

**Cloud Computing BSE-VB**

**Submitted By**

Tooba Shafique (2023-BSE-065)

**Submitted to**

Sir Shoaib

**LAB-04**

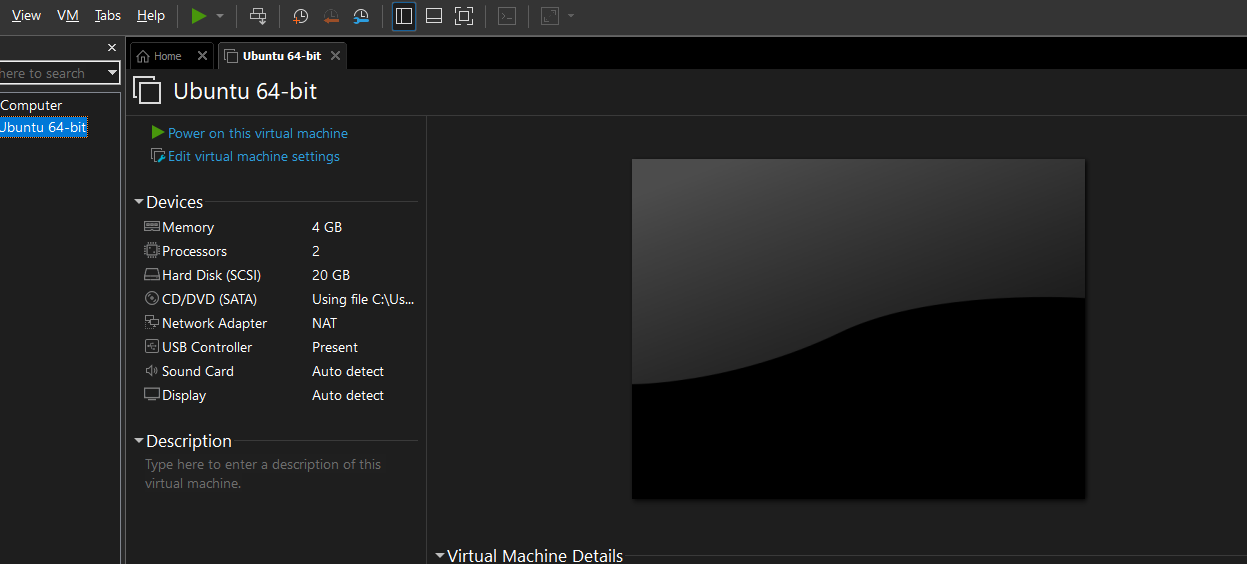
**Task 1 – Verify VM Resources in VMware**

**Step 1:** Open VMware Workstation and locate the Ubuntu Server VM used in Lab 1.

**Step 2:** Inspect the VM settings and note the following details:

* VM Name
* RAM
* CPU
* Disk
* Network Adapter Type

**Screenshot:** vm\_settings.png



**Task 2 – Start VM and Log In (Use Your Preferred Host Terminal Method Only)**

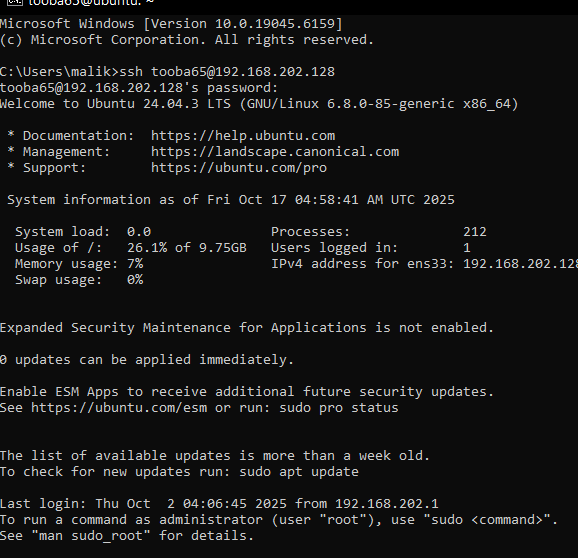
**Step 1:** Start or resume the VM in VMware Workstation on your host system.

**Step 2:** Open your preferred terminal on the host (e.g., Command Prompt, PowerShell, macOS Terminal, or Linux Terminal).

**Step 3:** Connect to the VM using SSH.

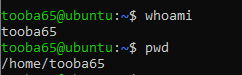
**Step 4:** After connecting, capture a screenshot showing the SSH login prompt or connection result.  
**Screenshot:** vm\_login.png

ssh tooba65@192.168.202.128



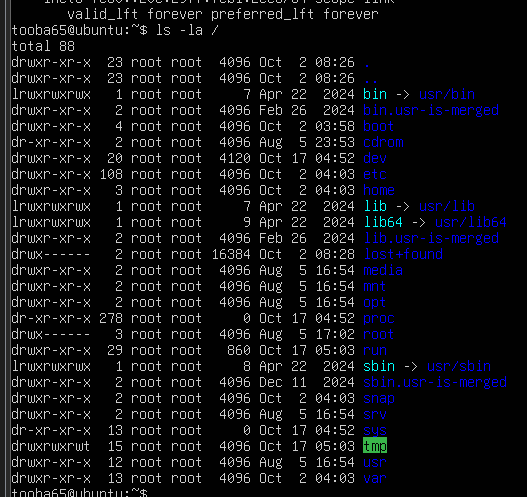
**Step 5:** Run both commands — whoami and pwd — in the same terminal window.

