

---

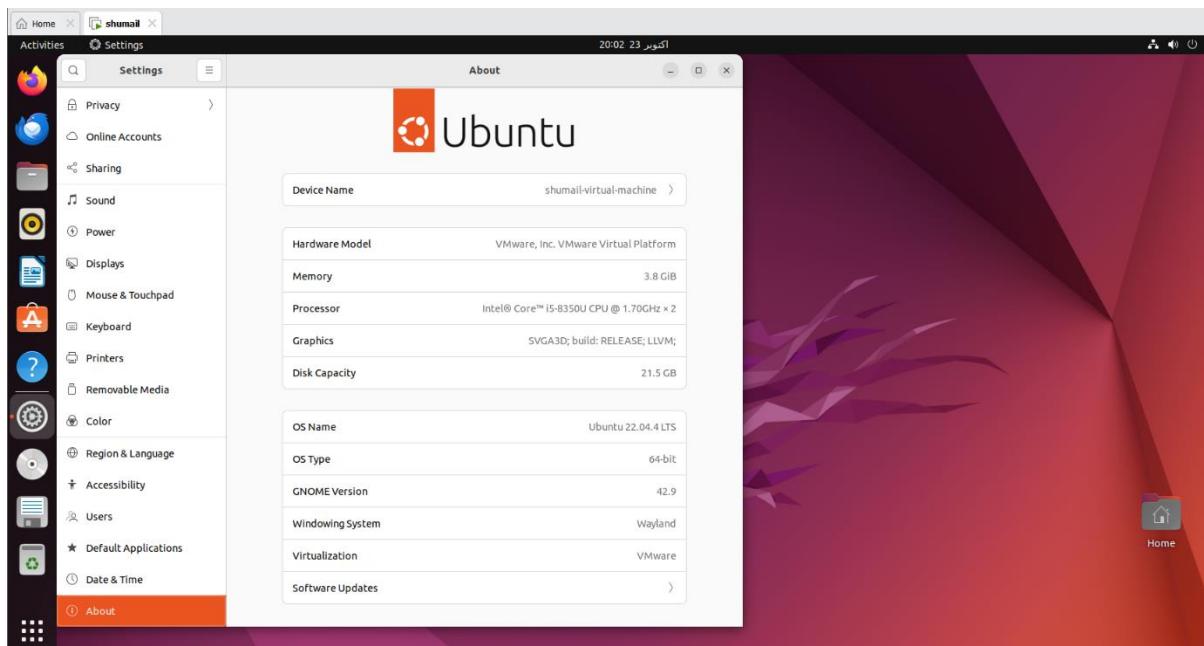
# **LAB 04**

---

**NAME: SHUMAIL ZAHRA  
REGISTRATION #: 2023-BSE-061  
DEPARTMENT: BSE(5B)**

## **LAB TASK**

### **Task 1 – Verify VM resources in VMware**



`vm_settings.png`

### **Task 2 – Start VM and log in (use your preferred host terminal method only)**

```
shumail@shumail-virtual-machine:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4b:47:b0 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.183.128/24 brd 192.168.183.255 scope global dynamic noprefixroute ens33
            valid_lft 1062sec preferred_lft 1062sec
        inet6 fe80::1ebab:2bdd:ca0e:1b26/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
shumail@shumail-virtual-machine: $ ssh shumail@192.168.183.128
The authenticity of host '192.168.183.128' (192.168.183.128) can't be established.
ED25519 key fingerprint is SHA256:M5baEBmbeBdRqYVoMEiQnPT8gHmf8fqGKCUk4N3JnaU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.183.128' (ED25519) to the list of known hosts.
shumail@192.168.183.128's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

263 updates can be applied immediately.
219 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

```
shumail@shumail-virtual-machine: $ ssh shumail@192.168.183.128
The authenticity of host '192.168.183.128' (192.168.183.128) can't be established.
ED25519 key fingerprint is SHA256:M5baEBmbeBdRqYVoMEiQnPT8gHmf8fqGKCUk4N3JnaU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.183.128' (ED25519) to the list of known hosts.
shumail@192.168.183.128's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

263 updates can be applied immediately.
219 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

shumail@shumail-virtual-machine: $
```

vm\_login.png

```
shumail@shumail-virtual-machine:~$ whoami
shumail
shumail@shumail-virtual-machine:~$ pwd
/home/shumail
shumail@shumail-virtual-machine:~$
```

whoami\_pwd.png

### Task 3 – Filesystem exploration — root tree and dotfiles

```
shumail@shumail-virtual-machine:~$ ls -la /
total 2191452
drwxr-xr-x 21 root root 4096 2024 25 سهیبر .
drwxr-xr-x 21 root root 4096 2024 25 سهیبر ..
drwxr-xr-x 3 root root 4096 2024 25 سهیبر app
lrwxrwxrwx 1 root root 7 2024 25 سهیبر bin -> usr/bin
drwxr-xr-x 4 root root 4096 2024 25 سهیبر boot
drwxrwxr-x 2 root root 4096 2024 25 سهیبر cdrom
drwxr-xr-x 19 root root 4160 19:56 23 اکتوبر dev
drwxr-xr-x 132 root root 12288 2024 25 سهیبر etc
drwxr-xr-x 4 root root 4096 2024 25 سهیبر home
lrwxrwxrwx 1 root root 7 2024 25 سهیبر lib -> usr/lib
lrwxrwxrwx 1 root root 9 2024 25 سهیبر lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 2024 25 سهیبر lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 2024 25 سهیبر libx32 -> usr/libx32
drwx----- 2 root root 16384 2024 25 سهیبر lost+found
drwxr-xr-x 4 root root 4096 2024 25 سهیبر media
drwxr-xr-x 2 root root 4096 2024 21 فروری mnt
drwxr-xr-x 2 root root 4096 2024 21 فروری opt
dr-xr-xr-x 366 root root 0 19:54 23 اکتوبر proc
drwx----- 5 root root 4096 2024 25 سهیبر root
drwxr-xr-x 36 root root 960 20:11 23 اکتوبر run
lrwxrwxrwx 1 root root 8 2024 25 سهیبر sbin -> usr/sbin
drwxr-xr-x 11 root root 4096 2024 21 فروری snap
drwxr-xr-x 2 root root 4096 2024 21 فروری srv
-rw----- 1 root root 2243952640 2024 25 سهیبر swapfile
dr-xr-xr-x 13 root root 0 19:54 23 اکتوبر sys
drwxrwxrwt 19 root root 4096 20:10 23 اکتوبر tmp
drwxr-xr-x 14 root root 4096 2024 21 فروری usr
drwxr-xr-x 14 root root 4096 2024 21 فروری var
shumail@shumail-virtual-machine:~$
```

ls\_root.png

```
shumail@shumail-virtual-machine:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 2024 25 سهیبر /bin -> usr/bin
```

ls\_bin.png

```
shumail@shumail-virtual-machine:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 2024 25 سهیبر /sbin -> usr/sbin
```

ls\_sbin.png

```
shumail@shumail-virtual-machine:~$ ls -la /usr
total 120
drwxr-xr-x 14 root root 4096 2024 21 فروری .
drwxr-xr-x 21 root root 4096 2024 25 سهیبر ..
drwxr-xr-x 2 root root 36864 2024 25 سهیبر bin
drwxr-xr-x 2 root root 4096 2024 21 فروری games
drwxr-xr-x 12 root root 4096 2024 25 سهیبر include
drwxr-xr-x 106 root root 4096 2024 25 سهیبر lib
drwxr-xr-x 2 root root 4096 2024 21 فروری lib32
drwxr-xr-x 2 root root 4096 2024 21 فروری lib64
drwxr-xr-x 23 root root 12288 2024 25 سهیبر libexec
drwxr-xr-x 2 root root 4096 2024 21 فروری libx32
drwxr-xr-x 10 root root 4096 2024 21 فروری local
drwxr-xr-x 2 root root 20480 2024 25 سهیبر sbin
drwxr-xr-x 267 root root 12288 2024 25 سهیبر share
drwxr-xr-x 6 root root 4096 2024 25 سهیبر src
```

ls\_usr.png

```
shumail@shumail-virtual-machine:~$ ls -la /opt
total 8
drwxr-xr-x 2 root root 4096 2024 21 فروري .
drwxr-xr-x 21 root root 4096 2024 25 سمبر ..
```

ls\_opt.png

