Mid Exam

Section 1: File and Directory Management:

1. Display the current working directory.

```
┌──(pp㊵pp)-[~]
└─$ pwd
/home/pp

┌──(pp㊵pp)-[~]
└─$ ▉
```

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

```
──(pp㊵pp)-[~]
─$ 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`.

```
┌──(pp㊵pp)-[~]
└─$ cd ~/Desktop

┌──(pp㊵pp)-[~/Desktop]
└─$ ▉
```

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

```
┌──(pp㊵pp)-[~/Desktop/000]
└─$ mkdir dir1 dir2

┌──(pp㊵pp)-[~/Desktop/000]
└─$ ls
dir1  dir2
```

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

```
┌──(pp㊵pp)-[~/Desktop/000]
└─$ touch dir1/file1.txt

┌──(pp㊵pp)-[~/Desktop/000]
└─$ cd dir1

┌──(pp㊵pp)-[~/Desktop/000/dir1]
└─$ ls
file1.txt
```

ENG / Ebrahim Khalil AL_Hattami

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

```
┌──(pp㊉pp)-[~/Desktop/000]
└─$ touch dir2/file2.txt

┌──(pp㊉pp)-[~/Desktop/000]
└─$ cd dir2

┌──(pp㊉pp)-[~/Desktop/000/dir2]
└─$ ls
file2.txt
```

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

```
┌──(pp㊉pp)-[~/Desktop/000]
└─$ nano dir1/file1.txt

┌──(pp㊉pp)-[~/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`.

```
┌──(pp㊉pp)-[~/Desktop/000]
└─$ cp dir1/file1.txt dir2/file2.txt

┌──(pp㊉pp)-[~/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`.

```
┌──(pp㊉pp)-[~/Desktop/000/dir1]
└─$ rm file1.txt

┌──(pp㊉pp)-[~/Desktop/000/dir1]
└─$ ls

┌──(pp㊉pp)-[~/Desktop/000/dir1]
```

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

```
┌──(pp㊉pp)-[~/Desktop/000]
└─$ rmdir dir1

┌──(pp㊉pp)-[~/Desktop/000]
└─$ ls
dir2

┌──(pp㊉pp)-[~/Desktop/000]
└─$
```

ENG / Ebrahim Khalil AL_Hattami

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 0×20<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.

```
┌──(pp⊕pp)-[~/Desktop]
└─$ ls -al
total 44
drwxr-xr-x  4 pp    pp     4096 Sep  3 15:08 .
drwx───── 25 pp    pp     4096 Sep  3 14:46 ..
drwxr-xr-x  3 pp    pp     4096 Sep  3 15:22 000
drwxr-xr-x  3 pp    pp     4096 Aug 30 12:43 Cam-Dumper
-rwx───r--  1 pp    pp       12 Aug  4 05:49 file
-rwxr-xr-x  1 root  pp       20 Aug  4 15:39 file1
-rw-r--r--  1 root  root 10237 Jul  4 08:35 game.apk
-rw-r--r--  1 pp    pp      710 Aug 18 14:19 network_inf
-rw───────  1 pp    pp     3643 Aug 25 02:34 quiz02.sh
-rw-r--r--  1 pp    pp        0 Aug 30 12:41 tesdir
```

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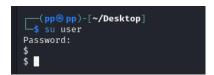
```
┌──(pp⊕pp)-[~/Desktop]
└─$ sudo cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nolo
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

```
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
```

ENG / Ebrahim Khalil AL_Hattami

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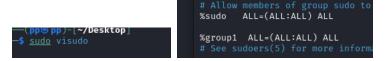
```
┌──(pp⊛pp)-[~/Desktop]
└─$ sudo groupadd group1
```

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.

```
┌──(pp⊛pp)-[~/Desktop]
└─$ sudo visudo
```
```
# Allow members of group sudo to
%sudo   ALL=(ALL:ALL) ALL

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

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
```

ENG / Ebrahim Khalil AL_Hattami

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
```

ENG / Ebrahim Khalil AL_Hattami

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<
```

