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

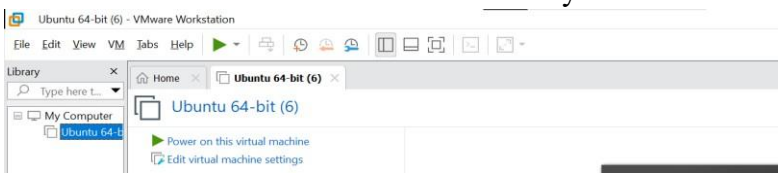
TASK:

Task 1: Verify VM resources in VMware

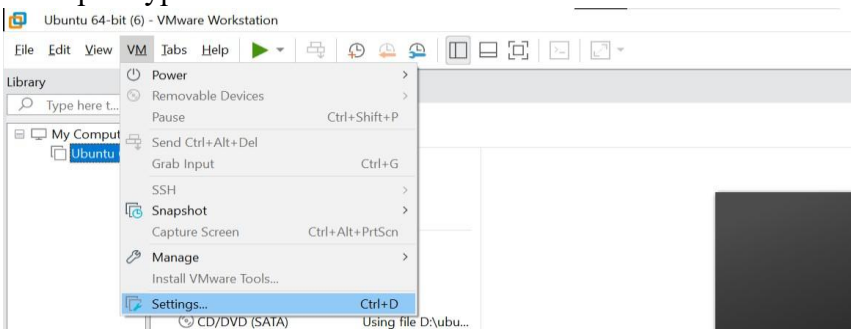
Confirm the VM resources that were allocated in Lab 1.

Steps

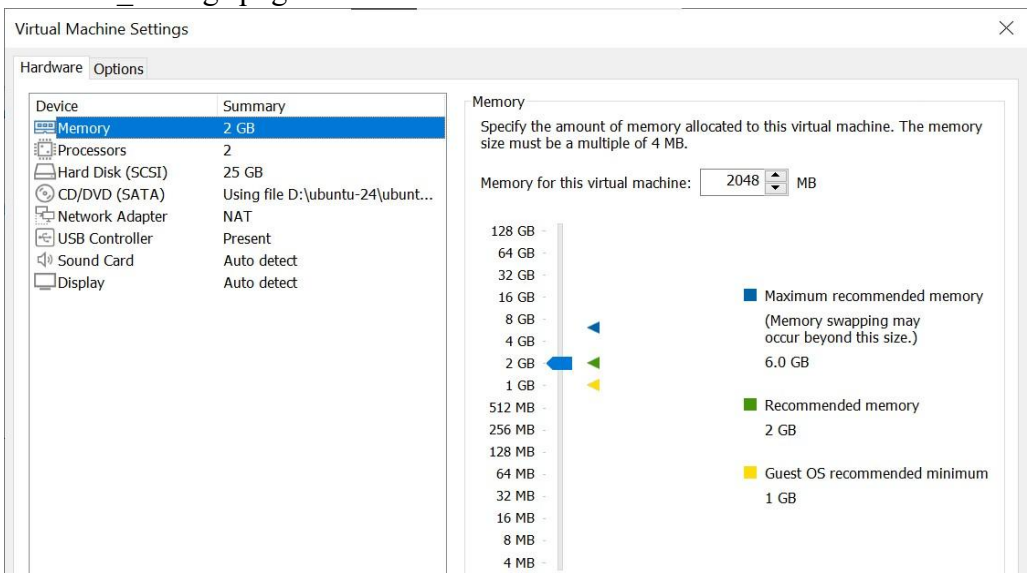
1. Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.



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

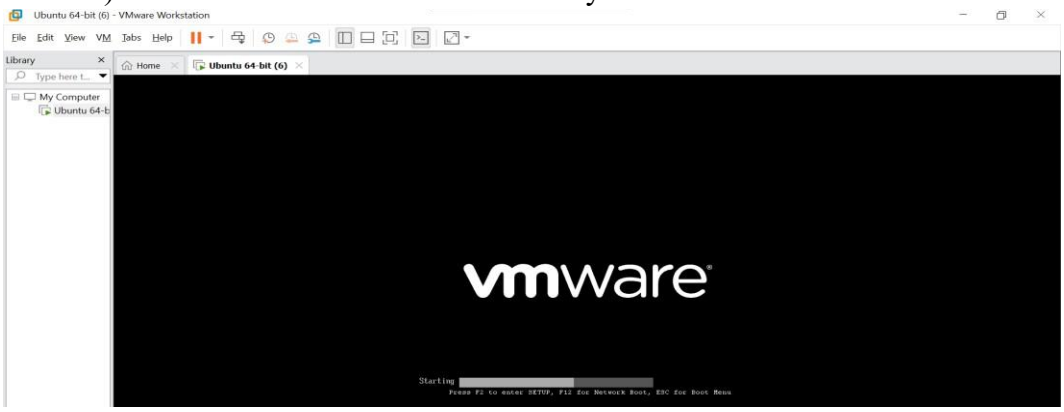


Task 2: Start VM and log in (use your preferred host terminal method only)

