

Fatima Jinnah Women University



*Cloud Computing
Lab 4*

Submitted By :

Iashal Nasir

Section :

A

Roll No:

38

Submitted To:

Sir Shoail

LAB TITLE: Virtualization & Linux Fundamentals

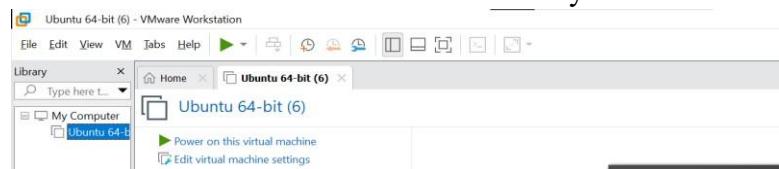
TASK:

Task 1: Verify VM resources in VMware

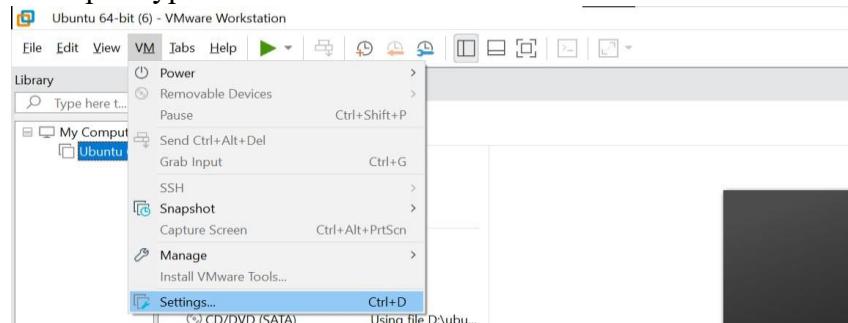
Confirm the VM resources that were allocated in Lab 1.

Steps

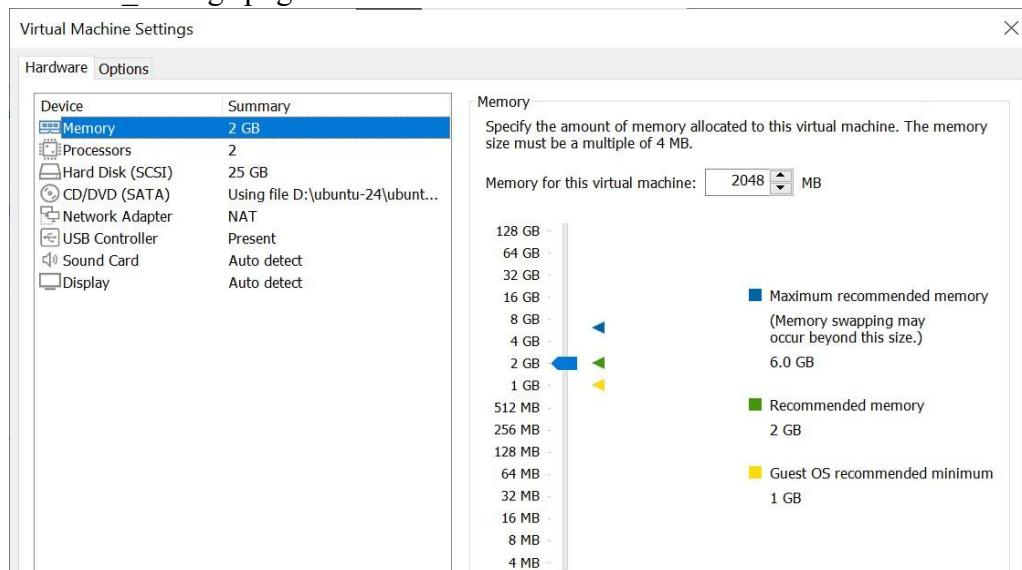
1. Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.



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

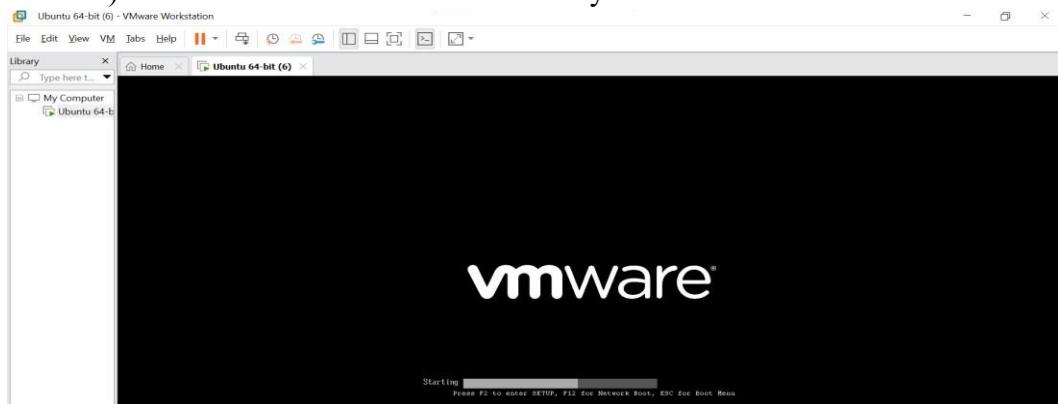


Task 2: Start VM and log in (use your preferred host terminal method only)

Use a single preferred host-terminal method to connect to the VM. Do not switch between methods during the task.

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>

1. Find the IP address of your Ubuntu Server using "ip addr"

```
ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6a:f6:87 brd ff:ff:ff:ff:ff:ff
      altname enp2s1
      inet 192.168.161.129/24 metric 100 brd 192.168.161.255 scope global dynamic ens33
        valid_lft 1082sec preferred_lft 1082sec
      inetc6 fe80::20c:29ff:fe6a:f687/64 scope link
        valid_lft forever preferred_lft forever
```

2. Connect via SSH from Windows

```
PS C:\Users\HP> ping 192.168.161.129

Pinging 192.168.161.129 with 32 bytes of data:
Reply from 192.168.161.129: bytes=32 time=1ms TTL=64
Reply from 192.168.161.129: bytes=32 time<1ms TTL=64
Reply from 192.168.161.129: bytes=32 time<1ms TTL=64
Reply from 192.168.161.129: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.161.129:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

3. Accept the fingerprint (first time only) Type yes when prompted.