```
shumail@shumail-virtual-machine:~$ ls -la /etc
total 1188
drwxr-xr-x 132 root root 12288 2024 25 سمبر .
drwxr-xr-x 21 root root 4096 2024 25 سمبر ..
drwxr-xr-x 3 root root 4096 2024 21 فروري acpi
-rw-r--r-- 1 root root 3028 2024 21 فروري adduser.conf
drwxr-xr-x 3 root root 4096 2024 21 فروري alsu
drwxr-xr-x 2 root root 12288 2024 25 سمبر alternatives
-rw-r--r-- 1 root root 335 2022 23 مارج anacrontab
-rw-r--r-- 1 root root 433 2022 23 مارج apg.conf
drwxr-xr-x 5 root root 4096 2024 21 فروري apm
drwxr-xr-x 3 root root 4096 2024 21 فروري apparmor
drwxr-xr-x 7 root root 4096 2024 25 سمبر apparmor.d
drwxr-xr-x 4 root root 4096 2024 21 فروري apport
-rw-r--r-- 1 root root 769 2022 22 فروري appstream.conf
drwxr-xr-x 8 root root 4096 2024 25 سمبر apt
drwxr-xr-x 3 root root 4096 2024 21 فروري avahi
-rw-r--r-- 1 root root 2319 2022 6 نوری bash.bashrc
-rw-r--r-- 1 root root 45 2021 11 نومبر bash_completion
drwxr-xr-x 2 root root 4096 2024 21 فروري bash_completion.d
-rw-r--r-- 1 root root 367 2020 16 سمبر bindresvport.blacklist
drwxr-xr-x 2 root root 4096 2022 8 ابريل binfmt.d
drwxr-xr-x 2 root root 4096 2024 21 فروري bluetooth
-rw-r----- 1 root root 33 2024 21 فروري brlapi.key
drwxr-xr-x 7 root root 4096 2024 21 فروري brltty
-rw-r--r-- 1 root root 29219 2022 28 حون brltty.conf
drwxr-xr-x 3 root root 4096 2024 21 فروري ca-certificates
-rw-r--r-- 1 root root 6253 2024 21 فروري ca-certificates.conf
-rw-r--r-- 1 root root 5529 2024 21 فروري ca-certificates.conf.dpkg-old
drwxr-s--- 2 root dip 4096 2024 21 فروري chatscripts
drwxr-xr-x 2 root root 4096 2024 25 سمبر console-setup
drwxr-xr-x 2 root root 4096 2024 21 فروري cracklib
drwxr-xr-x 2 root root 4096 2024 25 سمبر cron.d
drwxr-xr-x 2 root root 4096 2024 21 فروري cron.daily
drwxr-xr-x 2 root root 4096 2024 21 فروري cron.hourly
drwxr-xr-x 2 root root 4096 2024 21 فروري cron.monthly
-rw-r--r-- 1 root root 1136 2022 23 مارج crontab
drwxr-xr-x 2 root root 4096 2024 21 فروري cron.weekly
drwxr-xr-x 5 root lp 4096 19:56 23 آكتوبر cups
drwxr-xr-x 2 root root 4096 2024 21 فروري cupshelpers
drwxr-xr-x 4 root root 4096 2024 21 فروري dbus-1
drwxr-xr-x 4 root root 4096 2024 21 فروري dconf
-rw-r--r-- 1 root root 2969 2022 20 فروري debconf.conf
-rw-r--r-- 1 root root 13 2021 22 آگسٽ debian_version
drwxr-xr-x 3 root root 4096 2024 25 سمبر default
```

ls\_etc.png

```
shumail@shumail-virtual-machine:~$ ls -la /dev
total 4
drwxr-xr-x 19 root      root          4160 19:56 23 اكتوبر . .
drwxr-xr-x 21 root      root          4096 2024 25 سمبر ..
crw-r--r--  1 root      root          10, 235 19:55 23 اكتوبر autofs
drwxr-xr-x  2 root      root          360 19:56 23 اكتوبر block
drwxr-xr-x  2 root      root          100 19:54 23 اكتوبر bsg
crw-----  1 root      root          10, 234 19:55 23 اكتوبر btrfs-control
drwxr-xr-x  3 root      root          60 19:54 23 اكتوبر bus
lrwxrwxrwx  1 root      root          3 19:56 23 اكتوبر cdrom -> sr0
drwxr-xr-x  2 root      root          3800 19:56 23 اكتوبر char
crw-w----  1 root      tty           5,   1 19:55 23 اكتوبر console
lrwxrwxrwx  1 root      root          11 19:55 23 اكتوبر core -> /proc/kcore
drwxr-xr-x  4 root      root          80 19:55 23 اكتوبر cpu
crw-----  1 root      root          10, 123 19:55 23 اكتوبر cpu_dma_latency
crw-----  1 root      root          10, 203 19:55 23 اكتوبر cuse
drwxr-xr-x  8 root      root          160 19:55 23 اكتوبر disk
drwxr-xr-x  2 root      root          60 19:54 23 اكتوبر dma_heap
crw-rw---+ 1 root      audio         14,   9 19:55 23 اكتوبر mmapd
drwxr-xr-x  3 root      root          100 19:55 23 اكتوبر dri
crw-----  1 root      root          10, 125 19:55 23 اكتوبر encryptfs
crw-rw---  1 root      video         29,   0 19:55 23 اكتوبر fb0
lrwxrwxrwx  1 root      root          13 19:55 23 اكتوبر fd -> /proc/self/fd
brw-rw---  1 root      disk          2,   0 19:55 23 اكتوبر fd0
crw-rw-rw-  1 root      root          1,   7 19:55 23 اكتوبر full
crw-rw-rw-  1 root      root          10, 229 19:55 23 اكتوبر fuse
crw-----  1 root      root          241,   0 19:55 23 اكتوبر hidraw0
crw-----  1 root      root          10, 228 19:55 23 اكتوبر hpet
drwxr-xr-x  2 root      root          0 19:55 23 اكتوبر hugepages
crw-----  1 root      root          10, 183 19:55 23 اكتوبر hwrng
lrwxrwxrwx  1 root      root          12 19:55 23 اكتوبر initctl -> /run/initctl
drwxr-xr-x  4 root      root          320 19:56 23 اكتوبر input
crw-r--r--  1 root      root          1,  11 19:55 23 اكتوبر kmsg
lrwxrwxrwx  1 root      root          28 19:55 23 اكتوبر log -> /run/systemd/journal/dev-log
brw-rw---  1 root      disk          7,   0 19:55 23 اكتوبر loop0
brw-rw---  1 root      disk          7,   1 19:55 23 اكتوبر loop1
brw-rw---  1 root      disk          7,   2 19:55 23 اكتوبر loop2
brw-rw---  1 root      disk          7,   3 19:55 23 اكتوبر loop3
brw-rw---  1 root      disk          7,   4 19:55 23 اكتوبر loop4
brw-rw---  1 root      disk          7,   5 19:55 23 اكتوبر loop5
brw-rw---  1 root      disk          7,   6 19:55 23 اكتوبر loop6
brw-rw---  1 root      disk          7,   7 19:55 23 اكتوبر loop7
```

## ls\_dev.png