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-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
  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
```

    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%                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: $
```

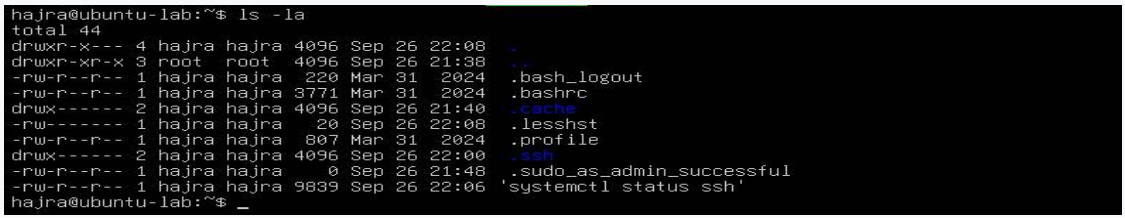
3. After logging in, run both commands and capture them together in a single screenshot:
   whoami
   pwd

Task 3: Filesystem exploration — root tree and dotfiles

Steps (run inside VM terminal)

1. List root directory contents:

   ls -la /



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

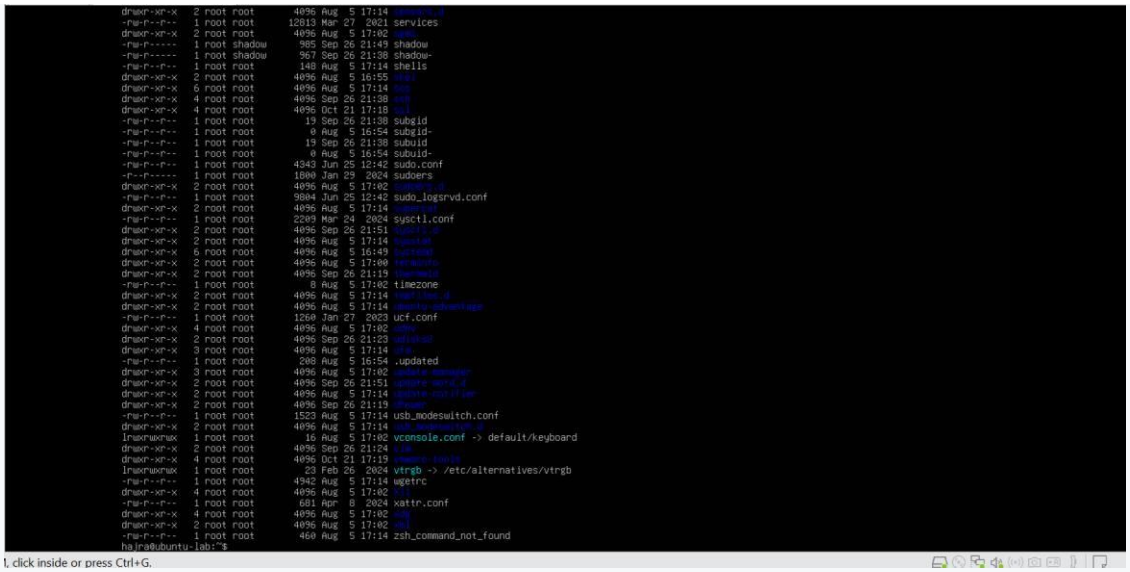
   ls -la /bin

   ls -la /sbin

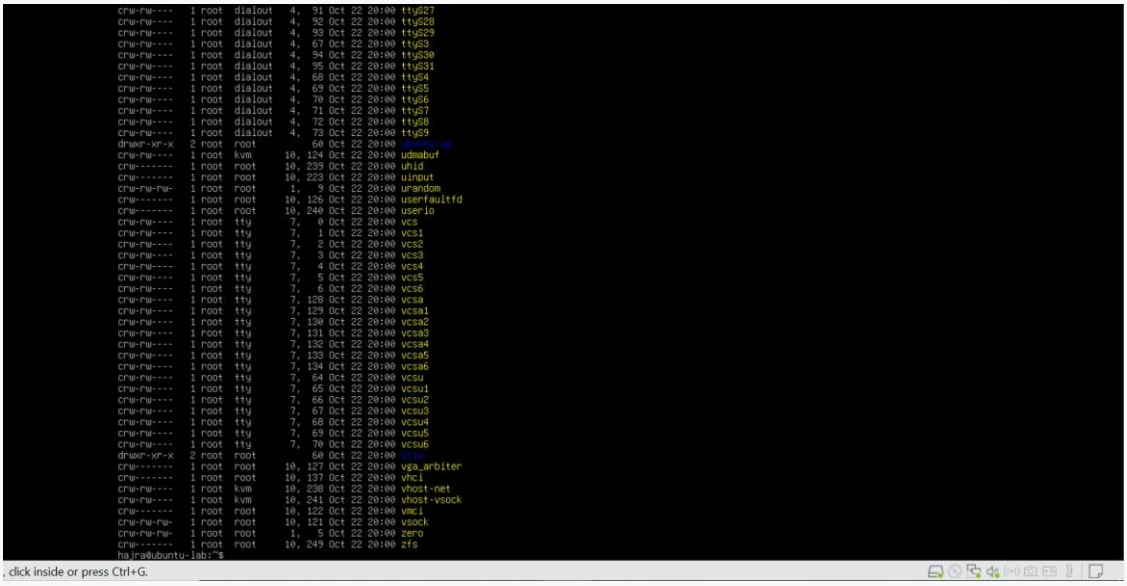
   ls -la /usr

   ls -la /opt

   ls -la /etc

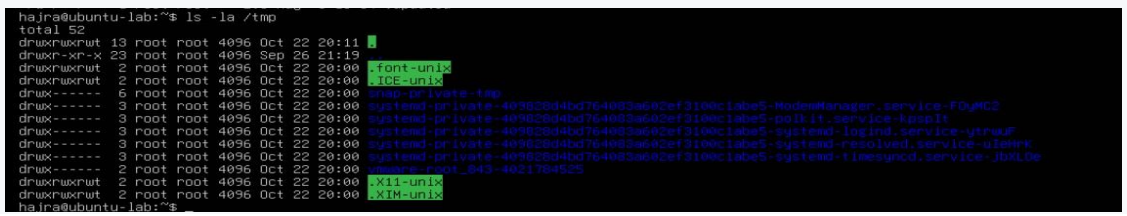


ls -la /dev



ls -la /var

ls -la /tmp

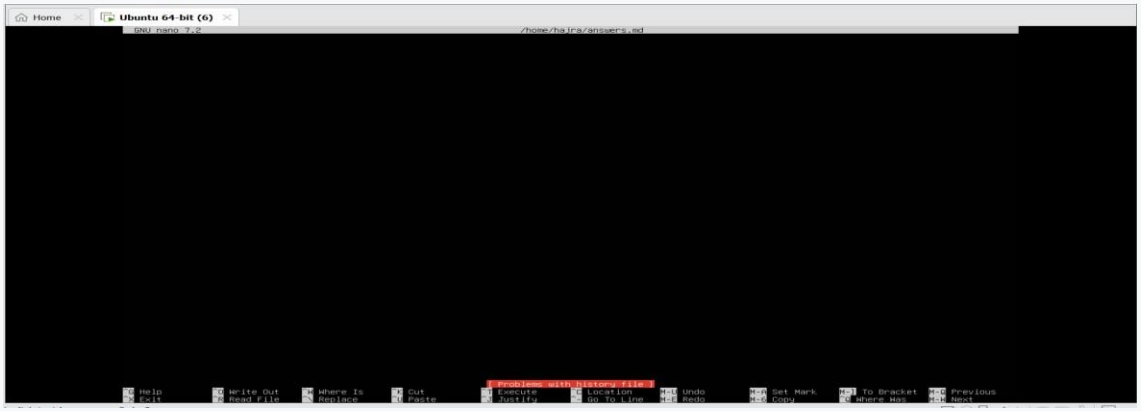


3. List your home directory and show hidden (dot) files:
   ls -la ~

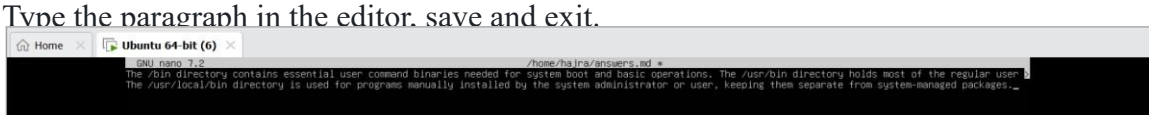
```
hajra@ubuntu-lab:~$ ls -la $HOME
total 48
drwxr-x--- 5 hajra hajra 4096 Oct 23 04:41  .
