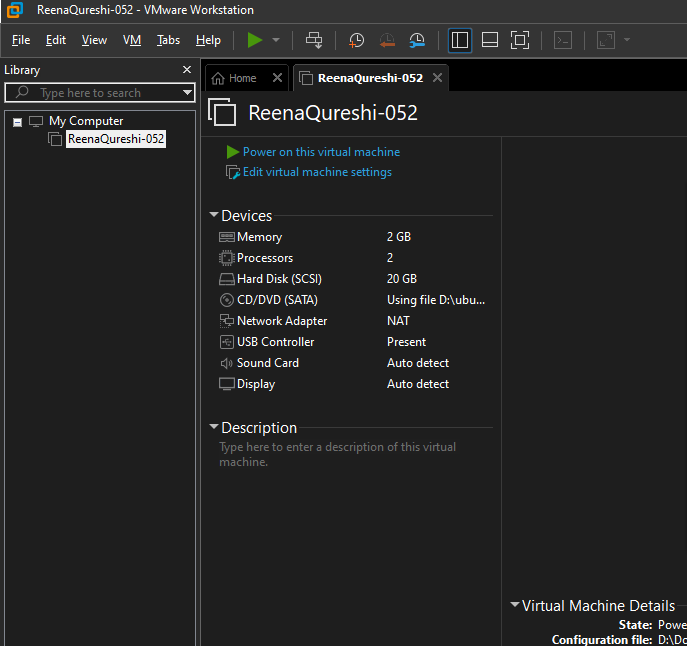
# Name : Reena Qureshi

# Reg No : 2023-BSE-052

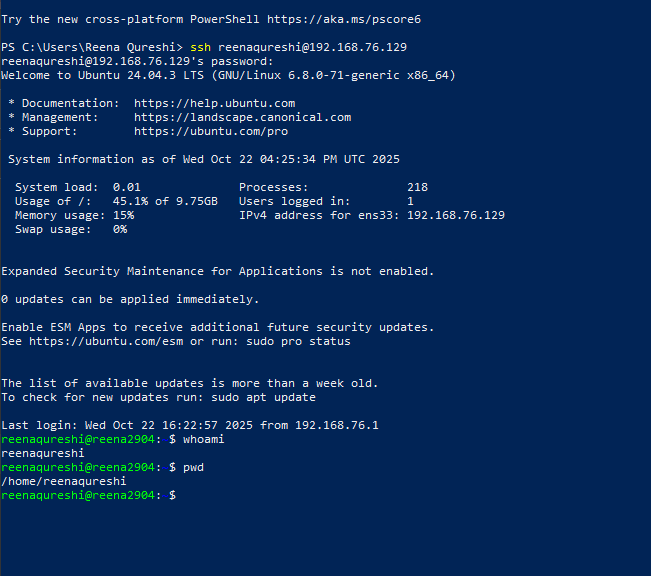
# Section : V-B

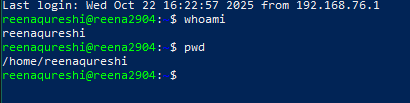
**Lab 4**

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



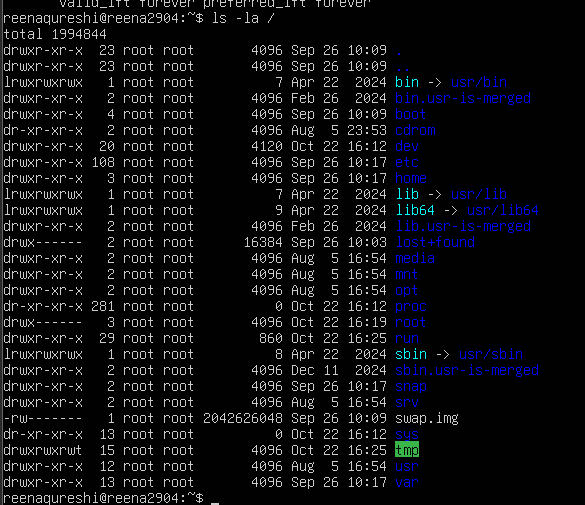
**Task 2 – Start VM and log in (use your preferred host terminal method only)**





**Task 3 – File system exploration — root tree and dot files**

List root directory contents:



