

**Name:** Lujain Zia  
**Roll no:** 2023-BSE-034  
**Date:** October 16, 2025



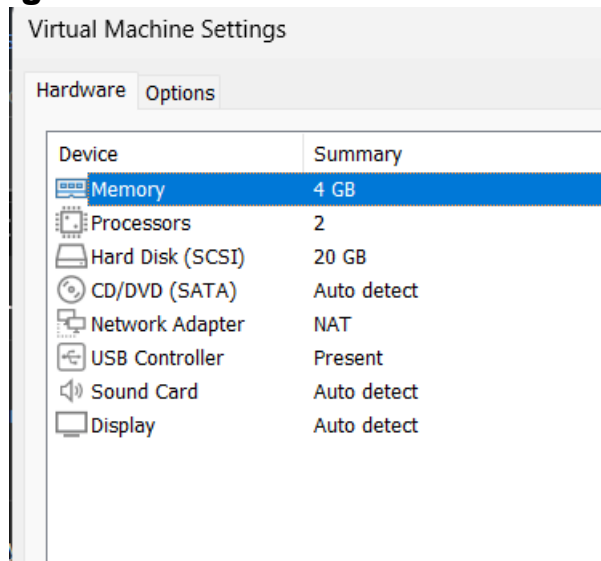
## Lab 4

### Task 1 – Verify VM resources in VMware

Confirm the VM resources that were allocated in Lab 1.

#### Steps

1. Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.
2. Inspect VM settings and note the following (no commands required for GUI): VM name, RAM, CPU, disk, and network adapter type.
3. Take a screenshot of the VM settings window showing RAM, CPU, disk and networking. Save screenshot as: **vm\_settings.png**



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

#### Steps

1. Start (or resume) the VM in VMware Workstation on your host.
2. From your host, open your preferred terminal (for example: Windows Command Prompt, PowerShell, macOS Terminal, or Linux Terminal) and connect to the VM using SSH. Example:

ssh student@<vm-ip-address>

**After connecting, save a screenshot of your host terminal showing the SSH login prompt/results as: vm\_login.png**

```
Expanded Security Maintenance for Applications is not enabled.

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

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

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

Last login: Fri Sep 26 21:01:03 2025 from 192.168.85.1
ubuntu@ubuntu-server:~$ |
```

**3. After logging in, run both commands and capture them together in a single screenshot:**

whoami

pwd

**Save a single screenshot that clearly shows both outputs as: whoami\_pwd.png**

```
Last login: Fri Sep 26 21:01:03 2025 from 192.168.85.1
ubuntu@ubuntu-server:~$ whoami
ubuntu
ubuntu@ubuntu-server:~$ pwd
/home/ubuntu
ubuntu@ubuntu-server:~$
```

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

**Steps (run inside VM terminal)**

**1. List root directory contents:**

ls -la /

**Save screenshot as: ls\_root.png**

```
ubuntu@ubuntu-server:~$ ls -la /
total 1994844
drwxr-xr-x 23 root root      4096 Sep 27 01:42 .
drwxr-xr-x 23 root root      4096 Sep 27 01:42 ..
lrwxrwxrwx  1 root root         7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x  2 root root      4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x  4 root root      4096 Sep 27 01:43 boot
dr-xr-xr-x  2 root root      4096 Aug  5 23:53 cdrom
drwxr-xr-x 20 root root     4120 Oct 20 12:16 dev
drwxr-xr-x 108 root root     4096 Sep 26 20:59 etc
drwxr-xr-x  3 root root      4096 Sep 27 01:48 home
lrwxrwxrwx  1 root root         7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx  1 root root         9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x  2 root root      4096 Feb 26  2024 lib.usr-is-merged
drwx----- 2 root root    16384 Sep 27 01:40 lost+found
drwxr-xr-x  2 root root      4096 Aug  5 16:54 media
drwxr-xr-x  2 root root      4096 Aug  5 16:54 mnt
drwxr-xr-x  2 root root      4096 Aug  5 16:54 opt
dr-xr-xr-x 280 root root       0 Oct 20 12:15 proc
drwx----- 4 root root      4096 Sep 26 21:03 root
drwxr-xr-x 29 root root       880 Oct 20 12:40 run
lrwxrwxrwx  1 root root         8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x  2 root root      4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x  2 root root      4096 Sep 27 01:48 snap
drwxr-xr-x  2 root root      4096 Aug  5 16:54 srv
-rw-----  1 root root 2042626048 Sep 27 01:42 swap.img
dr-xr-xr-x 13 root root       0 Oct 20 12:15 sys
drwxrwxrwt 15 root root      4096 Oct 20 12:32 tmp
```

## 2. Inspect these directories (run each command and screenshot the output):

ls -la /bin

**Save screenshot as ls\_bin.png.**

```
ubuntu@ubuntu-server:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
ubuntu@ubuntu-server:~$ |
```

ls -la /sbin

**Save screenshot as ls\_sbin.png.**

```
ubuntu@ubuntu-server:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
ubuntu@ubuntu-server:~$ |
```

ls -la /usr

**Save screenshot as ls\_usr.png.**

```
ubuntu@ubuntu-server:~$ ls -la /usr
total 92
drwxr-xr-x 12 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 27 01:42 ..
drwxr-xr-x  2 root root 32768 Sep 26 20:59 bin
drwxr-xr-x  2 root root 4096 Apr 22  2024 games
drwxr-xr-x 33 root root 4096 Sep 27 01:41 include
drwxr-xr-x 78 root root 4096 Sep 26 20:59 lib
drwxr-xr-x  2 root root 4096 Aug  5 17:01 lib64
drwxr-xr-x 11 root root 4096 Sep 27 01:42 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x  2 root root 20480 Sep 26 20:59 sbin
drwxr-xr-x 124 root root 4096 Sep 26 20:59 share
drwxr-xr-x  4 root root 4096 Sep 27 01:42 src
ubuntu@ubuntu-server:~$
```

ls -la /opt

**Save screenshot as ls\_opt.png.**

```
ubuntu@ubuntu-server:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 27 01:42 ..
ubuntu@ubuntu-server:~$
```

ls -la /etc

**Save screenshot as ls\_etc.png.**

```
ubuntu@ubuntu: ~  
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sysctl.d  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sysstat  
drwxr-xr-x 6 root root 4096 Aug 5 16:49 systemd  
drwxr-xr-x 2 root root 4096 Aug 5 17:00 terminfo  
drwxr-xr-x 2 root root 4096 Sep 27 01:42 thermald  
-rw-r--r-- 1 root root 8 Aug 5 17:02 timezone  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 tmpfiles.d  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 ubuntu-advantage  
-rw-r--r-- 1 root root 1260 Jan 27 2023 ucf.conf  
drwxr-xr-x 4 root root 4096 Aug 5 17:02 udev  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 udisks2  
drwxr-xr-x 3 root root 4096 Aug 5 17:14 ufw  
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated  
drwxr-xr-x 3 root root 4096 Aug 5 17:02 update-manager  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-motd.d  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-notifier  
drwxr-xr-x 2 root root 4096 Sep 27 01:42 UPower  
-rw-r--r-- 1 root root 1523 Aug 5 17:14 usb_modeswitch.conf  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 usb_modeswitch.d  
lrwxrwxrwx 1 root root 16 Aug 5 17:02 vconsole.conf -> default/  
drwxr-xr-x 2 root root 4096 Aug 5 17:14 vim  
drwxr-xr-x 4 root root 4096 Aug 5 17:14 vmware-tools  
lrwxrwxrwx 1 root root 23 Feb 26 2024 vtrgb -> /etc/alternative  
-rw-r--r-- 1 root root 4942 Aug 5 17:14 wgetrc  
drwxr-xr-x 4 root root 4096 Aug 5 17:02 X11  
-rw-r--r-- 1 root root 681 Apr 8 2024 xattr.conf  
drwxr-xr-x 4 root root 4096 Aug 5 17:02 xdg  
drwxr-xr-x 2 root root 4096 Aug 5 17:02 xml  
-rw-r--r-- 1 root root 460 Aug 5 17:14 zsh_command_not_found
```

