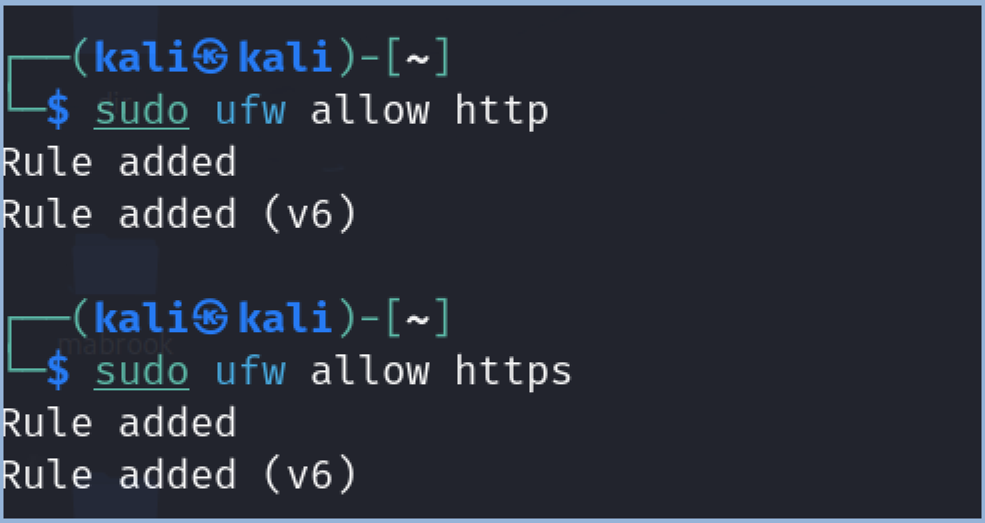
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)
```

55. Deny all incoming traffic by default.



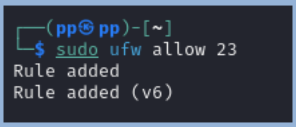
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

56. Allow HTTP and HTTPS traffic.



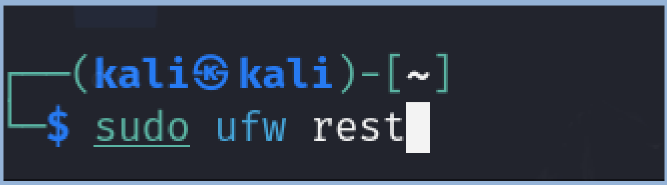
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow http
Rule added
Rule added (v6)

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

57. Allow port 23



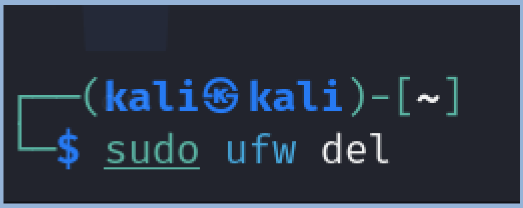
```
┌──(pp㉿pp)-[~]
└─$ sudo ufw allow 23
Rule added
Rule added (v6)
```

58. Reset the firewall settings.



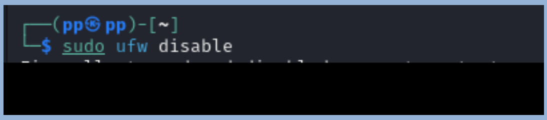
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw rest
```

59. Delete a rule from the firewall.



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

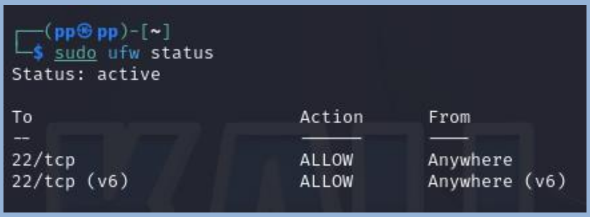
60. Disable the firewall.



