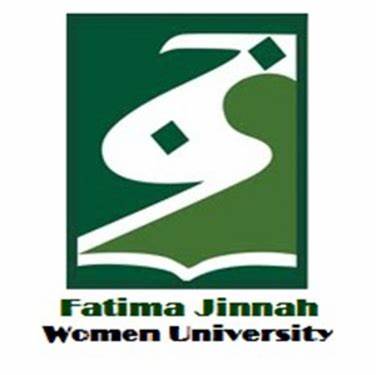
**CLOUD COMPUTING LAB**



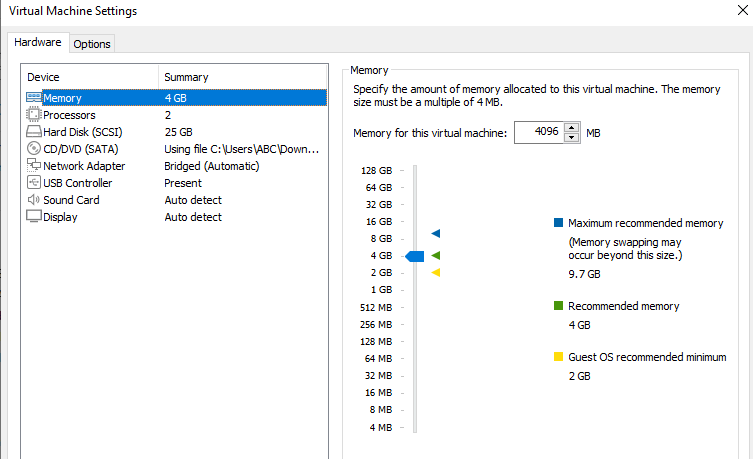
**SUBMITTED TO**SIR WAQAS SALEEM  
  
**SUBMITTED BY**  
HAMNA MAHMOOD

2023-BSE-025  
BSE V-A

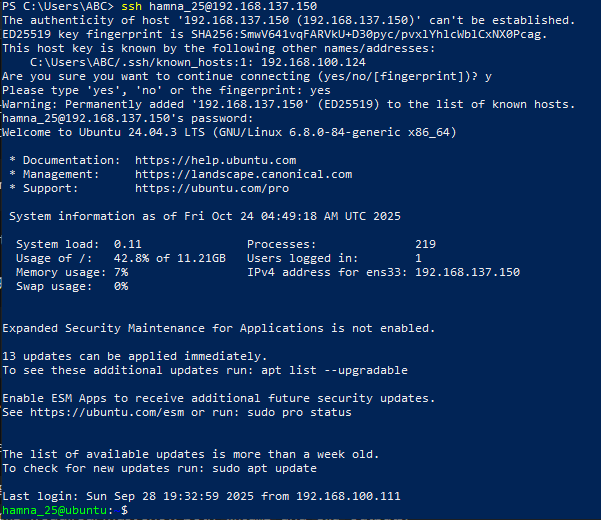
**Lab 04**

**Virtualization & Linux Fundamentals**

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

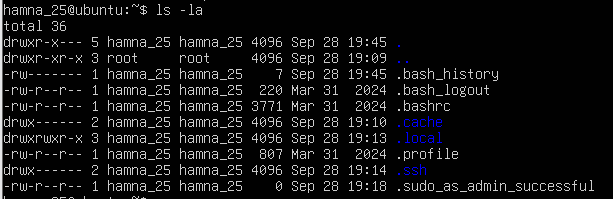
****

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

****

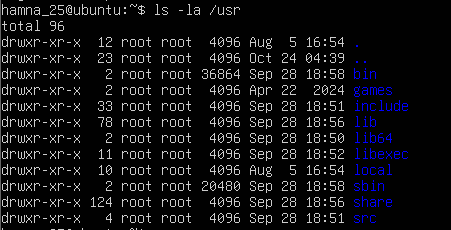
****

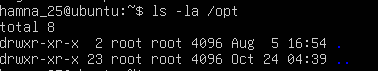
**Task 3- Filesystem exploration — root tree and dotfiles**