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

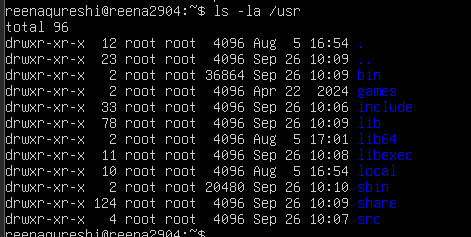
**ls -la /bin**



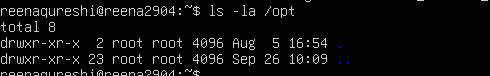
**ls -la /sbin**



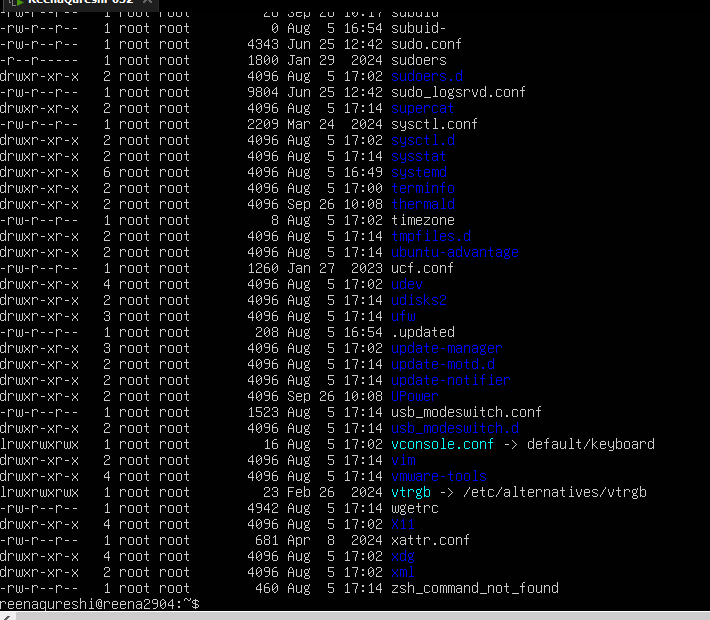
**ls -la /usr**



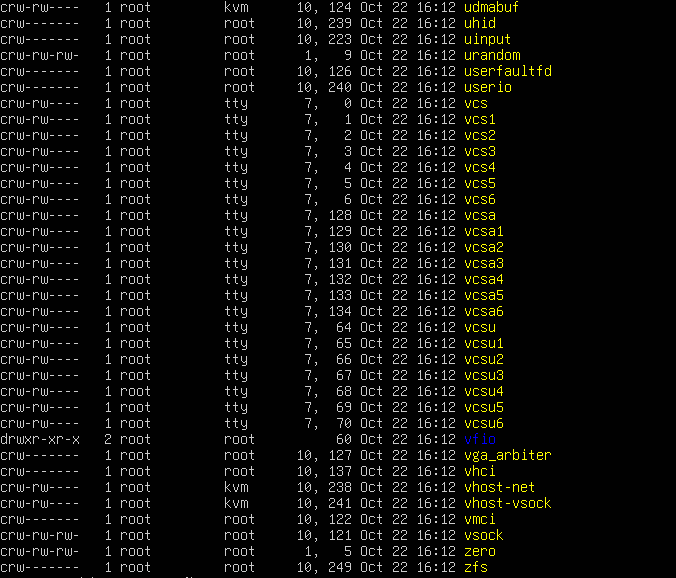
**ls –la /opt**



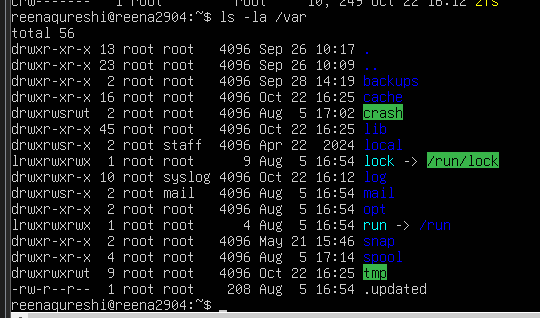
**ls -la /etc**



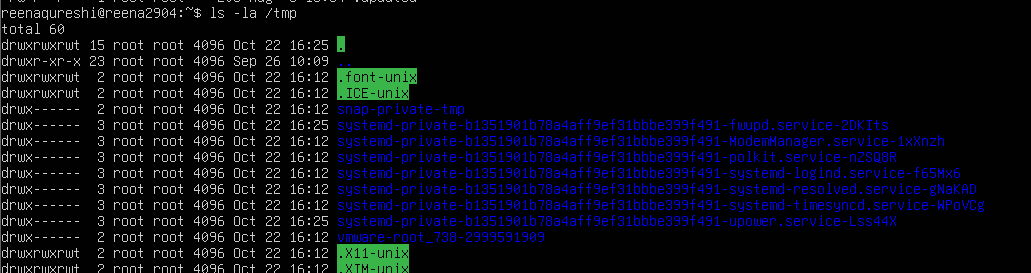
**ls -la /dev**



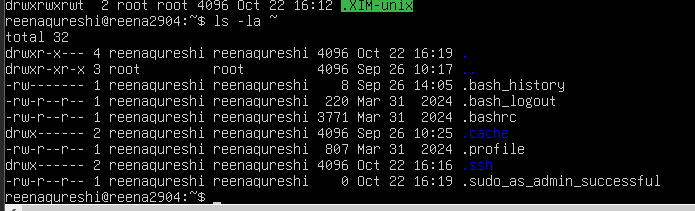
**ls –la /var**



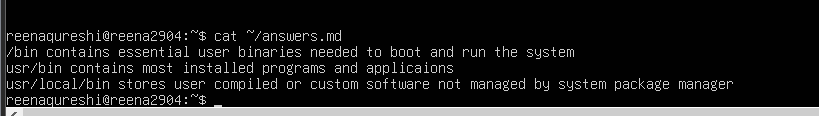
**ls –la /tmp**



**ls –la ~**



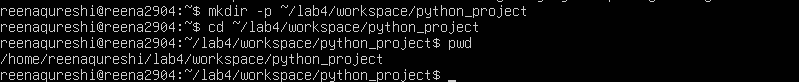
**nano ~/answers.md**



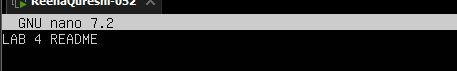
**Task 4 – Essential CLI tasks — navigation and file operations**

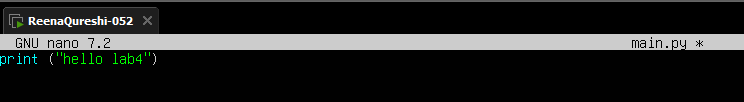