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

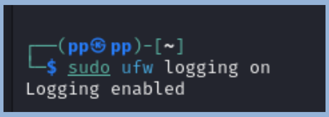
[redacted]

61. View the status of the firewall.



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

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

62. Log firewall activity and view it.

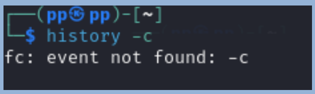


```
┌──(pp㉿pp)-[~]
└─$ sudo ufw logging on
Logging enabled
```

Section 7: Searching and System Information:

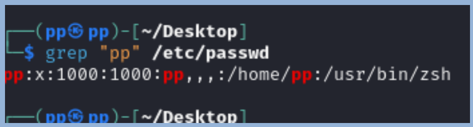
Section 7: Searching and System Information:

63. Delete the command history.:



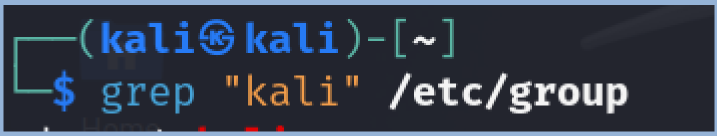
```
┌──(pp㉿pp)-[~]
└─$ history -c
fc: event not found: -c
```

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



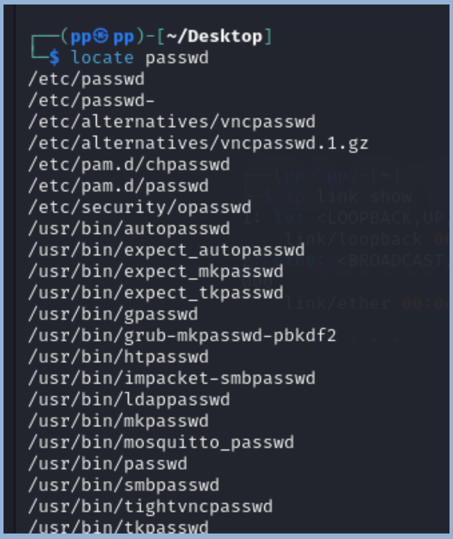
```
┌──(pp㉿pp)-[~/Desktop]
└─$ grep "pp" /etc/passwd
pp:x:1000:1000:pp,,,:/home/pp:/usr/bin/zsh

┌──(pp㉿pp)-[~/Desktop]
```

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



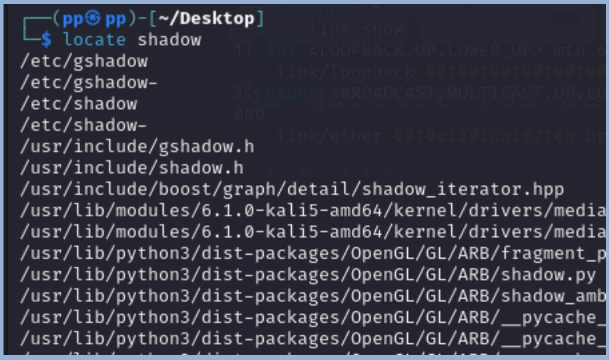
```
┌──(kali㉿kali)-[~]
└─$ grep "kali" /etc/group
```

66. Locate the `passwd` file.



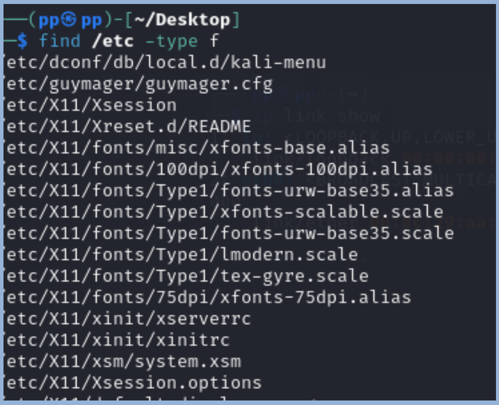
```
┌──(pp㉿pp)-[~/Desktop]
└─$ locate passwd
/etc/passwd
/etc/passwd-
/etc/alternatives/vncpasswd
/etc/alternatives/vncpasswd.1.gz
/etc/pam.d/chpasswd
/etc/pam.d/passwd
/etc/security/opasswd
/usr/bin/autopasswd
/usr/bin/expect_autopasswd
/usr/bin/expect_mkpasswd
/usr/bin/expect_tkpasswd
/usr/bin/gpasswd
/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
```