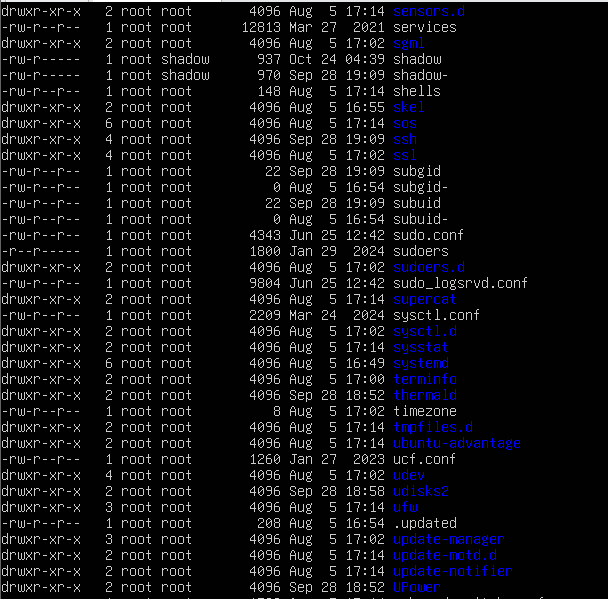
****

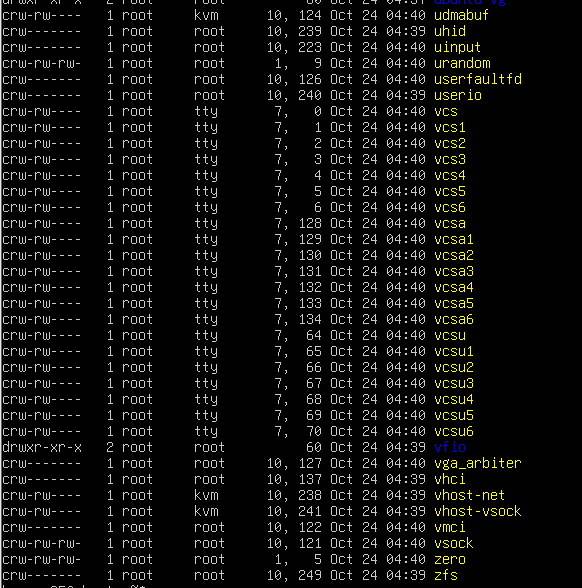
****

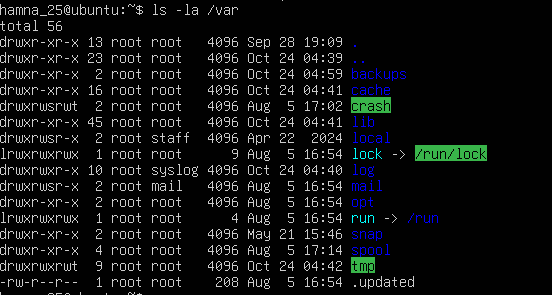
****

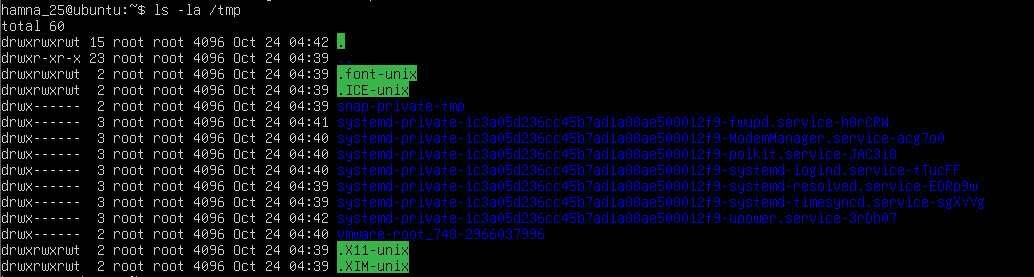
****

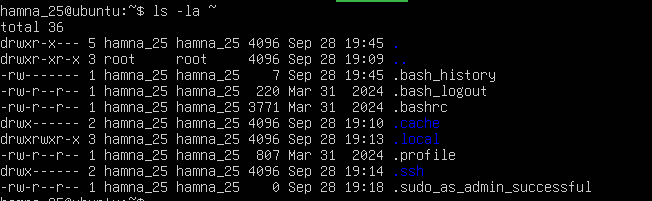
****

****

****

****

****

****

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

****

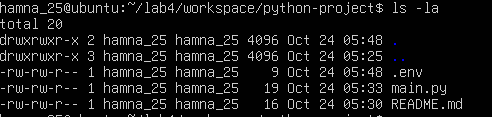