**Step 6:** Capture a single screenshot showing the outputs of both commands.  
**Screenshot:** whoami\_pwd.png



**Task 3 – Filesystem Exploration — Root Tree and Dotfiles**

**Step 1:**

  
**Screenshot:**

**Step 2:**   
**Screenshot:** os\_release.png



**Step 3:** Inspect these directories (run each command and screenshot the output):

ls -la /bin

* Save screenshot as ls\_bin.png



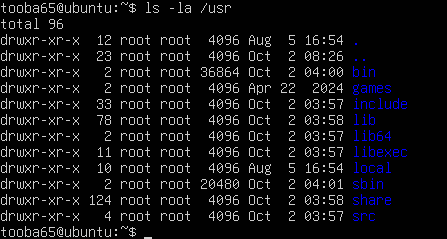
ls -la /sbin

* Save screenshot as ls\_sbin.png



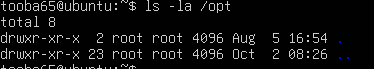
ls -la /usr

* Save screenshot as ls\_usr.png



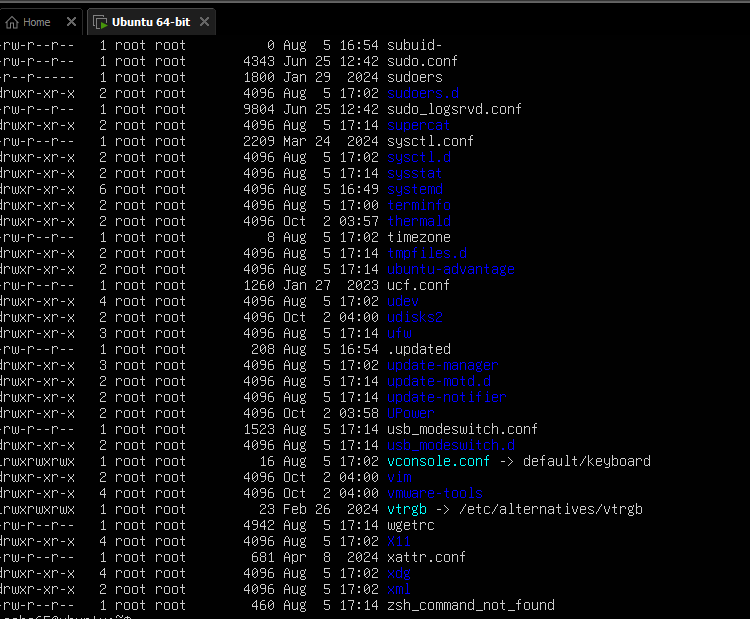
ls -la /opt

* Save screenshot as ls\_opt.png



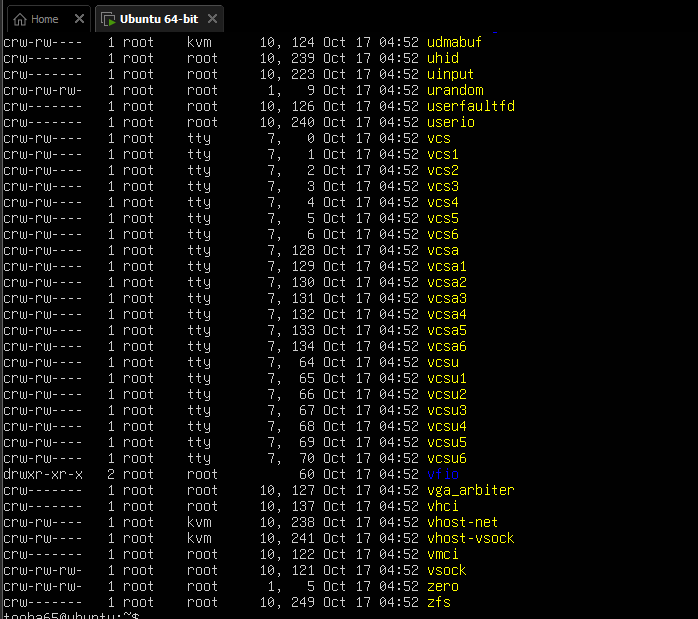
ls -la /etc

* Save screenshot as ls\_etc.png



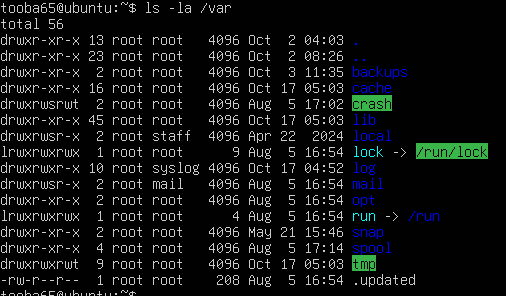
ls -la /dev

* Save screenshot as ls\_dev.png



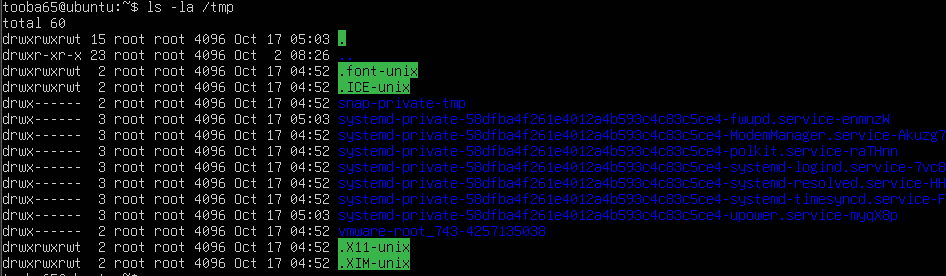
ls -la /var

* Save screenshot as ls\_var.png

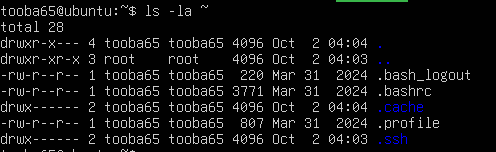


ls -la /tmp

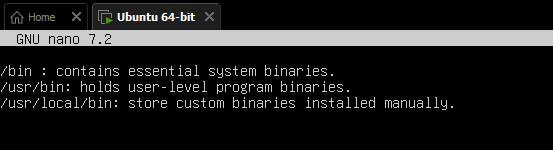
* Save screenshot as ls\_tmp.png



**Step 4:** List your home directory and show hidden (dot) files  
**Screenshot:** home\_ls.png



**Step 5:** Write a short paragraph (3–5 sentences) explaining the difference between /bin, /usr/bin, and /usr/local/bin.  
Open a text editor inside the terminal to write and save your explanation.  
**Screenshot:** answers\_md.png