```
shumail@shumail-virtual-machine:~$ ls -la /var
total 56
drwxr-xr-x 14 root root      4096 2024 21 فروري .
drwxr-xr-x 21 root root      4096 2024 25 سمبر ..
drwxr-xr-x  2 root root      4096 2024 26 سمبر backups
drwxr-xr-x 18 root root      4096 2024 26 سمبر cache
drwxrwsrwt  2 root whoopsie 4096 2024 21 فروري crash
drwxr-xr-x 69 root root      4096 2024 26 سمبر lib
drwxrwsr-x  2 root staff     4096 2022 18 ابريل local
lrwxrwxrwx  1 root root      9 2024 25 سمبر lock -> /run/lock
drwxrwxr-x 13 root syslog    4096 19:55 23 اكتوبر log
drwxrwsr-x  2 root mail     4096 2024 21 فروري mail
drwxrwsrwt  2 root whoopsie 4096 2024 21 فروري metrics
drwxr-xr-x  2 root root      4096 2024 21 فروري opt
lrwxrwxrwx  1 root root      4 2024 25 سمبر run -> /run
drwxr-xr-x 10 root root      4096 2024 21 فروري snap
drwxr-xr-x  7 root root      4096 2024 21 فروري spool
drwxrwsrwt 11 root root    4096 20:01 23 اكتوبر tmp
```

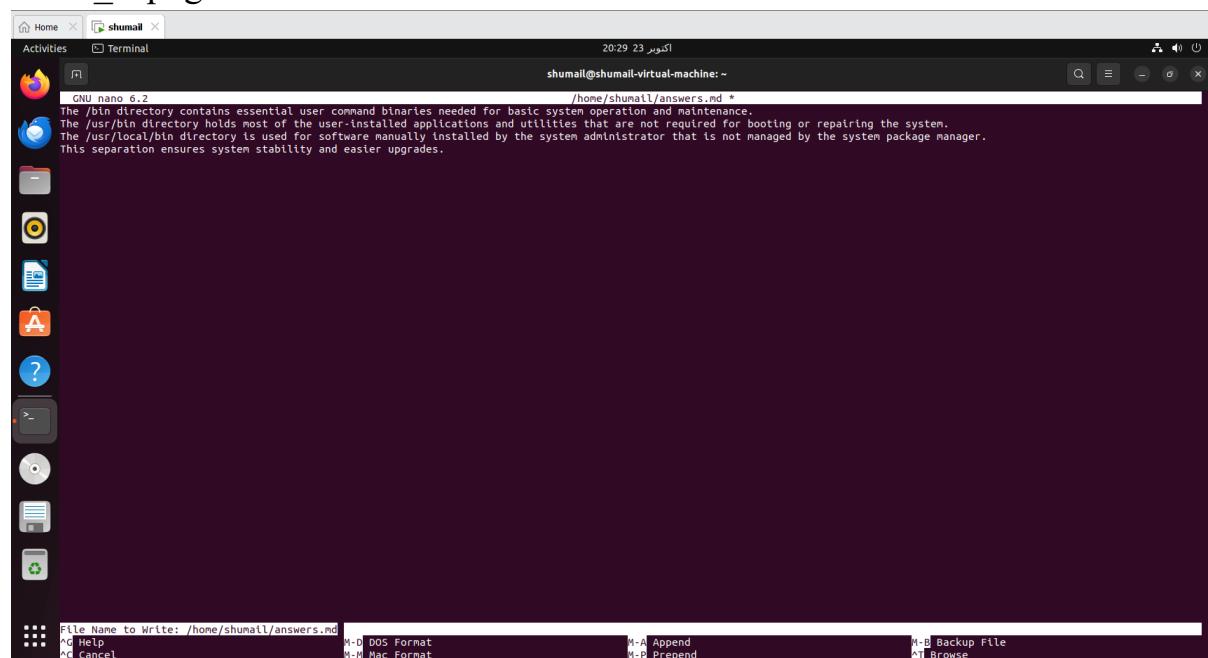
## ls\_var.png

```
shumail@shumail-virtual-machine: $ ls -la /tmp
total 92
drwxrwxrwt 19 root    root   4096 20:10 23 اکتوبر .
drwxr-xr-x 21 root    root   4096 2024 25 سپتامبر ..
drwxrwxrwt  2 root    root   4096 19:55 23 .font-unix
drwxrwxrwt  2 root    root   4096 19:56 23 .ICE-unix
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-tmp
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-systemd
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-colord.service-l7WVjq
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-ModemManager.service-PC1EUM
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-power-profiles-daemon.service-WaKCWj
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-switcheroo-control.service-DtakHj
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-systemd-logind.service-k1zySH
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-systemd-oomd.service-GPNNKy
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-systemd-resolved.service-lHl9rb
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-timesyncd.service-l2JXr
drwxrwxrwt  3 root    root   4096 19:55 23 .snap-private-314fbcd311264393b280a440fe770b35-upower.service-7AXLpE
drwxrwxrwt  2 root    root   4096 19:55 23 .Test-unix
drwxrwxrwt  2 root    root   4096 19:55 23 .VmwareDnD
drwxrwxrwt  2 root    root   4096 19:55 23 .VMware-root_634-2730496827
-rw-r--r--  1 shumail shumail 11 19:56 23 .X0-lock
-rw-r--r--  1 gdm     gdm    11 19:55 23 .X1024-lock
-rw-r--r--  1 gdm     gdm    11 19:55 23 .X1025-lock
drwxrwxrwt  2 root    root   4096 19:56 23 .X11-unix
drwxrwxrwt  2 root    root   4096 20:14 23 .X1-lock
drwxrwxrwt  2 root    root   4096 19:55 23 .XIM-unix
```

## ls\_tmp.png

```
shumail@shumail-virtual-machine: ~$ ls -la ~
total 72
drwxr-x--- 15 shumail shumail 4096 20:11 23 اکتوبر .
drwxr-xr-x  4 root    root    4096 2024 25 سپتامبر ..
-rw-----  1 shumail shumail   0 20:29 21 اکتوبر .bash_history
-rw-r--r--  1 shumail shumail 220 2024 25 سپتامبر .bash_logout
-rw-r--r--  1 shumail shumail 3771 2024 25 سپتامبر .bashrc
drwxr----- 15 shumail shumail 4096 20:14 23 اکتوبر .cache
drwxr----- 11 shumail shumail 4096 2024 25 سپتامبر .config
drwxr-xr-x  2 shumail shumail 4096 2024 25 سپتامبر Desktop
drwxr-xr-x  2 shumail shumail 4096 2024 25 سپتامبر Documents
drwxr-xr-x  2 shumail shumail 4096 2024 25 سپتامبر Downloads
drwxr----- 3 shumail shumail 4096 2024 25 سپتامبر .local
drwxr-xr-x  2 shumail shumail 4096 2024 25 سپتامبر Music
drwxr-xr-x  3 shumail shumail 4096 2024 25 سپتامبر Pictures
-rw-r--r--  1 shumail shumail 807 2024 25 سپتامبر .profile
drwxr-xr-x  2 shumail shumail 4096 2024 25 سپتامبر Public
drwxr----- 4 shumail shumail 4096 2024 25 سپتامبر snap
drwxr----- 2 shumail shumail 4096 20:11 23 اکتوبر .ssh
-rw-r--r--  1 shumail shumail   0 2024 25 سپتامبر .sudo_as_admin_successful
drwxr-xr-x  2 shumail shumail 4096 2024 25 سپتامبر Templates
drwxr-xr-x  2 shumail shumail 4096 2024 25 سپتامبر Videos
```

## home\_ls.png



## answers\_md.png

## Task 4 – Essential CLI tasks — navigation and file operations

```
shumail@shumail-virtual-machine:~$ nano ~/answers.md  
shumail@shumail-virtual-machine:~$ mkdir -p ~/lab4/workspace/python_project
```

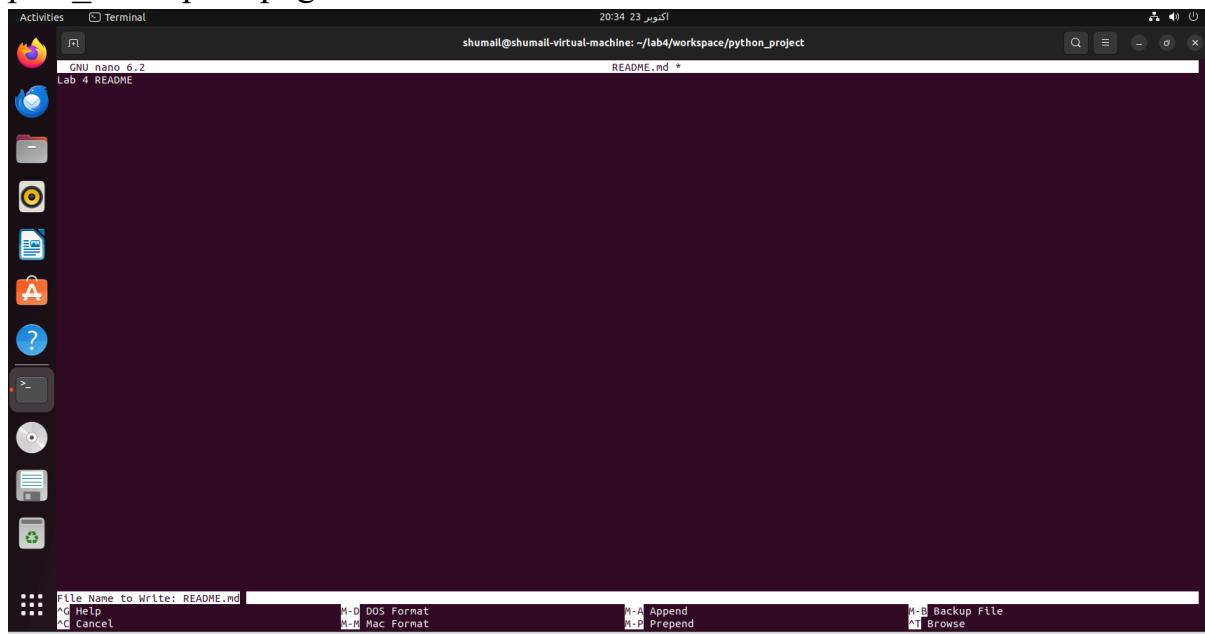
mkdir\_workspace.png