****

****

****

****

****

****

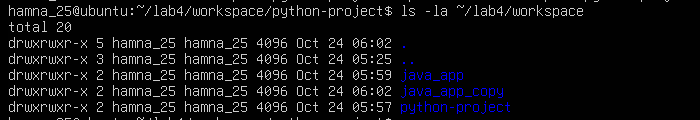
****

****

****

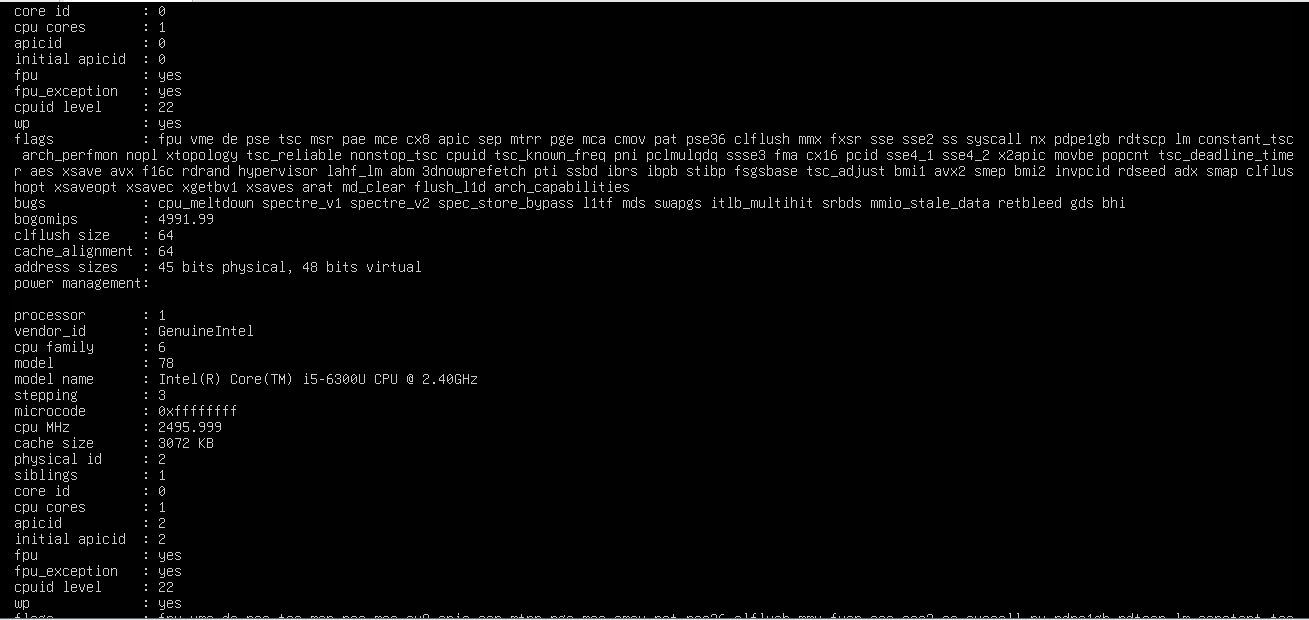
****

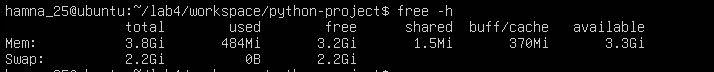
****

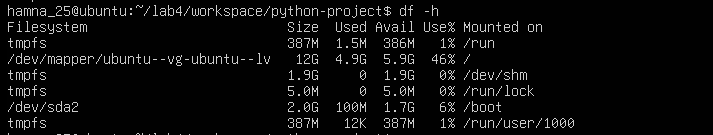
****

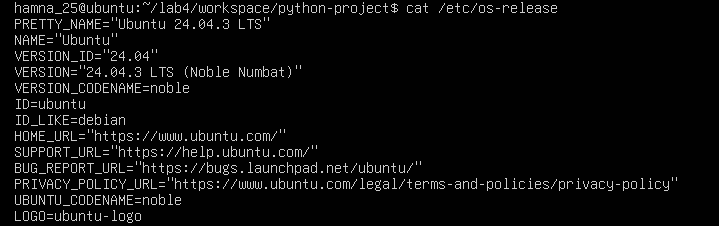
**Task 5 – System info, resources & processes**

