

Fatima Jinnah Women University



Cloud
Computing
Lab 4

Submitted By :

Inshal Nasir

Section :

A

Roll No:

38

Submitted To:

Sir Shoaib

LAB TITLE: Virtualization & Linux Fundamentals

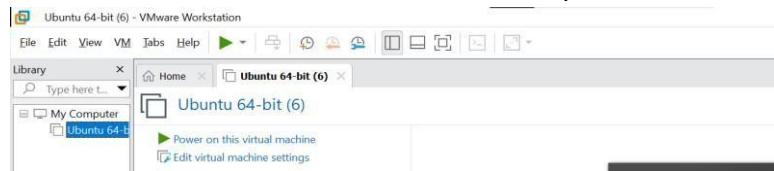
TASK:

Task 1: Verify VM resources in VMware

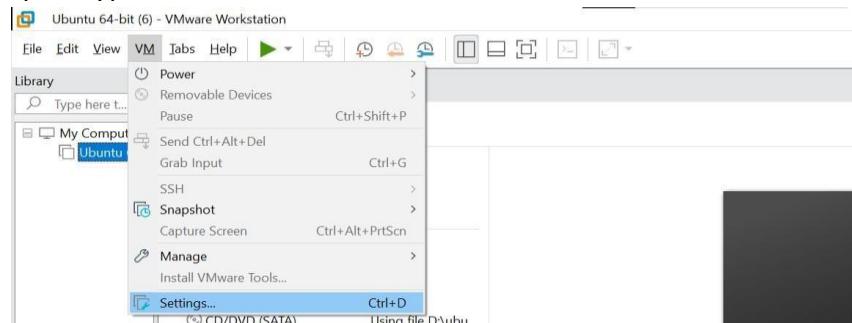
Confirm the VM resources that were allocated in Lab 1.

Steps

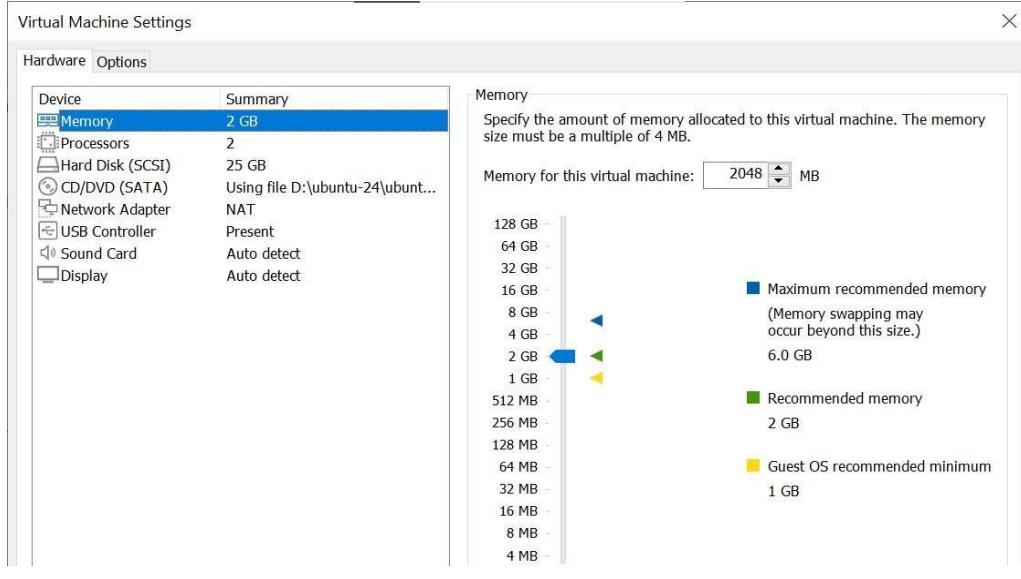
1. Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.