```
shumail@shumail-virtual-machine:~$ cd ~/lab4/workspace/python_project  
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$
```

cd\_workspace.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ pwd  
/home/shumail/lab4/workspace/python_project
```

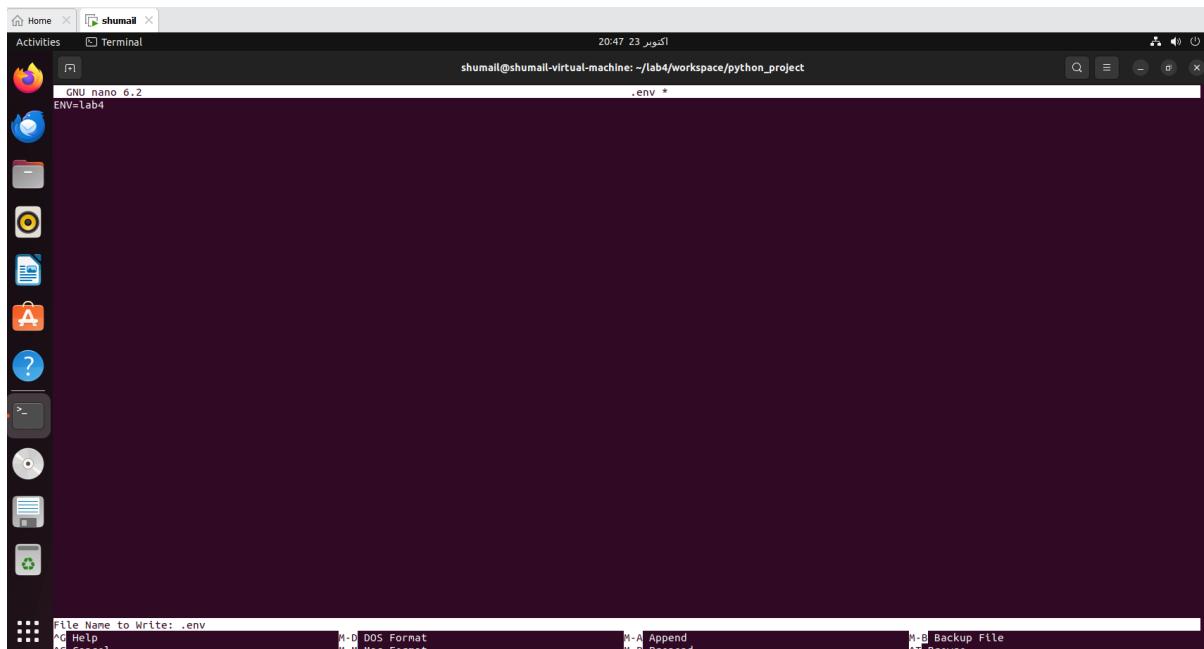
pwd\_workspace.png



nano\_readme.png



## nano\_main.png



## nano\_env.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 shumail shumail 4096 20:48 23 . اكتوبر
drwxrwxr-x 3 shumail shumail 4096 20:31 23 .. اكتوبر
-rw-rw-r-- 1 shumail shumail 9 20:48 23 .env اكتوبر
-rw-rw-r-- 1 shumail shumail 20 20:47 23 main.py اكتوبر
-rw-rw-r-- 1 shumail shumail 14 20:35 23 README.md اكتوبر
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$
```

## workspace\_ls.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ cp README.md README.copy.md
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$
```

## cp\_readme.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ mv README.copy.md README.dev.md
```

## mv\_readme.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ rm README.dev.md
```

## rm\_readme.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
```

## mkdir\_java\_app.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$
```

## cp\_recursive.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 shumail shumail 4096 20:53 23 اكتوبر .
drwxrwxr-x 3 shumail shumail 4096 20:31 23 اكتوبر ..
drwxrwxr-x 2 shumail shumail 4096 20:52 23 اكتوبر java_app
drwxrwxr-x 2 shumail shumail 4096 20:53 23 اكتوبر java_app_copy
drwxrwxr-x 2 shumail shumail 4096 20:51 23 اكتوبر python_project
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$
```

### copy\_verify.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ history
1 whoami
2 pwd
3 ls -la /
4 ls -la /bin
5 ls -la /sbin
6 ls -la /usr
7 ls -la /opt
8 ls -la /etc
9 ls -la /dev
10 ls -la /var
11 ls -la /tmp
12 ls -la ~
13 nano ~/answers.md
14 mkdir -p ~/lab4/workspace/python_project
15 cd ~/lab4/workspace/python_project
16 pwd
17 nano README.md
18 nano main.py
19 nano .env
20 ls -la~
21 ls -la
22 cp README.md README.copy.md
23 mv README.copy.md README.dev.md
24 rm README.dev.md
25 mkdir -p ~/lab4/workspace/java_app
26 cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
27 ls -la ~/lab4/workspace
28 history
```

### history.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ cat README.md
```

### tab\_completion.png

## Task 5 – System info, resources & processes

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ uname -a
Linux shumail-virtual-machine 6.8.0-49-generic #49~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Wed Nov  6 17:42:15 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
```

### Uname.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 142
model name     : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
stepping       : 10
microcode      : 0x6
cpu MHz        : 1895.999
cache size     : 6144 KB
physical id    : 0
siblings       : 1
core id        : 0
cpu cores      : 1
apicid         : 0
initial apicid: 0
fpu             : yes
fpu_exception  : yes
cpuid level   : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtsvp lm constant_tsc arch_perfmon nopl xt
cpu topology   : tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcld sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave aux f1sc rdrand hypervisor lah
f1m abm 3dnoprefetch pt1 ssbd tbrs ihpb stlbp Fsgsbbase tsc_adjust bni1 avx2 smep bm12 invpcld rdseed adx snap clflushopt xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_lid arc
h_capabilities: bugs : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbs mmio_stale_data retbleed gds bhi
bogomips       : 3791.99
clflush size   : 64
cache_alignment : 64
address sizes  : 45 bits physical, 48 bits virtual
power management:
processor       : 1
vendor_id      : GenuineIntel
cpu family     : 6
model          : 142
model name     : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
stepping       : 10
microcode      : 0x6
cpu MHz        : 1895.999
cache size     : 6144 KB
physical id    : 2
siblings       : 1
```

## Cpuinfo.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ free -h
              total        used        free      shared  buff/cache   available
Mem:       3.8Gi       991Mi      1.7Gi      40Mi      1.2Gi      2.5Gi
Swap:      2.1Gi          0B      2.1Gi
```

## Meminfo.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           387M  2.0M  385M  1% /run
/dev/sda3        20G   15G   4.0G  79% /
tmpfs           1.9G     0  1.9G  0% /dev/shm
tmpfs           5.0M   4.0K  5.0M  1% /run/lock
/dev/sda2        512M  6.1M  506M  2% /boot/efi
tmpfs           387M  112K  387M  1% /run/user/1000
/dev/sr0         152M  152M     0 100% /media/shumail/CDROM
```

## Diskinfo.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.4 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
```