ENG / Ebrahim Khalil AL_Hattami

35. Display a tree of all running processes.

```
┌──(pp☺pp)-[~/Desktop/000/dir2]
└─$ pstree
systemd─┬─ModemManager───2*[{ModemManager}]
        ├─NetworkManager───2*[{NetworkManager}]
        ├─agetty
        ├─colord───2*[{colord}]
        ├─cron
        ├─dbus-daemon
        ├─haveged
        ├─lightdm─┬─Xorg───{Xorg}
                  └─lightdm─┬─xfce4-session─┬─Thunar──2*
                                            ├─agent──2*[
                                            ├─blueman-app
                                            ├─light-locke
                                            └─nm-applet─
```

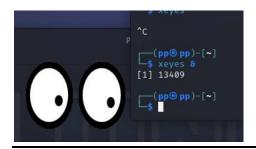36. Open the interactive process viewer and identify a process by its PID.

```
CPU[||||||||||||||||||||||||||||||||||     71.6%]  Tasks: 81, 136 thr, 107 kthr; 1 running
Mem[||||||||||||||||||              851M/3.79G]  Load average: 0.76 0.77 0.65
Swp[                                  0K/975M]  Uptime: 01:52:06

 Main    I/O
  PID△USER       PRI  NI   VIRT   RES   SHR S  CPU% MEM%   TIME+   Command
 1381 pp          20   0  12640   368     0 S   0.0  0.0  0:00.00   └ xcape -e Super_L Control
 1388 pp          20   0   281M 40980 30880 S   1.3  1.0  0:38.94  ─ /usr/bin/vmtoolsd -n vmusr
 1662 pp          20   0   281M 40980 30880 S   0.0  1.0  0:00.00   ├ /usr/bin/vmtoolsd -n vmu
 1663 pp          20   0   281M 40980 30880 S   0.0  1.0  0:00.00   ├ /usr/bin/vmtoolsd -n vmu
 1686 pp          20   0   281M 40980 30880 S   0.0  1.0  0:00.00   └ /usr/bin/vmtoolsd -n vmu
 1420 colord      20   0   238M 16680  9796 S   0.0  0.4  0:00.30  ─ /usr/libexec/colord
 1423 colord      20   0   238M 16680  9796 S   0.0  0.4  0:00.00   ├ /usr/libexec/colord
 1425 colord      20   0   238M 16680  9796 S   0.0  0.4  0:00.02   └ /usr/libexec/colord
 1555 pp          20   0   430M  105M 85472 S   0.0  2.7  0:25.40  ─ /usr/bin/qterminal
 1626 pp          20   0   430M  105M 85472 S   0.0  2.7  0:03.11   ├ /usr/bin/qterminal
 1661 pp          20   0   430M  105M 85472 S   0.0  2.7  0:00.00   ├ /usr/bin/qterminal
```

37. Kill a process with a specific PID.

```
File  Actions  Edit  View  Help
┌──(pp☺pp)-[~]
└─$ xeyes
```

```
File  Actions  Edit  View  Help
┌──(pp☺pp)-[~]
└─$ htop

┌──(pp☺pp)-[~]
└─$ kill 64372

┌──(pp☺pp)-[~]
└─$
```

```
┌──(pp☺pp)-[~]
└─$ xeyes
zsh: terminated   xeyes

┌──(pp☺pp)-[~]
└─$
```

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

```
┌──(pp☺pp)-[~]
└─$ xeyes
zsh: terminated   xeyes

┌──(pp☺pp)-[~]
└─$
```

```
┌──(pp☺pp)-[~]
└─$ htop

┌──(pp☺pp)-[~]
└─$ pkill xeyes

┌──(pp☺pp)-[~]
└─$
```

ENG / Ebrahim Khalil AL_Hattami

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

نحدد على العملية الذي نريد ايقافها ونقوم بضغط على **F9**

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

41. Check how long the system has been running.

42. List all jobs running in the background.

Section 5: Networking Commands:

43. Display the network configuration.

ENG / Ebrahim Khalil AL_Hattami

44. Check the IP address of your machine.

```
┌──(pp㉿pp)-[~]
$ ip addr show | grep inet
  inet 127.0.0.1/8 scope host lo
  inet6 ::1/128 scope host
  inet 192.168.179.128/24 brd 192.168.179.255 scope global dyna
  inet6 fe80::20c:29ff:feaa:f76b/64 scope link noprefixroute

┌──(pp㉿pp)-[~]
```