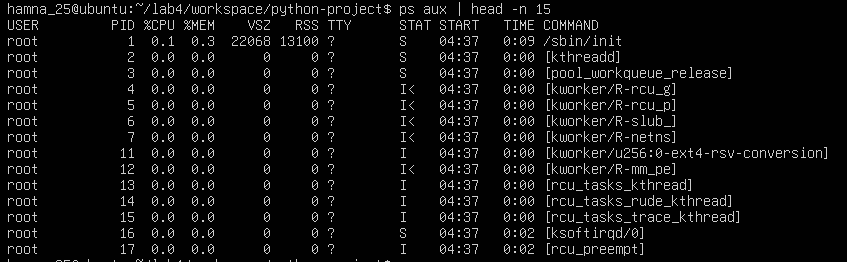
****

****

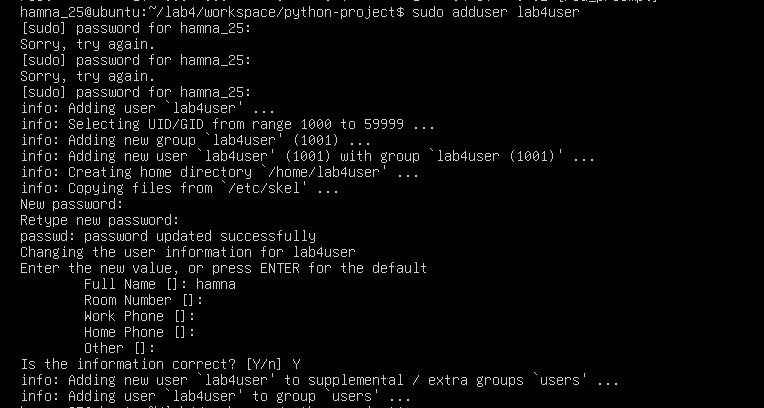
****

****

****

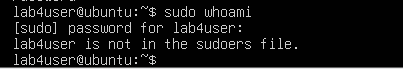
****

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

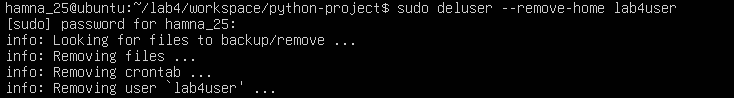
****

****

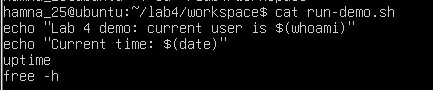
****

****

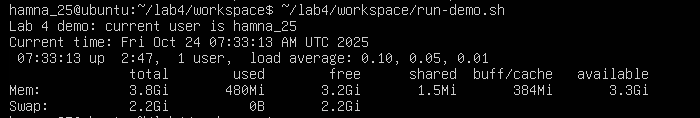
****

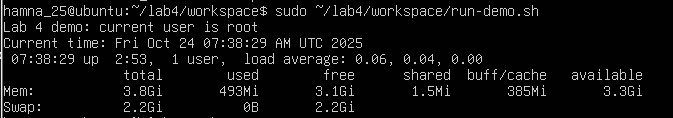
****

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

****

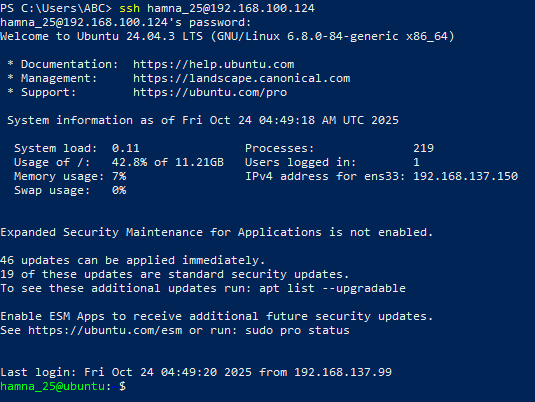