```
PS C:\Users\HP> ssh hajra@192.168.161.129
The authenticity of host '192.168.161.129 (192.168.161.129)' can't be established.
ED25519 key fingerprint is SHA256:M5unwK7+jxUhr6KM3bbMPRkghlGd+Kq5uspTQZ5Up3w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

4. Enter your password

Use the same password you set up during the Ubuntu Server installation.

```
Warning: Permanently added '192.168.161.129' (ED25519) to the list of known hosts.
hajra@192.168.161.129's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-84-generic x86_64)

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

 System information as of Sat 27 Sep 10:28:45 UTC 2025

 System load:  1.46          Processes:           276
 Usage of /:   70.2% of 11.21GB  Users logged in:     1
 Memory usage: 57%
 Swap usage:   9%

 Expanded Security Maintenance for Applications is not enabled.

 0 updates can be applied immediately.

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

hajra@ubuntu-1lab: $
```

3. After logging in, run both commands and capture them together in a single screenshot:
- ```
whoami
pwd
```

```
hajra@ubuntu-lab: $ whoami
hajra
hajra@ubuntu-lab: $ pwd
/home/hajra
hajra@ubuntu-lab: $
```

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

### Steps (run inside VM terminal)

1. List root directory contents:

```
ls -la /
```

```
hajra@ubuntu-lab:~$ ls -la
total 44
drwxr-x--- 4 hajra hajra 4096 Sep 26 22:08 .
drwxr-xr-x 3 root root 4096 Sep 26 21:38 ..
-rw-r--r-- 1 hajra hajra 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 hajra hajra 3771 Mar 31 2024 .bashrc
drwx----- 2 hajra hajra 4096 Sep 26 21:40 .cache
-rw----- 1 hajra hajra 20 Sep 26 22:08 .lessht
-rw----- 1 hajra hajra 807 Mar 31 2024 .profile
drwx----- 2 hajra hajra 4096 Sep 26 22:00 .ssh
-rw-r--r-- 1 hajra hajra 0 Sep 26 21:48 .sudo_as_admin_successful
-rw-r--r-- 1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$ _
```

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

```
ls -la /bin
```

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

```
ls -la /sbin
```

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

```
ls -la /usr
```

```
hajra@ubuntu-lab:~$ ls -la /usr
total 96
drwxr-xr-x 12 root root 4096 Aug 5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxr-xr-x 2 root root 36864 Oct 21 17:19 bin
drwxr-xr-x 2 root root 4096 Apr 22 2024 games
drwxr-xr-x 35 root root 4096 Oct 14 08:07 include
drwxr-xr-x 59 root root 4096 Oct 14 08:07 lib
drwxr-xr-x 2 root root 4096 Sep 26 21:18 lib64
drwxr-xr-x 13 root root 4096 Oct 14 08:06 libexec
drwxr-xr-x 18 root root 4096 Aug 5 16:54 local
drwxr-xr-x 2 root root 20480 Oct 21 17:18 sbin
drwxr-xr-x 128 root root 4096 Oct 14 08:07 share
drwxr-xr-x 7 root root 4096 Oct 21 17:20 src
hajra@ubuntu-lab:~$ _
```

```
ls -la /opt
```

```
hajra@ubuntu-lab:~$ ls -la /opt
total 16
drwxr-xr-x 4 root root 4096 Sep 26 21:51 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxr-xr-x 2 root root 4096 Sep 26 21:51 cru
drwxr-xr-x 4 root root 4096 Sep 26 21:51 containerd
hajra@ubuntu-lab:~$ _
```

```
ls -la /etc
```

```

drwxr-xr-x 2 root root 4096 Aug 5 17:14 .
-rw-r--r-- 2 root root 12813 Mar 27 2021 services
drwxr-xr-x 2 root root 4096 Aug 5 17:02 ..
-rw-r----- 1 root shadow 985 Sep 26 21:45 shadow
drwxr-xr-x 2 root root 5120 Aug 5 17:14 sudo
-rw-r--r-- 1 root root 148 Aug 5 17:14 shells
drwxr-xr-x 2 root root 4096 Aug 5 16:55 ssh
drwxr-xr-x 6 root root 4096 Aug 5 17:14 sshd
drwxr-xr-x 4 root root 4096 Aug 5 17:14 sshd
drwxr-xr-x 1 root root 4096 Oct 21 21:18 sshd
-rw-r--r-- 1 root root 19 Sep 26 21:38 subid
-rw-r--r-- 1 root root 0 Aug 5 16:55 subid
-rw-r--r-- 1 root root 19 Sep 26 21:38 subuid
-rw-r--r-- 1 root root 0 Aug 5 16:55 subuid
-rw-r--r-- 1 root root 1434 Jun 25 12:42 sudo.conf
-rw-r--r-- 1 root root 1804 Jan 29 2024 sudoers
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sudo
drwxr-xr-x 2 root root 3273 Jun 25 12:42 sudo_logsrvd.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sudo
drwxr-xr-x 1 root root 2201 Mar 24 2024 sysctl.conf
drwxr-xr-x 2 root root 4096 Sep 26 21:51 sysctl.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sysctl
drwxr-xr-x 2 root root 4096 Aug 5 16:49 sysctl
drwxr-xr-x 2 root root 4096 Aug 5 17:00 sysctl
drwxr-xr-x 2 root root 4096 Sep 26 21:19 sysctl
drwxr-xr-x 1 root root 4096 Aug 5 17:02 timezone
drwxr-xr-x 2 root root 4096 Aug 5 17:14 timezone
drwxr-xr-x 2 root root 4096 Aug 5 17:14 timezone
-rw-r--r-- 1 root root 1264 Jan 27 2023 ucf.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 udev
drwxr-xr-x 2 root root 4096 Sep 26 21:19 udev
drwxr-xr-x 1 root root 4096 Aug 5 17:14 udev
drwxr-xr-x 1 root root 268 Aug 5 16:54 updated
drwxr-xr-x 3 root root 4096 Aug 5 17:02 update-when-upgrade
drwxr-xr-x 2 root root 4096 Sep 26 21:51 update-when-upgrade
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-when-upgrade
drwxr-xr-x 2 root root 4096 Sep 26 21:19 update-when-upgrade
-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
drwxr-xr-x 1 root root 10 Aug 5 17:14 vconsole.conf -> default/keyboard
drwxr-xr-x 1 root root 4096 Sep 26 21:24 vconsole
drwxr-xr-x 4 root root 4096 Oct 21 17:19 vconsole
drwxr-xr-x 1 root root 23 Feb 26 2024 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r-- 1 root root 4945 Aug 5 17:14 vtrgb
drwxr-xr-x 4 root root 4096 Aug 5 17:02 vtrgb
drwxr-xr-x 2 root root 4096 Aug 5 17:02 vtrgb
drwxr-xr-x 1 root root 601 Apr 8 2024 kattro.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 vtrgb
drwxr-xr-x 2 root root 4096 Aug 5 17:02 vtrgb
-rw-r--r-- 1 root root 460 Aug 5 17:14 zsh_command_not_found
hajra@ubuntu-lab:~$
```

t, click inside or press Ctrl+G.