ls -la /dev

**Save screenshot as ls\_dev.png.**

```
ubuntu@ubuntuserver: ~  
crw-rw---- 1 root tty 7, 1 Oct 18 18:23 vcs1  
crw-rw---- 1 root tty 7, 2 Oct 18 18:23 vcs2  
crw-rw---- 1 root tty 7, 3 Oct 18 18:23 vcs3  
crw-rw---- 1 root tty 7, 4 Oct 18 18:23 vcs4  
crw-rw---- 1 root tty 7, 5 Oct 18 18:23 vcs5  
crw-rw---- 1 root tty 7, 6 Oct 18 18:23 vcs6  
crw-rw---- 1 root tty 7, 128 Oct 18 18:23 vcsa  
crw-rw---- 1 root tty 7, 129 Oct 18 18:23 vcsa1  
crw-rw---- 1 root tty 7, 130 Oct 18 18:23 vcsa2  
crw-rw---- 1 root tty 7, 131 Oct 18 18:23 vcsa3  
crw-rw---- 1 root tty 7, 132 Oct 18 18:23 vcsa4  
crw-rw---- 1 root tty 7, 133 Oct 18 18:23 vcsa5  
crw-rw---- 1 root tty 7, 134 Oct 18 18:23 vcsa6  
crw-rw---- 1 root tty 7, 64 Oct 18 18:23 vcsu  
crw-rw---- 1 root tty 7, 65 Oct 18 18:23 vcsu1  
crw-rw---- 1 root tty 7, 66 Oct 18 18:23 vcsu2  
crw-rw---- 1 root tty 7, 67 Oct 18 18:23 vcsu3  
crw-rw---- 1 root tty 7, 68 Oct 18 18:23 vcsu4  
crw-rw---- 1 root tty 7, 69 Oct 18 18:23 vcsu5  
crw-rw---- 1 root tty 7, 70 Oct 18 18:23 vcsu6  
drwxr-xr-x 2 root root 60 Oct 18 18:22 vfio  
crw----- 1 root root 10, 127 Oct 18 18:23 vga_arbiter  
crw----- 1 root root 10, 137 Oct 18 18:22 vhci  
crw-rw---- 1 root kvm 10, 238 Oct 18 18:22 vhost-net  
crw-rw---- 1 root kvm 10, 241 Oct 18 18:22 vhost-vsock  
crw----- 1 root root 10, 122 Oct 18 18:23 vmci  
crw-rw-rw- 1 root root 10, 121 Oct 18 18:23 vsock  
crw-rw-rw- 1 root root 1, 5 Oct 18 18:23 zero  
crw----- 1 root root 10, 249 Oct 18 18:22 zfs  
ubuntu@ubuntuserver:~$
```

ls -la /var

Save screenshot as ls\_var.png.

```
ubuntu@ubuntuserver:~$ ls -la /var  
total 56  
drwxr-xr-x 13 root root 4096 Sep 27 01:46 .  
drwxr-xr-x 23 root root 4096 Sep 27 01:42 ..  
drwxr-xr-x 2 root root 4096 Oct 18 19:14 backups  
drwxr-xr-x 16 root root 4096 Oct 18 18:29 cache  
drwxrwsrwt 2 root root 4096 Aug 5 17:02 crash  
drwxr-xr-x 45 root root 4096 Oct 18 18:29 lib  
drwxrwsr-x 2 root staff 4096 Apr 22 2024 local  
lrwxrwxrwx 1 root root 9 Aug 5 16:54 lock -> /run/lock  
drwxrwxr-x 10 root syslog 4096 Oct 18 18:23 log  
drwxrwsr-x 2 root mail 4096 Aug 5 16:54 mail  
drwxr-xr-x 2 root root 4096 Aug 5 16:54 opt  
lrwxrwxrwx 1 root root 4 Aug 5 16:54 run -> /run  
drwxr-xr-x 2 root root 4096 May 21 15:46 snap  
drwxr-xr-x 4 root root 4096 Aug 5 17:14 spool  
drwxrwsrwt 9 root root 4096 Oct 18 18:29 tmp  
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated  
ubuntu@ubuntuserver:~$
```

ls -la /tmp

Save screenshot as ls\_tmp.png.

```

ubuntu@ubuntuserver:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 18 18:29 .
drwxr-xr-x 23 root root 4096 Sep 27 01:42 ..
drwxrwxrwt  2 root root 4096 Oct 18 18:22 .font-unix
drwxrwxrwt  2 root root 4096 Oct 18 18:22 .ICE-unix
drwx----- 2 root root 4096 Oct 18 18:22 snap-private-tmp
drwx----- 3 root root 4096 Oct 18 18:29 systemd-private-cb11bc68b56
drwx----- 3 root root 4096 Oct 18 18:23 systemd-private-cb11bc68b56
drwx----- 3 root root 4096 Oct 18 18:23 systemd-private-cb11bc68b56
drwx----- 3 root root 4096 Oct 18 18:23 systemd-private-cb11bc68b56
drwx----- 3 root root 4096 Oct 18 18:22 systemd-private-cb11bc68b56
jff
drwx----- 3 root root 4096 Oct 18 18:22 systemd-private-cb11bc68b56
sxd
drwx----- 3 root root 4096 Oct 18 18:29 systemd-private-cb11bc68b56
drwx----- 2 root root 4096 Oct 18 18:23 vmware-root_752-2957190263
drwxrwxrwt  2 root root 4096 Oct 18 18:22 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 18 18:22 .XIM-unix
ubuntu@ubuntuserver:~$

```

### 3. List your home directory and show hidden (dot) files:

`ls -la ~`

**Save screenshot as: home\_ls.png**

```

ubuntu@ubuntuserver:~$ ls -la ~
total 32
drwxr-x--- 4 ubuntu ubuntu 4096 Sep 26 21:12 .
drwxr-xr-x 3 root   root   4096 Sep 27 01:48 ..
-rw----- 1 ubuntu ubuntu  12 Sep 26 21:12 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Mar 31 2024 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Sep 27 01:48 .cache
-rw-r--r-- 1 ubuntu ubuntu  807 Mar 31 2024 .profile
drwx----- 2 ubuntu ubuntu 4096 Sep 27 01:49 .ssh
-rw-r--r-- 1 ubuntu ubuntu   0 Sep 27 01:52 .sudo_as_admin_successful
ubuntu@ubuntuserver:~$

```

### 4. Write a short paragraph (3–5 sentences) that explains the difference between `/bin`, `/usr/bin` and `/usr/local/bin`. Open your editor:

`nano ~/answers.md`

Type the paragraph in the editor, save and exit.

After saving, open the editor display (or show the file) and capture a screenshot of the paragraph.