67. Locate the shadow file and open it.



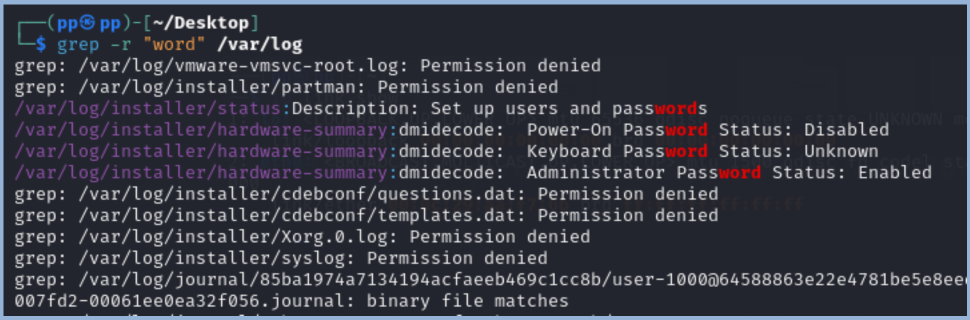
```
┌──(pp㉿pp)-[~/Desktop]
└─$ locate shadow
/etc/gshadow
/etc/gshadow-
/etc/shadow
/etc/shadow-
/usr/include/gshadow.h
/usr/include/shadow.h
/usr/include/boost/graph/detail/shadow_iterator.hpp
/usr/lib/modules/6.1.0-kali5-amd64/kernel/drivers/media
/usr/lib/modules/6.1.0-kali5-amd64/kernel/drivers/media
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/fragment_p
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/shadow.py
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/shadow_amb
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/__pycache_
/usr/lib/python3/dist-packages/OpenGL/GL/ARB/__pycache_
```

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



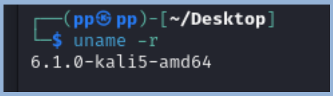
```
──(pp㉿pp)-[~/Desktop]
─$ find /etc -type f
/etc/dconf/db/local.d/kali-menu
/etc/guymager/guymager.cfg
/etc/X11/Xsession
/etc/X11/Xreset.d/README
/etc/X11/fonts/misc/xfonts-base.alias
/etc/X11/fonts/100dpi/xfonts-100dpi.alias
/etc/X11/fonts/Type1/fonts-urw-base35.alias
/etc/X11/fonts/Type1/xfonts-scalable.scale
/etc/X11/fonts/Type1/fonts-urw-base35.scale
/etc/X11/fonts/Type1/lmodern.scale
/etc/X11/fonts/Type1/tex-gyre.scale
/etc/X11/fonts/75dpi/xfonts-75dpi.alias
/etc/X11/xinit/xserverrc
/etc/X11/xinit/xinitrc
/etc/X11/xsm/system.xsm
/etc/X11/Xsession.options
```

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



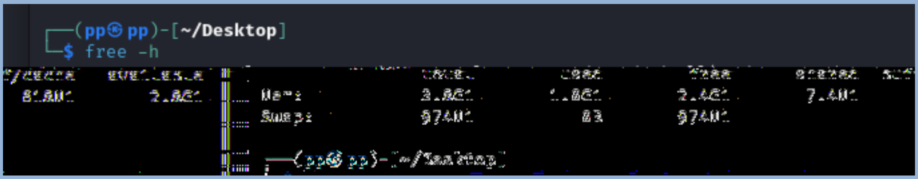
```
┌──(pp㉿pp)-[~/Desktop]
└─$ grep -r "word" /var/log
grep: /var/log/vmware-vmsvc-root.log: Permission denied
grep: /var/log/installer/partman: Permission denied
/var/log/installer/status:Description: Set up users and passwords
/var/log/installer/hardware-summary:dmidecode:  Power-On Password Status: Disabled
/var/log/installer/hardware-summary:dmidecode:  Keyboard Password Status: Unknown
/var/log/installer/hardware-summary:dmidecode:  Administrator Password Status: Enabled
grep: /var/log/installer/cdebconf/questions.dat: Permission denied
grep: /var/log/installer/cdebconf/templates.dat: Permission denied
grep: /var/log/installer/Xorg.0.log: Permission denied
grep: /var/log/installer/syslog: Permission denied
grep: /var/log/journal/85ba1974a7134194acfaeeb469c1cc8b/user-1000@64588863e22e4781be5e8ee
007fd2-00061ee0ea32f056.journal: binary file matches
```

70. View the system’s kernel version.



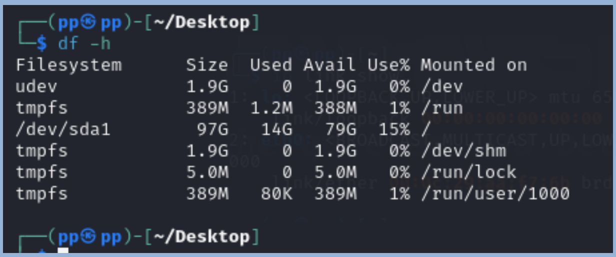
```
┌──(pp㉿pp)-[~/Desktop]
└─$ uname -r
6.1.0-kali5-amd64
```

