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

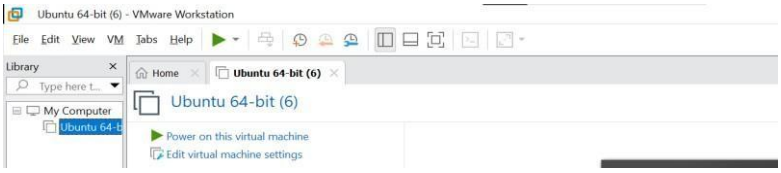
TASK:

Task 1: Verify VM resources in VMware

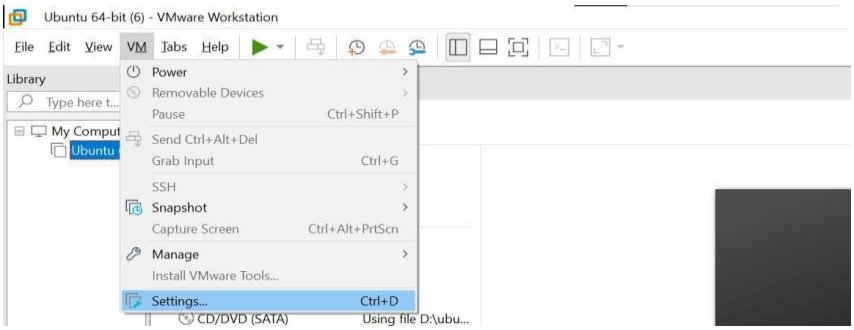
Confirm the VM resources that were allocated in Lab 1.

Steps

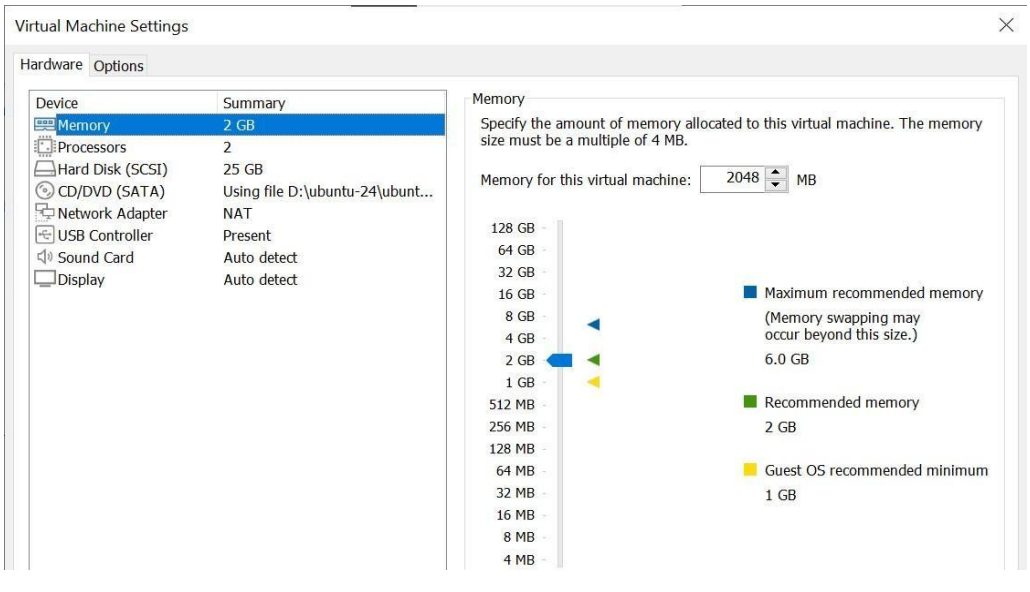
1. Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.



