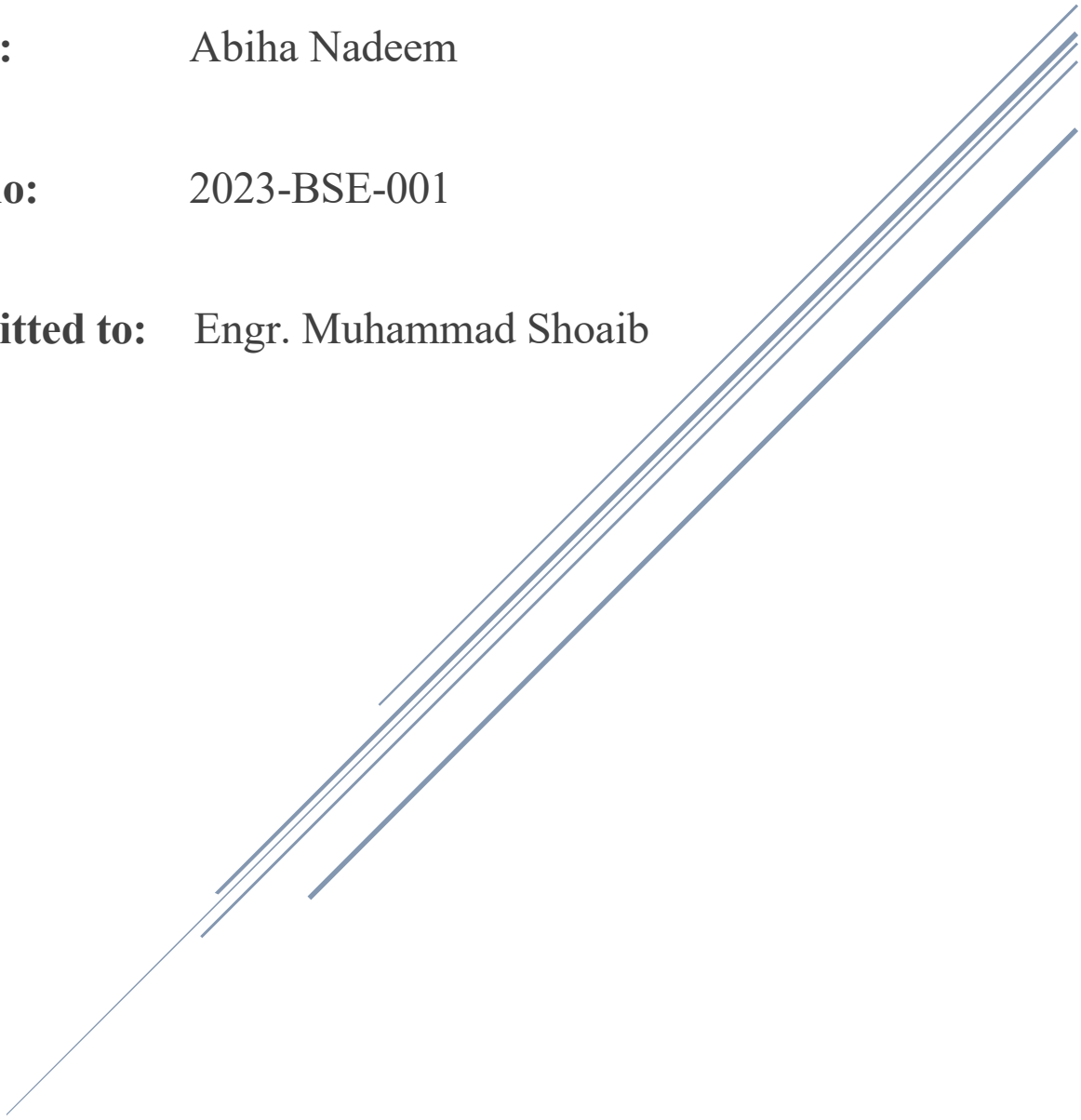
CLOUD COMPUTING

LAB 04

Name: Abiha Nadeem

Roll no: 2023-BSE-001

Submitted to: Engr. Muhammad Shoaib