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-ipaddress>

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

```
ens3: <>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 enp2s0
  inet 192.168.161.129/24 metric 100 brd 192.168.161.255 scope global dynamic ens3
    valid_lft 1082sec preferred_lft 1082sec
  inet6 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
```

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% 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: ~

```

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

```

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ whoami
Alli

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ /home/Alli
bash: /home/Alli: No such file or directory

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ pwd
/c/Users/Alli
Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ 

```

Task 3: Filesystem exploration — root tree and dotfiles

Steps (run inside VM terminal)

- List root directory contents:

```
ls -la /
```

```

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ ls -la
total 39593
drwxr-xr-x 1 Alli 197609 0 Nov 15 09:10 -/
drwxr-xr-x 1 Alli 197609 0 Oct 16 00:59 ./
-rw-r--r-- 1 Alli 197609 11439 Nov 20 01:26 .bash_history
drwxr-xr-x 1 Alli 197609 0 Dec 10 2024 .dotnet/
drwxr-xr-x 1 Alli 197609 0 Oct 18 03:51 .git/
-rw-r--r-- 1 Alli 197609 301 Oct 18 02:07 .gitconfig
drwxr-xr-x 1 Alli 197609 0 Dec 5 2024 .ok/
drwxr-xr-x 1 Alli 197609 0 Dec 5 2024 .gnupg/
-rw-r--r-- 1 Alli 197609 20 Oct 18 03:48 .lesshist

```

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

```
ls -la /bin
```

```

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ ls -la /bin
total 90304
drwxr-xr-x 1 Alli 197609 0 Oct 8 20:18 -/
drwxr-xr-x 1 Alli 197609 0 Oct 8 20:19 ./
drwxr-xr-x 1 Alli 197609 72418 Sep 29 21:49 .Font*

```

```
ls -la /sbin
```

```

lrwxrwxrwx 1 root root 8 Apr 22 2024 /sbin -> /usr/sbin
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 bin
drwxr-xr-x 2 root root 36864 Oct 21 17:19 lib
drwxr-xr-x 2 root root 4096 Apr 22 2024 games
drwxr-xr-x 35 root root 4096 Aug  5 16:54 include
drwxr-xr-x 8 root root 4096 Oct 21 17:20 lib64
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 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x 2 root root 20480 Oct 21 17:10 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

```
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 cni
drwxr-xr-x 4 root root 4096 Sep 26 21:51 containerd
haJra@ubuntu-lab:~$
```

ls -la /etc

```
total 16
drwxr-xr-x 2 root root 4096 Aug  5 17:14 .
-rw-r--r-- 1 root root 12813 Mar 27 2021 services
drwxr-xr-x 1 root root 4096 Aug  5 17:14 subuid
drwxr-xr-x 1 root shadow 395 Sep 26 21:49 shadow
-rw-r----- 1 root shadow 967 Sep 26 21:38 shadow-
-rw-r--r-- 1 root root 148 Aug  5 17:14 shells
drwxr-xr-x 2 root root 4096 Aug  5 17:14 sudo
drwxr-xr-x 6 root root 4096 Aug  5 17:14 sudo
drwxr-xr-x 4 root root 4096 Aug  5 17:14 sudo
drwxr-xr-x 4 root root 4096 Sep 26 21:38 sudo
drwxr-xr-x 4 root root 4096 Oct 21 17:18 sudo
-rw-r--r-- 1 root root 19 Sep 26 21:19 subuid
drwxr-xr-x 1 root root 4096 Aug  5 17:14 subuid-
drwxr-xr-x 1 root root 19 Sep 26 21:38 subuid
-rw-r--r-- 1 root root 6 Aug  5 16:54 subuid-
-rw-r--r-- 1 root root 4343 Jun 25 12:42 sudo.conf
-rw-r--r-- 1 root root 108 Aug  5 17:14 sudoers
drwxr-xr-x 2 root root 4096 Aug  5 17:14 sudo_logsrvd.conf
drwxr-xr-x 2 root root 4096 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 2289 Mar 24 2024 sysctl.conf
drwxr-xr-x 1 root root 4096 Aug  5 17:14 sysctl
drwxr-xr-x 2 root root 4096 Aug  5 17:14 sysctl
drwxr-xr-x 6 root root 4096 Aug  5 16:49 sysctl
drwxr-xr-x 2 root root 4096 Aug  5 17:00 sysctl
drwxr-xr-x 1 root root 4096 Aug  5 17:14 sysctl
drwxr-xr-x 1 root root 8 Aug  5 17:02 timezone
drwxr-xr-x 2 root root 4096 Aug  5 17:14 .
drwxr-xr-x 2 root root 4096 Aug  5 17:14 .
-rw-r--r-- 1 root root 1269 Jan 27 2023 ucf.conf
drwxr-xr-x 1 root root 4096 Aug  5 17:14 ucf
drwxr-xr-x 2 root root 4096 Sep 26 21:23 ucf
drwxr-xr-x 2 root root 4096 Sep 26 21:23 ucf
drwxr-xr-x 3 root root 4096 Aug  5 17:14 ucf
drwxr-xr-x 1 root root 208 Aug  5 16:54 .updated
drwxr-xr-x 1 root root 4096 Aug  5 17:14 .
drwxr-xr-x 2 root root 4096 Sep 26 21:51 .
drwxr-xr-x 2 root root 4096 Aug  5 17:14 .
drwxr-xr-x 2 root root 4096 Sep 26 21:19 .
drwxr-xr-x 1 root root 1533 Aug  5 17:14 usb_modeswitch.conf
drwxr-xr-x 1 root root 4096 Aug  5 17:14 .
drwxr-xr-x 1 root root 16 Aug  5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x 2 root root 4096 Sep 26 21:24 .
drwxr-xr-x 4 root root 4096 Oct 21 17:19 .
drwxr-xr-x 1 root root 4096 Aug  5 17:14 .
drwxr-xr-x 1 root root 4942 Aug  5 17:14 vtrgb -> /etc/alternatives/vtrgb
drwxr-xr-x 4 root root 4096 Aug  5 17:02 .
-rw-r--r-- 1 root root 681 Apr  8 2024 xattr.conf
drwxr-xr-x 4 root root 4096 Aug  5 17:14 .
drwxr-xr-x 1 root root 4096 Aug  5 17:02 .
-rw-r--r-- 1 root root 469 Aug  5 17:14 zsh_command_not_found
haJra@ubuntu-lab:~$
```