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:



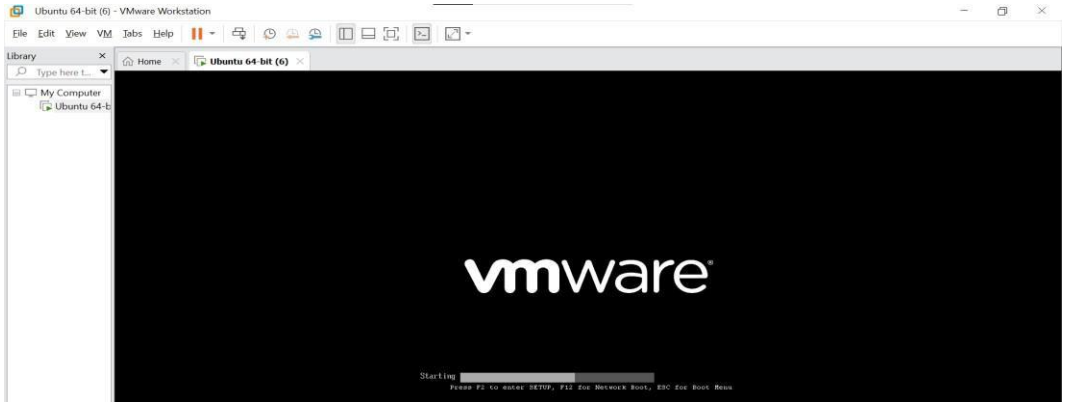
vm_settings.png

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"

```
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
 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: $
```

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

```
Alli@DESKTOP-KQE4P8O MINGW64 ~ (main)
$ whoami
Alli

Alli@DESKTOP-KQE4P8O MINGW64 ~ (main)
$ /home/Alli
bash: /home/Alli: No such file or directory

Alli@DESKTOP-KQE4P8O MINGW64 ~ (main)
$ pwd
/c/Users/Alli

Alli@DESKTOP-KQE4P8O MINGW64 ~ (main)
$
```

Task 3: Filesystem exploration — root tree and dotfiles

Steps (run inside VM terminal)

1. List root directory contents:
   ls -la /

```
Alli@DESKTOP-KQE4P8O 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_histor
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  .gk/
drwxr-xr-x 1 Alli 197609        0 Dec  5  2024  .gnupg/
-rw-r--r-- 1 Alli 197609       20 Oct 18 03:48  .lesshst
```

2. Inspect these directories (run each command and screenshot the output):
   ls -la /bin

```
Alli@DESKTOP-KQE4P8O 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  ../
```

   ls -la /sbin

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

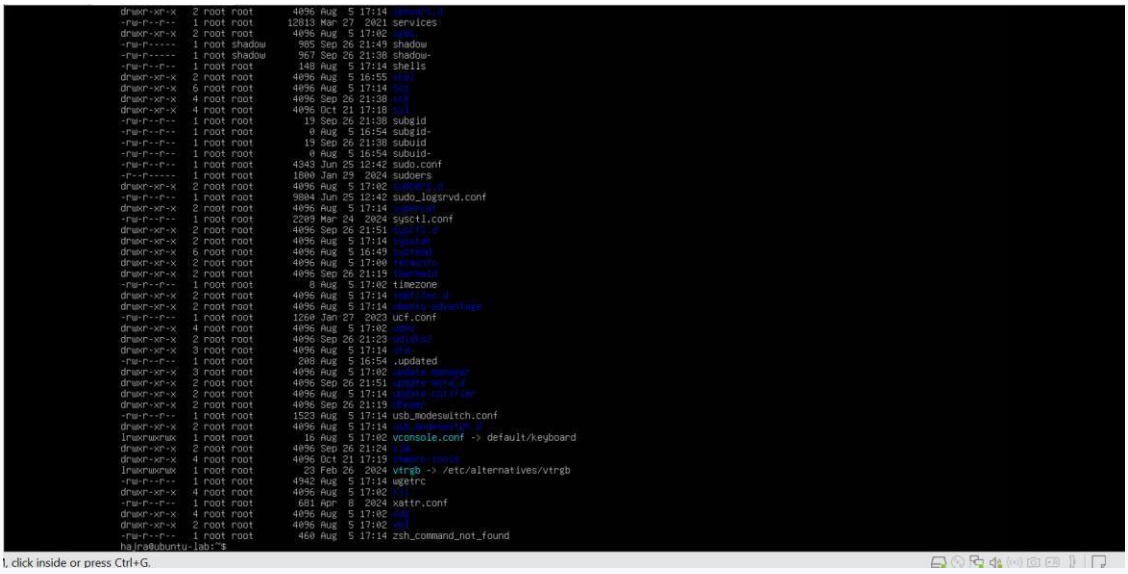
   ls -la /usr

```
total 96
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Sep 26 21:19 ..
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  83 root root  4096 Oct 21 17:20 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  10 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:~$
```