**Task 4 – Essential CLI Tasks — Navigation and File Operations**

**Steps**

**Step 1:**  
Create a workspace directory.  
Save screenshot as: **mkdir\_workspace.png**



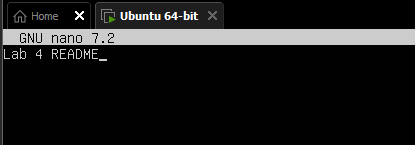
**Step 2:**  
Navigate to the newly created directory.  
Save screenshot as: **cd\_workspace.png**



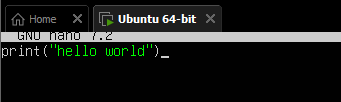
**Step 3:**  
Display your current directory path.  
Save screenshot as: **pwd\_workspace.png**



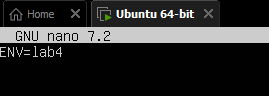
**Step 4:**  
Create a new file using nano editor named README.md and type:  
Lab 4 README  
Save screenshot as: **nano\_readme.png**



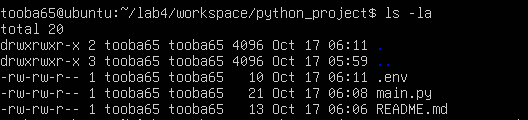
**Step 5:**  
Create another file using nano editor named main.py and type:  
print("hello lab4")  
Save screenshot as: **nano\_main.png**



**Step 6:**  
Create an environment file named .env and type:  
ENV=lab4  
Save screenshot as: **nano\_env.png**



**Step 7:**  
List all files (including hidden ones) in the current directory.  
Save screenshot as: **workspace\_ls.png**



**Step 8:**  
Copy the README file to a new file named README.copy.md.  
Save screenshot as: **cp\_readme.png**



**Step 9:**  
Rename (move) the copied file to README.dev.md.  
Save screenshot as: **mv\_readme.png**



**Step 10:**  
Remove the README.dev.md file.  
Save screenshot as: **rm\_readme.png**



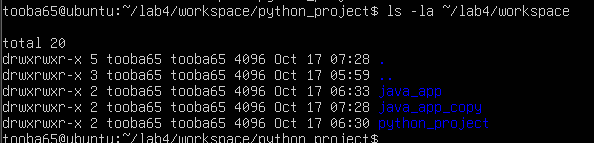
**Step 11:**  
Create a new directory for Java work:  
java\_app  
Save screenshot as: **mkdir\_java\_app.png**



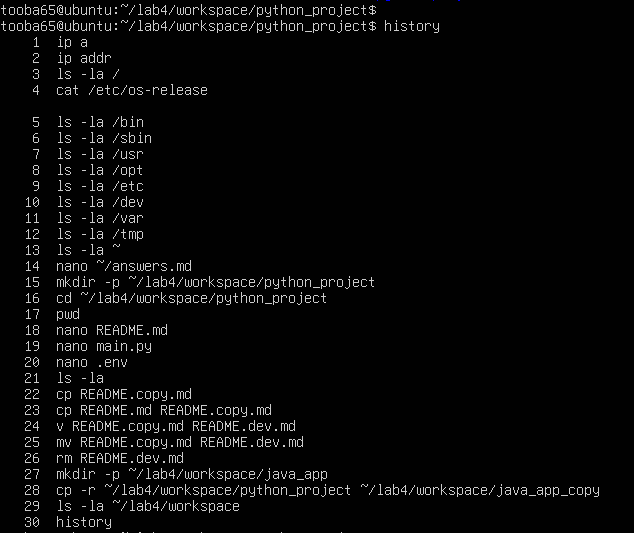
**Step 12:**  
Copy the entire python\_project folder into a new folder named java\_app\_copy.  
Save screenshot as: **cp\_recursive.png**



**Step 13:**  
List all directories inside workspace to verify the copy.  
Save screenshot as: **copy\_verify.png**



**Step 14:**  
Show recent command history.  
Save screenshot as: **history.png**



**Step 15:**  
Demonstrate tab completion (start typing a filename and press **Tab** to auto-complete).  
Save screenshot as: **tab\_completion.png**



**Task 5 – System info, resources & processes**

Collect system information and observe processes. Use screenshots only.