drwxr-xr-x 3 root  root  4096 Sep 26 21:38  ..
-rw-r--r-- 1 hajra hajra  220 Mar 31  2024  .bash_logout
-rw-r--r-- 1 hajra hajra 3771 Mar 31  2024  .bashrc
drwx------ 2 hajra hajra 4096 Sep 26 21:40  .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41  fesswr
-rw------- 1 hajra hajra   20 Sep 26 22:08  .lesshst
-rw-r--r-- 1 hajra hajra  807 Mar 31  2024  .profile
drwx------ 2 hajra hajra 4096 Sep 26 22:00  .ssh
-rw-r--r-- 1 hajra hajra    0 Sep 26 21:48  .sudo_as_admin_successful
-rw-r--r-- 1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$
```

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.

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

Task 4: Essential CLI Tasks — Navigation and File Operations

Steps Performed

1. **Create a Workspace and Navigate**

   mkdir -p ~/lab4/workspace/python_project

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

   Created a new workspace directory for the Python project.

   cd ~/lab4/workspace/python_project

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

Navigated into the newly created directory.

Pwd

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

Verified the current working directory path.

---

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

README.md

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

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

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

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

Created a copy of the README file.

mv README.copy.md README.dev.md

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

Renamed (moved) the copied file.

rm README.dev.md

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

Deleted the renamed file.

---

5. **Work with Directories**

mkdir -p ~/lab4/workspace/java_app

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ mkdir -p $HOME/laab4/workspace/java_app
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

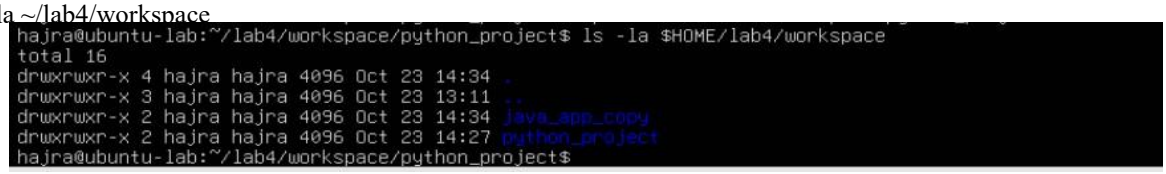
Created another directory for a Java app.

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

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

Copied the entire Python project directory recursively.

ls -la ~/lab4/workspace



Verified the copied directories.