! click inside or press Ctrl+G.



ls -la /dev

```

crw-rw---- 1 root dialout 4, 91 Oct 22 20:00 ttyS27
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, 67 Oct 22 20:00 ttyS30
crw-rw---- 1 root dialout 4, 94 Oct 22 20:00 ttyS30
crw-rw---- 1 root dialout 4, 95 Oct 22 20:00 ttyS31
crw-rw---- 1 root dialout 4, 68 Oct 22 20:00 ttyS32
crw-rw---- 1 root dialout 4, 79 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
dripr-xr-x 2 root root 10, 120 Oct 22 20:00 vesa
crw-rw---- 1 root kvm 10, 121 Oct 22 20:00 udmabuf
crw----- 1 root root 10, 230 Oct 22 20:00 uhid
crw-rw---- 1 root root 10, 221 Oct 22 20:00 userport
crw-rw---- 1 root root 10, 222 Oct 22 20:00 random
crw-rw---- 1 root root 10, 126 Oct 22 20:00 userfaultfd
crw-rw---- 1 root root 10, 246 Oct 22 20:00 userio
crw-rw---- 1 root tty 7, 0 Oct 22 20:00 vcs
crw-rw---- 1 root tty 7, 1 Oct 22 20:00 vcs1
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 vcsai
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, 65 Oct 22 20:00 vcsui
crw-rw---- 1 root tty 7, 66 Oct 22 20:00 vcsuu
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
crw-rw---- 1 root root 10, 127 Oct 22 20:00 vga_arbiter
crw----- 1 root root 10, 137 Oct 22 20:00 vhci
crw-rw---- 1 root kvm 10, 238 Oct 22 20:00 vhost-net
crw-rw---- 1 root kvm 10, 239 Oct 22 20:00 vhost-vsock
crw----- 1 root root 10, 122 Oct 22 20:00 vnc
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
ha.jra@ubuntu-lab:~$
```

click inside or press Ctrl+G.

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 1 root root 4096 Oct 22 00:00 cache
drwxr-xr-x 16 root root 4096 Oct 27 08:09 .
drwxrwsnwt 2 root root 4096 Aug 5 17:02 crash
drwxr-xr-x 46 root root 4096 Sep 27 08:39 .
drwxrwsnwt 2 root staff 4096 Apr 22 2024 local
lrwxrwxrwx 1 root root 9 Aug 5 16:54 lock -> /run/lock
drwxrwxrwx 12 root syslog 4096 Oct 22 20:00 log
drwxrwsnwt 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 29 20:00 snap
drwxr-xr-x 1 root root 4096 Sep 29 20:00 snapd
drwxrwsnwt 7 root root 4096 Oct 22 20:01 tmp
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated
ha.jra@ubuntu-lab:~$
```

ls -la /tmp