Create a workspace and navigate.

**mkdir -p ~/lab4/workspace/python\_project**

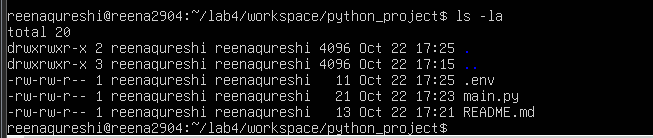


Create files using an editor (open each editor session and save a screenshot showing content):

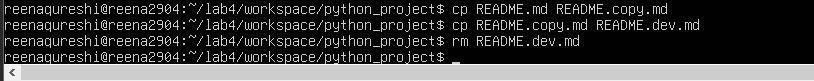




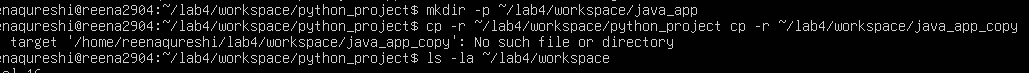
List files and capture:

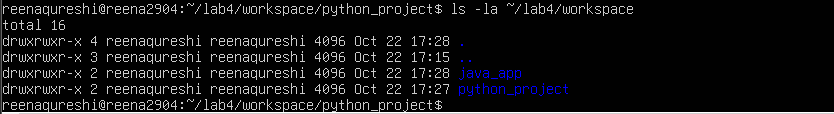


Copy, move and remove:

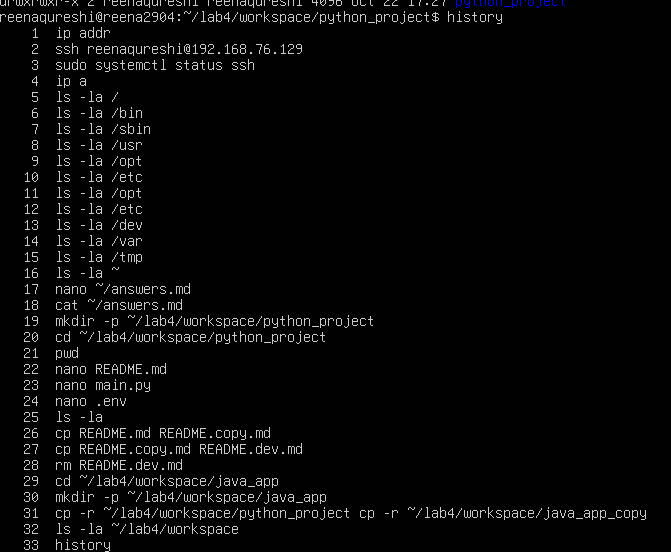


mkdir -p ~/lab4/workspace/java\_app





Use command history and tab completion



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

Kernel and OS:

uname -a



CPU (ensure model name visible):

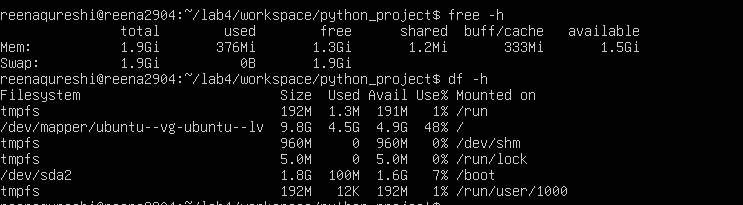
cat /proc/cpuinfo



Memory:

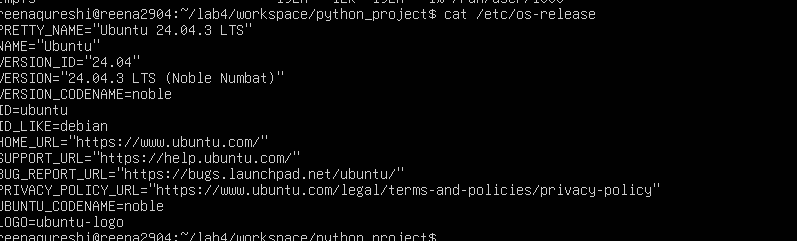


Disk:

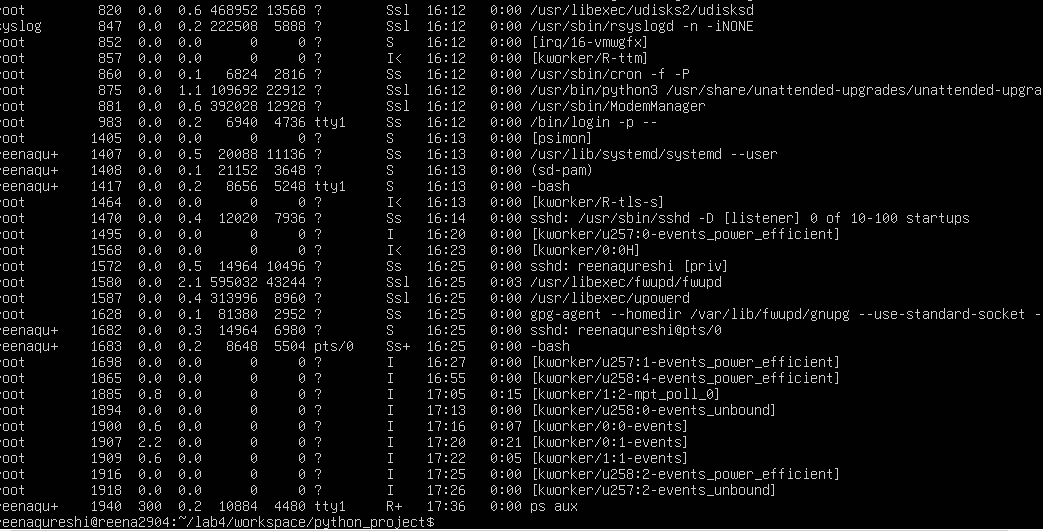


View OS release information:

cat /etc/os-release



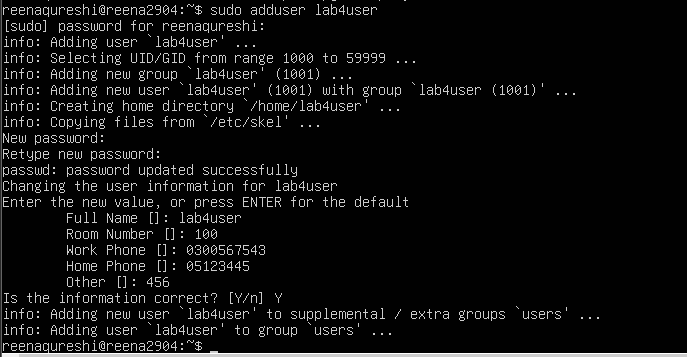
Processes (show top lines of ps output):



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

Create a new user named lab4user:

sudo adduser lab4user



Verify the user entry:

getent passwd lab4user



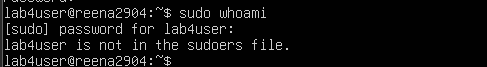
Switch to the new user to verify login:

su - lab4user



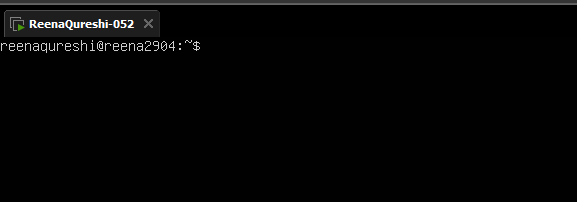
From the new user you may attempt a sudo command to show that sudo is not available for this account (expected failure), e.g.:

sudo whoami



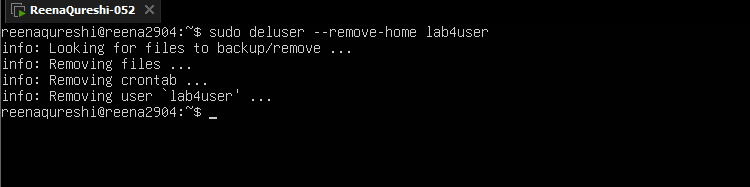
Return to the original user:

exit



(Optional) Remove the test user when finished:

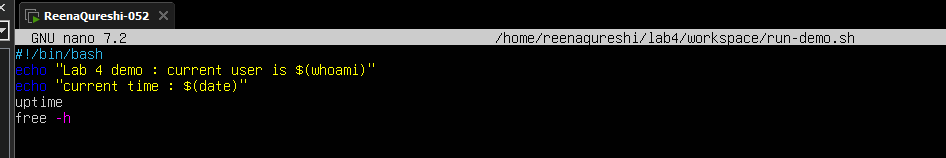
sudo deluser --remove-home lab4user



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

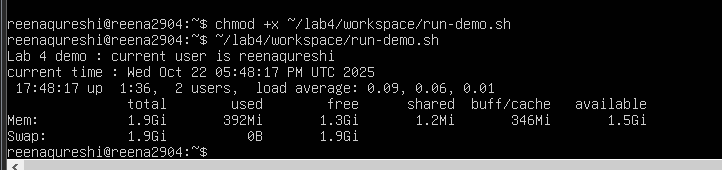
Open an editor to create the script:

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



Make the script executable:

Run the script as your regular user:

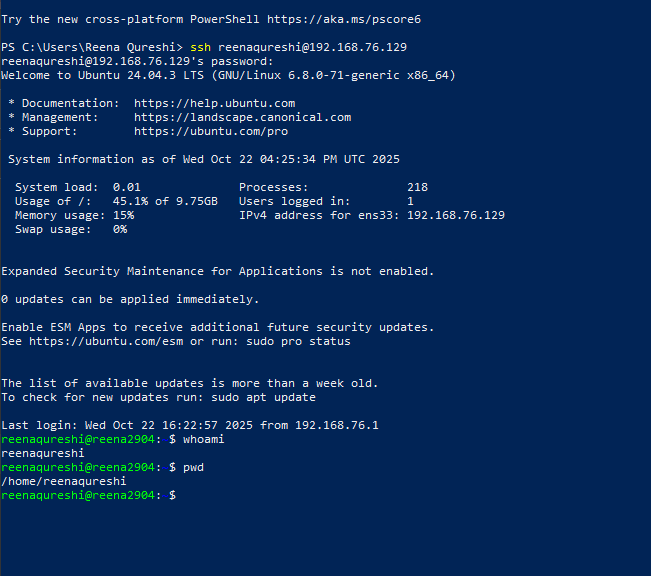


**Exam Evaluation Questions**

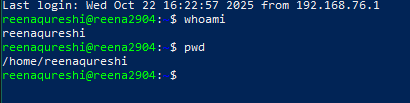
1. Remote Access Verification (Cyber Login Check)

**Steps:**

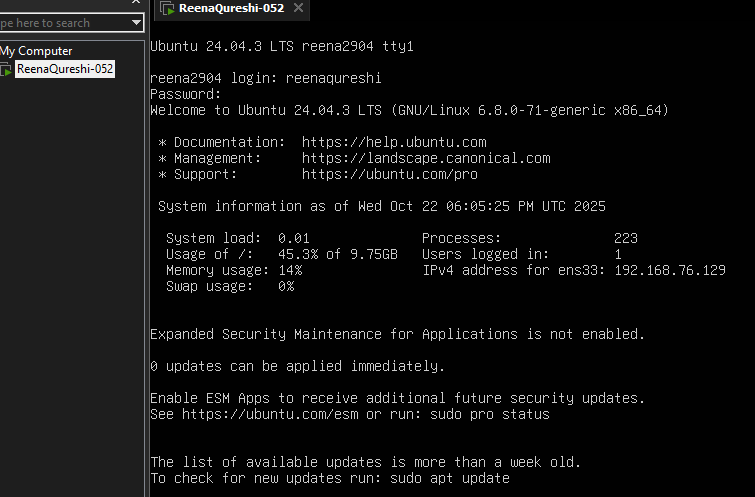
Connect to the Ubuntu VM remotely from your host terminal.