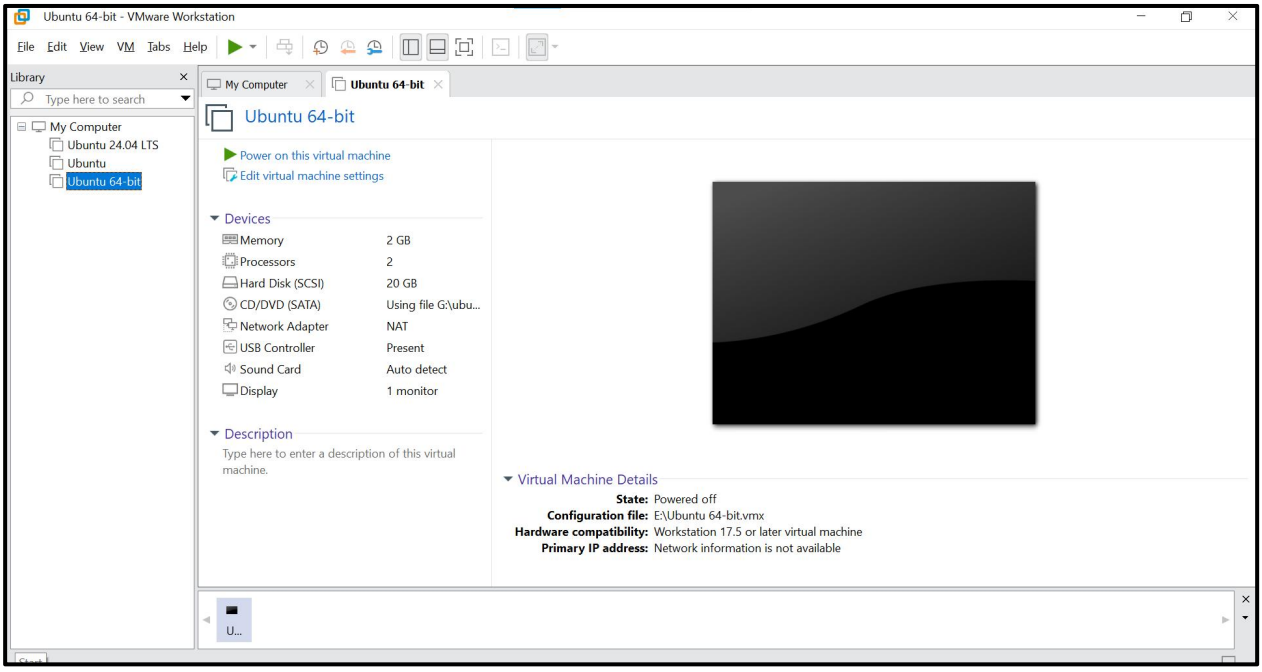
Virtualization & Linux Fundamentals

Task 1 – Verify VM resources in VMware

Confirm the VM resources that were allocated in Lab 1.