71. Display the system’s memory usage.



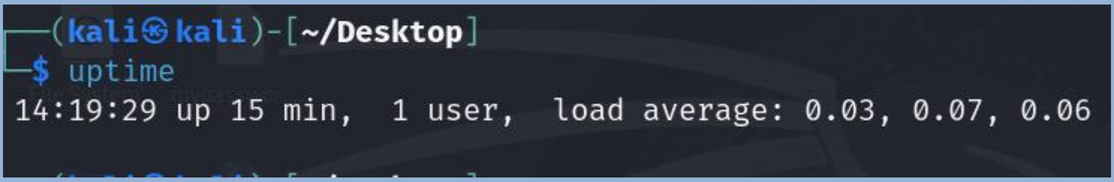
```
┌──(pp㉿pp)-[~/Desktop]
└─$ free -h
/cache   available        total        used        free      shared   buf
818Mi        2.8Gi   Mem:        3.8Gi       1.8Gi       2.4Gi       7.4Mi
                     Swap:       974Mi          0B       974Mi

                     ┌──(pp㉿pp)-[~/Desktop]
```

72. Show the system’s disk usage.



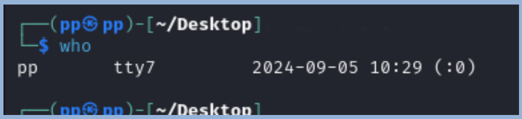
```
┌──(pp㉿pp)-[~/Desktop]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           389M  1.2M  388M   1% /run
/dev/sda1        97G   14G   79G  15% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           389M   80K  389M   1% /run/user/1000

┌──(pp㉿pp)-[~/Desktop]
```

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



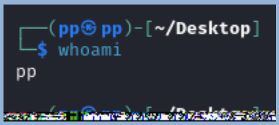
```
┌──(kali㉿kali)-[~/Desktop]
└─$ uptime
14:19:29 up 15 min,  1 user,  load average: 0.03, 0.07, 0.06
```

74. Display the current logged-in users.



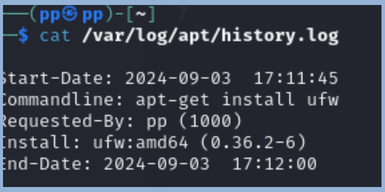
```
┌──(pp㉿pp)-[~/Desktop]
└─$ who
pp       tty7         2024-09-05 10:29 (:0)

┌──(pp㉿pp)-[~/Desktop]
```

75. Check the identity of the current user.



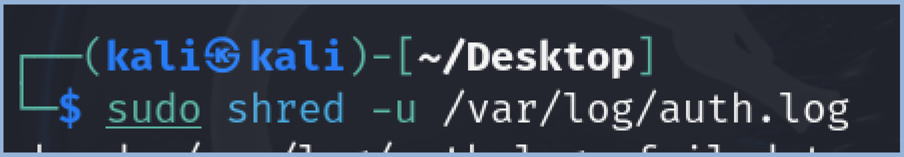
```
┌──(pp㉿pp)-[~/Desktop]
└─$ whoami
pp
```

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



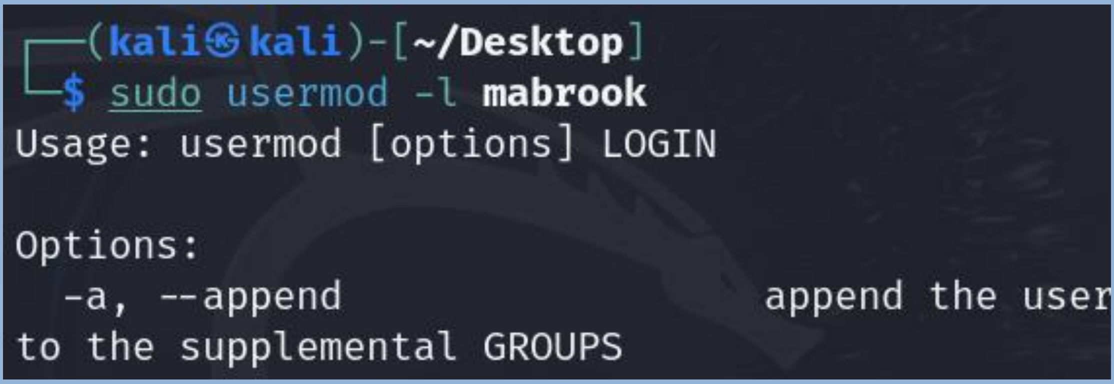
```
──(pp㉿pp)-[~]
─$ cat /var/log/apt/history.log

tart-Date: 2024-09-03  17:11:45
ommandline: apt-get install ufw
equested-By: pp (1000)
nstall: ufw:amd64 (0.36.2-6)
nd-Date: 2024-09-03  17:12:00
```