Verify your current user and home directory path



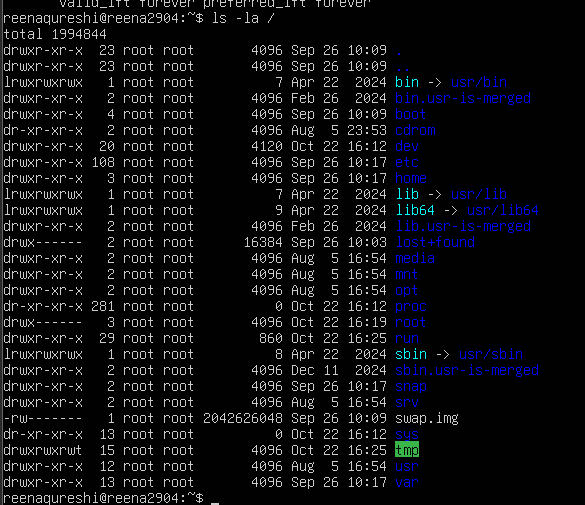
Confirm you are connected to the correct host machine



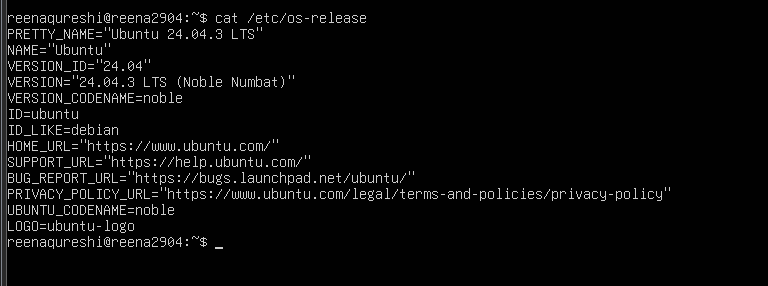
2. Filesystem Inspection for Forensic Evidence

**Steps:**

Display the contents of the root directory.