**Save that screenshot as: answers\_md.png**

```

ubuntu@ubuntuserver:~$ nano ~/answers.md
ubuntu@ubuntuserver:~$ cat ~/answers.md
The /bin directory contains essential system binaries needed for booting and basic system functionality. The /usr/bin directory holds most user-level programs and utilities that are not critical for booting but used in general operations. Meanwhile, /usr/local/bin is used for binaries installed manually or compiled from source by the system administrator. It helps keep custom software separate from system-managed files. This hierarchy ensures modularity and easier maintenance.

```

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

### Steps (inside VM terminal)

#### 1. Create a workspace and navigate:

`mkdir -p ~/lab4/workspace/python_project`

**Save screenshot as mkdir\_workspace.png.**

```
ubuntu@ubuntu-server:~$ mkdir -p ~/lab4/workspace/python_project
ubuntu@ubuntu-server:~$ |
```

**cd ~/lab4/workspace/python\_project**

**Save screenshot as cd\_workspace.png.**

```
ubuntu@ubuntu-server:~$ mkdir -p ~/lab4/workspace/python_project
ubuntu@ubuntu-server:~$ cd ~/lab4/workspace/python_project
ubuntu@ubuntu-server:~/lab4/workspace/python_project$ |
```

**pwd**

**Save screenshot as pwd\_workspace.png.**

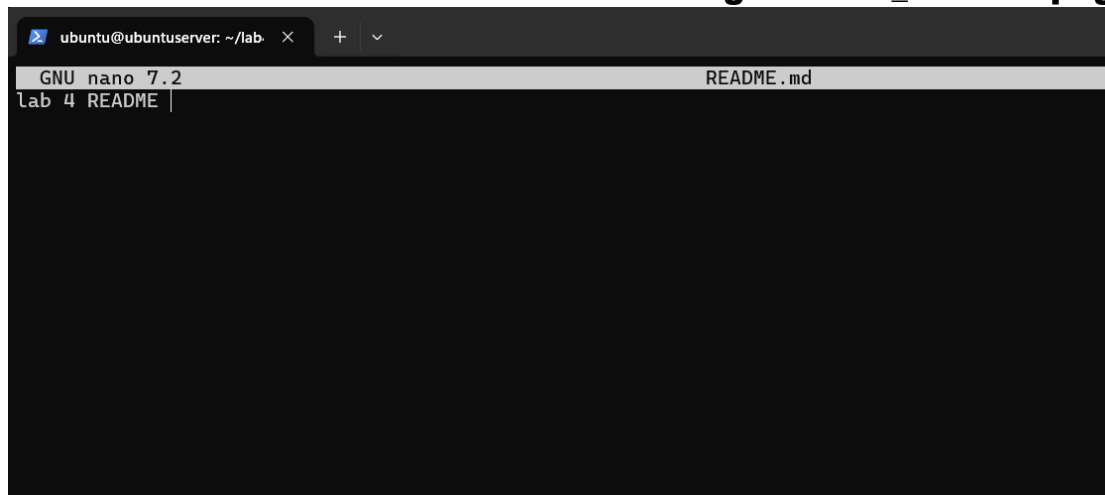
```
ubuntu@ubuntu-server:~$ cd ~/lab4/workspace/python_project
ubuntu@ubuntu-server:~/lab4/workspace/python_project$ pwd
/home/ubuntu/lab4/workspace/python_project
ubuntu@ubuntu-server:~/lab4/workspace/python_project$ |
```

**2. Create files using an editor (open each editor session and save a screenshot showing content):**

**nano README.md**

**Inside nano add: Lab 4 README and save.**

**Save screenshot of the editor after saving as nano\_readme.png.**



**nano main.py.**

**Inside nano add: print("hello lab4") and save.**

**Save screenshot as nano\_main.png.**

```
ubuntu@ubuntuserver: ~/lab. x + v
GNU nano 7.2 main.py
print("hello lab4")
```

**nano .env**

**Inside nano add: ENV=lab4 and save.**

**Save screenshot as nano\_env.png.**

```
ubuntu@ubuntuserver: ~/lab. x + v
GNU nano 7.2 .env
ENV=lab4
```

**3. List files and capture:**

**ls -la**

**Save screenshot as workspace\_ls.png.**

```
ubuntu@ubuntuserver: ~/lab4/workspace/python_project$ nano .env
ubuntu@ubuntuserver:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 ubuntu ubuntu 4096 Oct 18 19:50 .
drwxrwxr-x 3 ubuntu ubuntu 4096 Oct 18 19:44 ..
-rw-rw-r-- 1 ubuntu ubuntu  9 Oct 18 19:50 .env
-rw-rw-r-- 1 ubuntu ubuntu 20 Oct 18 19:50 main.py
-rw-rw-r-- 1 ubuntu ubuntu 14 Oct 18 19:48 README.md
ubuntu@ubuntuserver:~/lab4/workspace/python_project$
```

**4. Copy, move and remove:**

**cp README.md README.copy.md**

**After running, save screenshot as cp\_readme.png.**

```
ubuntu@ubuntuserver:~/lab4/workspace/python_project$ cp README.md READMEcopy.md
ubuntu@ubuntuserver:~/lab4/workspace/python_project$
```

**mv README.copy.md README.dev.md**

**After running, save screenshot as mv\_readme.png.**



```
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ mv READMEcopy.md README.dev.md
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ |
```

**rm README.dev.md**

**After running, save screenshot as rm\_readme.png.**

```
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ rm README.dev.md
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ |
```

**mkdir -p ~/lab4/workspace/java\_app**

**Save screenshot as mkdir\_java\_app.png.**

```
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ |
```

**cp -r ~/lab4/workspace/python\_project**

**~/lab4/workspace/java\_app\_copy**

**After running, save screenshot as cp\_recursive.png.**

```
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ |
```

**ls -la ~/lab4/workspace**

**Save screenshot as copy\_verify.png.**

```
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 ubuntu ubuntu 4096 Oct 18 19:55 .
drwxrwxr-x 3 ubuntu ubuntu 4096 Oct 18 19:44 ..
drwxrwxr-x 2 ubuntu ubuntu 4096 Oct 18 19:54 java_app
drwxrwxr-x 2 ubuntu ubuntu 4096 Oct 18 19:55 java_app_copy
drwxrwxr-x 2 ubuntu ubuntu 4096 Oct 18 19:53 python_project
ubuntu@ubuntuuserver:~/lab4/workspace/python_project$ |
```

**5. Use command history and tab completion:**

**history**

**Save screenshot as history.png.**

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

**Demonstrate tab completion (type partial name and press Tab) and capture that action as tab\_completion.png**

```
.cache/ lab4/ .local/ .ssh/
ubuntu@ubuntuuserver:~/lab4/workspace$ cd ~/lab4/workspace/python_project/|
```

## Task 5 – System info, resources & processes

### Steps (inside VM terminal)

#### 1. Kernel and OS:

uname -a

Save screenshot as uname.png.

```
ubuntu@ubuntu-server:~$ uname -a
Linux ubuntu-server 6.8.0-71-generic #71-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 22 16:52:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

#### 2. CPU (ensure model name visible):

cat /proc/cpuinfo

Save screenshot as cpuinfo.png.

```
Last login: Sat Oct 18 18:30:02 2025 from 192.168.85.1
ubuntu@ubuntu-server:~$ cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 142
model name     : Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz
stepping       : 12
microcode      : 0xffffffff
cpu MHz        : 1896.005
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
yscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni p
clmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowpre
fetch_pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt xsaveopt xsave
c xgetbv1 xsaves arat md_clear flush_lld arch_capabilities
bugs           : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs srbds mmio_stale_data retbleed gd
s bhi
bogomips       : 3792.01
clflush size   : 64
```

#### 3. Memory:

free -h

Save screenshot as meminfo.png.