---

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

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

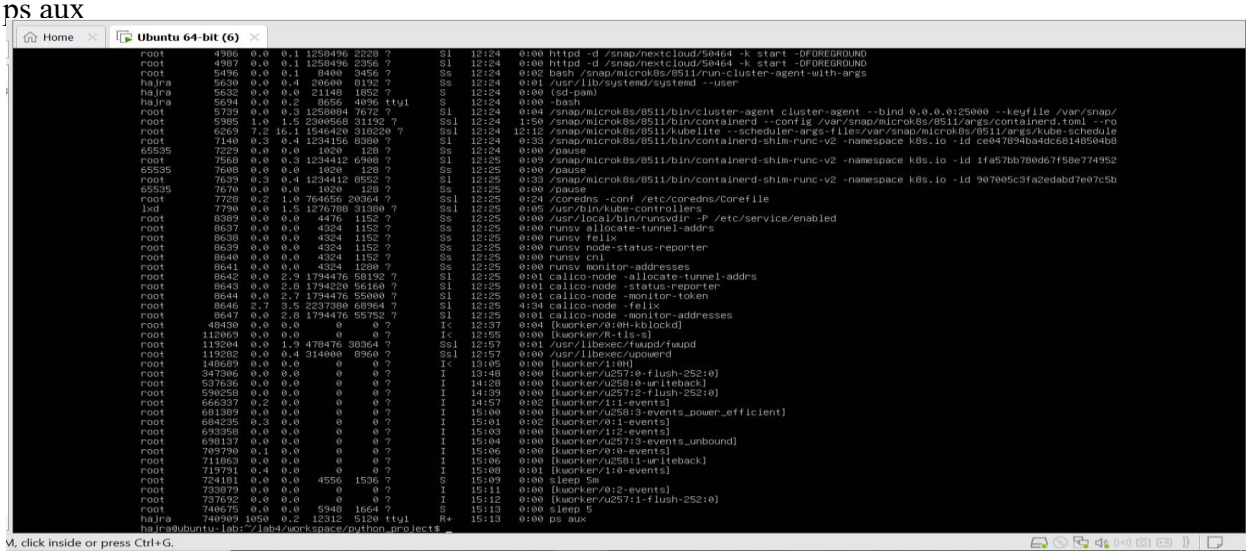
4. Disk:
   df -h

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ 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_project$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              192M  1.6M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   12G   11G  343M  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
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/ce047894ba4dc68148504b884d
dbe81bfeef7c1524cd31f3f71c0866c562fc57/shm
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/907005c3fa2edabd7e07c5bb55
f734ead13372884c9de10e7c3258af5f4114e6/shm
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/1fa57bb780d67f58e774952f1e
e1858625b771458a25591d41300447ba4e2367/shm
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

5. View OS release information:
   cat /etc/os-release

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

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

```
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)" uptime

free -h
```

```
  GNU nano 7.2                                  /home/hajra/lab4/workspace/python_project/run-demo.sh *
#!/bin/bash
echo 'Lab 4 demo: current user is $(whoami)'
echo 'Currrent 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)
Currrent 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

```
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)
Currrent 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:

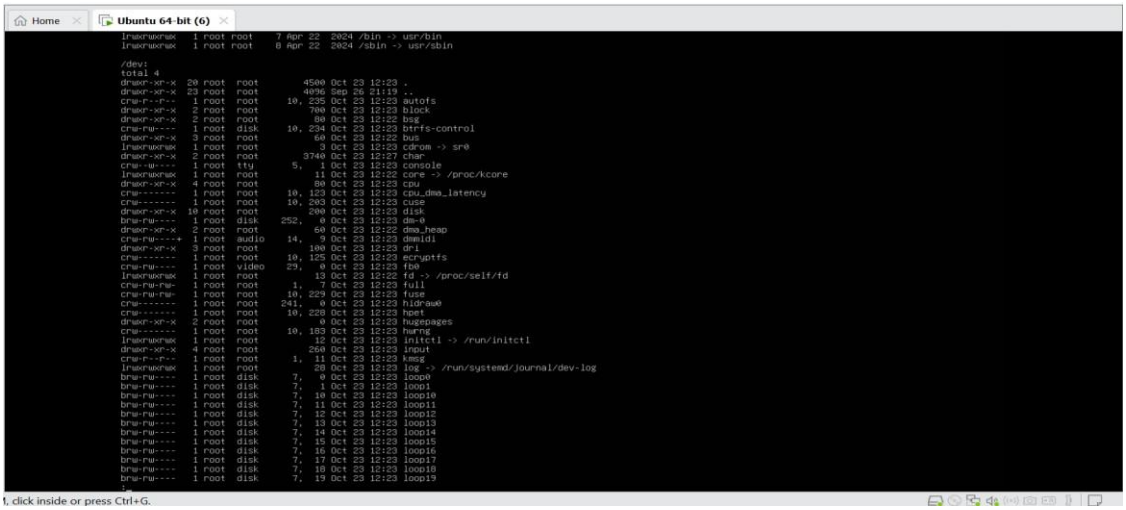
1. Display the contents of the root directory.

```
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
drwx------ 2 hajra hajra 4096 Sep 26 21:40  .cache
-rw------- 1 hajra hajra   20 Sep 26 22:08  .lesshst
-rw-r--r-- 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. 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 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_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 $HOME
total 48
drwxr-x--- 5 hajra hajra 4096 Oct 23 04:41  .
drwxr-xr-x 3 root  root  4096 Sep 26 21:38  ..
-rw-r--r-- 1 hajra hajra  220 Mar 31  2024  .bash_logout
-rw-r--r-- 1 hajra hajra 3771 Mar 31  2024  .bashrc
drwx------ 2 hajra hajra 4096 Sep 26 21:40  .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41  fesmdr
-rw------- 1 hajra hajra   20 Sep 26 22:08  .lesshst
-rw-r--r-- 1 hajra hajra  807 Mar 31  2024  .profile
drwx------ 2 hajra hajra 4096 Sep 26 22:00  .ssh
-rw-r--r-- 1 hajra hajra    0 Sep 26 21:48  .sudo_as_admin_successful
-rw-r--r-- 1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$
```