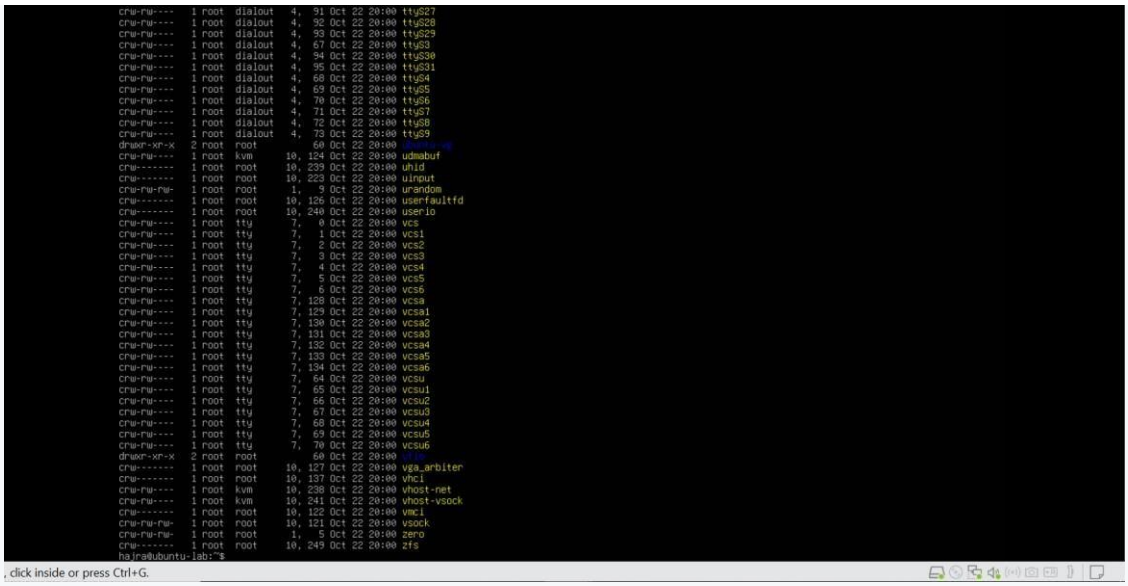
ls -la /opt

```
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
drwx--x--x  4 root root 4096 Sep 26 21:51 containerd
hajra@ubuntu-lab:~$
```