```
ubuntu@ubuntu-server:~$ free -h
               total        used        free        shared  buff/cache        available
Mem:           3.8Gi        486Mi        3.2Gi         1.5Mi         330Mi         3.3Gi
Swap:          1.9Gi           0B         1.9Gi
```

#### 4. Disk:

df -h

Save screenshot as diskinfo.png.

```
ubuntu@ubuntu-server:~$ df -h
Filesystem                Size      Used Avail Use% Mounted on
tmpfs                     387M        1.5M  386M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 9.8G      5.2G   4.1G  56% /
tmpfs                     1.9G         0    1.9G   0% /dev/shm
tmpfs                     5.0M         0    5.0M   0% /run/lock
/dev/sda2                 1.8G     100M   1.6G   7% /boot
tmpfs                     387M        12K  387M   1% /run/user/1000
```

#### 5. View OS release information:

cat /etc/os-release

Save screenshot as os-release.png.

```
ubuntu@ubuntu-server:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
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=noble
LOGO=ubuntu-logo
ubuntu@ubuntu-server:~$ |
```

## 6. Processes (show top lines of ps output):

ps aux

Save screenshot as processes.png.

```
ubuntu@ubuntu-server:~$ ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.6  0.3 22036 13056 ?        Ss   12:15   0:14 /sbin/init
root         2  0.0  0.0      0     0 ?        S    12:15   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    12:15   0:00 [pool_workqueue_release]
root         4  0.0  0.0      0     0 ?        I<   12:15   0:00 [kworker/R-rcu_g]
root         5  0.0  0.0      0     0 ?        I<   12:15   0:00 [kworker/R-rcu_p]
root         6  0.0  0.0      0     0 ?        I<   12:15   0:00 [kworker/R-slub_]
root         7  0.0  0.0      0     0 ?        I<   12:15   0:00 [kworker/R-netns]
root        11  0.0  0.0      0     0 ?        I    12:15   0:00 [kworker/u256:0-ext4-rsv-conversion]
root        12  0.0  0.0      0     0 ?        I<   12:15   0:00 [kworker/R-mm_pe]
root        13  0.0  0.0      0     0 ?        I    12:15   0:00 [rcu_tasks_kthread]
root        14  0.0  0.0      0     0 ?        I    12:15   0:00 [rcu_tasks_rude_kthread]
root        15  0.0  0.0      0     0 ?        I    12:15   0:00 [rcu_tasks_trace_kthread]
root        16  0.0  0.0      0     0 ?        S    12:15   0:00 [ksoftirqd/0]
root        17  0.0  0.0      0     0 ?        I    12:15   0:00 [rcu_preempt]
root        18  0.0  0.0      0     0 ?        S    12:15   0:00 [migration/0]
root        19  0.0  0.0      0     0 ?        S    12:15   0:00 [idle_inject/0]
root        20  0.0  0.0      0     0 ?        S    12:15   0:00 [cpuhp/0]
root        21  0.0  0.0      0     0 ?        S    12:15   0:00 [cpuhp/1]
root        22  0.0  0.0      0     0 ?        S    12:15   0:00 [idle_inject/1]
root        23  0.0  0.0      0     0 ?        S    12:15   0:00 [migration/1]
root        24  0.0  0.0      0     0 ?        S    12:15   0:00 [ksoftirqd/1]
root        28  0.3  0.0      0     0 ?        I    12:15   0:07 [kworker/u258:0-events_power_efficient]
root        29  0.0  0.0      0     0 ?        S    12:15   0:00 [kdevtmpfs]
root        30  0.0  0.0      0     0 ?        I<   12:15   0:00 [kworker/R-inet_]
```

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

### Steps (inside VM terminal)

#### 1. Create a new user named lab4user:

sudo adduser lab4user

During prompts, capture the terminal and save screenshot as adduser\_lab4user.png.

```
ubuntu@ubuntu-server:~$ sudo adduser lab4user
[sudo] password for ubuntu:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
info: Creating home directory `/home/lab4user' ...
info: Copying files from `/etc/skel' ...
New password: |
```

#### 2. Verify the user entry:

getent passwd lab4user

Save screenshot as lab4user\_passwd.png.

```
ubuntu@ubuntu-server:~$ getent passwd lab4user
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
ubuntu@ubuntu-server:~$ |
```

#### 3. Switch to the new user to verify login:

su - lab4user

**Save screenshot as su\_lab4user.png.**

```
ubuntu@ubuntuserver:~$ su - lab4user
Password:
lab4user@ubuntuserver:~$ |
```

**4. From the new user you may attempt a sudo command to show that sudo is not available for this account (expected failure), e.g.:**

sudo whoami

**Save screenshot as sudo\_whoami.png.**

```
lab4user@ubuntuserver:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntuserver:~$ |
```

**5. Return to the original user:**

exit

**Save screenshot as exit\_back.png.**

```
lab4user is not in the sudoers file.
lab4user@ubuntuserver:~$ exit
logout
ubuntu@ubuntuserver:~$ |
```

**6. (Optional) Remove the test user when finished:**

sudo deluser --remove-home lab4user

**If run, save screenshot as deluser.png.**

```
ubuntu@ubuntuserver:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user 'lab4user' ...
ubuntu@ubuntuserver:~$ |
```

**Task 7(bonus task):**

**Steps (inside VM)**

**1. Open an editor to create the script:**

nano ~/lab4/workspace/run-demo.sh

**Type the following lines into the editor (manually or paste), save and exit:**

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

**Save screenshot of the editor after saving the file as nano\_run\_demo.png.**

```
GNU nano 7.2 /home/ubuntu/lab4/workspace/run-demo.sh
#!/bin/bash
echo "Lab 4 demo: current user is $(whoami)"
echo "Current time: $(date)"
uptime
free -h
```

## 2. Make the script executable:

`chmod +x ~/lab4/workspace/run-demo.sh`

## Save screenshot as `chmod_run_demo.png`.

```
ubuntu@ubuntu-server:~$ chmod +x ~/lab4/workspace/run-demo.sh
ubuntu@ubuntu-server:~$
```

## 3. Run the script as your regular user:

`~/lab4/workspace/run-demo.sh`

## Save screenshot of the script output as `run_demo_output.png`.

```
ubuntu@ubuntu-server:~$ ~/lab4/workspace/run-demo.sh
Lab 4 demo: current user is ubuntu
Current time: Mon Oct 20 01:06:00 PM UTC 2025
13:06:00 up 50 min, 2 users, load average: 0.00, 0.00, 0.00
Mem:          total    used    free    shared buff/cache   available
Swap:         3.8Gi    477Mi    3.2Gi    1.5Mi    344Mi       3.3Gi
Swap:         1.9Gi      0B    1.9Gi
```

## 4. Optionally run it with `sudo`:

`sudo ~/lab4/workspace/run-demo.sh`

## Save screenshot as `run_demo_output_sudo.png`.