## os-release.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root      1  0.1  0.2 166684 11636 ?        Ss   19:54  0:05 /sbin/init auto noprompt splash
root      2  0.0  0.0     0   0 ?        S    19:54  0:00 [kthreadd]
root      3  0.0  0.0     0   0 ?        S    19:54  0:00 [pool_workqueue_release]
root      4  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-rcu_g]
root      5  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-rcu_p]
root      6  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-slub_]
root      7  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-netns]
root      8  0.0  0.0     0   0 ?        I   19:54  0:01 [kworker/0:0-events]
root      9  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/0:0-kblockd]
root     11  0.0  0.0     0   0 ?        I   19:54  0:00 [kworker/u256:0-floppy]
root     12  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-mm_pe]
root     13  0.0  0.0     0   0 ?        I   19:54  0:00 [rcu_tasks_kthread]
root     14  0.0  0.0     0   0 ?        I   19:54  0:00 [rcu_tasks_rude_kthread]
root     15  0.0  0.0     0   0 ?        I   19:54  0:00 [rcu_tasks_trace_kthread]
root     16  0.0  0.0     0   0 ?        S   19:54  0:00 [ksoftirqd/0]
root     17  0.0  0.0     0   0 ?        I   19:54  0:01 [rcu_preempt]
root     18  0.0  0.0     0   0 ?        S   19:54  0:00 [migration/0]
root     19  0.0  0.0     0   0 ?        S   19:54  0:00 [idle_inject/0]
root     20  0.0  0.0     0   0 ?        S   19:54  0:00 [cpuhp/0]
root     21  0.0  0.0     0   0 ?        S   19:54  0:00 [cpuhp/1]
root     22  0.0  0.0     0   0 ?        S   19:54  0:00 [idle_inject/1]
root     23  0.0  0.0     0   0 ?        S   19:54  0:01 [migration/1]
root     24  0.0  0.0     0   0 ?        S   19:54  0:00 [ksoftirqd/1]
root     29  0.0  0.0     0   0 ?        S   19:54  0:00 [kdevtmpfs]
root     30  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-inet_]
root     32  0.0  0.0     0   0 ?        S   19:54  0:00 [kaudittd]
root     34  0.0  0.0     0   0 ?        S   19:54  0:00 [khungtaskd]
root     35  0.0  0.0     0   0 ?        S   19:54  0:00 [oom_reaper]
root     37  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-write]
root     38  0.0  0.0     0   0 ?        S   19:54  0:00 [kcompactd0]
root     39  0.0  0.0     0   0 ?        SN  19:54  0:00 [ksmd]
root     42  0.0  0.0     0   0 ?        SN  19:54  0:00 [khugepaged]
```

## processes.png

## Task 6 – Users and account verification (no sudo group change)

```
Shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ sudo adduser lab4user
[sudo] password for shumail:
Adding user `lab4user' ...
Adding new group `lab4user' (1002) ...
Adding new user `lab4user' (1002) with group `lab4user' ...
Creating home directory `/home/lab4user' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lab4user
Enter the new value, or press ENTER for the default
      Full Name []: shumail zahra
      Room Number []: 1
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n] Y
```

adduser\_lab4user.png

```
Is the information correct? [Y/n] Y
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ getent passwd lab4user
lab4user:x:1002:1002:shumail zahra,1,:/home/lab4user:/bin/bash
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$
```

lab4user\_passwd.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ su - lab4user
Password:
```

su\_lab4user.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ sudo whoami
[sudo] password for shumail:
root
```

sudo\_whoami.png

```
Lab4User@shumail-virtual-machine:~$ exit
logout
```

exit\_back.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
Looking for files to backup/remove ...
Removing files ...
Removing user `lab4user' ...
Warning: group `lab4user' has no more members.
Done.
```

Deluser.png

## Bonus Task 7 – Create a small demo script using an editor and run it

```
GNU nano 6.2
#!/bin/bash
echo "Lab 4 demo: current user is $(whoami)"
echo "Current time: $(date)"
uptime
free -h
```

nano\_run\_demo.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ nano ~/lab4/workspace/run-demo.sh
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ chmod +x ~/lab4/workspace/run-demo.sh
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ ./run-demo.sh
```

chmod\_run\_demo.png

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ ./lab4/workspace/run-demo.sh
Lab 4 demo: current user is shumail
Current time: 21:24:37 ۹ PKT 2025
21:24:37 up 1:29, 2 users, load average: 0.16, 0.07, 0.04
           total        used        free      shared  buff/cache   available
Mem:       3.8Gi       977Mi      1.6Gi      40Mi       1.2Gi      2.6Gi
Swap:      2.1Gi          0B      2.1Gi
```

run\_demo\_output.png

## Exam Evaluation Questions:

### 1. Remote Access Verification (Cyber Login Check)

```
shumail@shumail-virtual-machine:~/lab4/workspace/python_project$ ssh shumail@192.168.183.128
shumail@192.168.183.128's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

263 updates can be applied immediately.
219 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Oct 23 20:11:21 2025 from 192.168.183.128
```

## Q1\_remote\_connection.png

```
shumail@shumail-virtual-machine:~$ whoami  
shumail  
shumail@shumail-virtual-machine:~$ pwd  
/home/shumail  
shumail@shumail-virtual-machine:~$
```

## Q1\_user\_verification.png

```
shumail@shumail-virtual-machine:~$ hostname  
shumail-virtual-machine  
shumail@shumail-virtual-machine:~$
```

## Q1 host confirmation.png

## 2. Filesystem Inspection for Forensic Evidence

```
shumall@shumall-virtual-machine:~$ ls /  
app bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv swapfile sys tmp usr var
```

## Q2\_root\_listing.png

```
shumail@shumail-virtual-machine:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.4 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
```

## Q2 os version.png

```
shumail@shumail-Virtual-Machine: ~ $ ls /bin
ls
ls /sbin
ls /usr
ls /opt
ls /etc
ls /dev
ls /var
ls /tmp
['', 'fonttosfnt', 'jrunscript', 'pipewire', 'systemd-notify',
'aa-enabled', 'foo2ddst', 'jsadebugd', 'pipewire-media-session', 'systemd-path',
'aa-exec', 'foo2ddst-wrapper', 'json_pp', 'pkaction', 'systemd-run',
'aa-features-abi', 'foo2dbpl2', 'jstack', 'pkcheck', 'systemd-socket-activate',
'aconnect', 'foo2dbpl2-wrapper', 'jstat', 'pkcon', 'systemd-tcpio-bridge',
'acpldbg', 'foo2diper', 'jstatd', 'pkexec', 'systemd-syssex',
'acpl_listen', 'foo2diper-wrapper', 'khdbinfo', 'pkkill', 'systemd-sysusers',
'add-apt-repository', 'foo2hp', 'khd node', 'pkmon', 'systemd-tmpfiles',
'addpart', 'foo2hp2600-wrapper', 'kbxutil', 'pkttymagent', 'systemd-tty-ask-password-agent',
'alrscan-discover', 'foo2lava', 'kernel-install', 'pl2pm', 'systemd-umount',
'alsabat', 'foo2lava-wrapper', 'kernelLoops-submit', 'pldd', 'tabs',
'alsaloop', 'foo2oak', 'keyring', 'plog', 'tac',
'alsamixer', 'foo2oak-wrapper', 'keytool', 'plymouth', 'tail',
'alsatplg', 'foo2qndl', 'kill', 'pmap', 'tar',
'alsaucm', 'foo2qndl-wrapper', 'killall', 'pmzppa', 'taskset',
'anidt', 'foo2s1x', 'knodn', 'pod2html', 'tbl',
'anixer', 'foo2s1x-wrapper', 'knodsign', 'pod2man', 'tccls',
'apg', 'foo2xqx', 'l2ping', 'pod2text', 'tccls8.6',
'apgfbm', 'foo2xqx-wrapper', 'last', 'pod2usage', 'tcpdump',
'aplayer', 'foo2zjs', 'laptop-detect', 'podchecker', 'tee',
'aplayermid', 'foo2zjs-lcc2ps', 'lastb', 'poff', 'telnet',
'aplayerviewer', 'foo2zjs-pstop', 'lastb', 'polocytool', 'telnet.netkit',
'apport-bug', 'foo2zjs-wrapper', 'lastlog', 'pon', 'tempfile',
'apport-call', 'foondroidc1', 'lastcode', 'POST', 'test',
'apport-collect', 'printidle-late', 'lef', 'pwpiprofilestcl', 'thunderbird',
'apport-unpack', 'printidle-enroll', 'lld', 'ppdc', 'tic',
'apres', 'printidle-list', 'less', 'ppdhtml', 'tificc',
'apstreamcli', 'printidle-verify', 'lessecho', 'ppdmerge', 'tine',
'apropos', 'free', 'lessfile', 'ppdmerge', 'timedatectl',
'apt', 'ftp', 'lesskey', 'ppdp0', 'timeout',
'apt-add-repository', 'funzlp', 'lesspipe', 'pphs', 'tload',
'apt-cache', 'fuser', 'lexbrog', 'pr', 'tnameserv',
'apt-cdrom', 'fusermount', 'llibnetcfg', 'prescat', 'tnftp]
```