ls -la /etc



ls -la /dev

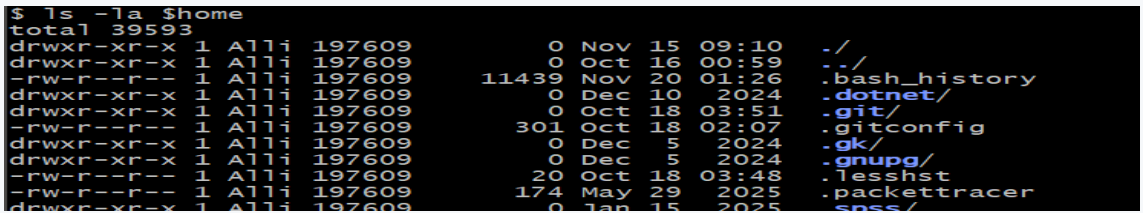


ls -la /var

ls -la /tmp

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

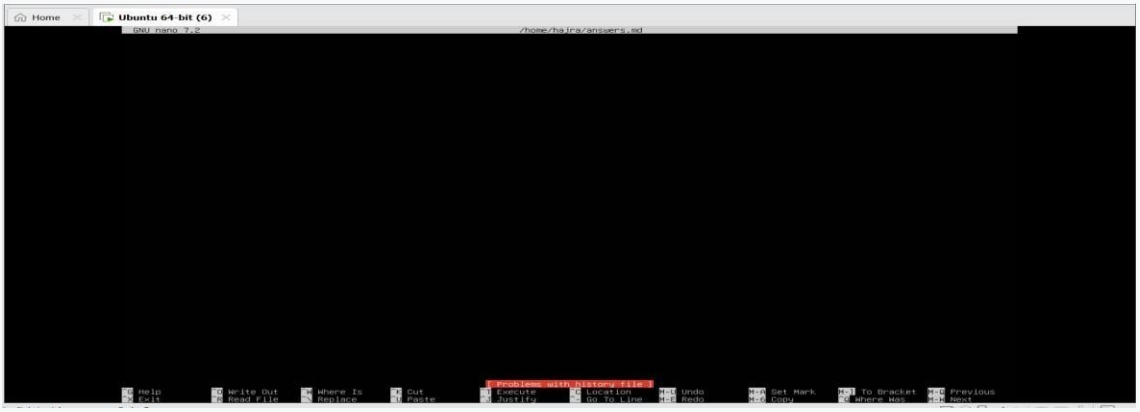
ls -la ~



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

Open your editor:

ıano ~/answers.md

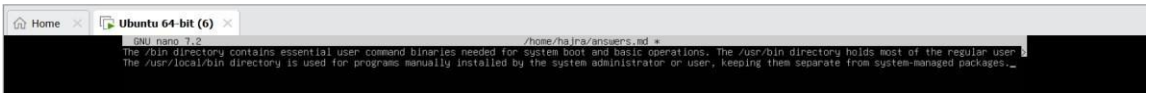


- Type the paragraph in the editor, save and exit.

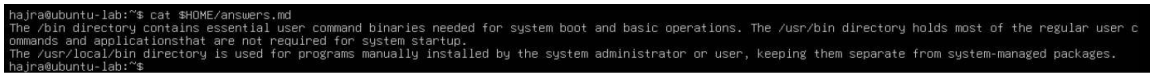
Navigated into the newly created directory.

Pwd

Verified the current working directory path.



- 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

1. **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

2. **Create Files Using an Editor** nano

   README.md

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

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

nano .env

Added the line **ENV=lab4** and saved the file.

3. **List Files**

ls -la

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

4. **Copy, Move, and Remove Files** cp README.md README.copy.md

Created a copy of the README file.

mv README.copy.md README.dev.md

Renamed (moved) the copied file.

rm README.dev.md

Copied the entire Python project directory recursively.

ls -la ~/lab4/workspace

Verified the copied directories.

5. **Work with Directories**

mkdir -p ~/lab4/workspace/java_app

Created another directory for a Java app.

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

6. **Use Command History and Tab Completion**

History

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.