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



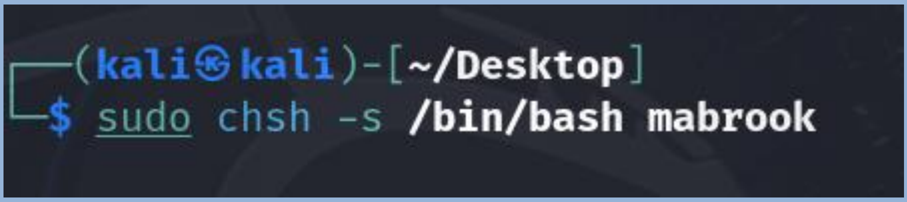
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo shred -u /var/log/auth.log
```

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



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

Options:
  -a, --append                  append the user
to the supplemental GROUPS
```

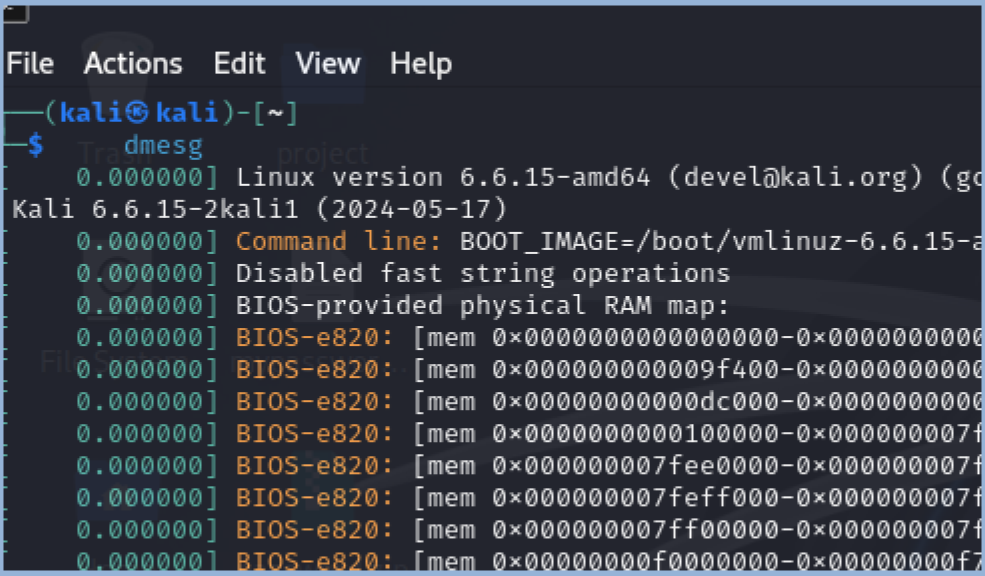
79. What command would you use to change a user's default shell.



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

sudo usermod -s /path/to/new/shell Ebrahim

80. Display the system's boot messages.



```
┌──(kali㉿kali)-[~]
└─$ dmesg
[    0.000000] Linux version 6.6.15-amd64 (devel@kali.org) (gc
Kali 6.6.15-2kali1 (2024-05-17)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-a
[    0.000000] Disabled fast string operations
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0×0000000000000000-0×0000000000
[    0.000000] BIOS-e820: [mem 0×000000000009f400-0×0000000000
[    0.000000] BIOS-e820: [mem 0×00000000000dc000-0×0000000000
[    0.000000] BIOS-e820: [mem 0×0000000000100000-0×000000007f
[    0.000000] BIOS-e820: [mem 0×000000007fee0000-0×000000007f
[    0.000000] BIOS-e820: [mem 0×000000007feff000-0×000000007f
[    0.000000] BIOS-e820: [mem 0×000000007ff00000-0×000000007f
[    0.000000] BIOS-e820: [mem 0×00000000f0000000-0×00000000f7
```