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
       ```

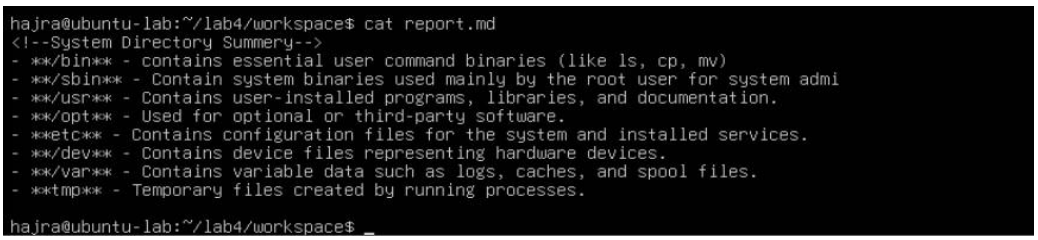
    2. Create and open a new Markdown file using **nano editor**:
       nano report.md

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

    3. Inside nano, type your short summary.

       ```
         GNU nano 7.2                                                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**.
    5. Verify your file exists and display its contents:
       cat report.md



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

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

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

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

Created a copy of the README file.

mv README.copy.md README.dev.md

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

Renamed (moved) the copied file.

rm README.dev.md

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

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_project$ mkdir -p $HOME/laab4/workspace/java_app
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

Created another directory for a Java app.

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

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

Copied the entire Python project directory recursively.

ls -la ~/lab4/workspace

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

Verified the copied directories.

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ 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/laab4/workspace/java_app
   16  cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/java_app_copy
   17  ls -la $HOME/lab4/workspace
   18  history
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _
```

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

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

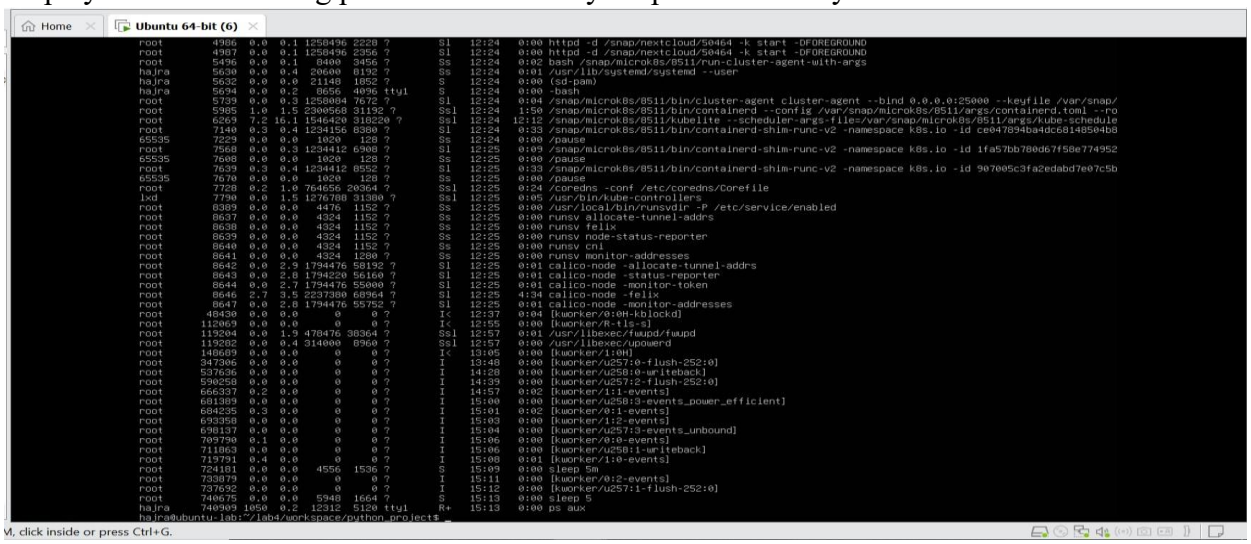
1. Display the system's OS and kernel version for the investigation report.

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

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:~$ _
```

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



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.

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

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