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

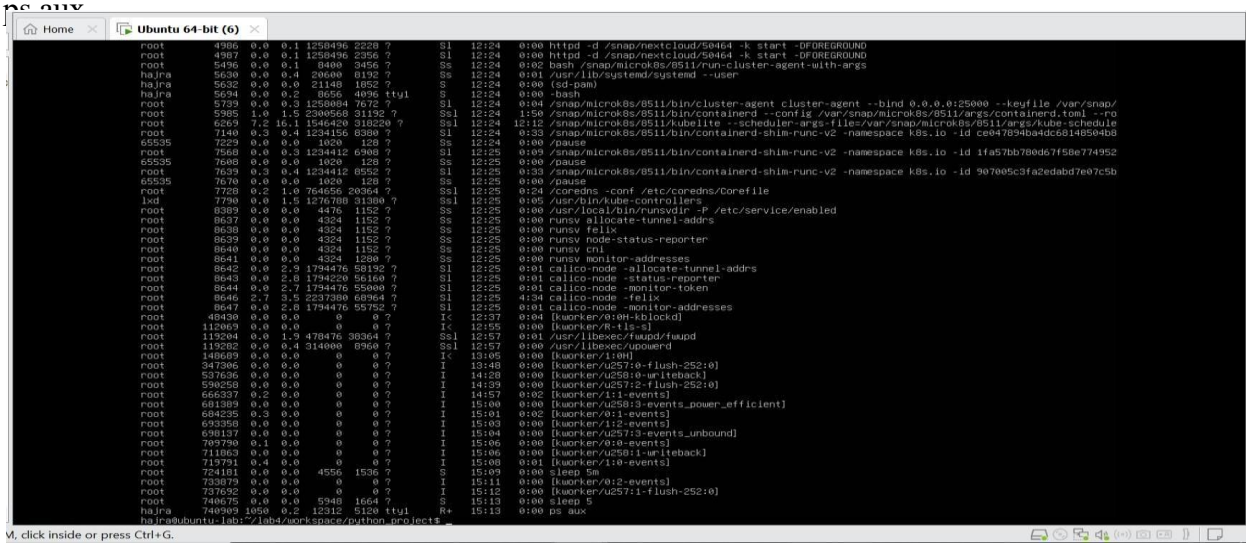
2. CPU (ensure model name visible):

   cat /proc/cpuinfo

3. Memory: free -h

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

ps aux



4. View OS release information:

   cat /etc/os-release

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

Steps (inside VM terminal)

1. 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:
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

```
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

```
~/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

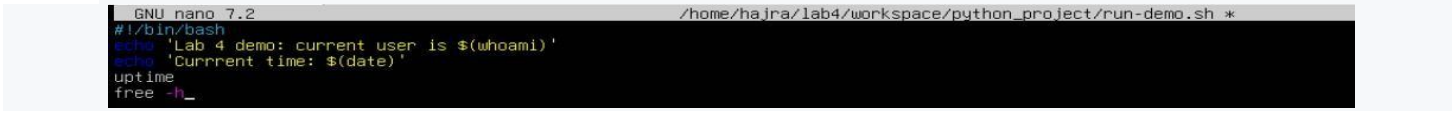
Steps (inside VM)