****

****

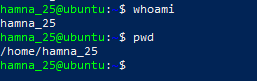
****

**Exam Evaluation Questions**

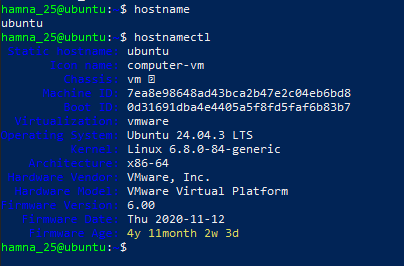
1. **Connect to the Ubuntu VM remotely from your host terminal**

****

**Verify your current user and home directory path.**

****

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

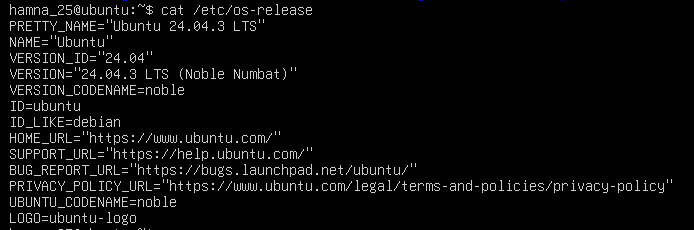
****

1. **Filesystem Inspection for Forensic Evidence**

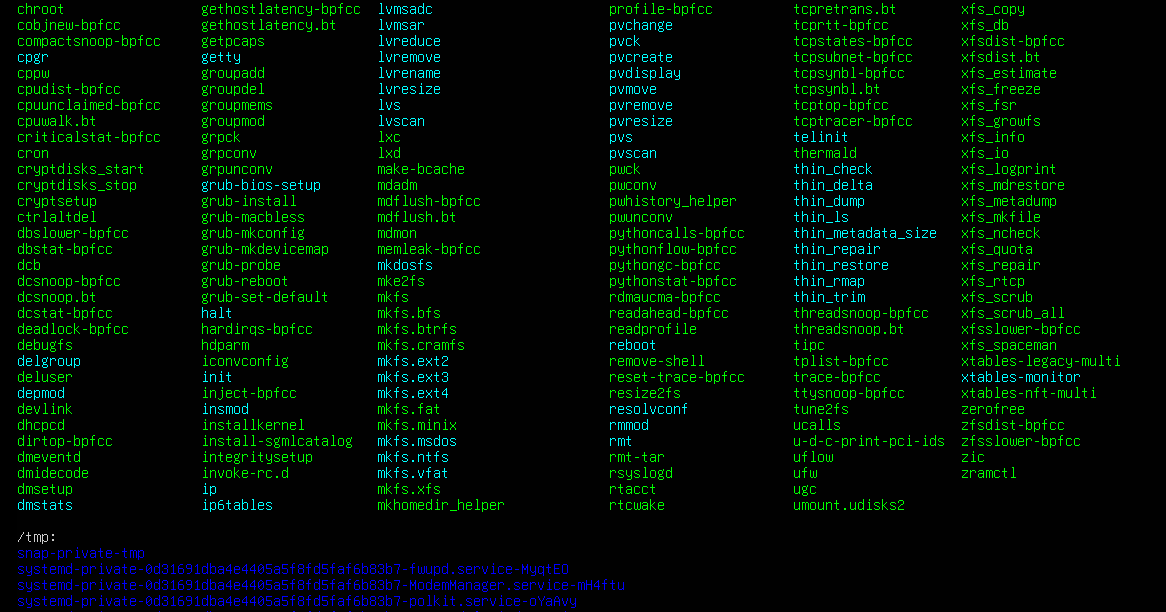
**Display the contents of the root directory**