```

total 52
drwxrwxnwt 13 root root 4096 Oct 22 20:11 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxrwxnwt 2 root root 4096 Oct 22 20:00 .font-unix
drwxrwxnwt 2 root root 4096 Oct 22 20:00 .ICE-unix
drwx----- 6 root root 4096 Oct 22 20:00 .pulse-private-100
drwx----- 3 root root 4096 Oct 22 20:00 systemd-private-40982094bd764093a0e2ef3100c1a0e5-ModeManager.service-FQyH0C
drwx----- 3 root root 4096 Oct 22 20:00 systemd-private-40982094bd764093a0e2ef3100c1a0e5-polkit1.service-kmpf
drwx----- 3 root root 4096 Oct 22 20:00 systemd-private-40982094bd764093a0e2ef3100c1a0e5-systemd-logind.service-geuny
drwx----- 3 root root 4096 Oct 22 20:00 systemd-private-40982094bd764093a0e2ef3100c1a0e5-systemd-resolved.service-uzemy
drwx----- 2 root root 4096 Oct 22 20:00 .X11-unix
drwxrwxnwt 2 root root 4096 Oct 22 20:00 .X11-unix_043-492170429
drwxrwxnwt 2 root root 4096 Oct 22 20:00 .XIM-unix
drwxrwxnwt 2 root root 4096 Oct 22 20:00 .XIM-unix_
ha.jra@ubuntu-lab:~$
```

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

ls -la ~

```

$ ls -la $home
total 39593
drwxr-xr-x 1 A11i 197609          0 Nov 15 09:10  /
drwxr-xr-x 1 A11i 197609          0 Oct 16 00:59  .-
drwxr-xr-x 1 A11i 197609 11439 Nov 20 01:26 .bash_history
drwxr-xr-x 1 A11i 197609          0 Dec 10 2024 .dotnet/
drwxr-xr-x 1 A11i 197609          0 Oct 18 03:51 .git/
drwxr-xr-x 1 A11i 197609 301 Oct 18 02:07 .gitconfig
drwxr-xr-x 1 A11i 197609          0 Dec 5 2024 .ok/
drwxr-xr-x 1 A11i 197609          0 Dec 5 2024 .gnupg/
drwxr-xr-x 1 A11i 197609 20 Oct 18 03:48 .lessht
drwxr-xr-x 1 A11i 197609 174 May 29 2025 .packettracer
drwxr-xr-x 1 A11i 197609          0 Jan 15 2025 .ssns/
```

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



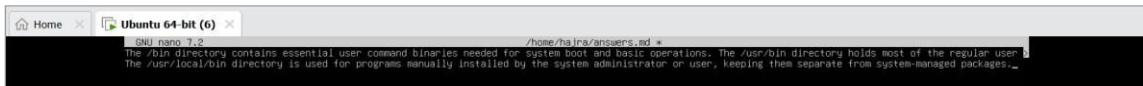
- Type the paragraph in the editor, save and exit.

Navigated into the newly created directory.

Pwd

```
~/lab4/workspace/python_project$ pwd
workspace/python_project
~/lab4/workspace/python_project$ _
```

Verified the current working directory path.



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

```
hajra@ubuntu-lab:~$ cat $HOME/answers.md
The /bin directory contains essential user command binaries needed for system boot and basic operations. The /usr/bin directory holds most of the regular user commands and applications that are not required for system startup.
The /usr/local/bin directory is used for programs manually installed by the system administrator or user, keeping them separate from system-managed packages.
hajra@ubuntu-lab:~$ 
```

Task 4: Essential CLI Tasks — Navigation and File Operations

Steps Performed

1. Create a Workspace and Navigate

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

```
~$ mkdir -p $HOME/lab4/workspace/python_project
~$ _
```

Created a new workspace directory for the Python project.

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

```
~$ cd $HOME/lab4/workspace/python_project
~/lab4/workspace/python_project$ _
```

2. Create Files Using an Editor nano

```
README.md
```

```
GNU nano 7.2
lab 4 README_
README.md *
```

Added the text “**Lab 4 README**” and saved the file. nano
main.py

```
GNU nano 7.2 main.py *
print ('hello lab4')
```

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

```
GNU nano 7.2 .env *
ENV = lab4_
```

Added the line ENV=lab4 and saved the file.

3. List Files

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 14:14 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

```
lab4/workspace/python_projects$ cp README.md README.md.copy.md
lab4/workspace/python_projects$
```

Created a copy of the README file.

mv README.copy.md README.dev.md