1. Open an editor to create the script:

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

- 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
```



2. Make the script executable:

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

3. Run the script as your regular user:

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

4. Optionally run it with sudo:

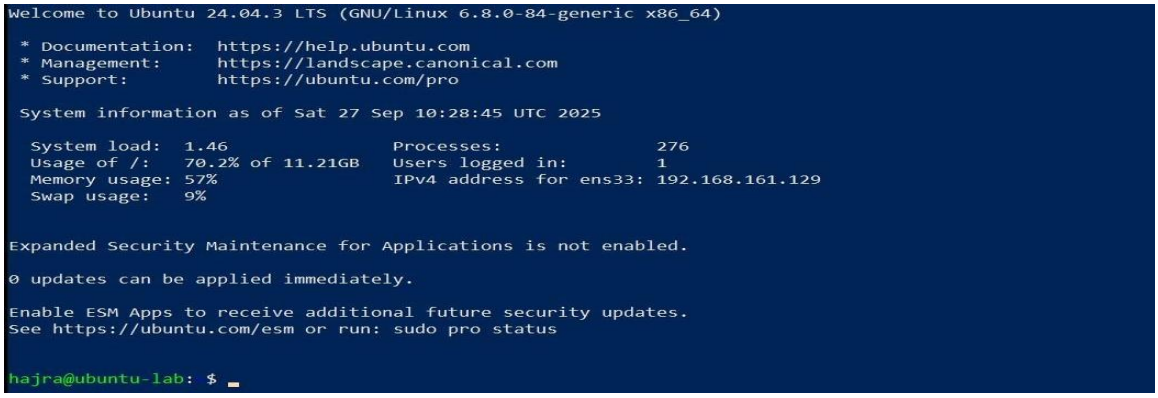
```
sudo ~/lab4/workspace/run-demo.sh
```

Exam Evaluation Questions

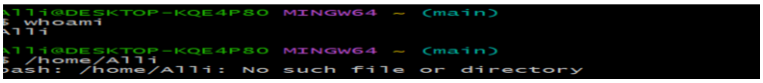
1. **Remote Access Verification (Cyber Login Check) Scenario:**

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:



2. Verify your current user and home directory path.



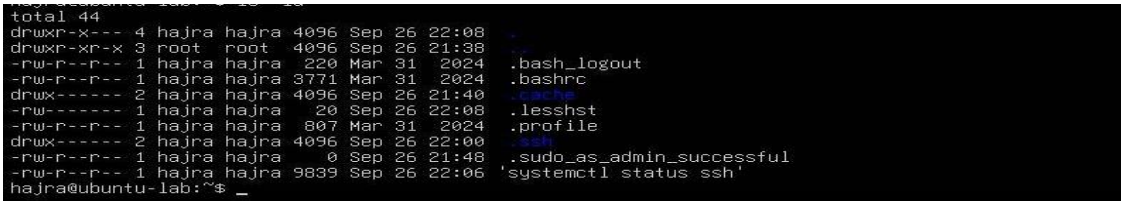
3. Confirm you are connected to the correct host machine.

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.

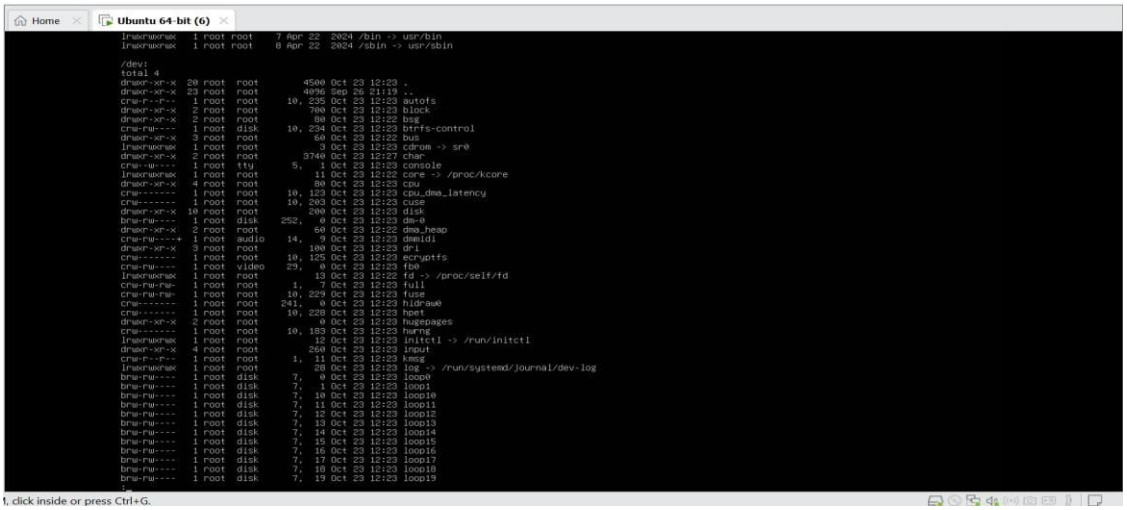
Steps:

1. Display the contents of the root directory.



Display the OS version and release information.

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



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
drwx------ 2 hajra hajra 4096 Sep 26 21:40  .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41  .lesshst
-rw------- 1 hajra hajra   20 Sep 26 22:08  .profile
-rw-r--r-- 1 hajra hajra  807 Mar 31  2024  .ssh
drwx------ 2 hajra hajra 4096 Sep 26 22:00  .sudo_as_admin_successful
-rw-r--r-- 1 hajra hajra    0 Sep 26 21:48  'systemctl status ssh'
-rw-r--r-- 1 hajra hajra 9839 Sep 26 22:06
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

   ```
   ~$ cd ~/lab4/workspace
   ```

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

   nano report.md

   ```
   ~/lab4/workspace$ nano report.md_
   ```

3. Inside nano, type your short summary.