**Display the OS version and release information.**



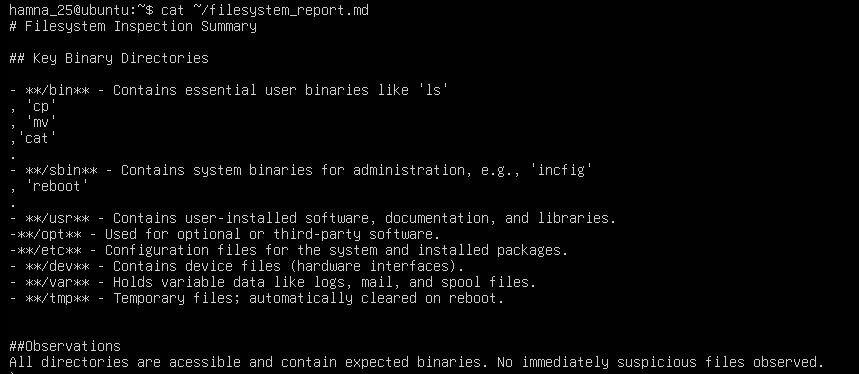
**Explore and record directory listings for /bin, /sbin, /usr, /opt, /etc, /dev, /var, and /tmp.**



**Display all hidden files in your home directory.**

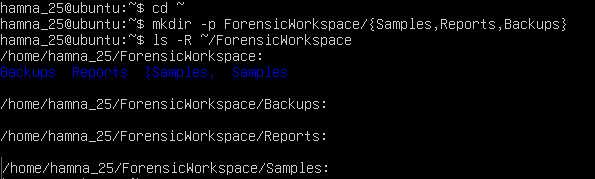


**Create a markdown file summarizing your findings on key binary directories.**

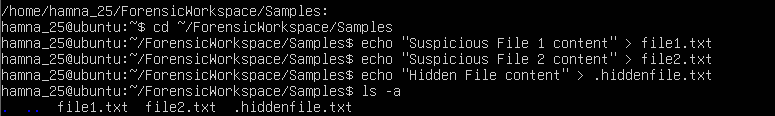


1. **Evidence handling & File Operations**

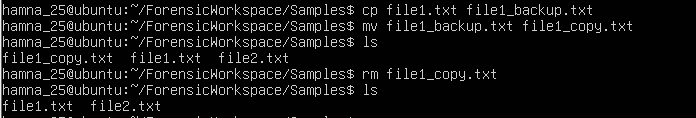
**Create a structured folder hierarchy under your home directory for analysis.**

****

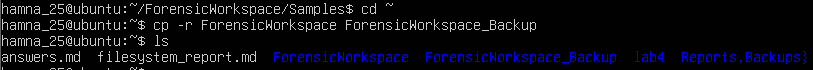
**Create three text files, including one hidden file, in your workspace.**

****

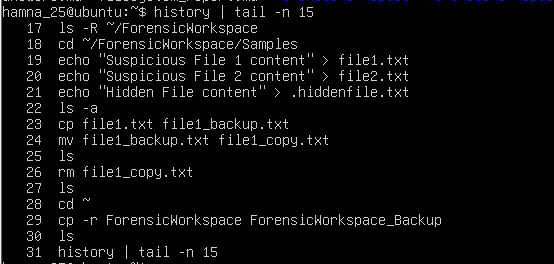
**Create a backup copy of one file, rename it, and then delete it after verification.**