Display the OS version and release information



Explore and record directory listings for /bin, /sbin

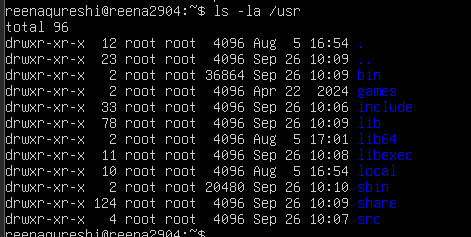
ls -la /bin



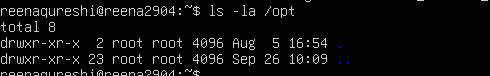
ls -la /sbin



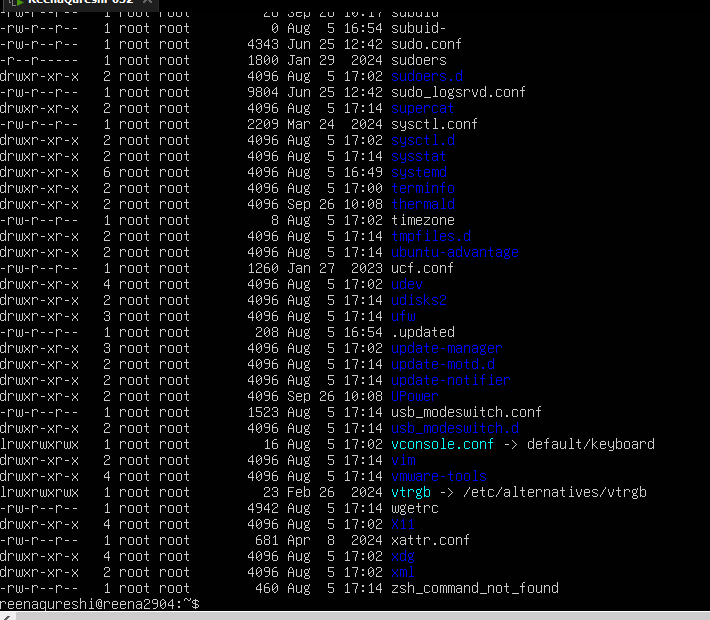
ls -la /usr



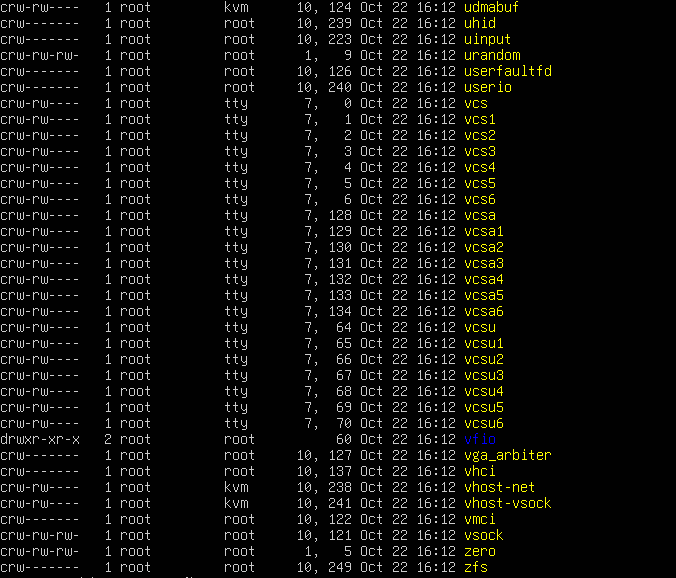
ls –la /opt



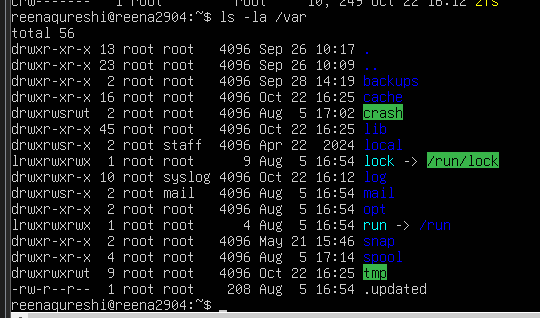
ls -la /etc



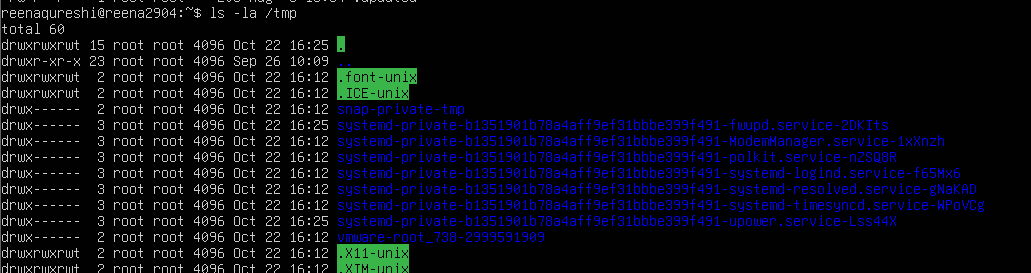
ls -la /dev



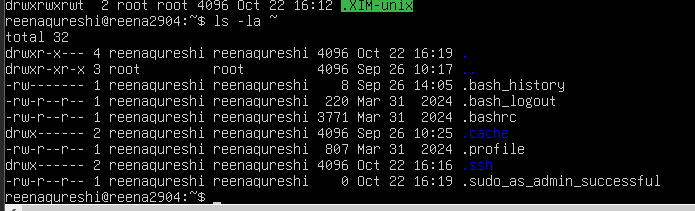
ls -la /var



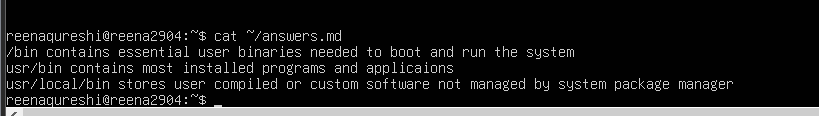
ls -la /tmp



Display all hidden files in your home directory.

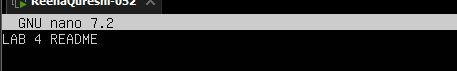


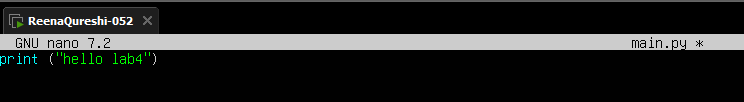
Create a markdown file summarizing your findings on key binary directories.



Evidence Handling & File Operations

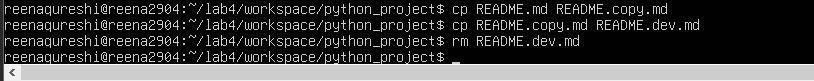
Create three text files, including one hidden file, in your workspace.



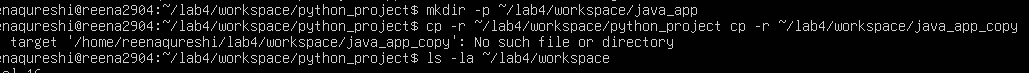




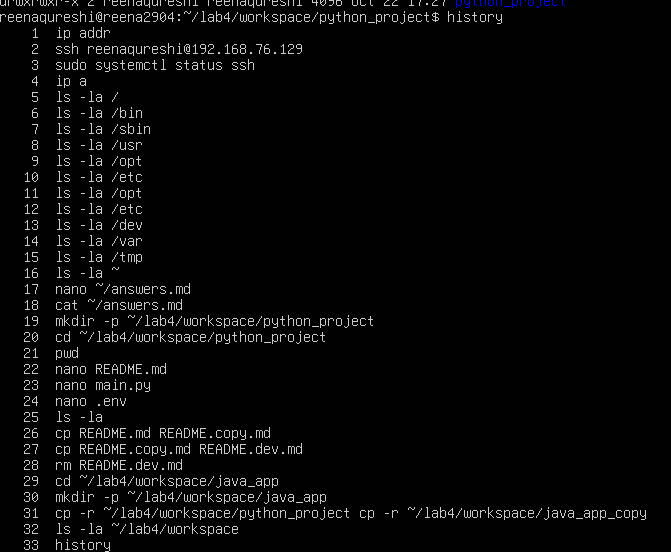
Create a backup copy of one file, rename it, and then delete it after verification.