## Q2 directory evidence.png

```
cd-create-profile          gpg-connect-agent      mandb          reminna-file-wrapper    view
cd-flx-profile           gpparsemail        manpath        reminna-gnome       viewres
cd-iccdump               gpgsm             man-recode     rendercheck        vtn.tiny
cd-it8                   gpgsplit          mapscrn       renice          vmhgfs-fuse
chacl                   gpgtar            mawk          reset           vmstat
chage                   gpgv              mcookie      restzecons       vm-support
chardet                 gpg-wks-server    mdssum       reszepart       vmtoolsd
chardetect              gpg-zip          mdssum_textutils resvectl       vmware-alias-import
chatr                   gplc              mesg          rev             vmware-checkin
chcon                   gpu-manager       mesa-overlays-control py rfcctrl       vmware-crashdump
chcon-klanguage-support  grdcctl          migrate-pubring-from-classic-gpg rhythmbox
chown                  grops            mtn12xxw     rhythmbox-client   vmware-hgfsclient
chown                   grotty           mtkfifo      rlogin          vmware-nitespace-cmd
chroot                  groups            mtkfontdir   rm              vmware-rpctool
chrt                   grub-editenv     mtkfontscale rmdir          vmware-toolbox-cmd
chsh                   grub_file       mtklsofs     rmic           vmware-user
chvt                   grub_fstab      mtkmod       rmid           vmware-user-suid-wrapper
ciptool                grub_glue-efi    mtksquashfs rrsync         vmware-vgabatch-cmd
ckbcomp                grub_kbdcomp   mtktemp      rmiic          vmware-vmblock-fuse
cksum                  grub_menulst2cfg mtkzftree    rnano          vmware-xferlogs
clear                  grub_mkfont     mtkzftree    routeF         vstp
clear_console           grub_mkimage    mtklayout    routel         w
clhsdb                 grub_mklayout   mtknetdir   monitor-sensor   wall
cmp                   grub_mkpasswd-pbkdf2 more          rrtstat        watch
codepage               grub_mkrecpath  mount       runcon         watchchngnupg
col                   grub_mkrescue   mountpoint  run-mailcap   wc
colorgrm              grub_mkstandalone mousetweaks run-parts      wget
colm                  grub_mkstandalone mscompress  run-wtmp-aspell
column                 grub_ntldr-img  msexpand    run-parts      whereis
comm                  grub_render-label mt           rsync          which
compose                grub_script-check  mtk-gnu     rsync-ssl       which.debianutils
corelist               grub_systinux2cfg mtk-packet  rsyncctl        whiptail
cr                     gs               nativeAsciil samefind-scanner rvview
cspan                 gsj1              nanel       saveLog        who
spanis.34-x86_64-linux-gnu gsj2              nano       sbattach       whoami
cspan                 gsj3              nanel       sbkeysync     whoopsie
cpp                   gsettings        nautilus    sbsiglist      whoopsie-preferences
cppo                  gsj4              nanel       sbshsign      word-list-compress
cppower               gsj5              nautilus    sbvarsign     upa_passphrase
c_rehash               gsj6              nautilus-autorun-software sbsiglist      write
crontab               gsnd             nautilus-sendto schenanagen  write.ul

```

## Q2 directory evidencee.png

Q2 directory evidenceee.png

```
shumail@shumail-virtual-machine: ~ ls -a ~
. answers.md .bash_logout .cache Desktop Downloads .local Pictures Public .ssh Templates
.. .bash_history .bashrc .config Documents lab4 Music .profile snap .sudo_as_admin_successful Videos
```

## Q2 hidden files.png

```

shumail@shumail-virtual-machine:~$ nano forensic_report.md
shumail@shumail-virtual-machine:~$ cat forensic_report.md
# Forensic Filesystem Report

## Key System Directories

- **/bin**: Contains essential binary executables for all users.
- **/sbin**: System administration binaries for root users.
- **/usr**: Contains user-level programs and libraries.
- **/opt**: Optional software packages.
- **/etc**: Configuration files for the system and applications.
- **/dev**: Device files representing hardware and peripherals.
- **/var**: Variable data like logs and caches.
- **/tmp**: Temporary files used by running processes.

**Findings:**
No suspicious files found in system directories at this stage.

```

Q2\_report\_file.png

### 3. Evidence Handling & File Operations

```

shumail@shumail-virtual-machine:~$ mkdir -p ~/forensics_lab/sandbox/evidence
shumail@shumail-virtual-machine:~$ ls -R ~/forensics_lab
/home/shumail/forensics_lab:
sandbox

/home/shumail/forensics_lab/sandbox:
evidence

/home/shumail/forensics_lab/sandbox/evidence:

```

Q3\_workspace\_created.png

```

/home/shumail/forensics_lab/sandbox/evidence:
shumail@shumail-virtual-machine:~$ cd ~/forensics_lab/sandbox/evidence
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ nano suspect1.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ nano suspect2.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ nano .notes.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ ls -la
total 20
drwxrwxr-x 2 shumail shumail 4096 21:41 23 اكتوبر .
drwxrwxr-x 3 shumail shumail 4096 21:38 23 اكتوبر ..
-rw-rw-r-- 1 shumail shumail 23 21:41 23 اكتوبر .notes.txt
-rw-rw-r-- 1 shumail shumail 29 21:40 23 اكتوبر suspect1.txt
-rw-rw-r-- 1 shumail shumail 26 21:40 23 اكتوبر suspect2.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$
```

Q3\_files\_created.png

```

shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ cp suspect1.txt suspect1_backup.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ mv suspect1_backup.txt suspect1_renamed.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ rm suspect1_renamed.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ ls -la
total 20
drwxrwxr-x 2 shumail shumail 4096 21:42 23 اكتوبر .
drwxrwxr-x 3 shumail shumail 4096 21:38 23 اكتوبر ..
-rw-rw-r-- 1 shumail shumail 23 21:41 23 اكتوبر .notes.txt
-rw-rw-r-- 1 shumail shumail 29 21:40 23 اكتوبر suspect1.txt
-rw-rw-r-- 1 shumail shumail 26 21:40 23 اكتوبر suspect2.txt

```

Q3\_backup\_handling.png

```
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ cd ~
shumail@shumail-virtual-machine:~$ cp -r forensics_lab forensics_lab_backup
shumail@shumail-virtual-machine:~$ ls -la
total 92
drwxr-x--- 18 shumail shumail 4096 21:43 23 اکتوبر .
drwxr-xr-x 4 root root 4096 21:22 23 اکتوبر ..
-rw-rw-r-- 1 shumail shumail 464 20:31 23 اکتوبر answers.md
-rw----- 1 shumail shumail 0 20:29 21 اکتوبر .bash_history
-rw-r--r-- 1 shumail shumail 220 2024 25 سهبر .bash_logout
-rw-r--r-- 1 shumail shumail 3771 2024 25 سهبر .bashrc
drwx----- 15 shumail shumail 4096 20:14 23 اکتوبر .cache
drwx----- 11 shumail shumail 4096 2024 25 سهبر .config
drwxr-xr-x 2 shumail shumail 4096 2024 25 سهبر Desktop
drwxr-xr-x 2 shumail shumail 4096 2024 25 سهبر Documents
drwxr-xr-x 2 shumail shumail 4096 2024 25 سهبر Downloads
-rw-rw-r-- 1 shumail shumail 590 21:37 23 اکتوبر forensic_report.md
drwxrwxr-x 3 shumail shumail 4096 21:38 23 اکتوبر forensics_lab
drwxrwxr-x 3 shumail shumail 4096 21:43 23 اکتوبر forensics_lab_backup
drwxrwxr-x 3 shumail shumail 4096 20:31 23 اکتوبر lab4
drwx----- 3 shumail shumail 4096 2024 25 سهبر .local
drwxr-xr-x 2 shumail shumail 4096 2024 25 سهبر Music
drwxr-xr-x 3 shumail shumail 4096 2024 25 سهبر Pictures
-rw-r--r-- 1 shumail shumail 807 2024 25 سهبر .profile
drwxr-xr-x 2 shumail shumail 4096 2024 25 سهبر Public
drwx----- 4 shumail shumail 4096 2024 25 سهبر snap
drwx----- 2 shumail shumail 4096 20:11 23 اکتوبر .ssh
-rw-r--r-- 1 shumail shumail 0 2024 25 سهبر .sudo_as_admin_successful
drwxr-xr-x 2 shumail shumail 4096 2024 25 سهبر Templates
drwxr-xr-x 2 shumail shumail 4096 2024 25 سهبر Videos
shumail@shumail-virtual-machine:~$
```