**Steps (inside VM terminal)**

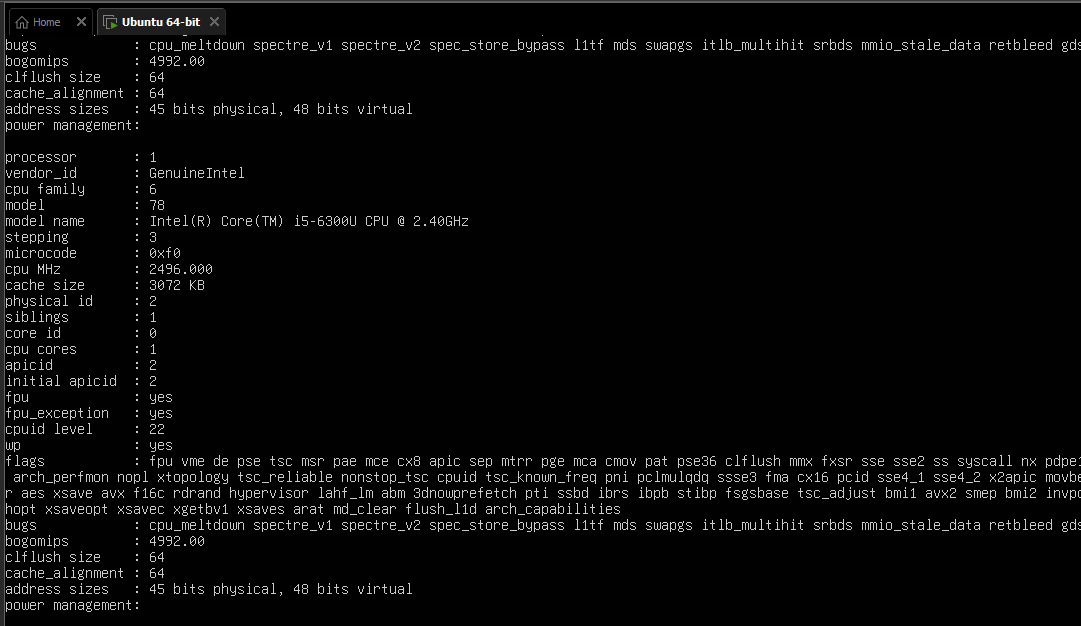
**Step 1:** Kernel and OS

Save screenshot as uname.png.



**Step 2:** CPU (ensure model name visible):

Save screenshot as cpuinfo.png.



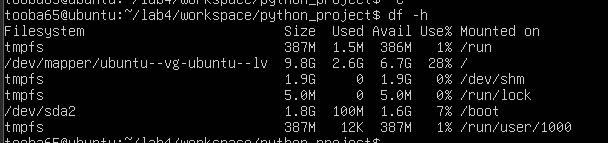
**Step 3:** Memory:

Save screenshot as meminfo.png.



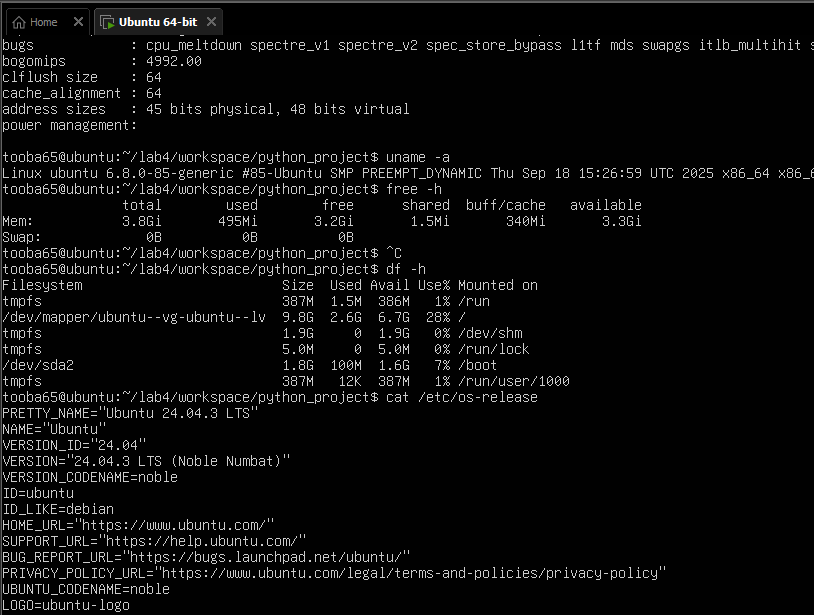
**Step 4:** Disk:

Save screenshot as diskinfo.png.



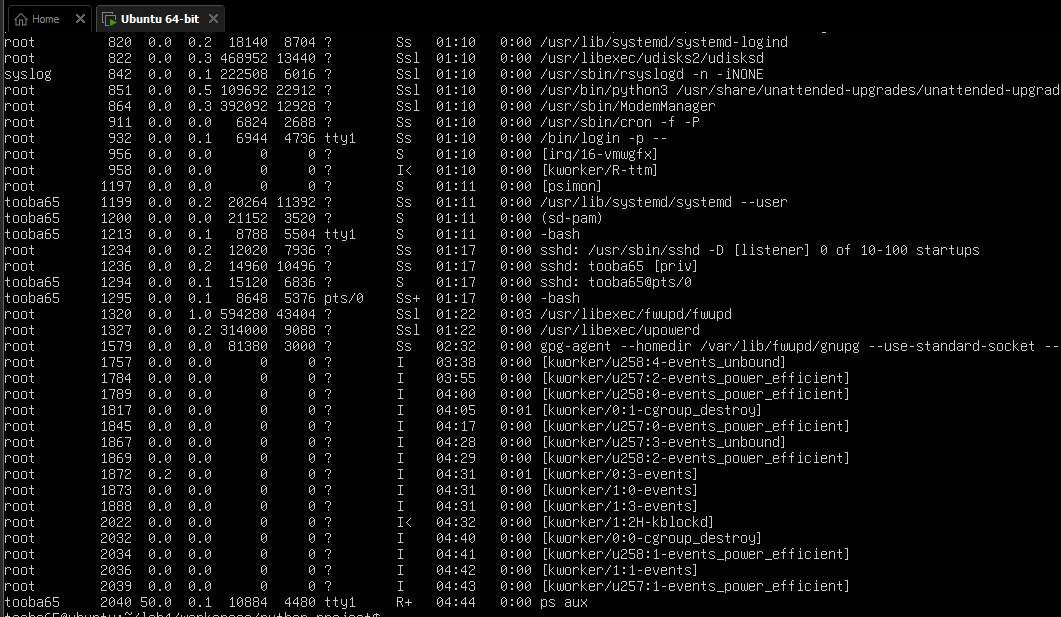
**Step 5:** Os Release:

Save screenshot as os-release.png.