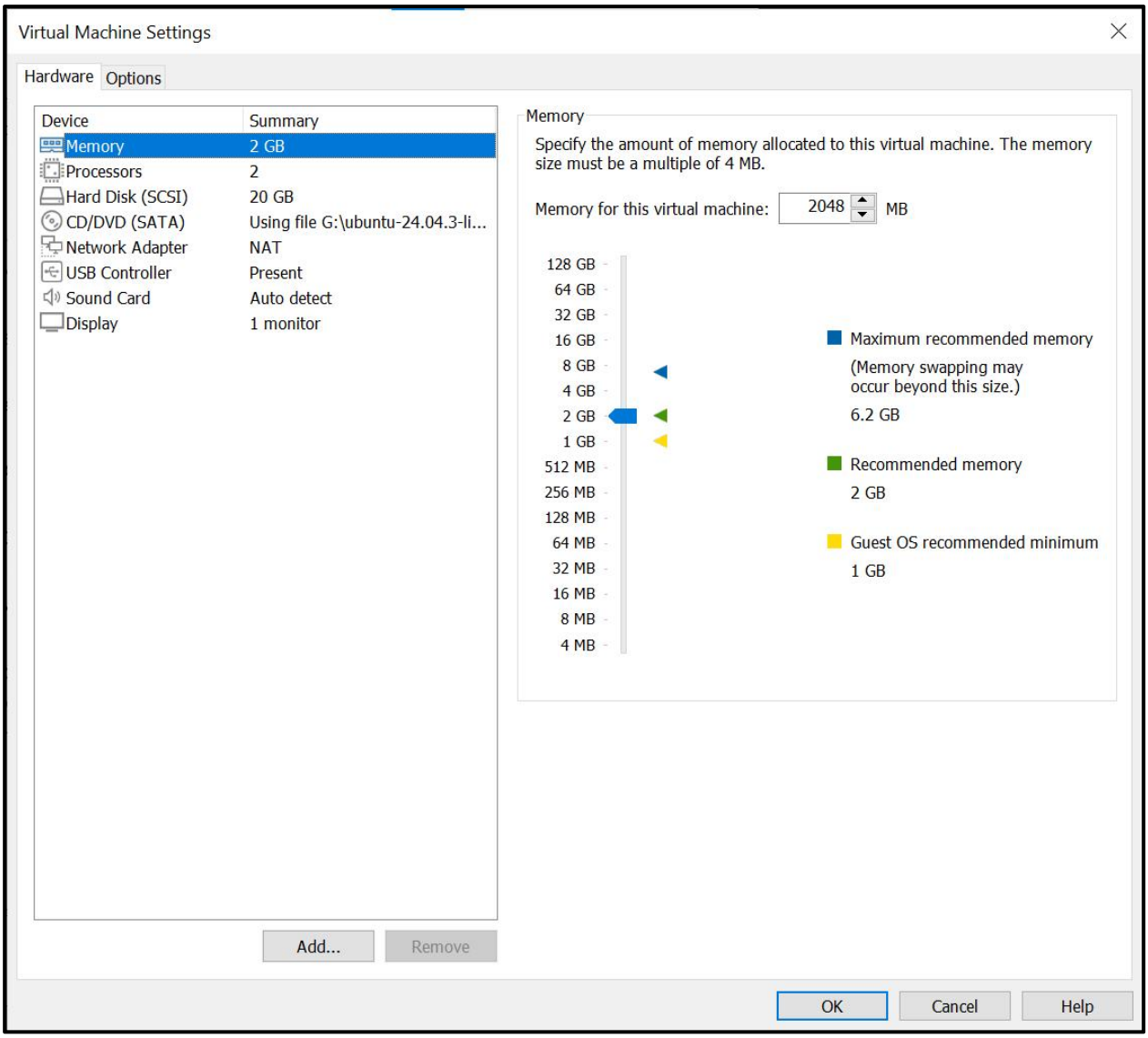
Steps

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



1. Inspect VM settings and note the following (no commands required for GUI): VM name, RAM, CPU, disk, and network adapter type.