```
ubuntu@ubuntu-server:~$ sudo ~/lab4/workspace/run-demo.sh
Lab 4 demo: current user is root
Current time: Mon Oct 20 01:06:43 PM UTC 2025
13:06:43 up 51 min, 2 users, load average: 0.00, 0.00, 0.00
Mem:          total    used    free    shared buff/cache   available
Swap:         3.8Gi    479Mi    3.2Gi    1.5Mi    344Mi       3.3Gi
Swap:         1.9Gi      0B    1.9Gi
```

# Exam evaluation questions:

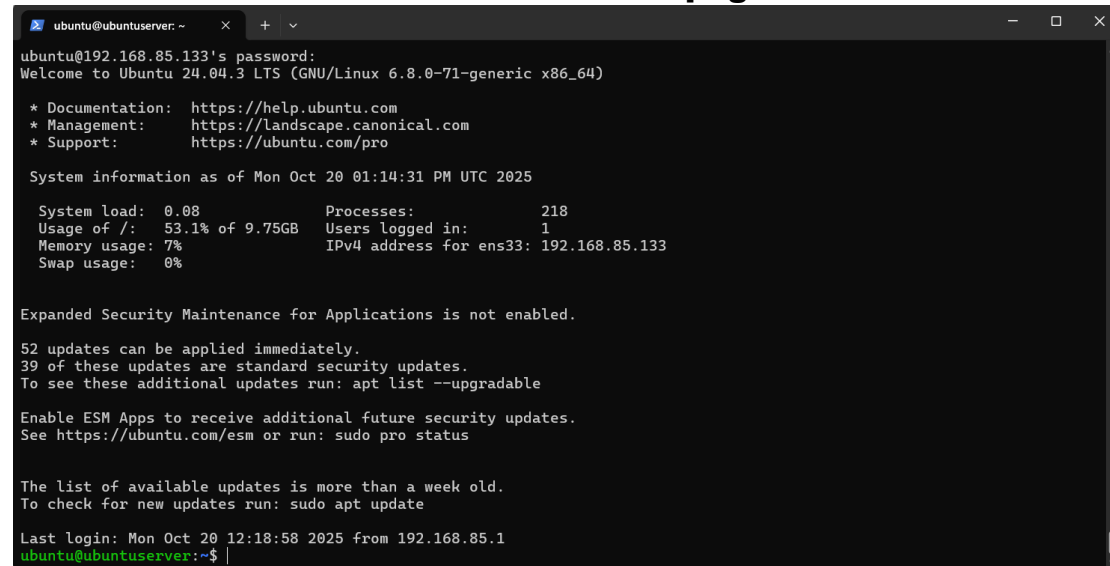
## 1. Remote Access Verification (Cyber Login Check)

### Scenario:

**You are part of a SOC (Security Operations Center) investigating unauthorized access to a Linux server hosted on VMware. Prove you can securely connect and verify your identity.**

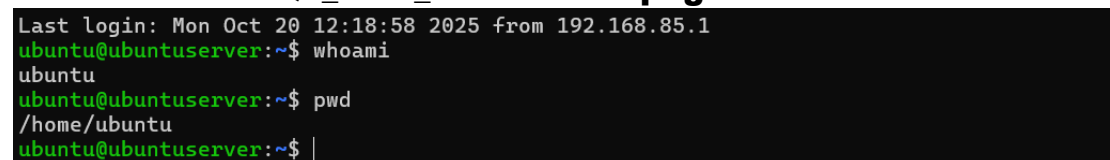
### Steps:

## Connect to the Ubuntu VM remotely from your host terminal. Screenshot as Q1\_remote\_connection.png



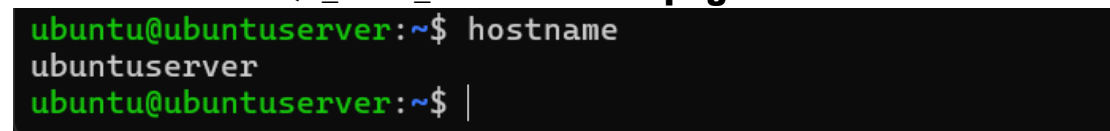
```
ubuntu@ubuntuserver: ~  
ubuntu@192.168.85.133's password:  
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
System information as of Mon Oct 20 01:14:31 PM UTC 2025  
  
System load:  0.08      Processes:      218  
Usage of /:   53.1% of 9.75GB   Users logged in: 1  
Memory usage: 7%      IPv4 address for ens33: 192.168.85.133  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
52 updates can be applied immediately.  
39 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Mon Oct 20 12:18:58 2025 from 192.168.85.1  
ubuntu@ubuntuserver:~$
```

## Verify your current user and home directory path. Screenshot as Q1\_user\_verification.png



```
Last login: Mon Oct 20 12:18:58 2025 from 192.168.85.1  
ubuntu@ubuntuserver:~$ whoami  
ubuntu  
ubuntu@ubuntuserver:~$ pwd  
/home/ubuntu  
ubuntu@ubuntuserver:~$
```

## Confirm you are connected to the correct host machine. Screenshot as Q1\_host\_confirmation.png



```
ubuntu@ubuntuserver:~$ hostname  
ubuntuserver  
ubuntu@ubuntuserver:~$
```

## 2. Filesystem Inspection for Forensic Evidence

### Scenario:

The incident response team suspects malicious files in system directories. You must explore the filesystem to locate and document the system's structure.

### Steps:

Display the contents of the root directory.

### Screenshot as Q2\_root\_listing.png

```
ubuntu@ubuntu-server:~$ ls -la /
total 1994844
drwxr-xr-x 23 root root      4096 Sep 27 01:42 .
drwxr-xr-x 23 root root      4096 Sep 27 01:42 ..
lrwxrwxrwx 1 root root         7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x 2 root root      4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x 4 root root      4096 Sep 27 01:43 boot
dr-xr-xr-x 2 root root      4096 Aug  5 23:53 cdrom
drwxr-xr-x 20 root root     4120 Oct 20 12:16 dev
drwxr-xr-x 108 root root     4096 Oct 20 13:02 etc
drwxr-xr-x 3 root root      4096 Oct 20 13:02 home
lrwxrwxrwx 1 root root         7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx 1 root root         9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x 2 root root      4096 Feb 26  2024 lib.usr-is-merged
drwx----- 2 root root    16384 Sep 27 01:40 lost+found
drwxr-xr-x 2 root root      4096 Aug  5 16:54 media
drwxr-xr-x 2 root root      4096 Aug  5 16:54 mnt
drwxr-xr-x 2 root root      4096 Aug  5 16:54 opt
dr-xr-xr-x 277 root root       0 Oct 20 12:15 proc
drwx----- 4 root root      4096 Sep 26 21:03 root
drwxr-xr-x 29 root root       900 Oct 20 13:14 run
lrwxrwxrwx 1 root root         8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x 2 root root      4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x 2 root root      4096 Sep 27 01:48 snap
drwxr-xr-x 2 root root      4096 Aug  5 16:54 srv
-rw----- 1 root root 2042626048 Sep 27 01:42 swap.img
dr-xr-xr-x 13 root root       0 Oct 20 12:43 sys
drwxrwxrwt 15 root root      4096 Oct 20 12:32 tmp
```

**Display the OS version and release information.**

**Screenshot as Q2\_os\_version.png**

```
ubuntu@ubuntu-server:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
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=noble
LOGO=ubuntu-logo
ubuntu@ubuntu-server:~$ |
```

**Explore and record directory listings for /bin, /sbin, /usr, /opt, /etc, /dev, /var, and /tmp.**

**Screenshot as Q2\_directory\_evidence.png**