**Step 6:** Processes (show top lines of ps output):

* Save screenshot as processes.png



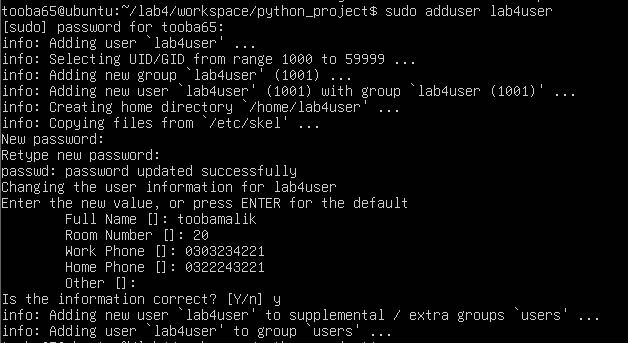
**Task 6 – Users and account verification (no sudo group change)**

Create a non‑root user and verify the account exists. This task does NOT add the created user to the sudo group.

**Steps (inside VM terminal)**

**Step 1:** Create a new user named lab4user:

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



**Step 2:** Verify the user entry:

* Save screenshot as lab4user\_passwd.png.



**Step 3:** Switch to the new user to verify login:

* Save screenshot as su\_lab4user.png.



**Step 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.:

* Save screenshot as sudo\_whoami.png.



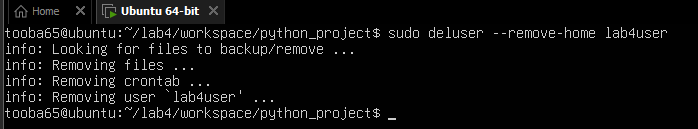
**Step 5:** Return to the original user:

* Save screenshot as exit\_back.png.
* When I exit it moves to the original user.



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

* If run, save screenshot as deluser.png.



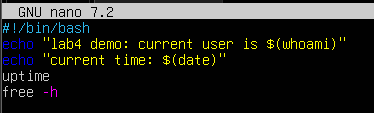
**Bonus Task 7 – Create a small demo script using an editor and run it**

This task is optional — complete it for extra practice or extra credit. It is not required for passing the core lab tasks.

**Steps (inside VM)**

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

* Type the following lines into the editor (manually or paste), save and exit:
* Save screenshot of the editor after saving the file as nano\_run\_demo.png.



**Step 2:** Make the script executable:

* Save screenshot as chmod\_run\_demo.png.



**Step 3:** Run the script as your regular user:

* Save screenshot of the script output as run\_demo\_output.png.



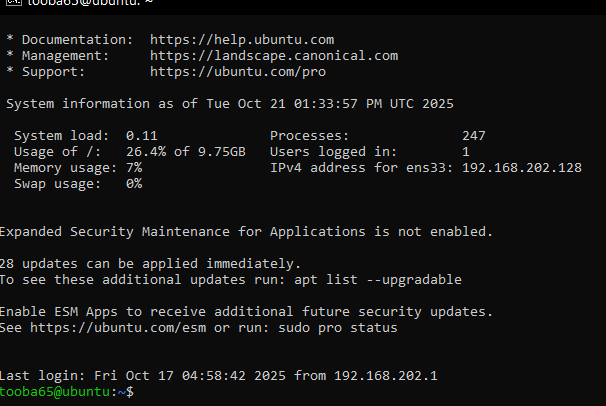
**Exam Evaluation Questions**

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

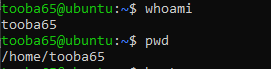
**Scenario:**  
You are part of a SOC (Security Operations Center) investigating unauthorized access to a Linux server hosted on VMware. Prove you can securely connect and verify your identity.

**Steps:**

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



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



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

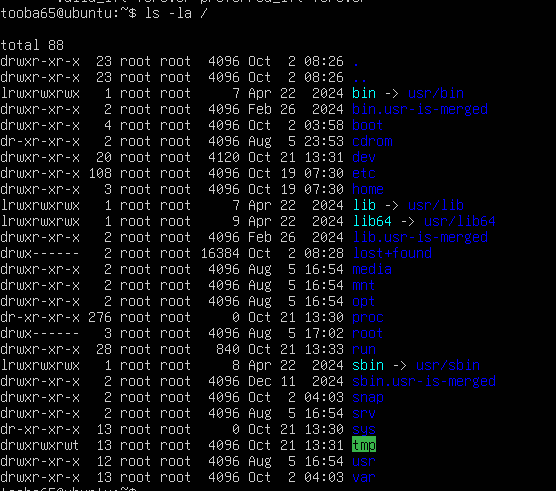


**2. Filesystem Inspection for Forensic Evidence**

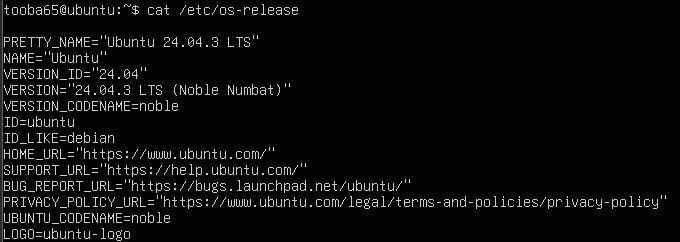
**Scenario:**  
The incident response team suspects malicious files in system directories. You must explore the filesystem to locate and document the system’s structure.

**Steps:**

1. Display the contents of the root directory.
   * Screenshot as Q2\_root\_listing.png



1. Display the OS version and release information.
   * Screenshot as Q2\_os\_version.png



1. Explore and record directory listings for /bin, /sbin, /usr, /opt, /etc, /dev, /var, and /tmp.
   * Screenshot as Q2\_directory\_evidence.png