ls -la /dev

```

crw-rw---- 1 root dialout 4, 91 Oct 22 20:00 ttys07
crw-rw---- 1 root dialout 4, 92 Oct 22 20:00 ttys28
crw-rw---- 1 root dialout 4, 93 Oct 22 20:00 ttys29
crw-rw---- 1 root dialout 4, 97 Oct 22 20:00 ttys3
crw-rw---- 1 root dialout 4, 98 Oct 22 20:00 ttys30
crw-rw---- 1 root dialout 4, 99 Oct 22 20:00 ttys31
crw-rw---- 1 root dialout 4, 100 Oct 22 20:00 ttys32
crw-rw---- 1 root dialout 4, 69 Oct 22 20:00 ttys5
crw-rw---- 1 root dialout 4, 70 Oct 22 20:00 ttys6
crw-rw---- 1 root dialout 4, 71 Oct 22 20:00 ttys7
crw-rw---- 1 root dialout 4, 72 Oct 22 20:00 ttys8
crw-rw---- 1 root dialout 4, 73 Oct 22 20:00 ttys9
drwxr-xr-x 2 root root 4096 Oct 22 20:00 vcs
crw-rw---- 1 root kvm 10, 12 Oct 22 20:00 udnabuf
crw-rw---- 1 root root 10, 239 Oct 22 20:00 uhfbuf
crw-rw---- 1 root root 10, 22 Oct 22 20:00 unctrl
crw-rw---- 1 root root 1, 9 Oct 22 20:00 urandom
crw-rw---- 1 root root 10, 126 Oct 22 20:00 userfaultfd
crw-rw---- 1 root root 10, 245 Oct 22 20:00 userio
crw-rw---- 1 root tty 7, 6 Oct 22 20:00 vcs
crw-rw---- 1 root tty 7, 1 Oct 22 20:00 vcs0
crw-rw---- 1 root tty 7, 2 Oct 22 20:00 vcs2
crw-rw---- 1 root tty 7, 3 Oct 22 20:00 vcs3
crw-rw---- 1 root tty 7, 4 Oct 22 20:00 vcs4
crw-rw---- 1 root tty 7, 5 Oct 22 20:00 vcs5
crw-rw---- 1 root tty 7, 6 Oct 22 20:00 vcs6
crw-rw---- 1 root tty 7, 128 Oct 22 20:00 vcsa
crw-rw---- 1 root tty 7, 129 Oct 22 20:00 vcsal
crw-rw---- 1 root tty 7, 130 Oct 22 20:00 vcsa2
crw-rw---- 1 root tty 7, 131 Oct 22 20:00 vcsa3
crw-rw---- 1 root tty 7, 132 Oct 22 20:00 vcsa4
crw-rw---- 1 root tty 7, 133 Oct 22 20:00 vcsa5
crw-rw---- 1 root tty 7, 134 Oct 22 20:00 vcsa6
crw-rw---- 1 root tty 7, 64 Oct 22 20:00 vcsu
crw-rw---- 1 root tty 7, 121 Oct 22 20:00 vcsu1
crw-rw---- 1 root tty 7, 65 Oct 22 20:00 vcsu2
crw-rw---- 1 root tty 7, 67 Oct 22 20:00 vcsu3
crw-rw---- 1 root tty 7, 68 Oct 22 20:00 vcsu4
crw-rw---- 1 root tty 7, 69 Oct 22 20:00 vcsu5
crw-rw---- 1 root tty 7, 70 Oct 22 20:00 vcsu6
drwxr-xr-x 2 root root 4096 Oct 22 20:00 vga_arbitrer
crw-rw---- 1 root root 10, 127 Oct 22 20:00 vga_arbitrer
crw-rw---- 1 root root 10, 137 Oct 22 20:00 vhci
crw-rw---- 1 root kvm 10, 238 Oct 22 20:00 vhci-net
crw-rw---- 1 root root 10, 111 Oct 22 20:00 vsock
crw-rw---- 1 root root 10, 122 Oct 22 20:00 vsock
crw-rw---- 1 root root 10, 121 Oct 22 20:00 vsock
crw-rw---- 1 root root 1, 5 Oct 22 20:00 zero
crw-rw---- 1 root root 10, 249 Oct 22 20:00 zfs
hajra@ubuntu-lab:~$
```

.click inside or press Ctrl+G.

ls -la /var

```

hajra@ubuntu-lab:~$ ls -la /var
total 56
drwxr-xr-x 13 root root 4096 Sep 26 21:38 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxr-xr-x 2 root root 4096 Oct 22 00:00 backups
drwxr-xr-x 16 root root 4096 Sep 27 08:39 cache
drwxr-xr-x 1 root root 4095 Aug 5 16:54 crash
drwxr-xr-x 46 root root 4096 Oct 27 08:39 cron
drwxr-xr-x 2 root staff 4096 Apr 22 2024 local
lrwxrwxrwx 1 root root 9 Aug 5 16:54 lock -> /run/lock
drwxrwxr-x 12 root syslog 4096 Oct 22 20:00 log
drwxrwxr-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 20 root root 4096 Sep 26 22:00 snap
drwxr-xr-x 4 root root 4096 Aug 5 17:14 tmp
drwxrwxr-x 7 root root 4096 Oct 22 20:01 tmp
drwxr-xr-x 1 root root 208 Aug 5 16:54 updated
hajra@ubuntu-lab:~$
```

ls -la /tmp

```

hajra@ubuntu-lab:~$ ls -la /tmp
total 52
drwxr-xr-x 18 root root 4096 Oct 22 20:11 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxrwxr-x 2 root root 4096 Oct 22 20:00 font-unix
drwxrwxr-x 2 root root 4096 Oct 22 20:00 ICE- unix
drwxr-xr-x 6 root root 4096 Oct 22 20:00 snap-private-tmp
drwxr-xr-x 3 root root 4096 Oct 22 20:00 systemd-private-40328d4bd764983682ef3100c1a0e5-ModemManager.service-fDymC2
drwxr-xr-x 3 root root 4096 Oct 22 20:00 systemd-private-40328d4bd764983682ef3100c1a0e5-polkit.service-kpspt
drwxr-xr-x 3 root root 4096 Oct 22 20:00 systemd-private-40328d4bd764983682ef3100c1a0e5-systemd-logind.service-yrsuUF
drwxr-xr-x 2 root root 4096 Oct 22 20:00 systemd-private-40328d4bd764983682ef3100c1a0e5-systemd-resolved.service-zHMK
drwxr-xr-x 2 root root 4096 Oct 22 20:00 systemd-private-043-402178452
drwxrwxr-x 2 root root 4096 Oct 22 20:00 X11- unix
drwxrwxr-x 2 root root 4096 Oct 22 20:00 XIM- unix
hajra@ubuntu-lab:~$
```