```
/lab4/workspace/python_projects$ mv README.md.copy.md README.dev.md
/lab4/workspace/python_projects$
```

Renamed (moved) the copied file.

rm README.dev.md

Copied the entire Python project directory recursively.

ls -la ~/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. Work with Directories

mkdir -p ~/lab4/workspace/java_app

```
lab4/workspace/python_projects$ mkdir -p $HOME/lab4/workspace/java_app
lab4/workspace/python_projects$
```

Created another directory for a Java app.

cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy

```
/lab4/workspace/python_projects$ cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/java_app_copy
/lab4/workspace/python_projects$
```

6. Use Command History and Tab Completion

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 $HOME/lab4/workspace
18 history
haира@ubuntu-lab:~/lab4/workspace/python_projects$
```

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.

```
print ('hello lab4')
```

Task 5: System info, resources & processes

Collect system information and observe processes. Use screenshots only.

Steps (inside VM terminal)

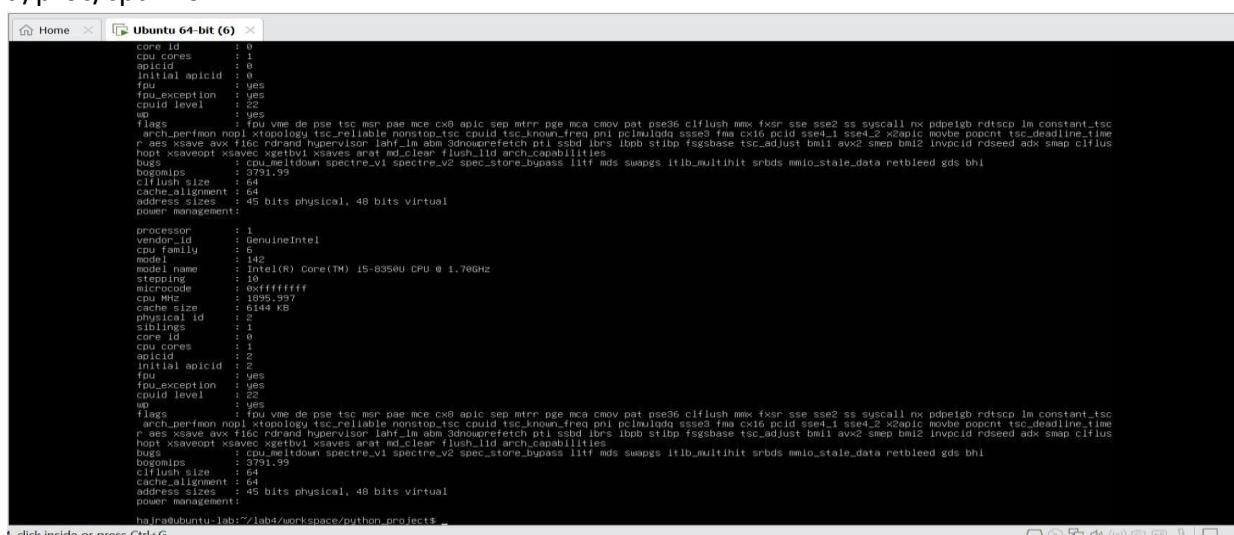
1. Kernel and OS:

```
uname -a
```

```
haира@ubuntu-lab:~/lab4/workspace/python_projects$ uname -a
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
```

2. CPU (ensure model name visible):

```
cat /proc/cpuinfo
```



```
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 142
model name : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
stepping : 10
microcode : 0x1f1fffff
cpu MHz : 1095.997
cache size : 1104 KB
physical id : 0
siblings : 2
cores : 4
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 sev ntrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon nonstop_tsc cpuid tsc_reliable tsc_known_freq pni pclmulqdq sse3 fma cx16 pcld sse4_1 sse4_2 x2apic movebe popcnt tsc_deadline_timer r_pes xsave avx fsgsbase hyperervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bm1 avx2 smep bm2 invpcid rdseed adx smep clflushopt bugs : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbs mmio_stale_data retbleed gds bhi
bogomips : 9791.99
clflush size : 64
cache_alignment : 64
address sizes : 48 bits physical, 48 bits virtual
power management:
```

3. Memory: free -h



	total	used	free	shared	buff/cache	available
Mem:	1.9Gi	1.2Gi	132Mi	12Mi	734Mi	667Mi
Swap:	2.0Gi	223Mi	1.8Gi			

```
haира@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
```