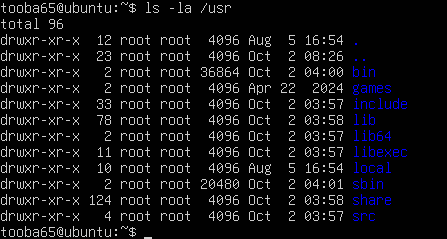
ls -la /bin



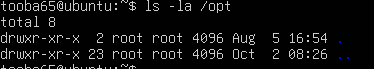
ls -la /sbin



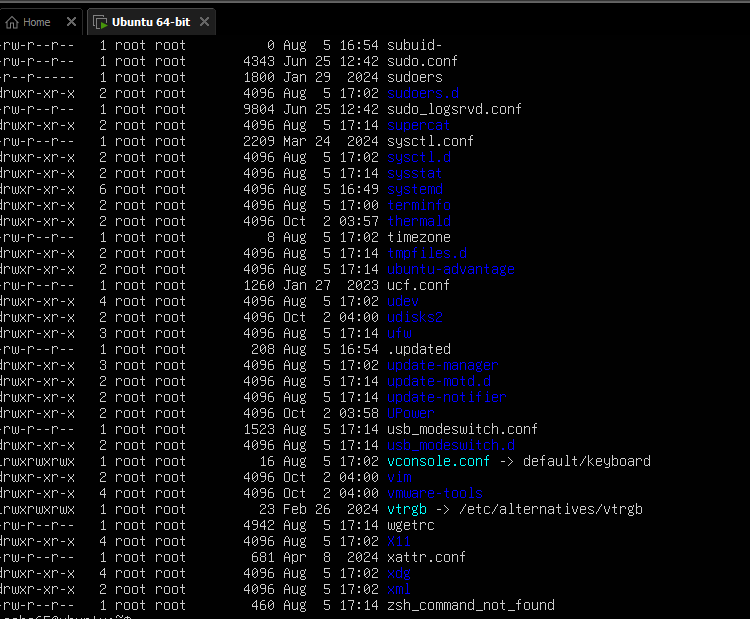
ls -la /usr



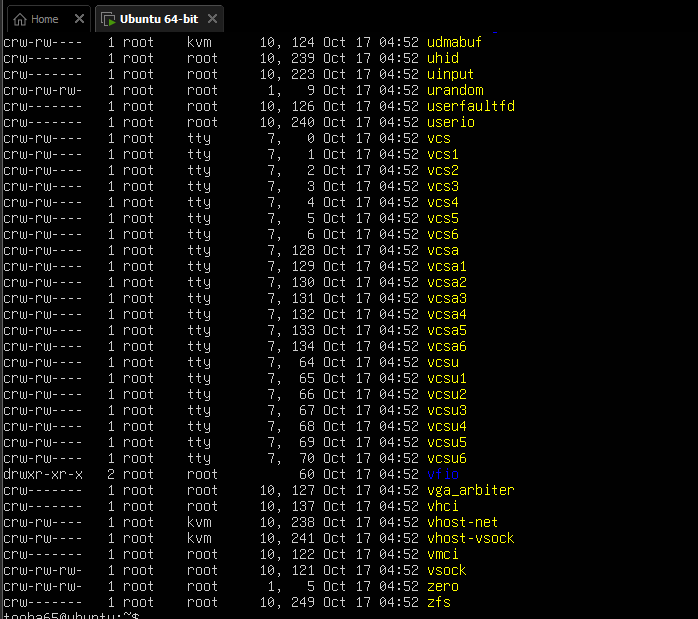
ls -la /opt



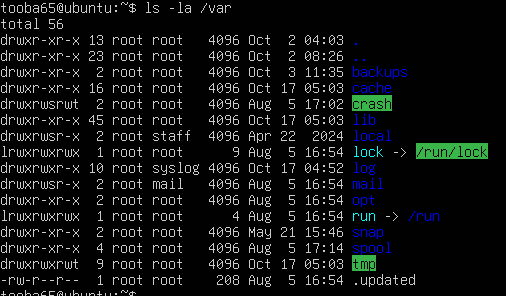
ls -la /etc



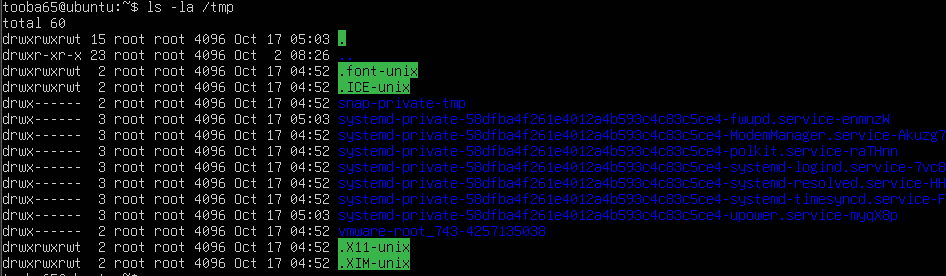
ls -la /dev



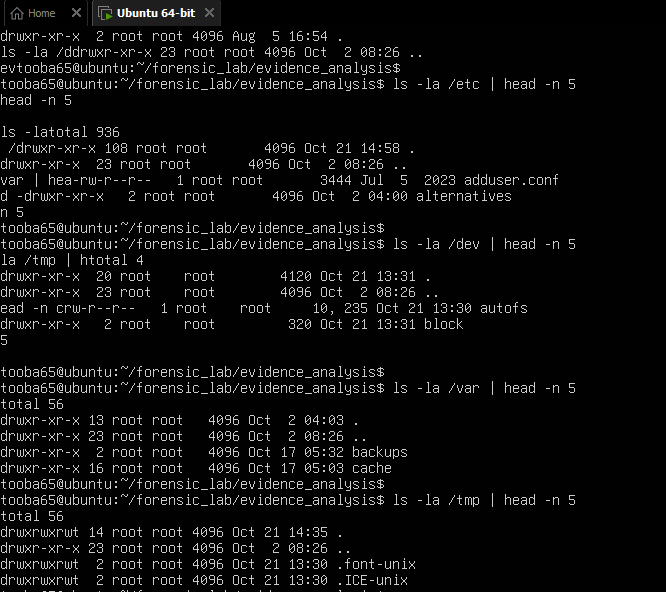
ls -la /var



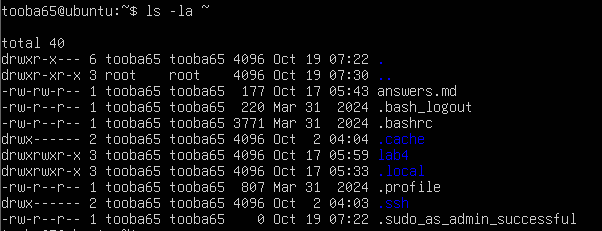
ls -la /tmp



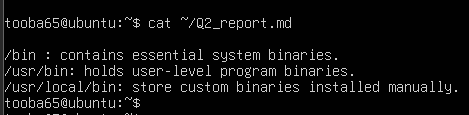
Here I print directory name + top few entries for each, all in one terminal view.