2. Take a screenshot of the VM settings window showing RAM, CPU, disk and networking. Save screenshot as:

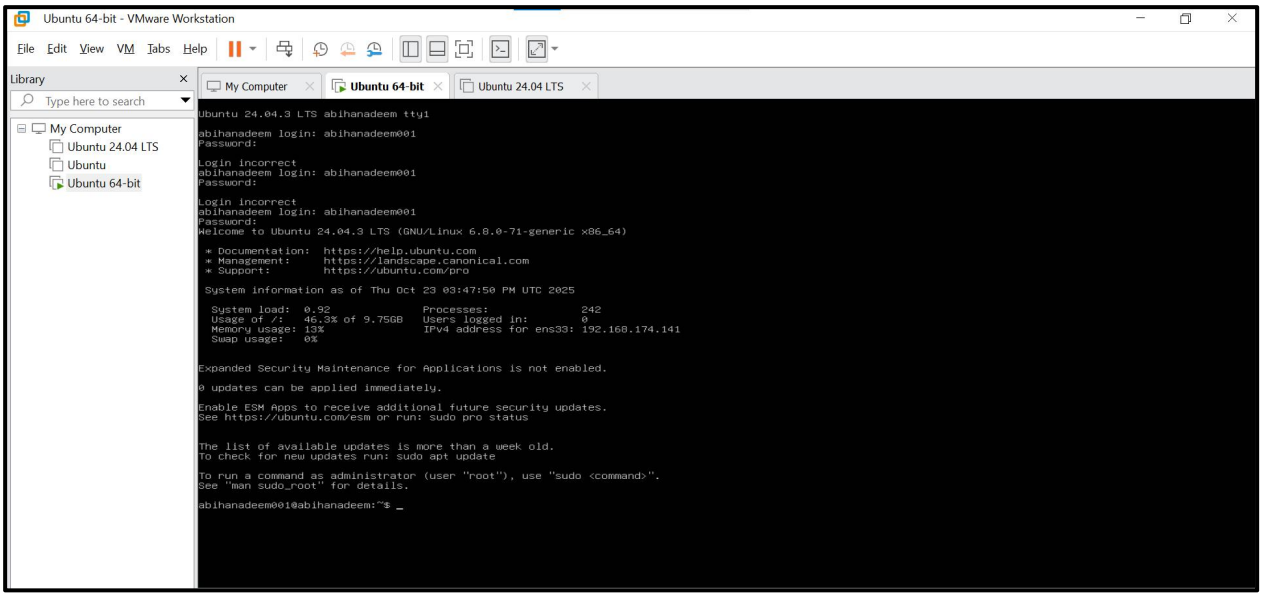


Task 2 – Start VM and log in (use your preferred host terminal method only)

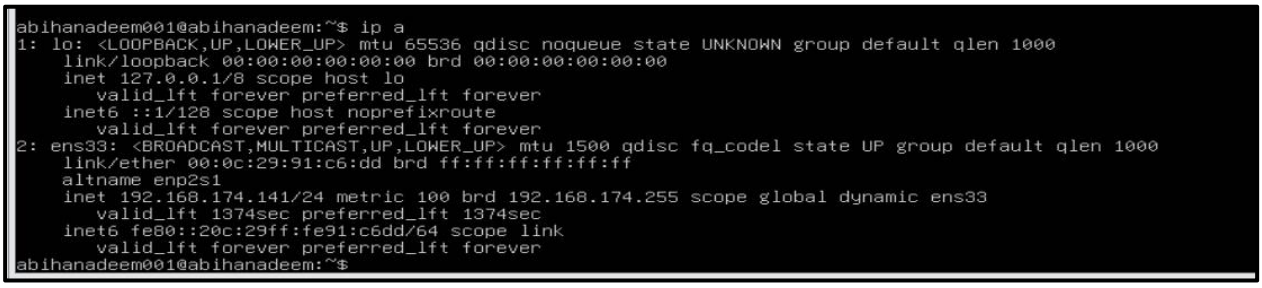
Use a single preferred host-terminal method to connect to the VM. Do not switch between methods during the task.