****

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

****

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

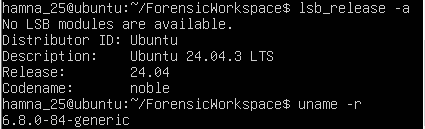
****

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

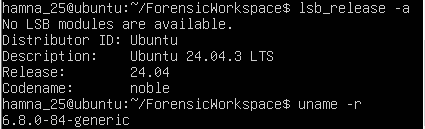
****

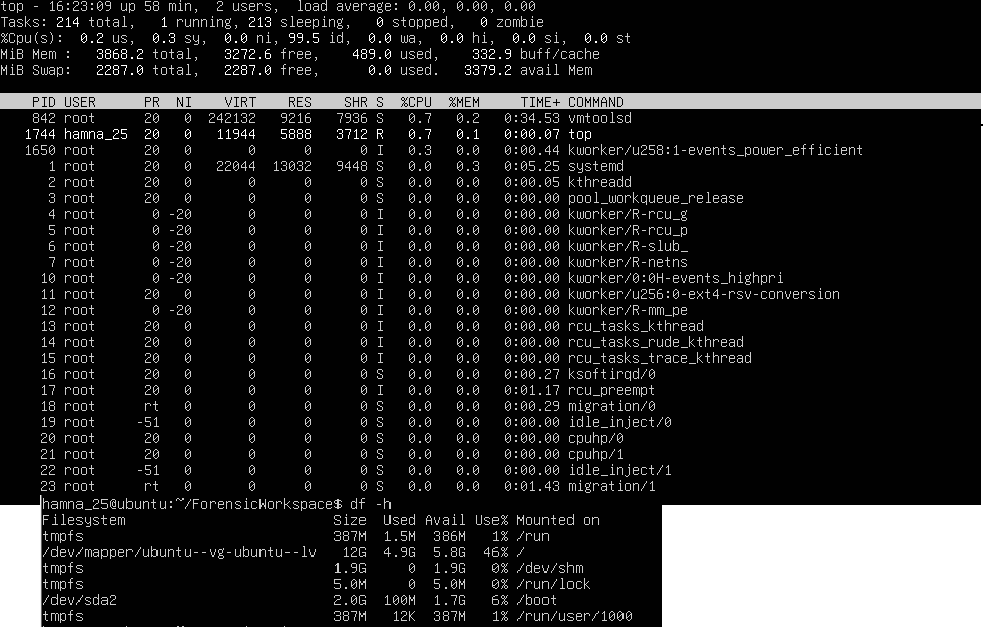
1. **System Profiling and Process Monitoring**