1. Display all hidden files in your home directory.
   * Screenshot as Q2\_hidden\_files.png



1. Create a markdown file summarizing your findings on key binary directories.
   * Screenshot as Q2\_report\_file.png



**3. Evidence Handling & File Operations**

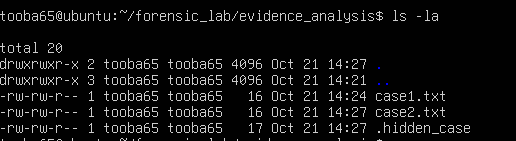
**Scenario:**  
You are creating a sandbox environment to safely analyze and handle suspicious files collected from a compromised system.

**Steps:**

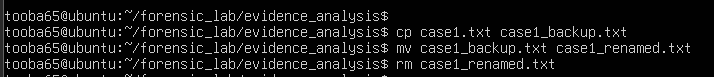
1. Create a structured folder hierarchy under your home directory for analysis.
   * Screenshot as Q3\_workspace\_created.png



1. Create three text files, including one hidden file, in your workspace.
   * Screenshot as Q3\_files\_created.png



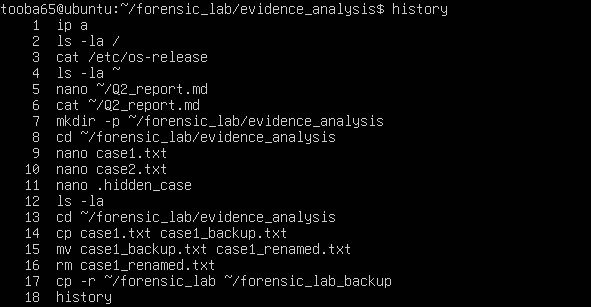
1. Create a backup copy of one file, rename it, and then delete it after verification.
   * Screenshot as Q3\_backup\_handling.png



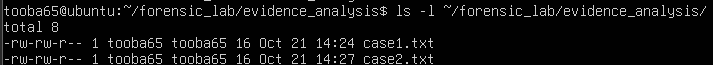
1. Copy the entire workspace as an evidence backup folder.
   * Screenshot as Q3\_workspace\_backup.png



1. Display your command history to document all actions performed.
   * Screenshot as Q3\_command\_history.png



1. Demonstrate Linux auto-completion by typing a partial command or filename.
   * Screenshot as Q3\_autocomplete.png



**4. System Profiling and Process Monitoring**

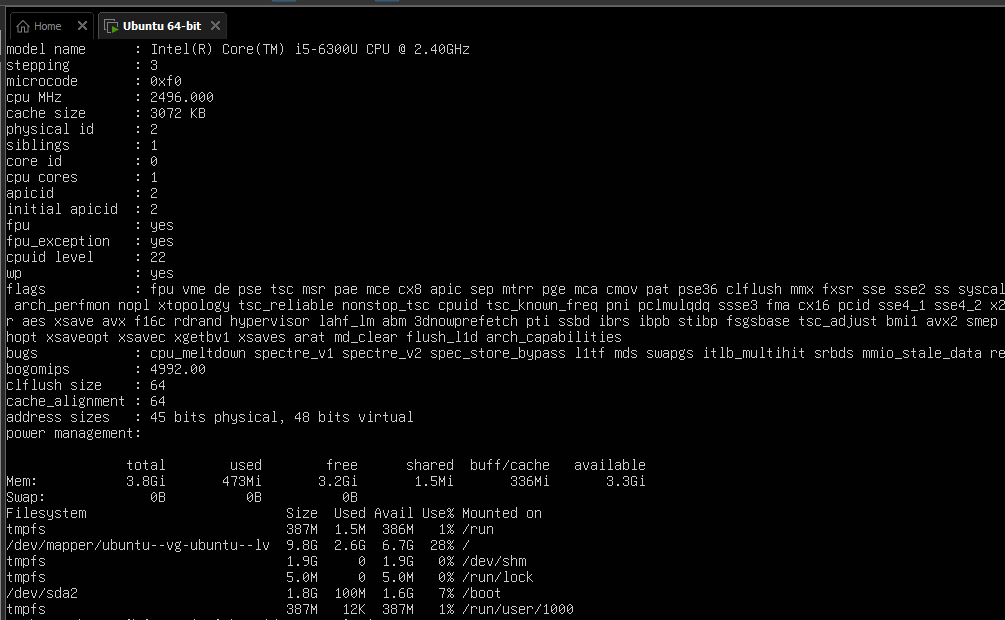
**Scenario:**  
You are investigating a potential malware infection that is consuming excessive resources on the Linux VM.