Q3\_workspace\_backup.png

```
shumail@shumail-virtual-machine:~$ history | tail -n 15
17 mkdir -p ~/forensics_lab/sandbox/evidence
18 ls -R ~/forensics_lab
19 cd ~/forensics_lab/sandbox/evidence
20 nano suspect1.txt
21 nano suspect2.txt
22 nano .notes.txt
23 ls -la
24 cp suspect1.txt suspect1_backup.txt
25 mv suspect1_backup.txt suspect1_renamed.txt
26 rm suspect1_renamed.txt
27 ls -la
28 cd ~
29 cp -r forensics_lab forensics_lab_backup
30 ls -la
31 history | tail -n 15
```

Q3\_command\_history.png

```
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ cat suspect
suspect1.txt suspect2.txt
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ cat suspect
```

Q3\_autocomplete.png

## 4. System Profiling and Process Monitoring

```
cat: suspect: No such file or directory
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.4 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ uname -r
6.8.0-49-generic
```

## Q4\_system\_info.png

```
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Address sizes:         45 bits physical, 48 bits virtual
Byte Order:            Little Endian
CPU(s):                2
On-line CPU(s) list:  0,1
Vendor ID:             GenuineIntel
Model name:            Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
CPU family:             6
Model:                 142
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):              2
Stepping:               10
BogomIPS:              3791.99
Flags:                 fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon
                       nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcld sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xs
                       avx avx2 f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pt1 ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 bmi2 avx2 smep bmi2 invpcid rdseed adx smap clflushop
                       t xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_lid arch_capabilities
Virtualization features:
Hyperervisor vendor:   VMware
Virtualization type:   full
Caches (sum of all):
  L1d:                  64 KiB (2 instances)
  L1i:                  64 KiB (2 instances)
  L2:                  512 KiB (2 instances)
  L3:                  12 MiB (2 instances)
NUMA:
  NUMA node(s):         1
  NUMA node0 CPU(s):    0,1
Vulnerabilities:
  Gather data sampling: Unknown: Dependent on hypervisor status
  Itlb multithit:       KVM: Mitigation: VMX unsupported
  L1tf:                 Mitigation: PTE Inversion
  Mds:                  Mitigation: Clear CPU buffers; SMT Host state unknown
  Meltdown:              Mitigation: PTI
  Mmio stale data:      Mitigation: Clear CPU buffers; SMT Host state unknown
  Reg file data sampling: Not affected
  Retbleed:              Mitigation: IBRS
  Spec rstack overflow: Not affected
  Spec store bypass:    Mitigation: Speculative Store Bypass disabled via prctl
  L2:                  512 KiB (2 instances)
  L3:                  12 MiB (2 instances)
NUMA:
  NUMA node(s):         1
  NUMA node0 CPU(s):    0,1
Vulnerabilities:
  Gather data sampling: Unknown: Dependent on hypervisor status
  Itlb multithit:       KVM: Mitigation: VMX unsupported
  L1tf:                 Mitigation: PTE Inversion
  Mds:                  Mitigation: Clear CPU buffers; SMT Host state unknown
  Meltdown:              Mitigation: PTI
  Mmio stale data:      Mitigation: Clear CPU buffers; SMT Host state unknown
  Reg file data sampling: Not affected
  Retbleed:              Mitigation: IBRS
  Spec rstack overflow: Not affected
  Spec store bypass:    Mitigation: Speculative Store Bypass disabled via prctl
  Spectre v1:            Mitigation: usercopy/swaps barriers and __user pointer sanitization
  Spectre v2:            Mitigation: IBRS; IBPB conditional; STIBP disabled; RSB filling; PBRSB-eIBRS Not affected; BHI SW loop, KVM SW loop
  Srbds:                Unknown: Dependent on hypervisor status
  Tsx async abort:      Not affected
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ free -h
              total        used        free      shared  buff/cache   available
Mem:      3.8Gi       975Mi     1.4Gi      40Mi      1.5Gi      2.5Gi
Swap:      2.1Gi        0B      2.1Gi
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ df -h
Filesystem  Size  Used Avail Use% Mounted on
tmpfs      387M   2.0M  385M  1% /run
/dev/sda3   20G   14G  4.2G  77% /
tmpfs      1.9G     0  1.9G  0% /dev/shm
tmpfs      5.0M   4.0K  5.0M  1% /run/lock
/dev/sda2   512M   6.1M  506M  2% /boot/efi
tmpfs      387M  112K  387M  1% /run/user/1000
/dev/sr0    152M   152M     0 100% /media/shumail/CDROM
```