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

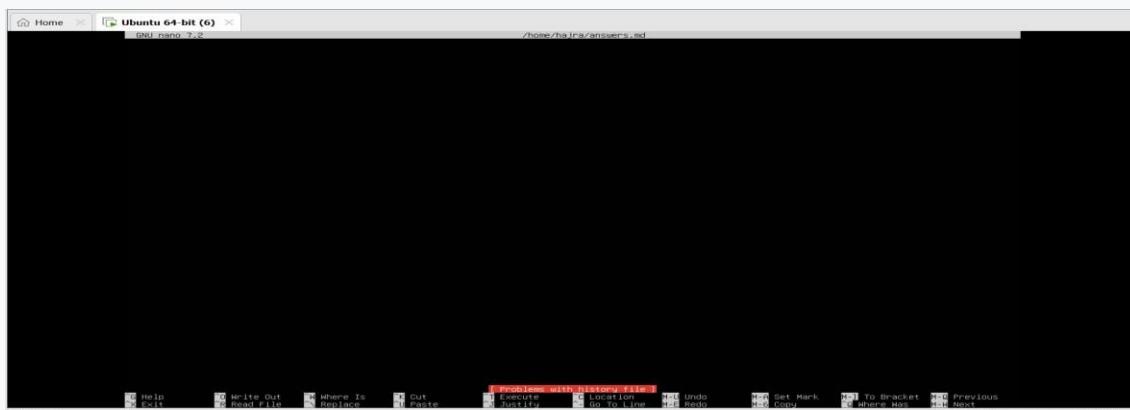
```
ls -la ~
```

```
hajra@ubuntu-lab:~$ ls -la $HOME
total 48
drwxr-x--- 5 hajra hajra 4096 Oct 23 04:41 .
drwxr-xr-x 3 root root 4096 Sep 26 21:38 ..
-rw-r--r-- 1 hajra hajra 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 hajra hajra 3771 Mar 31 2024 .bashrc
drwx----- 2 hajra hajra 4096 Sep 26 21:40 .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41 .fedorarpm
-rw----- 1 hajra hajra 20 Sep 26 22:08 .lessshst
-rw-r--r-- 1 hajra hajra 807 Mar 31 2024 .profile
drwx----- 2 hajra hajra 4096 Sep 26 22:08 .ssh
-rw-r--r-- 1 hajra hajra 0 Sep 26 21:48 .sudo_as_admin_successful
-rw-r--r-- 1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$
```

4. Write a short paragraph (3–5 sentences) that explains the difference between /bin, /usr/bin and /usr/local/bin.

Open your editor:

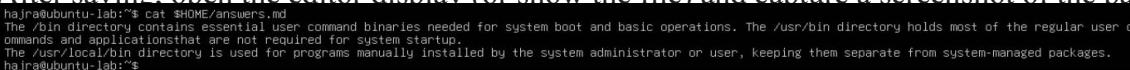
```
nano ~/answers.md
```



- 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.



## Task 4: Essential CLI Tasks — Navigation and File Operations

### Steps Performed

- Create a Workspace and Navigate

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



Created a new workspace directory for the Python project.

```
cd ~/lab4/workspace/python_project
```



Navigated into the newly created directory.

Pwd

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ pwd
/home/hajra/lab4/workspace/python_project
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

Verified the current working directory path.

---

## 2. Create Files Using an Editor nano

README.md

```
GNU nano 7.2
lab 4 README_
```

Added the text “Lab 4 README” and saved the file.

nano main.py

```
GNU nano 7.2
print ('hello lab4')
```

Added the Python code: print("hello lab4") and saved the file.

nano .env

```
GNU nano 7.2
ENV = lab4_
```

Added the line ENV=lab4 and saved the file.

---

## 3. List Files

ls -la

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ ls -la
total 20
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:14 .
drwxrwxr-x 3 hajra hajra 4096 Oct 23 13:11 ..
-rw-rw-r-- 1 hajra hajra 11 Oct 23 14:14 .env
-rw-rw-r-- 1 hajra hajra 21 Oct 23 14:11 main.py
-rw-rw-r-- 1 hajra hajra 13 Oct 23 14:07 README.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Displayed all files, including hidden ones, in the current directory.

---

## 4. Copy, Move, and Remove Files cp README.md

README.copy.md

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ cp README.md README.md.copy.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Created a copy of the README file.

mv README.copy.md README.dev.md

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ mv README.md.copy.md README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Renamed (moved) the copied file.

rm README.dev.md

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ rm README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Deleted the renamed file.

---

## 5. Work with Directories

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ mkdir -p $HOME/lab4/workspace/java_app
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Created another directory for a Java app.

cp -r ~/lab4/workspace/python\_project ~/lab4/workspace/java\_app\_copy

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/java_app_copy
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Copied the entire Python project directory recursively.

```
ls -la ~/lab4/workspace
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ ls -la $HOME/lab4/workspace
total 16
drwxrwxr-x 4 hajra hajra 4096 Oct 23 14:34 .
drwxrwxr-x 3 hajra hajra 4096 Oct 23 13:11 ..
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:34 java_app_copy
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:27 python_project
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Verified the copied directories.

---

## 6. Use Command History and Tab Completion

History

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ history
 1 ls -la $HOME
 2 nano $HOME/answers.md
 3 cat $HOME/answers.md
 4 mkdir -p $HOME/lab4/workspace/python_project
 5 cd $HOME/lab4/workspace/python_project
 6 pud
 7 nano README.md
 8 nano main.py
 9 nano .env
10 ls -la
11 cp README.md README.md.copy.md
12 mv README.copy.md README.dev.md
13 mv README.md.copy.md README.dev.md
14 rm README.dev.md
15 mkdir -p $HOME/lab4/workspace/java_app
16 cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/java_app_copy
17 ls -la $HOME/lab4/workspace
18 history
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

Displayed a list of previously executed commands.

- Demonstrated tab completion by typing part of a file or directory name and pressing **Tab** to autocomplete it.

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ cat main.py
print ('hello lab4')
```

---

## Task 5: System info, resources & processes

Collect system information and observe processes. Use screenshots only.