45. Test connectivity to an external server.

```
┌──(pp㉿pp)-[~]
└─$ ping 192.168.179.128
PING 192.168.179.128 (192.168.179.128) 56(84) bytes of data.
64 bytes from 192.168.179.128: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 192.168.179.128: icmp_seq=2 ttl=64 time=0.082 ms
64 bytes from 192.168.179.128: icmp_seq=3 ttl=64 time=0.080 ms
64 bytes from 192.168.179.128: icmp_seq=4 ttl=64 time=0.071 ms
64 bytes from 192.168.179.128: icmp_seq=5 ttl=64 time=0.084 ms
64 bytes from 192.168.179.128: icmp_seq=6 ttl=64 time=0.072 ms
64 bytes from 192.168.179.128: icmp_seq=7 ttl=64 time=0.073 ms
64 bytes from 192.168.179.128: icmp_seq=8 ttl=64 time=0.121 ms
64 bytes from 192.168.179.128: icmp_seq=9 ttl=64 time=0.073 ms
64 bytes from 192.168.179.128: icmp_seq=10 ttl=64 time=0.074 ms
64 bytes from 192.168.179.128: icmp_seq=11 ttl=64 time=0.072 ms
```

46. Display the routing table.

```
┌──(pp㉿pp)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.179.2   0.0.0.0         UG    100    0        0 eth0
192.168.179.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0

┌──(pp㉿pp)-[~]
```

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.

```
┌──(pp㉿pp)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    link/ether 00:0c:29:aa:f7:6b brd ff:ff:ff:ff:ff:ff
    inet 192.168.179.128/24 brd 192.168.179.255 scope global dynamic noprefixroute
       valid_lft 1190sec preferred_lft 1190sec
    inet6 fe80::20c:29ff:feaa:f76b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

ENG / Ebrahim Khalil AL_Hattami

49. Trace the route to an external server.

```
┌──(pp㉿pp)-[~]
└─$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.179.2 (192.168.179.2)  0.573 ms  0.451 ms  0.261 ms
 2  192.168.179.2 (192.168.179.2)  0.477 ms !N  0.240 ms !N  0.600 ms !N
```

50. Find out the default gateway.

```
┌──(pp㉿pp)-[~]
└─$ ip route show
default via 192.168.179.2 dev eth0 proto dhcp src 192.168.179.128 metric 100
192.168.179.0/24 dev eth0 proto kernel scope link src 192.168.179.128 metric 100
```

51. Check the MAC address of your network interface.

```
┌──(pp㉿pp)-[~]
└─$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group d
    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
000
    link/ether 00:0c:29:aa:f7:6b brd ff:ff:ff:ff:ff:ff
```

52. Ensure that the VM can access external networks.

```
┌──(pp㉿pp)-[~]
└─$ ping 192.168.179.128
PING 192.168.179.128 (192.168.179.128) 56(84) bytes of data.
64 bytes from 192.168.179.128: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 192.168.179.128: icmp_seq=2 ttl=64 time=0.082 ms
64 bytes from 192.168.179.128: icmp_seq=3 ttl=64 time=0.080 ms
64 bytes from 192.168.179.128: icmp_seq=4 ttl=64 time=0.071 ms
64 bytes from 192.168.179.128: icmp_seq=5 ttl=64 time=0.084 ms
64 bytes from 192.168.179.128: icmp_seq=6 ttl=64 time=0.072 ms
64 bytes from 192.168.179.128: icmp_seq=7 ttl=64 time=0.073 ms
64 bytes from 192.168.179.128: icmp_seq=8 ttl=64 time=0.121 ms
64 bytes from 192.168.179.128: icmp_seq=9 ttl=64 time=0.073 ms
64 bytes from 192.168.179.128: icmp_seq=10 ttl=64 time=0.074 ms
64 bytes from 192.168.179.128: icmp_seq=11 ttl=64 time=0.072 ms
```

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.

```
File  Actions  Edit  View  Help
┌──(pp㉿pp)-[~]
└─$ sudo ufw allow ssh
[sudo] password for pp:
Rule added
Rule added (v6)

┌──(pp㉿pp)-[~]
```

ENG / Ebrahim Khalil AL_Hattami

55. Deny all incoming traffic by default.

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

56. Allow HTTP and HTTPS traffic.

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

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

57. Allow port 23

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

58. Reset the firewall settings.