```
<!--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$ _
```

```
 GNU nano 7.2                                                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.
```

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.

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

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

cp README.md README.copy.md

Created a copy of the README file.

mv README.copy.md README.dev.md

Renamed (moved) the copied file.

rm README.dev.md

Deleted the renamed file.

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

mkdir -p ~/lab4/workspace/java_app

Created another directory for a Java app.

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

Copied the entire Python project directory recursively.

ls -la ~/lab4/workspace

Verified the copied directories.

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

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

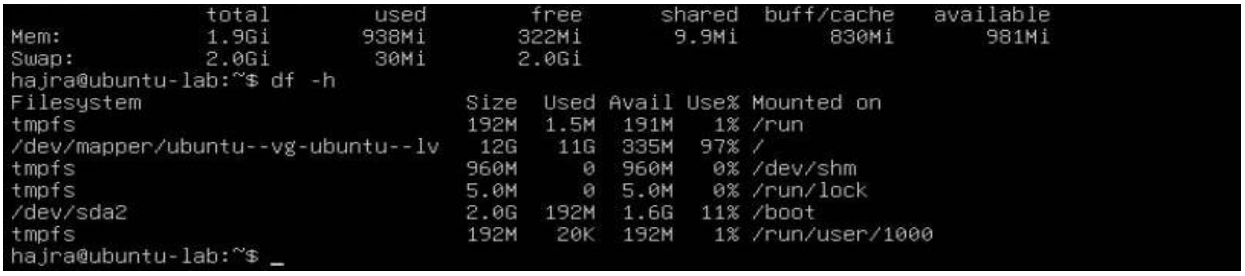
4. System Profiling and Process Monitoring Scenario:

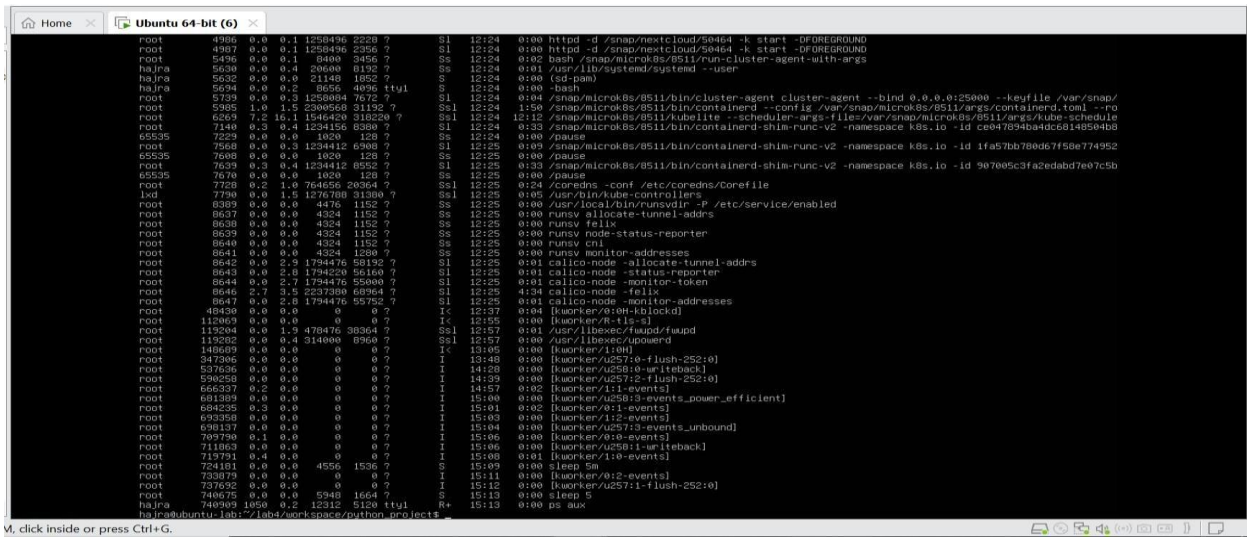
You are investigating a potential malware infection that is consuming excessive resources on the Linux VM.

Steps:

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

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





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 []: 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 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_project$ _
```

3. Log in as lab4user and confirm successful login.

```
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.

```
~/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$ _
```