```
ubuntu@ubuntu-server:~$ ls -la /bin
ls -la /sbin
ls -la /usr
ls -la /opt
ls -la /etc
ls -la /dev
ls -la /var
ls -la /tmp
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
total 92
drwxr-xr-x 12 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 27 01:42 ..
drwxr-xr-x 2 root root 32768 Sep 26 20:59 bin
drwxr-xr-x 2 root root 4096 Apr 22  2024 games
drwxr-xr-x 33 root root 4096 Sep 27 01:41 include
drwxr-xr-x 78 root root 4096 Sep 26 20:59 lib
drwxr-xr-x 2 root root 4096 Aug  5 17:01 lib64
drwxr-xr-x 11 root root 4096 Sep 27 01:42 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x 2 root root 20480 Sep 26 20:59 sbin
drwxr-xr-x 124 root root 4096 Sep 26 20:59 share
drwxr-xr-x 4 root root 4096 Sep 27 01:42 src
total 8
drwxr-xr-x 2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 27 01:42 ..
total 936
```

```

drwxr-xr-x 2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 27 01:42 ..
total 936
drwxr-xr-x 108 root root      4096 Oct 20 13:02 .
drwxr-xr-x 23 root root      4096 Sep 27 01:42 ..
-rw-r--r-- 1 root root      3444 Jul  5 2023 adduser.conf
drwxr-xr-x 2 root root      4096 Aug  5 17:14 alternatives
drwxr-xr-x 2 root root      4096 Aug  5 17:02 apparmor
drwxr-xr-x 9 root root      4096 Aug  5 17:14 apparmor.d
drwxr-xr-x 3 root root      4096 Aug  5 17:02 apport
drwxr-xr-x 9 root root      4096 Sep 27 01:39 apt
-rw-r--r-- 1 root root     2319 Mar 31 2024 bash.bashrc
-rw-r--r-- 1 root root      45 Aug  5 17:14 bash_completion
drwxr-xr-x 2 root root      4096 Aug  5 17:14 bash_completion.d
-rw-r--r-- 1 root root     367 Aug  2 2022 bindresvport.blacklist
drwxr-xr-x 2 root root      4096 Jul  2 14:04 binfmt.d
drwxr-xr-x 2 root root      4096 Aug  5 17:14 byobu
drwxr-xr-x 3 root root      4096 Aug  5 17:02 ca-certificates
-rw-r--r-- 1 root root     6288 Aug  5 17:02 ca-certificates.conf
drwxr-xr-x 5 root root      4096 Sep 27 01:49 cloud
drwxr-xr-x 2 root root      4096 Sep 27 01:41 console-setup
drwx----- 2 root root      4096 Jul  2 14:04 credstore
drwx----- 2 root root      4096 Jul  2 14:04 credstore.encrypted
drwxr-xr-x 2 root root      4096 Aug  5 17:14 cron.d
drwxr-xr-x 2 root root      4096 Aug  5 17:14 cron.daily
drwxr-xr-x 2 root root      4096 Aug  5 17:14 cron.hourly
drwxr-xr-x 2 root root      4096 Aug  5 17:14 cron.monthly
-rw-r--r-- 1 root root      11 Apr 22 2024 debian_version
drwxr-xr-x 3 root root      4096 Sep 26 20:59 default
-rw-r--r-- 1 root root     1706 Jul  5 2023 deluser.conf
drwxr-xr-x 2 root root      4096 Aug  5 17:02 depmod.d
drwxr-xr-x 3 root root      4096 Aug  5 17:02 dhcp
-rw-r--r-- 1 root root     1429 May  7 2024 dhcpcd.conf
drwxr-xr-x 4 root root      4096 Aug  5 17:01 dpkg
-rw-r--r-- 1 root root      685 Apr  8 2024 e2scrub.conf
-rw-r--r-- 1 root root      106 Aug  5 16:54 environment
-rw-r--r-- 1 root root     1853 Oct 17 2022 ethertypes
drwxr-xr-x 4 root root      4096 Sep 27 01:42 fonts
-rw-r--r-- 1 root root      657 Sep 27 01:42 fstab
-rw-r--r-- 1 root root      694 Apr  8 2024 fuse.conf
drwxr-xr-x 4 root root      4096 Aug  5 17:14 fwupd
-rw-r--r-- 1 root root     2584 Jan 31 2024 gai.conf
drwxr-xr-x 2 root root      4096 Aug  5 17:01 gnutls
drwxr-xr-x 2 root root      4096 Aug  5 17:02 groff
-rw-r--r-- 1 root root      808 Oct 20 13:02 group
-rw-r--r-- 1 root root      833 Oct 20 12:59 group-
drwxr-xr-x 2 root root      4096 Sep 27 01:41 grub.d
-rw-r----- 1 root shadow     685 Oct 20 13:02 gshadow
-rw-r----- 1 root shadow     706 Oct 20 12:59 gshadow-
drwxr-xr-x 3 root root      4096 Aug  5 17:02 gss
-rw-r--r-- 1 root root     4436 Aug  5 17:14 hdparm.conf
-rw-r--r-- 1 root root      92 Apr 22 2024 host.conf
-rw-r--r-- 1 root root      13 Sep 27 01:43 hostname
-rw-r--r-- 1 root root      227 Sep 27 01:43 hosts
-rw-r--r-- 1 root root      411 Sep 26 20:59 hosts.allow
-rw-r--r-- 1 root root      711 Sep 26 20:59 hosts.deny
drwxr-xr-x 2 root root      4096 Sep 26 20:59 init.d
drwxrwxr-x 10 root syslog  4096 Oct 20 12:16 log
drwxrwsr-x 2 root mail    4096 Aug  5 16:54 mail
drwxr-xr-x 2 root root    4096 Aug  5 16:54 opt
lrwxrwxrwx 1 root root      4 Aug  5 16:54 run -> /run
drwxr-xr-x 2 root root    4096 May 21 15:46 snap
drwxr-xr-x 4 root root    4096 Aug  5 17:14 spool
drwxrwxrwt 9 root root    4096 Oct 20 12:32 tmp
-rw-r--r-- 1 root root     208 Aug  5 16:54 .updated
total 60
drwxrwxrwt 15 root root  4096 Oct 20 12:32 .
drwxr-xr-x 23 root root  4096 Sep 27 01:42 ..
drwxrwxrwt 2 root root  4096 Oct 20 12:16 .font-unix
drwxrwxrwt 2 root root  4096 Oct 20 12:16 .ICE-unix
drwx----- 2 root root  4096 Oct 20 12:16 snap-private-tmp
drwx----- 3 root root  4096 Oct 20 12:32 systemd-private-fdca5643613742d583ef5876daeab612-fwupd.service-IeRLkS
drwx----- 3 root root  4096 Oct 20 12:16 systemd-private-fdca5643613742d583ef5876daeab612-ModemManager.service-TALV
drwx----- 3 root root  4096 Oct 20 12:16 systemd-private-fdca5643613742d583ef5876daeab612-polkit.service-2w421x
drwx----- 3 root root  4096 Oct 20 12:16 systemd-private-fdca5643613742d583ef5876daeab612-systemd-logind.service-g06
drwx----- 3 root root  4096 Oct 20 12:16 systemd-private-fdca5643613742d583ef5876daeab612-systemd-resolved.service-
uY
drwx----- 3 root root  4096 Oct 20 12:16 systemd-private-fdca5643613742d583ef5876daeab612-systemd-timesyncd.service-
KNK
drwx----- 3 root root  4096 Oct 20 12:32 systemd-private-fdca5643613742d583ef5876daeab612-upower.service-e4NmX
drwx----- 2 root root  4096 Oct 20 12:16 vmware-root_748-2966037996
drwxrwxrwt 2 root root  4096 Oct 20 12:16 .X11-unix
drwxrwxrwt 2 root root  4096 Oct 20 12:16 .XIM-unix
ubuntu@buntuserver:~$

```

**Display all hidden files in your home directory.**

**Screenshot as Q2\_hidden\_files.png**



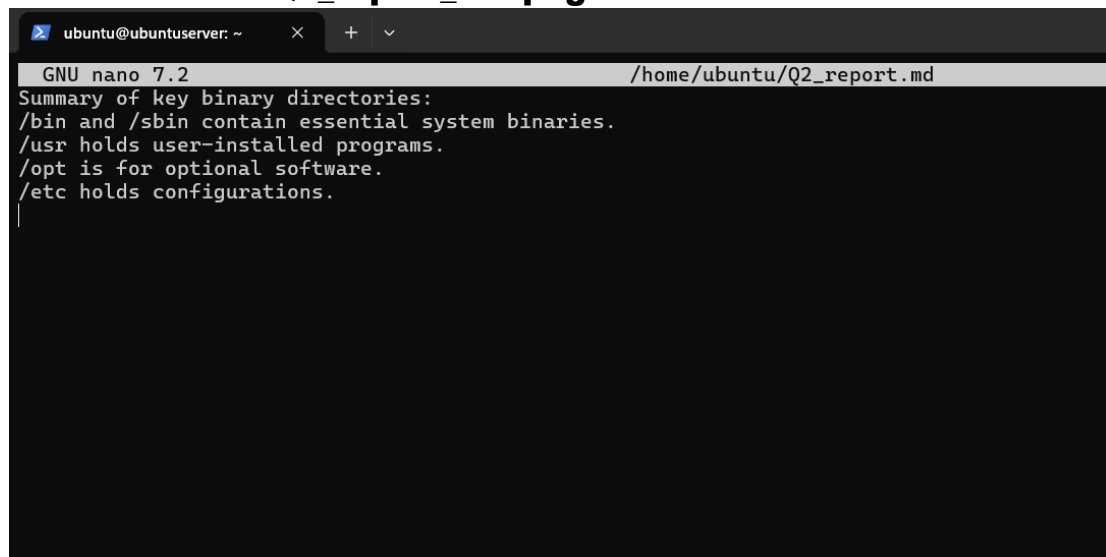
```