Steps (inside VM terminal)

- Kernel and OS:

```
uname -a
```

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ uname -a
Linux ubuntu-lab 6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

- CPU (ensure model name visible):

```
cat /proc/cpuinfo
```

```
Home > Ubuntu 64-bit (6) >
core_id : 0
cpu_cores : 1
cpu_id : 0
initial_apicid : 0
fpu : yes
fpu_exception : yes
cpuid_level : 22
wp : yes
flags : fpu vme vme_of_pae tsc msr pae pse mce cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtsvc lm constant_tsc arch_perfmon nopl xtogiology tsc_reliable nonstop_tsc cpuid tsc_known_freq pnpi pclmu1dqg sse3 fma cx16 pcld sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_time r aes xsave avx f16c rdrand hypervisor lshfi lmb abm 3dnowprefetch pt1 ssbd lbrs lbbp stibg tsgsbase tsc_adjust bmi1 avx2 smp bmi2 invpcid rdseed adx snap clifus bugs : cpuid_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbsb 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 : 142
model_name : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
stepping : 1
microcode : 0xffffffff
cpu_MHz : 1095.997
cache_size : 6144 KB
physical_id : 0
siblings : 1
core_id : 0
core_type : 1
apicid : 2
initial_apicid : 2
fpu : yes
fpu_exception : yes
cpuid_level : 22
wp : yes
flags : fpu vme vme_of_pae tsc msr pae mce cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtsvc lm constant_tsc arch_perfmon nopl xtogiology tsc_reliable nonstop_tsc cpuid tsc_known_freq pnpi pclmu1dqg sse3 fma cx16 pcld sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_time r aes xsave avx f16c rdrand hypervisor lshfi lmb abm 3dnowprefetch pt1 ssbd lbrs lbbp stibg tsgsbase tsc_adjust bmi1 avx2 smp bmi2 invpcid rdseed adx snap clifus bugs : cpuid_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbsb 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:
```

### 3. Memory: free -h

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ free -h
 total used free shared buff/cache available
Mem: 1.9Gi 1.2Gi 132Mi 12Mi 734Mi 667Mi
Swap: 2.0Gi 223Mi 1.8Gi
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

## 4. Disk:

df-h

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ free -h
 total used free shared buff/cache available
Mem: 1.9Gi 1.2Gi 132Mi 12Mi 734Mi 667Mi
Swap: 223Mi 1.8Gi
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ df -h
Filesystem Size Used Avail Capacity Mounted on
udev 192M 16M 181M 1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 196G 343M 192G 2% /
tmpfs 960M 10G 950M 1% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
/dev/sda2 2.0G 192M 1.6G 11% /boot
tmpfs 192M 20K 192M 1% /run/user/1000
shm 64M 0 64M 0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/ce047894ba4dc681480504b884d
de081befef7c1524cd31f3f71c08665625f57/shm
shm 64M 0 64M 0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/907005c3fa2edab7e07c5bb55
7e4ead3372884c9de10e7c3258af5f411965/shm
shm 64M 0 64M 0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/1fa57bb780d67f59e774952f1e
185862585771458a25591d1300e427b4ae2367/shm
hajra@ubuntu-lab:~/lab4/workspace/python_projects$
```

## 5. View OS release information:

```
cat /etc/os-release
```

```
ha@raja-OptiPlex-5090:~$ 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
be[in@raja-OptiPlex-5090:~]$
```

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

ps aux

```

root 4960 0.0 0.1 1256496 2220 ? S 12:24 0:00 httpd -d /snap/nextcloud/50464 -k start -DFOREGROUND
root 4987 0.0 0.1 1256496 2356 ? S 12:24 0:00 httpd -d /snap/nextcloud/50464 -k start -DFOREGROUND
root 5297 0.0 0.0 1256496 2356 ? S 12:24 0:00 httpd -d /snap/nextcloud/50464 -k start -DFOREGROUND
hajra 5630 0.0 0.4 296000 8192 ? Ss 12:24 0:01 /usr/lib/systemd/systemd --user
hajra 5632 0.0 0.0 21148 1852 ? S 12:24 0:00 (sd-pam)
hajra 5634 0.0 0.0 4096 4096 ? S 12:24 0:00 basekit
root 5723 0.0 0.3 1256896 12520 ? S 12:24 0:04 /snap/microk8s/8511/bin/containerd-shim-agent cluster-agent --bind 0.0.0.0:25000 --keyfile /var/snap/microk8s/8511/bin/containerd -c /var/snap/microk8s/8511/config/containerd.toml --root /var/snap/microk8s/8511/kubelite --scheduler args --files /var/snap/microk8s/8511/args/kube-schedule
root 6290 0.0 0.0 1380000 31192 ? S 12:24 0:33 snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id ced47e93be4dc081d594989
root 7149 0.3 0.4 1234156 6396 ? S 12:24 0:33 snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id ffa57bb70dd7f58e774952
root 7229 0.0 0.0 1020 128 ? S 12:24 0:00 pause
root 7563 0.0 0.0 1256496 6096 ? S 12:24 0:09 /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id ced47e93be4dc081d594989
root 7565 0.0 0.0 4096 4096 ? S 12:24 0:09 /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id ffa57bb70dd7f58e774952
root 7639 0.3 0.4 1234112 8552 ? S 12:24 0:33 /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id 9e700c3fa2edabd7ee7c5b
root 7670 0.0 0.0 1020 128 ? S 12:24 0:00 pause
root 7700 0.0 0.0 1276788 2032 ? S 12:24 0:00 /etc/init.d/monit reload -c /etc/monitrc -conf /etc/monitrc.corefile
root 7790 0.0 1.5 1276788 31396 ? S 12:25 0:05 /usr/bin/runsvd -P /etc/service/enabled
root 8389 0.0 0.0 4476 1152 ? S 12:25 0:00 /usr/local/bin/runsvsd -P
root 8450 0.0 0.0 4324 1152 ? S 12:25 0:00 runsv node-state-reporter
root 8630 0.0 0.0 4324 1152 ? S 12:25 0:00 runsv node-tunnel-addrs
root 8639 0.0 0.0 4324 1152 ? S 12:25 0:00 runsv node-tunnel-addrs-reporter
root 8640 0.0 0.0 4324 1152 ? S 12:25 0:00 runsv monitor-addresses
root 8641 0.0 0.0 4324 1280 ? S 12:25 0:00 runsv monitor-addrs
root 8642 0.0 2.9 1794476 58192 ? S 12:25 0:01 calico-node -allocate-tunnel-addrs
root 8643 0.0 2.9 1794476 58192 ? S 12:25 0:01 calico-node -status-reporter
root 8644 0.0 2.9 1794476 55999 ? S 12:25 0:01 calico-node -sync-token
root 8645 2.7 3.5 2237380 68964 ? S 12:25 0:14 calico-node -felix
root 8646 0.0 2.0 1794476 55762 ? S 12:25 0:01 calico-node -monitor-addresses
root 8647 0.0 0.0 0 0 ? I< 12:27 0:04 [kworker/0:0@memlock]
root 112063 0.0 0.0 0 0 ? I< 12:25 0:00 [kworker/0:0@tis-s]
root 113264 0.0 1.9 478476 38364 ? S 12:57 0:01 /usr/libexec/fuupd/fwupd
root 132469 0.0 0.0 314860 69652 ? S 12:25 0:00 /usr/libexec/fwupd/fwupdd
root 146693 0.0 0.0 0 0 ? I< 13:05 0:00 [kworker/11:0]
root 347365 0.0 0.0 0 0 ? I< 13:48 0:00 [kworker/u257:0-flush-252:0]
root 532471 0.0 0.0 0 0 ? I< 13:58 0:00 [kworker/u257:0-flush-252:0]
root 598258 0.0 0.0 0 0 ? I< 14:39 0:00 [kworker/u257:2-flush-252:0]
root 666337 0.2 0.0 0 0 ? I< 14:57 0:02 [kworker/11:events]
root 689358 0.0 0.0 0 0 ? I< 15:01 0:00 [kworker/11:events_power_efficient]
root 684235 0.3 0.0 0 0 ? I< 15:01 0:02 [kworker/11:events]
root 693358 0.0 0.0 0 0 ? I< 15:03 0:00 [kworker/11:events]
root 696180 0.0 0.0 0 0 ? I< 15:06 0:00 [kworker/11:events_bound]
root 707793 0.1 0.0 0 0 ? I< 15:06 0:00 [kworker/10:0@pmcs]
root 711863 0.0 0.0 0 0 ? I< 15:06 0:00 [kworker/u258:1-writeback]
root 713791 0.0 0.0 0 0 ? I< 15:08 0:00 [kworker/10:events]
root 732456 0.0 0.0 4556 1532 ? S 15:08 0:00 [kworker/u257:0-flush-252:0]
root 733879 0.0 0.0 0 0 ? I< 15:11 0:00 [kworker/0:2-events]
root 737692 0.0 0.0 0 0 ? I< 15:12 0:00 [kworker/u257:1-flush-252:0]
root 740909 0.0 0.0 5936 1667 ? S 15:12 0:00 sleep 5
hajra 746909 1050 0.2 12312 5120 ? S 15:13 0:00 ps aux

```

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

### Steps (inside VM terminal)

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

sudo adduser lab4user