```
┌──(pp⊕pp)-[~]
└─$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y
Backing up 'user.rules' to '/etc/ufw/user.rules.20240907_173908'
Backing up 'before.rules' to '/etc/ufw/before.rules.20240907_173908'
Backing up 'after.rules' to '/etc/ufw/after.rules.20240907_173908'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20240907_173908'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20240907_173908
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20240907_173908'
```

59. Delete a rule from the firewall.

sudo ufw delete

60. Disable the firewall.

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

ENG / Ebrahim Khalil AL_Hattami

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:

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.

```
┌──(pp◉pp)-[~/Desktop]
└─$ grep "pp" /etc/group
adm:x:4:pp
dialout:x:20:pp
cdrom:x:24:pp
floppy:x:25:pp
sudo:x:27:pp
audio:x:29:pulse,pp
dip:x:30:pp
video:x:44:pp
plugdev:x:46:pp
users:x:100:pp
netdev:x:106:pp
wireshark:x:117:pp
bluetooth:x:120:pp
scanner:x:129:saned,pp
pp:x:1000:
kaboxer:x:140:pp

┌──(pp◉pp)-[~/Desktop]
```

ENG / Ebrahim Khalil AL_Hattami

66. Locate the `passwd` file.

```
┌──(pp㊷pp)-[~/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.

```
┌──(pp㊷pp)-[~/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.

```
┌──(pp㊷pp)-[~/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
```

ENG / Ebrahim Khalil AL_Hattami

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

```
┌──(pp㊀pp)-[~/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.

```
┌──(pp㊀pp)-[~/Desktop]
└─$ uname -r
6.1.0-kali5-amd64
```

71. Display the system's memory usage.

```
┌──(pp㊀pp)-[~/Desktop]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       1.0Gi       2.4Gi       7.4Mi       618Mi       2.8Gi
Swap:          974Mi          0B       974Mi
┌──(pp㊀pp)-[~/Desktop]
```

72. Show the system's disk usage.

```
┌──(pp㊀pp)-[~/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
┌──(pp㊀pp)-[~/Desktop]
```

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

```
┌──(pp㊀pp)-[~/Desktop]
└─$ uptime
 10:57:36 up 28 min,  1 user,  load average: 0.76, 0.84, 0.72
```

74. Display the current logged-in users.

```
┌──(pp㊀pp)-[~/Desktop]
└─$ who
pp       tty7         2024-09-05 10:29 (:0)
┌──(pp㊀pp)-[~/Desktop]
```

ENG / Ebrahim Khalil AL_Hattami

75. Check the identity of the current user.

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

┌──(pp㉿pp)-[~/Desktop]
```

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

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

Start-Date: 2024-09-03  17:11:45
Commandline: apt-get install ufw
Requested-By: pp (1000)
Install: ufw:amd64 (0.36.2-6)
End-Date: 2024-09-03  17:12:00
```

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

```
┌──(pp㉿pp)-[~]
└─$ sudo shred -u /var/log/auth.log
shred: /var/log/auth.log: failed to open for writ
```

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

```
┌──(pp㉿pp)-[~]
└─$ sudo usermod -l user2
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
```

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

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

80. Display the system's boot messages.

ENG / Ebrahim Khalil AL_Hattami

```
┌──(pp⊛ pp)-[~]
└─$ dmesg
[    0.000000] Linux version 6.1.0-kali5-amd64 (devel@kali.org) (gcc-12 (Debian 1
U Binutils for Debian) 2.40) #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02
e94788f5c ro quiet splash
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.1.0-kali5-amd64 root=UUID
e94788f5c ro quiet splash
[    0.000000] Disabled fast string operations
[    0.000000] x86/fpu: Supporting XSAVE feature 0×001: 'x87 floating point regis
[    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, u
[    0.000000] signal: max sigframe size: 1776
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0×0000000000000000-0×000000000009ebff] usable
[    0.000000] BIOS-e820: [mem 0×000000000009ec00-0×000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0×00000000000dc000-0×00000000000fffff] reserved
```

ENG / Ebrahim Khalil AL_Hattami