## Q4\_resource\_info.png

```

shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root      1  0.0  0.2 166684 11636 ?        Ss  19:54  0:05 /sbin/init auto noprompt splash
root      2  0.0  0.0     0   0 ?        S     19:54  0:00 [kthreadd]
root      3  0.0  0.0     0   0 ?        S     19:54  0:00 [pool_workqueue_release]
root      4  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-rCU_g]
root      5  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-rCU_p]
root      6  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-slub_]
root      7  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-netns]
root      9  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/0:0H-kblockd]
root     11  0.0  0.0     0   0 ?        I     19:54  0:00 [kworker/u256:0-floppy]
root     12  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-mm_pe]
root     13  0.0  0.0     0   0 ?        I     19:54  0:00 [rcu_tasks_kthread]
root     14  0.0  0.0     0   0 ?        I     19:54  0:00 [rcu_tasks_rude_kthread]
root     15  0.0  0.0     0   0 ?        I     19:54  0:00 [rcu_tasks_trace_kthread]
root     16  0.0  0.0     0   0 ?        S     19:54  0:00 [ksoftirqd/0]
root     17  0.0  0.0     0   0 ?        I     19:54  0:02 [rcu_preempt]
root     18  0.0  0.0     0   0 ?        S     19:54  0:00 [migration/0]
root     19  0.0  0.0     0   0 ?        S     19:54  0:00 [idle_inject/0]
root     20  0.0  0.0     0   0 ?        S     19:54  0:00 [cpuhp/0]
root     21  0.0  0.0     0   0 ?        S     19:54  0:00 [cpuhp/1]
root     22  0.0  0.0     0   0 ?        S     19:54  0:00 [idle_inject/1]
root     23  0.0  0.0     0   0 ?        S     19:54  0:01 [migration/1]
root     24  0.0  0.0     0   0 ?        S     19:54  0:00 [ksoftirqd/1]
root     29  0.0  0.0     0   0 ?        S     19:54  0:00 [kdevtmpfs]
root     30  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-inet_]
root     32  0.0  0.0     0   0 ?        S     19:54  0:00 [kaudittd]
root     34  0.0  0.0     0   0 ?        S     19:54  0:00 [khungtaskd]
root     35  0.0  0.0     0   0 ?        S     19:54  0:00 [oom_reaper]
root     37  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-write]
root     38  0.0  0.0     0   0 ?        S     19:54  0:00 [kcompactd0]
root     39  0.0  0.0     0   0 ?        SN    19:54  0:00 [ksmd]
root     42  0.0  0.0     0   0 ?        SN    19:54  0:00 [khugepaged]
root     43  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-kinte]
root     44  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-kbloc]
root     45  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-blkg]
root     46  0.0  0.0     0   0 ?        S     19:54  0:00 [irq/9-acpi]
root     47  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-tpm_d]
root     48  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-ata_s]
root     49  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-md]
root     50  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-md_bi]
root     51  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-edac_]
root     52  0.0  0.0     0   0 ?        I<  19:54  0:00 [kworker/R-devfr]

shumail 2151 0.0  0.5 306312 22532 ?        Sl  19:56  0:00 /snap/snapd-desktop-integration/83/usr/bin/snapd-desktop-integration
shumail 2155 0.0  0.3 755226 14336 ?        Ssl 19:56  0:00 /usr/libexec/xdg-desktop-portal
shumail 2156 0.0  0.7 663264 29548 ?        Ssl 19:56  0:00 /usr/libexec/xdg-desktop-portal-gnome
shumail 2178 0.0  0.1 163832 7689 ?        Sl  19:56  0:03 /usr/libexec/bus-engine-simple
shumail 2181 0.0  2.0 235308 61519 ?        S  19:56  0:04 /usr/bin/Xwayland :0 -rootless -noreset -accessx -core -auth /run/user/1000/.mutter-Xwaylandauth.EYPMEl -listen 4
shumail 2269 0.0  0.6 2399852 83394 ?        Sl  19:56  0:00 /usr/share/gjs /usr/share/gnome-shell/org.gnome.ScreenSaver
shumail 2268 0.0  0.6 547010 80016 ?        Sl  19:56  0:00 /usr/libexec/gdm-settings
shumail 2271 0.0  0.6 145184 25676 ?        Ssl 19:56  0:00 /usr/libexec/gdm-terminal-settings
shumail 2397 0.0  0.6 194556 25392 ?        Sl  19:56  0:00 /usr/libexec/ibus-x11
shumail 2402 0.0  0.8 495896 32348 ?        Sl  19:56  0:01 update-notifier
shumail 2719 0.8  1.4 559520 57480 ?        Rsl 20:06  1:01 /usr/libexec/gnome-terminal-server
shumail 2737 0.0  0.1 11360 5248 pts/0       Ss  20:06  0:00 bash
shumail 2776 0.0  0.2 17276 8448 pts/0       S+ 20:11  0:00 ssh shumail@192.168.183.128
root    2777 0.0  0.2 17432 11088 ?        Ss  20:11  0:00 sshd: shumail [priv]
shumail 2780 0.0  0.1 9796 5632 ?        S  20:11  0:00 /usr/bin/ssh-agent -D -a /run/user/1000/keyring/.ssh
shumail 2859 0.0  0.2 17564 8008 ?        R  20:11  0:00 sshd: shumail@pts/1
shumail 2861 0.0  0.1 11564 5632 pts/1      Ss  20:11  0:00 -bash
shumail 2875 0.0  0.0 0   0 ?        I<  20:11  0:00 [kworker/R-tls-s]
root    2937 0.0  0.0 0   0 ?        I<  20:20  0:00 [kworker/261:0-ttm]
root    3123 0.0  0.0 0   0 ?        I<  20:47  0:00 [kworker/260:5-ttm]
root    3186 0.0  0.0 0   0 ?        I  20:55  0:00 [kworker/260:5-events_unbound]
root    3218 0.0  0.0 0   0 ?        I<  21:07  0:00 [kworker/261:3-ttm]
root    3219 0.0  0.0 0   0 ?        I  21:07  0:00 [kworker/257:3-events_unbound]
root    3241 0.2  0.0 0   0 ?        I  21:11  0:06 [kworker/1:1-events]
root    3245 0.0  0.0 0   0 ?        I  21:12  0:02 [kworker/0:2-mpt_poll_0]
shumail 3266 0.0  1.5 2788976 62092 ?        Sl  21:12  0:02 gjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/ding.js -E -P /usr/share/gnome-shell/extensions/ding@ras
root    3283 0.0  0.0 0   0 ?        I<  21:12  0:00 [kworker/260:0-ttm]
root    3374 0.0  0.0 0   0 ?        I  21:21  0:00 [kworker/257:0-events_unbound]
shumail 3461 0.0  0.2 17276 8192 pts/1      S+ 21:27  0:00 ssh shumail@192.168.183.128
root    3469 0.0  0.2 17424 11040 ?        Ss  21:27  0:00 sshd: shumail [priv]
shumail 3549 0.0  0.2 17556 8004 ?        D  21:27  0:00 sshd: shumail@pts/2
shumail 3550 0.0  0.1 11616 5504 pts/2      Ss  21:27  0:01 -bash
root    3558 0.0  0.0 0   0 ?        I  21:28  0:00 [kworker/u257:2-events_power_efficient]
root    3620 0.0  0.0 0   0 ?        I  21:40  0:00 [kworker/u258:1-events_unbound]
root    4138 0.0  0.0 0   0 ?        I  21:48  0:00 [kworker/0:8-rCU_par_g]
root    4141 0.0  0.0 0   0 ?        I  21:48  0:00 [kworker/u258:2-events_power_efficient]
root    4142 0.0  0.0 0   0 ?        I  21:48  0:00 [kworker/1:8-rCU_par_g]
root    4175 0.0  0.0 0   0 ?        I  21:56  0:00 [kworker/0:12-events]
root    4578 0.0  0.0 0   0 ?        I  21:56  0:00 [kworker/u258:8-flush-8:0]
root    4579 0.0  0.0 0   0 ?        I  21:56  0:00 [kworker/1:2]
root    4580 0.0  0.0 0   0 ?        I<  21:56  0:00 [kworker/0:2H-kblockd]
root    4601 0.0  0.0 0   0 ?        I  21:59  0:00 [kworker/u257:1-events_unbound]
shumail 4607 0.0  0.0 13024 3456 pts/2      R+ 22:00  0:00 ps aux

```

## Q4\_process\_list

## 5. User Account Audit & Privilege Escalation Simulation

```
shumail@shumail-virtual-machine:~/forensics_lab/sandbox/evidence$ sudo adduser lab4user
Adding user `lab4user' ...
Adding new group `lab4user' (1002) ...
Adding new user `lab4user' (1002) with group `lab4user' ...
Creating home directory `/home/lab4user' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lab4user
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
```

Q5\_user\_created.png

```
shumail@shumail-virtual-machine:~$ sudo adduser lab4user
adduser: The user `lab4user' already exists.
```

```
adduser: The user `lab4user' already exists.
shumail@shumail-virtual-machine:~$ grep lab4user /etc/passwd
lab4user:x:1002:1002:,:/home/lab4user:/bin/bash
shumail@shumail-virtual-machine:~$
```

Q5\_user\_verified.png

```
shumail@shumail-virtual-machine:~$ su - lab4user
Password:
lab4user@shumail-virtual-machine:~$ whoami
lab4user
lab4user@shumail-virtual-machine:~$
```

Q5\_user\_login.png

```
lab4user@shumail-virtual-machine:~$ sudo apt update
[sudo] password for lab4user:
lab4user is not in the sudoers file. This incident will be reported.
```

Q5\_permission\_denied.png

```
lab4user@shumail-virtual-machine:~$ exit
logout
shumail@shumail-virtual-machine:~$ whoami
shumail
shumail@shumail-virtual-machine:~$
```

Q5\_switch\_back.png

```
shumail@shumail-virtual-machine: $ sudo cat /var/log/auth.log | grep lab4user | tail -n 10
Oct 23 22:03:00 shumail-virtual-machine groupadd[4612]: group added to /etc/gshadow: name=lab4user
Oct 23 22:03:00 shumail-virtual-machine groupadd[4612]: new group: name=lab4user, GID=1002
Oct 23 22:03:00 shumail-virtual-machine useradd[4618]: new user: name=lab4user, UID=1002, GID=1002, home=/home/lab4user, shell=/bin/bash, from=/dev/pts/3
Oct 23 22:03:20 shumail-virtual-machine passwd[4629]: pam_unix(passwd:chauthtok): password changed for lab4user
Oct 23 22:03:23 shumail-virtual-machine chfn[4630]: changed user `lab4user' information
Oct 23 22:04:31 shumail-virtual-machine sudo: shumail : TTY=pts/2 ; PWD=/home/shumail ; USER=root ; COMMAND=/usr/sbin/adduser lab4user
Oct 23 22:06:03 shumail-virtual-machine su: (to lab4user) shumail on pts/2
Oct 23 22:06:03 shumail-virtual-machine su: pam_unix(su-l:session): session opened for user lab4user(uid=1002) by shumail(uid=1000)
Oct 23 22:07:06 shumail-virtual-machine sudo: lab4user : user NOT in sudoers ; TTY=pts/2 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/apt update
Oct 23 22:07:46 shumail-virtual-machine su: pam_unix(su-l:session): session closed for user lab4user
```

### Q5\_authlog\_analysis.png

```
shumail@shumail-virtual-machine:~$ sudo deluser --remove-home lab4user
Looking for files to backup/remove ...
Removing files ...
Removing user `lab4user' ...
Warning: group `lab4user' has no more members.
Done.
shumail@shumail-virtual-machine:~$ grep lab4user /etc/passwd
```

### Q5\_user\_removed

---