```

hajra@ubuntu-lab:~/lab4/workspace/python_project$ sudo adduser lab4user
[sudo] password for hajra:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1002) ...
info: Adding new user `lab4user' (1002) with group `lab4user' (1002) ...
info: Creating home directory `/home/lab4user' ...
info: 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 []: hajra
 Room Number []: twenty two
 Work Phone []: 03two7-5007883
 Home Phone []: 03two7-5007883
 Other []: nil
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
hajra@ubuntu-lab:~/lab4/workspace/python_project$

```

#### 2. Verify the user entry:

getent passwd lab4user

```

hajra@ubuntu-lab:~/lab4/workspace/python_project$ getent passwd lab4user
lab4user:x:1002:1002:hajra,twenty two,03two7-5007883,03two7-5007883,nill:/home/lab4user:/bin/bash
hajra@ubuntu-lab:~/lab4/workspace/python_project$

```

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

su - lab4user

```

hajra@ubuntu-lab:~/lab4/workspace/python_project$ su - lab4user
Password:
lab4user@ubuntu-lab:~$ _

```

#### 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

```
password:
lab4user@ubuntu-lab:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu-lab:~$ _
```

5. Return to the original user:

[Exit](#)

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _
```

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

`sudo deluser --remove-home lab4user`

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
[sudo] password for hajra:
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _
```

## Bonus Task 7: Create a small demo script using an editor and run it Steps (inside VM)

1. Open an editor to create the script:

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ nano $HOME/lab4/workspace/python_project/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)"

free -h
```

```
GNU nano 7.2
#!/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`

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ chmod +x ~/lab4/workspace/python_project/run-demo.sh
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _
```

3. Run the script as your regular user:

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ ~/lab4/workspace/python_project/run-demo.sh
Lab 4 demo: current user is $(whoami)
Current time: $(date)
19:02:29 up 6:39, 1 user, load average: 0.78, 0.74, 0.76
 total used free shared buff/cache available
Mem: 1.9Gi 1.2Gi 111Mi 740Ki 730Mi 652Mi
Swap: 2.0Gi 225Mi 1.8Gi
```

4. Optionally run it with sudo:

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ sudo ~/lab4/workspace/python_project/run-demo.sh
[sudo] password for hajra:
Lab 4 demo: current user is $(whoami)
Current time: $(date)
19:03:47 up 6:41, 1 user, load average: 0.57, 0.66, 0.73
 total used free shared buff/cache available
Mem: 1.9Gi 1.2Gi 128Mi 824Ki 731Mi 671Mi
Swap: 2.0Gi 225Mi 1.8Gi
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

## 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:

1. Connect to the Ubuntu VM remotely from your host terminal.

```
Warning: Permanently added '192.168.161.129' (ED25519) to the list of known hosts.
hajra@192.168.161.129's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-84-generic x86_64)

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

System information as of Sat 27 Sep 10:28:45 UTC 2025

 System load: 1.46 Processes: 276
 Usage of /: 70.2% of 11.21GB Users logged in: 1
 Memory usage: 57% IPv4 address for ens33: 192.168.161.129
 Swap usage: 9%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

hajra@ubuntu-lab: $ -
```

2. Verify your current user and home directory path.

```
hajra@ubuntu-lab: $ whoami
hajra
hajra@ubuntu-lab: $ pwd
/home/hajra
hajra@ubuntu-lab: $
```

3. Confirm you are connected to the correct host machine.

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ hostname
ubuntu-lab
```

### 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:

1. Display the contents of the root directory.

```

hajra@ubuntu-lab:~$ ls -la
total 44
drwxr-x--- 4 hajra hajra 4096 Sep 26 22:08 .
drwxr-xr-x 3 root root 4096 Sep 26 21:38 ..
-rw-r--r-- 1 hajra hajra 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 hajra hajra 3771 Mar 31 2024 .bashrc
drwxr---- 2 hajra hajra 4096 Sep 26 21:40 .cache
-rw-r--r-- 1 hajra hajra 20 Sep 26 22:08 .lessht
-rw-r--r-- 1 hajra hajra 807 Mar 31 2024 .profile
drwxr---- 2 hajra hajra 4096 Sep 26 22:00 .ssh
-rw-r--r-- 1 hajra hajra 0 Sep 26 21:48 .sudo_as_admin_successful
-rw-r--r-- 1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$