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

```

root      496  0.0  0.1 12584496 2268 ?    S1 12:24  0:00 httpd -d /snap/nextcloud/50464 -k start -DFOREGROUND
root      4987 0.0  0.1 1258496 2356 ?    S1 12:24  0:00 httpd -d /snap/nextcloud/50464 -k start -DFOREGROUND
root     5496  0.0  0.1 8400 3456 ?    Ss 12:24  0:02 bash /snap/microk8s/8511/run-cluster-agent-with-args
haира   5639  0.0  0.1 20696 8192 ?    Ss 12:24  0:01 /usr/lib/systemd/systemd -user
haира   5640  0.0  0.1 20696 8232 ?    Ss 12:24  0:01 /usr/lib/systemd/systemd -user
haира   5694  0.0  0.2 8656 4096 ttys1  S 12:24  0:00 -bash
root    5739  0.0  0.1 1258084 4672 ?    S1 12:24  0:04 /snap/microk8s/8511/bin/containerd -c /var/snap/microk8s/8511/bin/containerd -c config=/var/snap/microk8s/8511/args/containerd.toml --ro
root    5897  0.0  0.1 1258084 5132 ?    S1 12:24  0:01 /snap/microk8s/8511/bin/containerd -c config=/var/snap/microk8s/8511/args/containerd.toml --ro
root    6269  7.2 16.1 1546420 318226 ?    Ss 12:24  0:12 /snap/microk8s/8511/bin/kubelite -scheduler-args-file=/var/snap/microk8s/8511/args/kube-schedule
root    7149  0.3  0.4 1234158 8380 ?    S1 12:24  0:33 /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id ce047894ba4dc6614850488
65535  7568  0.0  0.3 1234112 6908 ?    S1 12:25  0:09 /snap/microk8s/8511/bin/containerd-shim-runc-v2 -namespace k8s.io -id 1fa57bb780d67f58e774952
65535  7568  0.0  0.0 1020 128 ?    Ss 12:25  0:00 /pause
root    7670  0.0  0.0 12584496 8232 ?    Ss 12:25  0:00 /snap/microk8s/8511/bin/containerd -c /var/snap/microk8s/8511/args/containerd.toml --ro
root    7728  0.2  1.0 7646556 20364 ?    Ss 12:25  0:24 /coredns/_config /etc/coredns/Corefile
haира  7740  0.0  0.0 1258084 318226 ?    S1 12:25  0:00 /snap/microk8s/8511/bin/containerd -c /var/snap/microk8s/8511/args/containerd.toml --ro
root    8389  0.0  0.0 4476 1152 ?    Ss 12:25  0:00 //usr/local/bin/runsvcid -P /etc/service/enabled
root    8637  0.0  0.0 4324 1152 ?    Ss 12:25  0:00 runsvd allocate-tunnel-addrs
root    8638  0.0  0.0 4324 1152 ?    Ss 12:25  0:00 runsvd tellis
root    8639  0.0  0.0 4324 1152 ?    Ss 12:25  0:00 runsvd status-reporter
root    8640  0.0  0.0 4324 1152 ?    Ss 12:25  0:00 runsvd cni
root    8641  0.0  0.0 4324 1152 ?    Ss 12:25  0:00 runsv monitor-addresses
root    8642  0.0  2.7 1794476 992 ?    S1 12:25  0:01 /snap/microk8s/8511/bin/containerd -c /var/snap/microk8s/8511/args/containerd.toml --ro
root    8643  0.0  2.8 17944220 5616 ?    S1 12:25  0:01 calico-node -status-reporter
root    8644  0.0  2.7 1794476 55908 ?    S1 12:25  0:01 calico-node -monitor-token
root    8645  0.0  2.8 1794476 55752 ?    S1 12:25  0:01 calico-node -flush-252:0
root    8647  0.0  2.8 1794476 55752 ?    S1 12:25  0:01 calico-node -monitor-addresses
root    8648  0.0  0.0 0 0 ?    I< 12:37  0:04 [kworker/0:0h-kblockd]
root    8649  0.0  0.0 0 0 ?    I< 12:37  0:04 [kworker/0:0h-kblockd]
root    115204 0.0  1.9 478476 38364 ?    Ss 12:57  0:01 /usr/libexec/fwupd/fwupd
root    115282 0.0  0.4 314090 8960 ?    Ss 12:57  0:00 /usr/libexec/upowerd
root    140000 0.0  0.0 0 0 ?    I< 12:57  0:00 [kworker/0:0h-kblockd]
root    347396 0.0  0.0 0 0 ?    I< 13:48  0:00 [kworker/0:0h-kblockd]
root    537636 0.0  0.0 0 0 ?    I< 14:28  0:00 [kworker/0:0h-kblockd]
root    596258 0.0  0.0 0 0 ?    I< 14:57  0:00 [kworker/0:0h-kblockd]
root    656128 0.0  0.0 0 0 ?    I< 14:57  0:00 [kworker/0:0h-kblockd]
root    681389 0.0  0.0 0 0 ?    I< 15:00  0:00 [kworker/0:0h-events_power_efficient]
root    684235 0.3  0.0 0 0 ?    I< 15:01  0:02 [kworker/0:1-events]
root    691039 0.0  0.0 0 0 ?    I< 15:01  0:02 [kworker/0:1-events]
root    698137 0.0  0.0 0 0 ?    I< 15:04  0:00 [kworker/0:1-events_unbound]
root    785790 0.1  0.0 0 0 ?    I< 15:06  0:00 [kworker/0:1-events]
root    791791 0.0  0.0 0 0 ?    I< 15:06  0:00 [kworker/0:1-flush-252:0]
root    791791 0.4  0.0 0 0 ?    I< 15:08  0:01 [kworker/1:0-events]
root    724181 0.0  0.0 4556 1536 ?    S 15:09  0:00 sleep 5m
root    730392 0.0  0.0 0 0 ?    I< 15:10  0:00 [kworker/0:2-events]
root    737692 0.0  0.0 0 0 ?    I< 15:12  0:00 [kworker/0:2-flush-252:0]
root    740675 0.0  0.0 5948 1664 ?    S 15:13  0:00 sleep 5
root    haира 740989 1850 0.2 12312 5120 ttys1+ 15:13  0:00 ps aux
haира@ubuntu-lab:~$ lab4/workspace/python_projects$ 