**Steps:**

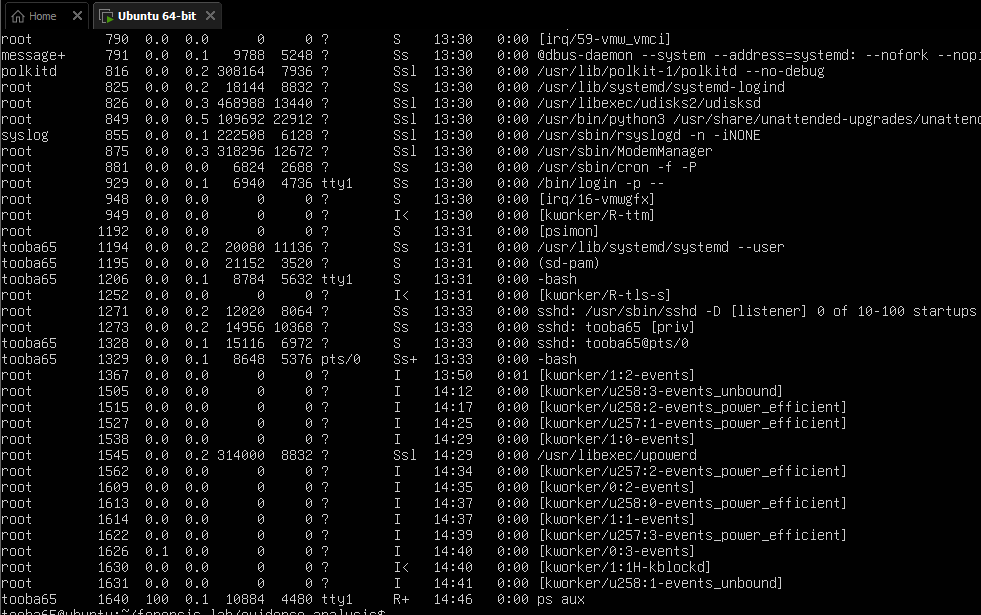
1. Display the system’s OS and kernel version for the investigation report.
   * Screenshot as Q4\_system\_info.png



1. Display CPU, memory, and disk usage information.
   * Screenshot as Q4\_resource\_info.png



1. Display all active running processes to identify suspicious activity.
   * Screenshot as Q4\_process\_list.png

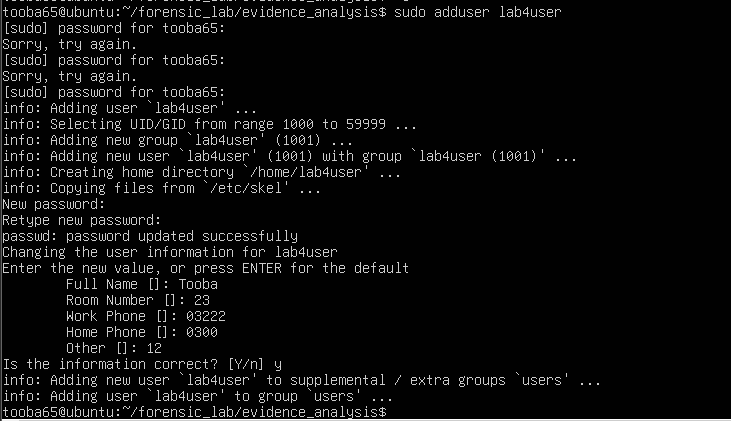


**5. User Account Audit & Privilege Escalation Simulation**

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



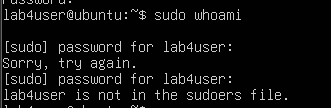
1. Verify that the new user record exists in the system’s user database.
   * Screenshot as Q5\_user\_verified.png



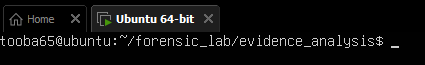
1. Log in as lab4user and confirm successful login.
   * Screenshot as Q5\_user\_login.png



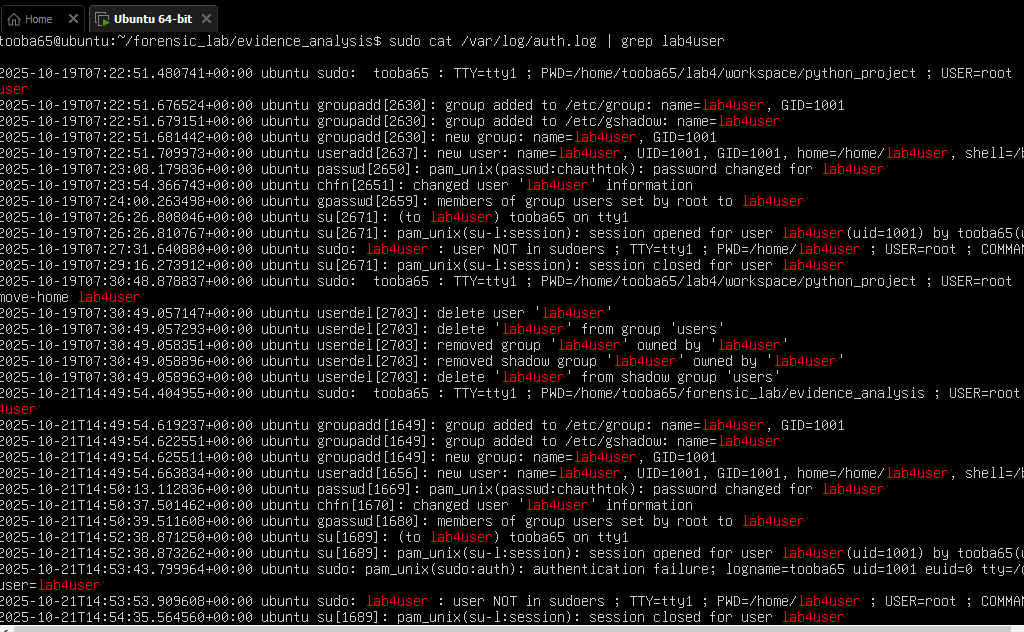
1. Attempt to run an administrative command as lab4user (expect permission denied).
   * Screenshot as Q5\_permission\_denied.png



1. Switch back to your main analyst account.
   * Screenshot as Q5\_switch\_back.png



1. Inspect the system authentication logs located at /var/log/auth.log to determine whether the lab4user account attempted any logins (successful or failed).
   * Screenshot as Q5\_authlog\_analysis.png



1. (Optional) Remove the lab4user account after the audit and verify deletion.
   * Screenshot as Q5\_user\_removed.png