```

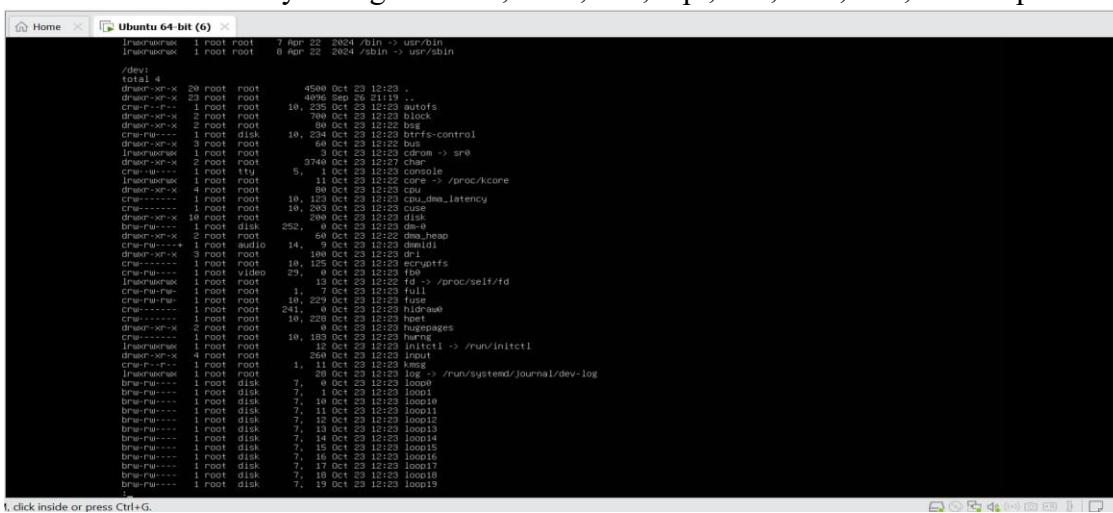
2. Display the OS version and release information.

```

hajra@ubuntu-lab:~/lab4/workspace/python_project$ uname -a
Linux ubuntu-lab 6.8.0-85-generic #85-Ubuntu PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
hajra@ubuntu-lab:~/lab4/workspace/python_project$

```

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



4. Display all hidden files in your home directory.

```

hajra@ubuntu-lab:~$ ls -la $HOME
total 48
drwxr-x--- 5 hajra hajra 4096 Oct 23 04:41 .
drwxr-xr-x 3 root root 4096 Sep 26 21:38 ..
-rw-r--r-- 1 hajra hajra 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 hajra hajra 3771 Mar 31 2024 .bashrc
drwxr---- 2 hajra hajra 4096 Sep 26 21:40 .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41 .lessht
-rw-r--r-- 1 hajra hajra 20 Sep 26 22:08 .profile
drwxr---- 2 hajra hajra 4096 Sep 26 22:00 .ssh
-rw-r--r-- 1 hajra hajra 0 Sep 26 21:48 .sudo_as_admin_successful
-rw-r--r-- 1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$

```

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

1. Go to your **home directory** (or your lab workspace folder):

cd ~ or cd ~/lab4/workspace

```

hajra@ubuntu-lab:~$ cd ~/lab4/workspace

```

2. Create and open a new Markdown file using **nano editor**:

nano report.md

```

hajra@ubuntu-lab:~/lab4/workspace$ nano report.md_

```

3. Inside nano, type your short summary.

```

GNU nano 7.2
<!--System Directory Summary-->
- **/bin** - contains essential user command binaries (like ls, cp, mv)
- **/sbin** - Contain system binaries used mainly by the root user for system admin
- **/usr** - Contains user-installed programs, libraries, and documentation.
- **/opt** - Used for optional or third-party software.
- **/etc** - Contains configuration files for the system and installed services.
- **/dev** - Contains device files representing hardware devices.
- **/var** - Contains variable data such as logs, caches, and spool files.
- **/tmp** - Temporary files created by running processes.

```

4. When done, **save and exit nano**.

5. Verify your file exists and display its contents:

cat report.md

```
hajra@ubuntu-lab:~/lab4/workspace$ cat report.md
<!--System Directory Summery-->
- ***/bin** - contains essential user command binaries (like ls, cp, mv)
- ***/sbin** - Contain system binaries used mainly by the root user for system admi
- ***/usr** - Contains user-installed programs, libraries, and documentation.
- ***/opt** - Used for optional or third-party software.
- ***/etc** - Contains configuration files for the system and installed services.
- ***/dev** - Contains device files representing hardware devices.
- ***/var** - Contains variable data such as logs, caches, and spool files.
- ***/tmp** - Temporary files created by running processes.

hajra@ubuntu-lab:~/lab4/workspace$
```

### 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:

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ pwd
/home/hajra/lab4/workspace/python_project
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ ls -la
total 20
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:14 .
drwxrwxr-x 3 hajra hajra 4096 Oct 23 13:11 ..
-rw-rw-r-- 1 hajra hajra 11 Oct 23 14:14 .env
-rw-rw-r-- 1 hajra hajra 21 Oct 23 14:11 main.py
-rw-rw-r-- 1 hajra hajra 13 Oct 23 14:07 README.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

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

```
cp README.md README.copy.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ cp README.md README.md.copy.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

Created a copy of the README file.

```
mv README.copy.md README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ mv README.md.copy.md README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

Renamed (moved) the copied file.

```
rm README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ rm README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

Deleted the renamed file.

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

```
mkdir -p ~/lab4/workspace/java_app
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ mkdir -p $HOME/lab4/workspace/Java_app
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

Created another directory for a Java app.

```
cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/Java_app_copy
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

Copied the entire Python project directory recursively.

```
ls -la ~/lab4/workspace
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ ls -la $HOME/lab4/workspace
total 16
drwxrwxr-x 4 hajra hajra 4096 Oct 23 14:34 .
drwxrwxr-x 3 hajra hajra 4096 Oct 23 13:11 ..
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:34 Java_app_copy
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:27 python_project
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

Verified the copied directories.

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ history
1 ls -la $HOME
2 nano $HOME/answers.md
3 cat $HOME/answers.md
4 mkdir -p $HOME/lab4/workspace/python_project
5 cd $HOME/lab4/workspace/python_project
6 pwd
7 nano README.md
8 nano main.py
9 nano .env
10 ls -la
11 cp README.md README.md.copy.md
12 mv README.copy.md README.dev.md
13 mv README.md.copy.md README.dev.md
14 rm README.dev.md
15 mkdir -p $HOME/lab4/workspace/Java_app
16 cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/Java_app_copy
17 ls -la $HOME/lab4/workspace
18 history
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ cat main.py
print ('hello lab4')
```

## 4. System Profiling and Process Monitoring

### Scenario:

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

### Steps:

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ uname -a
Linux ubuntu-lab 6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ _
```

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

```

hajra@ubuntu-lab:~$ free -h
 total used free shared buff/cache available
Mem: 1.9Gi 938Mi 322Mi 9.9Mi 830Mi 981Mi
Swap: 2.0Gi 30Mi 2.0Gi

hajra@ubuntu-lab:~$ df -h
Filesystem Size Used Avail Use% Mounted on
tmpfs 192M 1.5M 191M 1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 12G 11G 335M 97% /
tmpfs 960M 0 960M 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
/dev/sda2 2.0G 192M 1.6G 11% /boot
tmpfs 192M 20K 192M 1% /run/user/1000
hajra@ubuntu-lab:~$ _