```

Ctrl+G: click inside or press Ctrl+G.

	total	used	free	shared	buff/cache	available
Mem:	1.96i	1.26i	132Mi	12Mi	734Mi	667Mi
Swap:	2.86i	223Mi	1.88i			

```

haира@ubuntu-lab:~/lab4/workspace/python_projects$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           192M   19M   173M  1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 12G   11G   934M  97% /
tmpfs            960M   960M   0  100% /dev/shm
tmpfs             5.0M   5.0M   0  100% /run/lock
/dev/sda2        2.0G  192M  1.66G  11% /boot
tmpfs            192M   20K   192M  1% /run/user/1000
tmpfs            40M   64M   0  100% /tmp
tmpfs            64M   0  64M  0% /var/snap/microk8s/8511/run/containerd/grpc.v1.cri/sandboxes/ce047894ba4dc68148504884d
shm              64M   0  64M  0% /var/snap/microk8s/8511/run/containerd/grpc.v1.cri/sandboxes/907005c3fa2edabd7e07c5bb55
shm              64M   0  64M  0% /var/snap/microk8s/8511/run/containerd/grpc.v1.cri/sandboxes/1fa57bb780d67f58e774952f1e
e1b80625b771c524cd31f3f71c0866c562fc57/shm
shm              64M   0  64M  0% /var/snap/microk8s/8511/run/containerd/grpc.v1.cri/sandboxes/1fa57bb780d67f58e774952f1e
haира@ubuntu-lab:~/lab4/workspace/python_projects$ 

```

4. View OS release information:

```
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
haира@ubuntu-lab:~/lab4/workspace/python_projects$ 

```

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

Steps (inside VM terminal)

- Create a new user named lab4user:

```
sudo adduser lab4user
```

```
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
```

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

3. Switch to the new user to verify login:

```
su - lab4user
```

```
Password:
hajra@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
```

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

5. Return to the original user:

[Exit](#)

```
~/lab4/workspace/python_project$
```

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

```
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
```

```
[~/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)"
uptime 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
```

```
[lab4/workspace/python_project]$ chmod +x ~/lab4/workspace/python_project/run-demo.sh
[lab4/workspace/python_project]$
```

3. Run the script as your regular user:

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

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

4. Optionally run it with sudo:

```
sudo ~/lab4/workspace/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:

```
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: ~
```

- Verify your current user and home directory path.