ubuntu@ubuntu-server:~$ ls -la ~
total 44
drwxr-x--- 6 ubuntu ubuntu 4096 Oct 18 19:44 .
drwxr-xr-x 3 root root 4096 Oct 20 13:02 ..
-rw-rw-r-- 1 ubuntu ubuntu 482 Oct 18 19:36 answers.md
-rw----- 1 ubuntu ubuntu 361 Oct 20 13:13 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Mar 31 2024 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Sep 27 01:48 .cache
drwxrwxr-x 3 ubuntu ubuntu 4096 Oct 18 19:44 lab4
drwxrwxr-x 3 ubuntu ubuntu 4096 Oct 18 19:36 .local
-rw-r--r-- 1 ubuntu ubuntu 807 Mar 31 2024 .profile
drwx----- 2 ubuntu ubuntu 4096 Sep 27 01:49 .ssh
-rw-r--r-- 1 ubuntu ubuntu 0 Sep 27 01:52 .sudo_as_admin_successful
ubuntu@ubuntu-server:~$

```

**Create a markdown file summarizing your findings on key binary directories.**

**Screenshot as Q2\_report\_file.png**



### 3. Evidence Handling & File Operations

**Scenario:**

**You are creating a sandbox environment to safely analyze and handle suspicious files collected from a compromised system.**

**Steps:**

**Create a structured folder hierarchy under your home directory for analysis.**

**Screenshot as Q3\_workspace\_created.png**

```

ubuntu@ubuntu-server:~$ mkdir -p ~/analysis_lab/suspicious_files
ubuntu@ubuntu-server:~$

```

**Create three text files, including one hidden file, in your workspace.**

**Screenshot as Q3\_files\_created.png**

```
ubuntu@ubuntu-server:~$ mkdir -p ~/analysis_lab/suspicious_files
ubuntu@ubuntu-server:~$ cd ~/analysis_lab/suspicious_files
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ nano file2.txt
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ nano file1.txt
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ nano file3.txt
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ |
```

**Create a backup copy of one file, rename it, and then delete it after verification.**

**Screenshot as Q3\_backup\_handling.png**

```
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ cp file1.txt file1_backup.txt
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ mv file1_backup.txt file1_copy.txt
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ rm file1_copy.txt
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ |
```

**Copy the entire workspace as an evidence backup folder.**

**Screenshot as Q3\_workspace\_backup.png**

```
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ cp -r ~/analysis_lab ~/evidence_backup
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ |
```

**Display your command history to document all actions performed.**

**Screenshot as Q3\_command\_history.png**

```
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ history
1  whoami
2  exit
3  cat /proc/cpuinfo
4  uname
5  uname
6  uname -a
7  ls -la /sbin
8  ls -la /bin
9  ls -la /
10 free -h
11 df -h
12 cat /etc/os-release
13 ps aux
14 sudo adduser lab4user
15 getent passwd lab4user
16 su - lab4user
17 sudo deluser --remove-home lab4user
18 nano ~/lab4/workspace/run-demo.sh
19 chmod +x ~/lab4/workspace/run-demo.sh
20 ~/lab4/workspace/run-demo.sh
21 sudo ~/lab4/workspace/run-demo.sh
22 exit
23 whoami
24 pwd
25 hostname
```

**Demonstrate Linux auto-completion by typing a partial command or filename.**

**Screenshot as Q3\_autocomplete.png**

```
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ cat
file1.txt      file2.txt      .hidden1.txt
ubuntu@ubuntu-server:~/analysis_lab/suspicious_files$ cd ~/analysis_lab/suspicious_files/|
```

## 4. System Profiling and Process Monitoring

**Scenario:**

**You are investigating a potential malware infection that is consuming excessive resources on the Linux VM.**

**Steps:**

**Display the system's OS and kernel version for the investigation report.**

**Screenshot as Q4\_system\_info.png**

```
ubuntu@ubuntuuserver:~$ uname -a
Linux ubuntuuserver 6.8.0-71-generic #71-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 22 16:52:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
ubuntu@ubuntuuserver:~$ |
```

**Display CPU, memory, and disk usage information.**

**Screenshot as Q4\_resource\_info.png**

```
ubuntu@ubuntuuserver:~$ free -h
df -h
```

	total	used	free	shared	buff/cache	available
Mem:	3.8Gi	522Mi	2.9Gi	1.5Mi	644Mi	3.3Gi
Swap:	1.9Gi	0B	1.9Gi			

Filesystem	Size	Used	Avail	Use%	Mounted on
tmpfs	387M	1.6M	386M	1%	/run
/dev/mapper/ubuntu--vg-ubuntu--lv	9.8G	5.2G	4.1G	57%	/
tmpfs	1.9G	0	1.9G	0%	/dev/shm
tmpfs	5.0M	0	5.0M	0%	/run/lock
/dev/sda2	1.8G	100M	1.6G	7%	/boot
tmpfs	387M	12K	387M	1%	/run/user/1000

```
ubuntu@ubuntuuserver:~$ |
```

**Display all active running processes to identify suspicious activity.**

**Screenshot as Q4\_process\_list.png**