```

- Display all active running processes to identify suspicious activity.

```

hajra@ubuntu-lab:~$ ps aux
root 4986 0.0 0.1 1258496 2220 ? S 12:24 0:00 httpd -d /snap/nextcloud/59464 -k start -DFOREGROUND
root 4987 0.0 0.1 1258496 2356 ? S 12:24 0:00 httpd -d /snap/nextcloud/59464 -k start -DFOREGROUND
root 5000 0.0 0.1 8400 3079 ? S 12:24 0:00 bash /snap/microk8s/8511/run-cluster-agent-with-args
hajra 5630 0.0 0.4 26040 1192 ? S 12:24 0:01 bash /lib/systemd/systemd-user
hajra 5632 0.0 0.0 21148 1852 ? S 12:24 0:00 (sd-pam)
hajra 5634 0.0 0.2 6565 4096 ? ttyp1 12:24 0:00 -bash
root 5703 0.0 0.0 1258496 2064 ? S 12:24 0:00 snap/microk8s/8511/bin/containerd-agent --bind 0.0.0.0:25000 --keyfile /var/snap/microk8s/8511/args/containerd.toml --ro
root 5985 1.0 1.5 2300568 31192 ? S 12:24 1:58 /snap/microk8s/8511/bin/containerd -c /var/snap/microk8s/8511/args/containerd.toml --ro
root 6269 7.2 16.1 1546420 318229 ? S 12:24 12:12 /snap/microk8s/8511/args/-scheduler-args-file=/var/snap/microk8s/8511/args/kube-schedule
root 6440 0.0 0.0 1258496 2064 ? S 12:24 0:00 /bin/bash /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id ceo47894be4cc6814856b8
65535 7229 0.0 0.0 1020 128 ? S 12:24 0:00 /usr/bin/pause
root 7568 0.0 0.3 1234412 6598 ? S 12:25 0:03 /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id ife57bb780d67f58e774952
65535 7569 0.0 0.3 1234412 6592 ? S 12:25 0:03 /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id 9e7005c53fa2edabd7e07c5b
65535 7676 0.0 0.0 1828 128 ? S 12:25 0:00 /usr/bin/pause
root 7700 0.0 1.0 1767688 26016 ? S 12:25 0:00 /etc/consul/conf /etc/consul/corefile
root 7790 0.0 0.5 1276788 31398 ? S 12:25 0:05 /usr/bin/kube-controllers
root 8383 0.0 0.0 4476 1152 ? S 12:25 0:00 /usr/local/bin/runsvdir -P /etc/service/enabled
root 8637 0.0 0.0 4324 1152 ? S 12:25 0:00 /usr/runs/allocate-tunnel-addr
root 8638 0.0 0.0 4324 1152 ? S 12:25 0:00 /usr/runs/alloc11
root 8639 0.0 0.0 4324 1152 ? S 12:25 0:00 runsy node-status-reporter
root 8640 0.0 0.0 4324 1152 ? S 12:25 0:00 runsy cni
root 8641 0.0 0.0 4324 1152 ? S 12:25 0:00 runsy monitor-addresses
root 8642 0.0 2.9 1794476 58192 ? S 12:25 0:01 calico-node -allocate-tunnel-addr
root 8643 0.0 2.8 1794228 56168 ? S 12:25 0:01 calico-node -status-reporter
root 8644 0.0 2.8 1794228 56168 ? S 12:25 0:01 calico-node -monitor-addr
root 8646 2.7 3.5 2237380 68964 ? S 12:25 4:34 calico-node -felix
root 8647 0.0 2.8 1794476 55752 ? S 12:25 0:01 calico-node -monitor-addresses
root 8649 0.0 0.0 4476 1152 ? S 12:25 0:00 /usr/bin/runsvdir -P /etc/service/locked
root 112869 0.0 0.0 0 0 ? I< 12:55 0:00 [kworker/R-tls-s]
root 119289 0.0 1.9 478476 38364 ? S 12:57 0:01 /usr/libexec/fuupd/fuupd
root 132490 0.0 0.0 3140898 8964 ? S 13:05 0:00 /usr/libexec/fuupd/fuupd
root 148669 0.0 0.0 0 0 ? I< 13:05 0:00 [kworker/1:1]
root 347306 0.0 0.0 0 0 ? I 13:48 0:00 [kworker/UZ57:0-flush-252:0]
root 837656 0.0 0.0 0 0 ? I 14:28 0:00 [kworker/U58:0-whiteback]
root 656337 0.0 0.0 0 0 ? I 14:57 0:02 [kworker/11:events]
root 681389 0.0 0.0 0 0 ? I 14:58 0:00 [kworker/UZ58:0-events_power_efficient]
root 693358 0.0 0.0 0 0 ? I 15:03 0:00 [kworker/11:events]
root 696137 0.0 0.0 0 0 ? I 15:04 0:00 [kworker/UZ57:0-events_unbound]
root 729063 0.0 0.0 0 0 ? I 15:05 0:00 [kworker/UZ57:0-events_bound]
root 711063 0.0 0.0 0 0 ? I 15:06 0:00 [kworker/U58:0-witeback]
root 717971 0.4 0.0 0 0 ? I 15:08 0:01 [kworker/11:events]
root 730387 0.0 0.0 0 0 ? I 15:11 0:00 [kworker/0:2-events]
root 737652 0.0 0.0 0 0 ? I 15:12 0:00 [kworker/UZ57:1-flush-252:0]
root 746676 0.0 0.0 5984 1662 ? S 15:13 0:00 sleep 5
hajra 746679 1958 0.2 12312 5120 ?ttyp1 R+ 15:13 0:00 ps aux
hajra@ubuntu-lab:~$ lab4/workspace/python_projects_

```

## 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.

```

hajra@ubuntu-lab:~/lab4/workspace/python_projects$ sudo adduser lab4user
[sudo] password for hajra:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1002)
info: Adding new user `lab4user' (1002) with group `lab4user (1002)'
info: Creating home directory `/home/lab4user'
info: 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 []: hajra
 Room Number []: twenty two
 Work Phone []: 03tw07-5007883
 Home Phone []: 03tw07-5007883
 Other []: nil
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
hajra@ubuntu-lab:~/lab4/workspace/python_projects$

```

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

```

hajra@ubuntu-lab:~/lab4/workspace/python_projects$ getent passwd lab4user
lab4user:x:1002:1002:hajra,twenty two,03tw07-5007883,03tw07-5007883,nil:/home/lab4user:/bin/bash
hajra@ubuntu-lab:~/lab4/workspace/python_projects$

```

3. Log in as lab4user and confirm successful login.

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ su - lab4user
Password:
lab4user@ubuntu-lab:~$ _
```

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

```
lab4user@ubuntu-lab:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu-lab:~$ _
```

5. Switch back to your main analyst account.

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _
```

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
[sudo] password for hajra:
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _
```

---