```
111@DESKTOP-KQE4P80 MINGW64 ~ C:\main>
111@DESKTOP-KQE4P80 MINGW64 ~ C:\main>cd /home/Alli
bash: /home/Alli: No such file or directory
```

- Confirm you are connected to the correct host machine.

```
ubuntu-lab
```

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.

```
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 8771 Mar 31 2024 .bashrc
drwxr----- 2 hajra hajra 4096 Sep 26 21:40 .cache
-rw-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:~$
```

Display the OS version and release information.

```
/lab4/workspace/python_project$ uname -a
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
/lab4/workspace/python_project$
```

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

```

ls -al
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-x--- 2 hajra hajra 4096 Sep 26 21:40 .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41 .lesshst
-rw-r--r-- 1 hajra hajra 20 Sep 26 22:08 .profile
drwxr-x--- 2 hajra hajra 4096 Sep 26 22:00 .profile
-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:~$ 

```

3. Display all hidden files in your home directory.

```

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-x--- 2 hajra hajra 4096 Sep 26 21:40 .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41 .lesshst
-rw-r--r-- 1 hajra hajra 20 Sep 26 22:08 .profile
drwxr-x--- 2 hajra hajra 4096 Sep 26 22:00 .profile
-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. 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
```

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

```
nano report.md
```

3. Inside nano, type your short summary.

```

hajra@ubuntu-lab:~/lab4/workspace$ cat report.md
<!--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 administration.
- **/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$ 

```

```

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 administration.
- **/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$ 

```

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

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_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 5 hajra hajra 4096 Oct 23 14:11 .  
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:11 ..  
rw-rw-r-- 1 hajra hajra 21 Oct 23 14:11 main.py  
-rw-rw-r-- 1 hajra hajra 21 Oct 23 14:11 README.md
```

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 README_copy.md
```

Created a copy of the README file.

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

Renamed (moved) the copied file.

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

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
```

Created another directory for a Java app.

```
cp -r ~/workspace/python_project ~/Lab4/workspace/java_app_copy  
hajra@ubuntu-lab:~/lab4/workspace/python_projects$ cp -r ~/workspace/python_project $HOME/Lab4/workspace/java_app_copy
```

Copied the entire Python project directory recursively.

```
ls -l $HOME/Lab4/workspace/python_projects  
hajra@ubuntu-lab:~/Lab4/workspace/python_projects$ ls -la $HOME/Lab4/workspace
```

total 16
drwxrwxr-x 4 hajra hajra 4096 Oct 23 14:34 .
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:34 ..
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:34 JavaApp
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:34 Lab4
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:34 python_projects

Verified the copied directories.

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

```
hajra@ubuntu-lab:~/Lab4/workspace/python_projects$ history  
2 nano .gitignore_and_main.py  
3 rm .gitignore_and_main.py  
4 rm -rf .git  
5 rm -rf .gitignore_and_main.py  
6 rm -rf .gitignore_and_main.py  
7 rm -rf .gitignore_and_main.py  
8 rm -rf .gitignore_and_main.py  
9 rm -rf .gitignore_and_main.py  
10 rm -rf .gitignore_and_main.py  
11 cp README.md README_copy.md  
12 rm -rf README_copy.md  
13 mv README_copy.md README.dev.md  
14 rm -rf README.dev.md  
15 rm -rf $HOME/Lab4/workspace/java_app  
16 rm -rf $HOME/Lab4/workspace/python_project  
17 ls -la $HOME/Lab4/workspace  
18 ls -la $HOME/Lab4/workspace
```

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.

	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:~\$ _						

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:

1. Create a new test user named lab4user.

```
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 []: 03two07-5007883
      Home Phone []: 03two07-5007883
      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-lu:~/lab4/unrkspace/python_projects$
```

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

```
lab4user:x:1002:1002:hajra,twenty_two,03two7-5007883,03two7-5007883,nil:/home/lab4user:/bin/bash  
hajra@ubuntu-lab:~/Lab4/workspace/python_projects$
```

3. Log in as lab4user and confirm successful login.

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

```
root@lab4user:~$ sudo whoami  
[sudo] password for lab4user:  
lab4user is not in the sudoers file.  
1lab4user@ubuntu-1:~$
```

- ## 5. Switch back to your main analyst account.

'/lab4/workspace/python_project\$ _

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

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