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

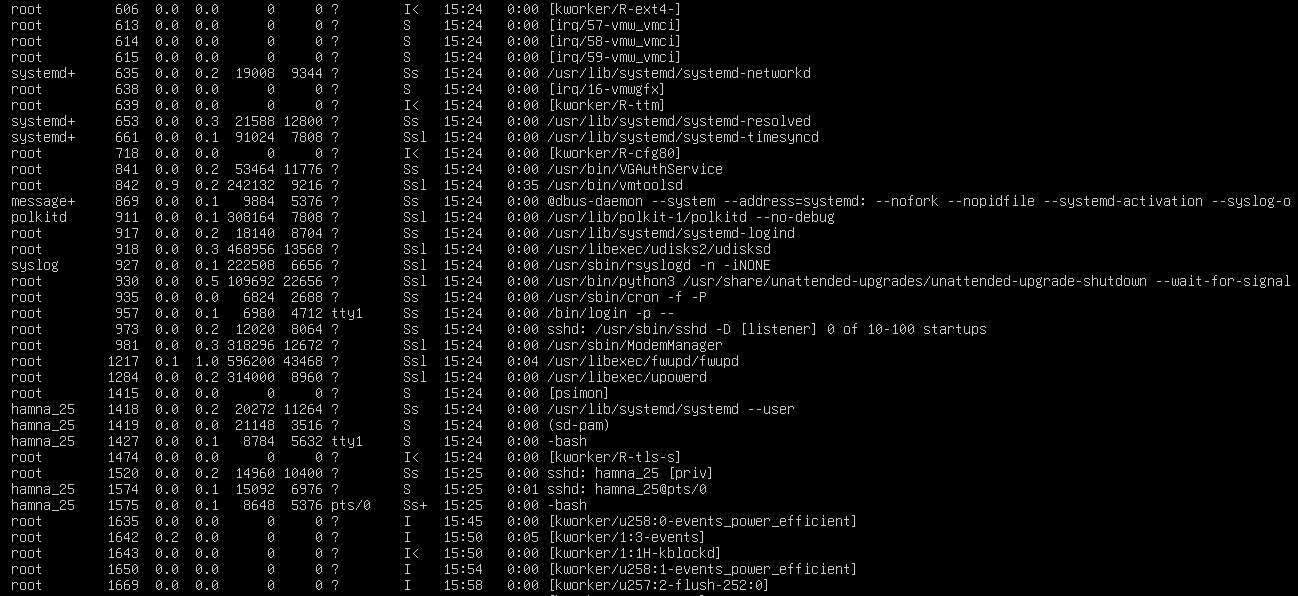
****

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

****

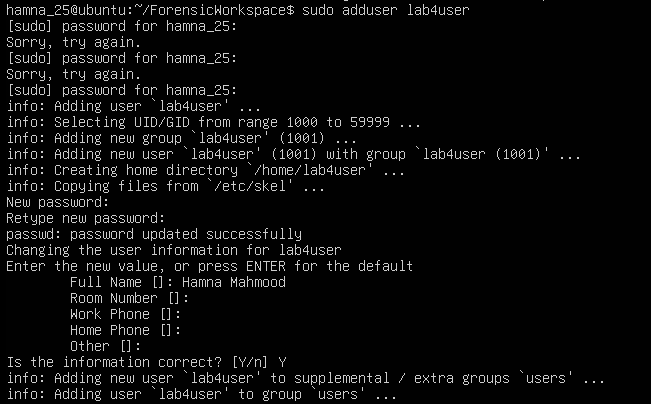
****

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

****

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

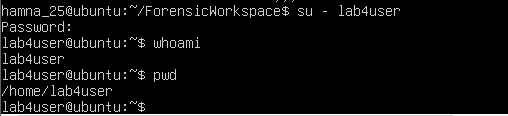
**Create a new test user named lab4user.**

****

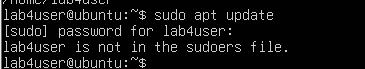
**Verify that the new user record exists in the system’s user database.**

****

**Log in as lab4user and confirm successful login.**

****

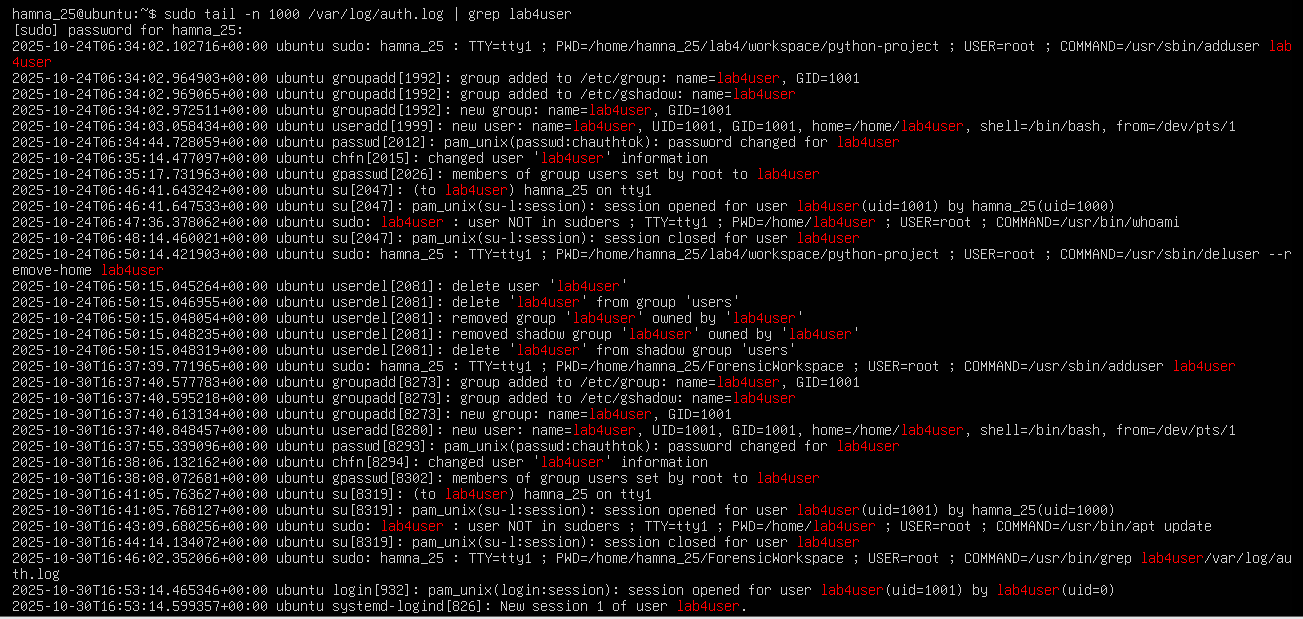
**Attempt to run an administrative command as lab4user (expect permission denied).**

****

**Switch back to your main analyst account.**

****

**Inspect the system authentication logs located at /var/log/auth.log to determine whether the lab4user account attempted any logins (successful or failed).**

****