Copy the entire workspace as an evidence backup folder.



Display your command history to document all actions performed.



**4. System Profiling and Process Monitoring**

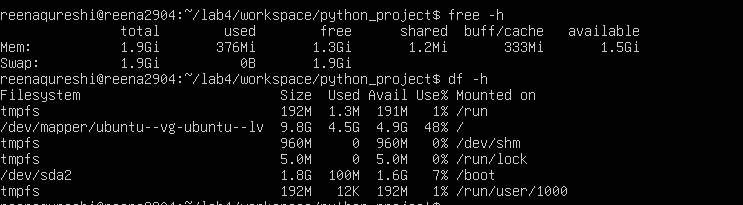
Display the system’s OS and kernel version for the investigation report.



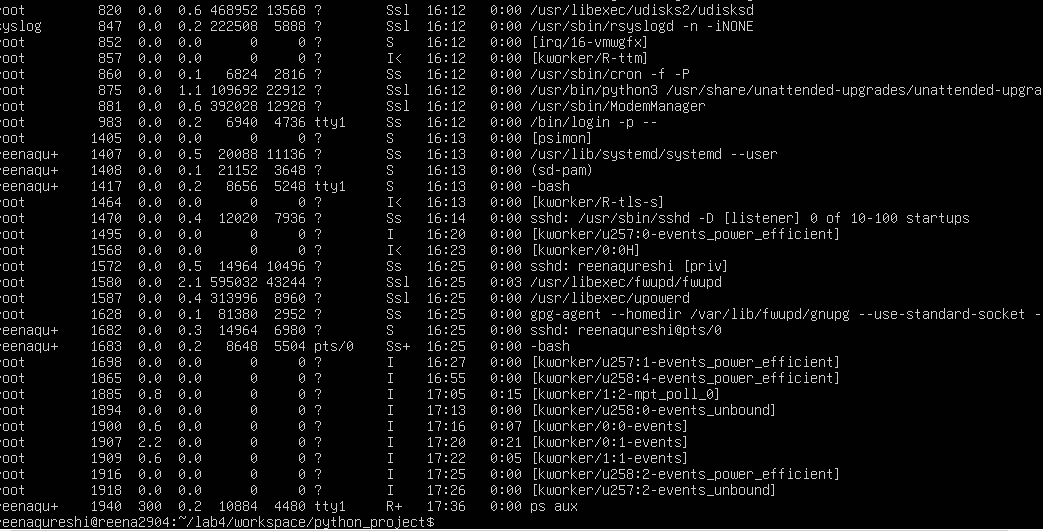
Display CPU, memory, and disk usage information





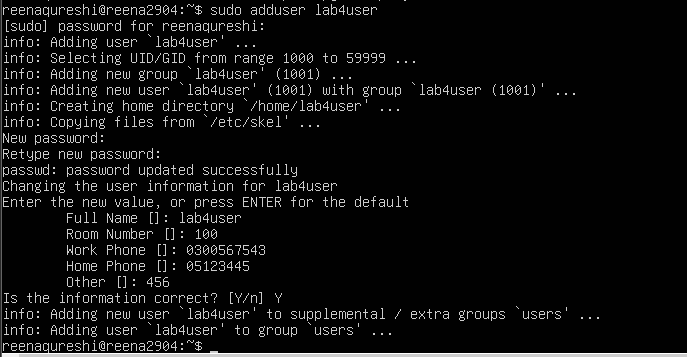


Display all active running processes to identify suspicious activity.



**User Account Audit & Privilege Escalation Simulation**

Create a new test user named lab4user.



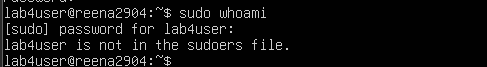
Verify that the new user record exists in the system’s user database.



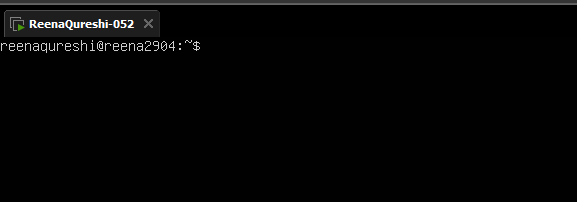
Log in as lab4user and confirm successful login.



Attempt to run an administrative command as lab4user (expect permission



Switch back to your main analyst account.



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