```
ubuntu@ubuntuuserver:~$ ps aux
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.3	0.3	22240	13056	?	Ss	12:15	0:14	/sbin/init
root	2	0.0	0.0	0	0	?	S	12:15	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	12:15	0:00	[pool_workqueue_release]
root	4	0.0	0.0	0	0	?	I<	12:15	0:00	[kworker/R-rcu_g]
root	5	0.0	0.0	0	0	?	I<	12:15	0:00	[kworker/R-rcu_p]
root	6	0.0	0.0	0	0	?	I<	12:15	0:00	[kworker/R-slub_]
root	7	0.0	0.0	0	0	?	I<	12:15	0:00	[kworker/R-netns]
root	11	0.0	0.0	0	0	?	I	12:15	0:00	[kworker/u256:0-ext4-rsv-conversion]
root	12	0.0	0.0	0	0	?	I<	12:15	0:00	[kworker/R-mm_pe]
root	13	0.0	0.0	0	0	?	I	12:15	0:00	[rcu_tasks_kthread]
root	14	0.0	0.0	0	0	?	I	12:15	0:00	[rcu_tasks_rude_kthread]
root	15	0.0	0.0	0	0	?	I	12:15	0:00	[rcu_tasks_trace_kthread]
root	16	0.0	0.0	0	0	?	S	12:15	0:00	[ksoftirqd/0]
root	17	0.0	0.0	0	0	?	I	12:15	0:01	[rcu_preempt]
root	18	0.0	0.0	0	0	?	S	12:15	0:00	[migration/0]
root	19	0.0	0.0	0	0	?	S	12:15	0:00	[idle_inject/0]
root	20	0.0	0.0	0	0	?	S	12:15	0:00	[cpuhp/0]
root	21	0.0	0.0	0	0	?	S	12:15	0:00	[cpuhp/1]
root	22	0.0	0.0	0	0	?	S	12:15	0:00	[idle_inject/1]
root	23	0.0	0.0	0	0	?	S	12:15	0:00	[migration/1]
root	24	0.0	0.0	0	0	?	S	12:15	0:00	[ksoftirqd/1]
root	28	0.1	0.0	0	0	?	I	12:15	0:07	[kworker/u258:0-flush-252:0]
root	29	0.0	0.0	0	0	?	S	12:15	0:00	[kdevtmpfs]
root	30	0.0	0.0	0	0	?	I<	12:15	0:00	[kworker/R-inet_]
root	32	0.0	0.0	0	0	?	S	12:15	0:00	[kauditd]
root	33	0.2	0.0	0	0	?	I	12:15	0:09	[kworker/0:2-events]
root	34	0.0	0.0	0	0	?	S	12:15	0:00	[khungtaskd]
root	35	0.0	0.0	0	0	?	S	12:15	0:00	[oom_reaper]

## **5. User Account Audit & Privilege Escalation Simulation**

**Scenario:**

**You are performing a user activity audit on a compromised Linux server.**

**The SOC suspects a newly created account (lab4user) may have been used for unauthorized access.**

**Your task is to simulate the account creation, perform privilege tests, and analyze authentication logs for forensic evidence.**

**Steps:**

**Create a new test user named lab4user.**

**Screenshot as Q5\_user\_created.png.**

```
ubuntu@ubuntuserver:~$ sudo adduser lab4user
[sudo] password for ubuntu:
info: Adding user 'lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'lab4user' (1001) ...
info: Adding new user 'lab4user' (1001) with group 'lab4user (1001)' ...
info: Creating home directory '/home/lab4user' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
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
info: Adding new user 'lab4user' to supplemental / extra groups 'users' ...
info: Adding user 'lab4user' to group 'users' ...
ubuntu@ubuntuserver:~$
```

**Verify that the new user record exists in the system's user database.**

**Screenshot as Q5\_user\_verified.png**

```
ubuntu@ubuntuserver:~$ getent passwd lab4user
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
ubuntu@ubuntuserver:~$
```

**Log in as lab4user and confirm successful login.**

**Screenshot as Q5\_user\_login.png**

```
ubuntu@ubuntuserver:~$ su - lab4user
Password:
lab4user@ubuntuserver:~$
```

**Attempt to run an administrative command as lab4user (expect permission denied).**

**Screenshot as Q5\_permission\_denied.png**

```
lab4user@ubuntuserver:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntuserver:~$
```

**Switch back to your main analyst account.**

**Screenshot as Q5\_switch\_back.png**

```
lab4user@ubuntuserver:~$ exit
logout
ubuntu@ubuntuserver:~$
```

**Inspect the system authentication logs located at `/var/log/auth.log` to determine whether the `lab4user` account attempted any logins (successful or failed).**

**Screenshot as Q5\_authlog\_analysis.png**

```
ubuntu@ubuntu:server: ~  
2025-10-20T12:58:19.862710+00:00 ubuntu:server sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/adduser lab4user  
2025-10-20T12:58:19.864849+00:00 ubuntu:server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)  
2025-10-20T12:58:20.021864+00:00 ubuntu:server groupadd[1783]: group added to /etc/group: name=lab4user, GID=1001  
2025-10-20T12:58:20.023545+00:00 ubuntu:server groupadd[1783]: group added to /etc/gshadow: name=lab4user  
2025-10-20T12:58:20.025769+00:00 ubuntu:server groupadd[1783]: new group: name=lab4user, GID=1001  
2025-10-20T12:58:20.050244+00:00 ubuntu:server useradd[1790]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/bin/bash, from=/dev/pts/1  
2025-10-20T12:59:12.007897+00:00 ubuntu:server passwd[1803]: pam_unix(passwd:chauthtok): password changed for lab4user  
2025-10-20T12:59:18.757597+00:00 ubuntu:server chfn[1804]: changed user 'lab4user' information  
2025-10-20T12:59:20.687433+00:00 ubuntu:server gpasswd[1813]: members of group users set by root to lab4user  
2025-10-20T12:59:20.690550+00:00 ubuntu:server sudo: pam_unix(sudo:session): session closed for user root  
2025-10-20T13:00:20.440600+00:00 ubuntu:server su[1824]: (to lab4user) ubuntu on pts/0  
2025-10-20T13:00:20.441710+00:00 ubuntu:server su[1824]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by ubuntu(uid=1000)  
2025-10-20T13:00:59.611144+00:00 ubuntu:server sudo: lab4user : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/whoami  
2025-10-20T13:01:39.400433+00:00 ubuntu:server su[1824]: pam_unix(su-l:session): session closed for user lab4user  
2025-10-20T13:02:11.637070+00:00 ubuntu:server sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/deluser --remove-home lab4user  
2025-10-20T13:02:11.639731+00:00 ubuntu:server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)  
2025-10-20T13:02:11.777481+00:00 ubuntu:server userdel[1845]: delete user 'lab4user'  
2025-10-20T13:02:11.777573+00:00 ubuntu:server userdel[1845]: delete 'lab4user' from group 'users'  
2025-10-20T13:02:11.778302+00:00 ubuntu:server userdel[1845]: removed group 'lab4user' owned by 'lab4user'  
2025-10-20T13:02:11.778698+00:00 ubuntu:server userdel[1845]: removed shadow group 'lab4user' owned by 'lab4user'  
2025-10-20T13:02:11.778744+00:00 ubuntu:server userdel[1845]: delete 'lab4user' from shadow group 'users'  
2025-10-20T13:02:11.797178+00:00 ubuntu:server sudo: pam_unix(sudo:session): session closed for user root
```

**(Optional) Remove the `lab4user` account after the audit and verify deletion.**

**Screenshot as Q5\_user\_removed.png**

```
ubuntu@ubuntu:server: ~$ sudo deluser --remove-home lab4user  
info: Looking for files to backup/remove ...  
info: Removing files ...  
info: Removing crontab ...  
info: Removing user 'lab4user' ...  
ubuntu@ubuntu:server: ~$
```