Steps

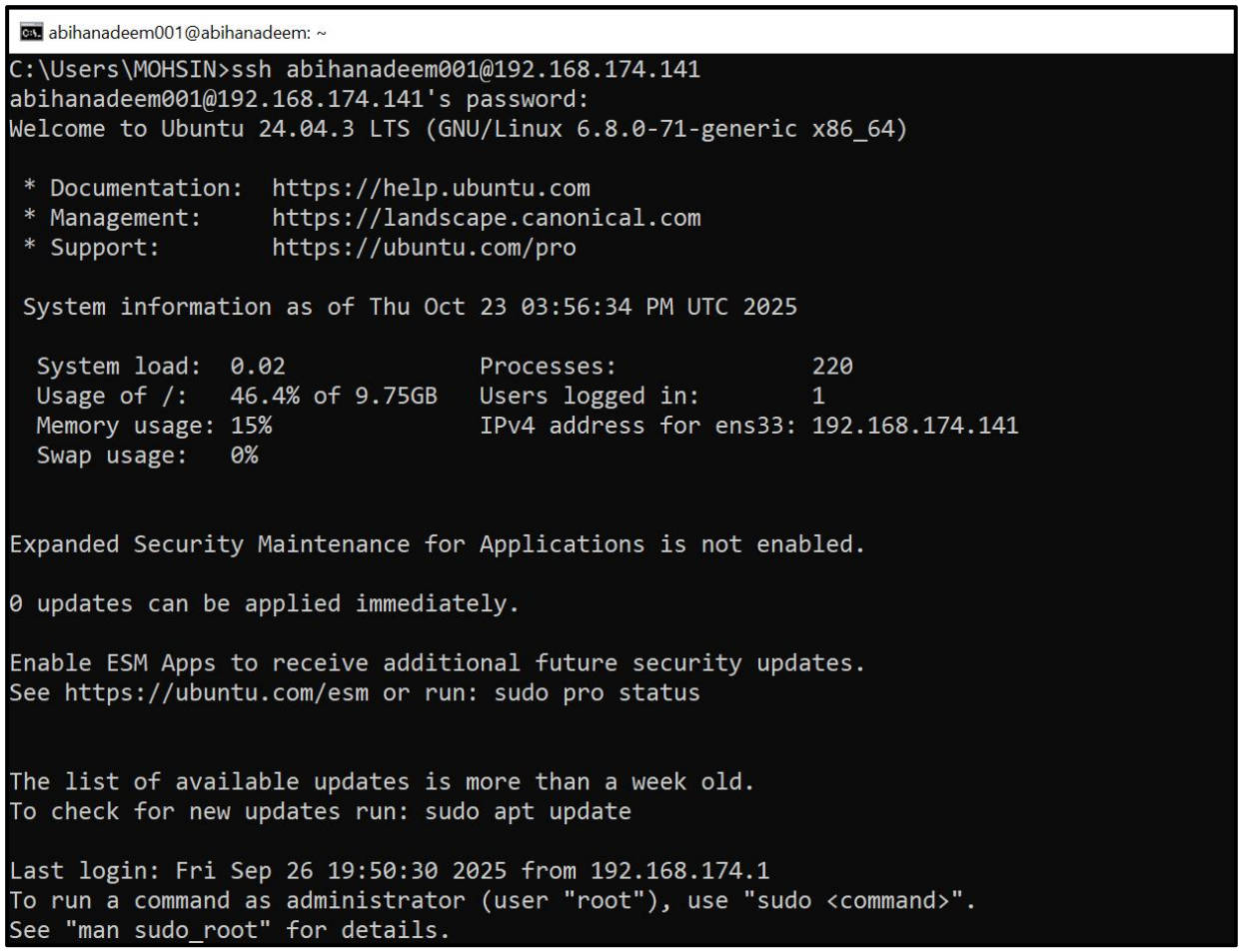
1. Start (or resume) the VM in VMware Workstation on your host.



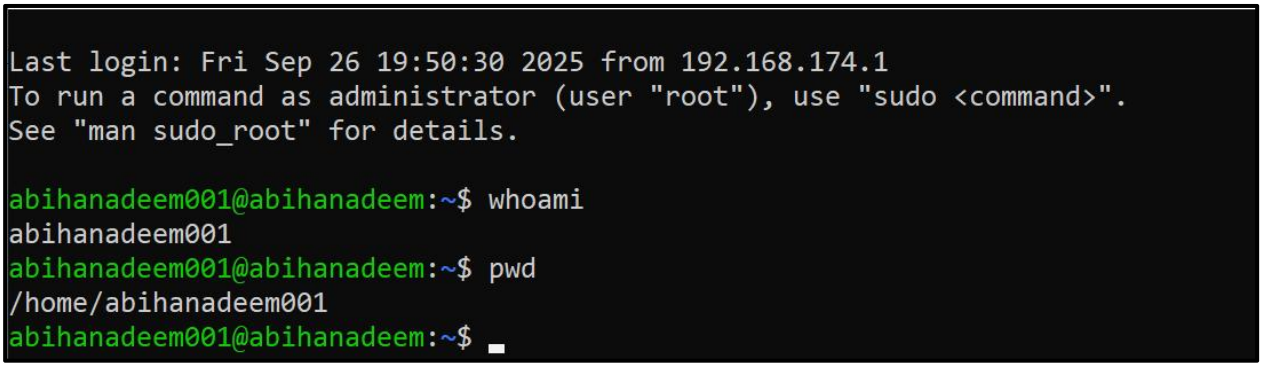
2. From your host, open your preferred terminal (for example: Windows Command Prompt, PowerShell, macOS Terminal, or Linux Terminal) and connect to the VM using SSH. Example:



- After connecting, save a screenshot of your host terminal showing the SSH login prompt/results as: vm_login.png



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



Task 3 – Filesystem exploration — root tree and dotfiles

Steps (run inside VM terminal)

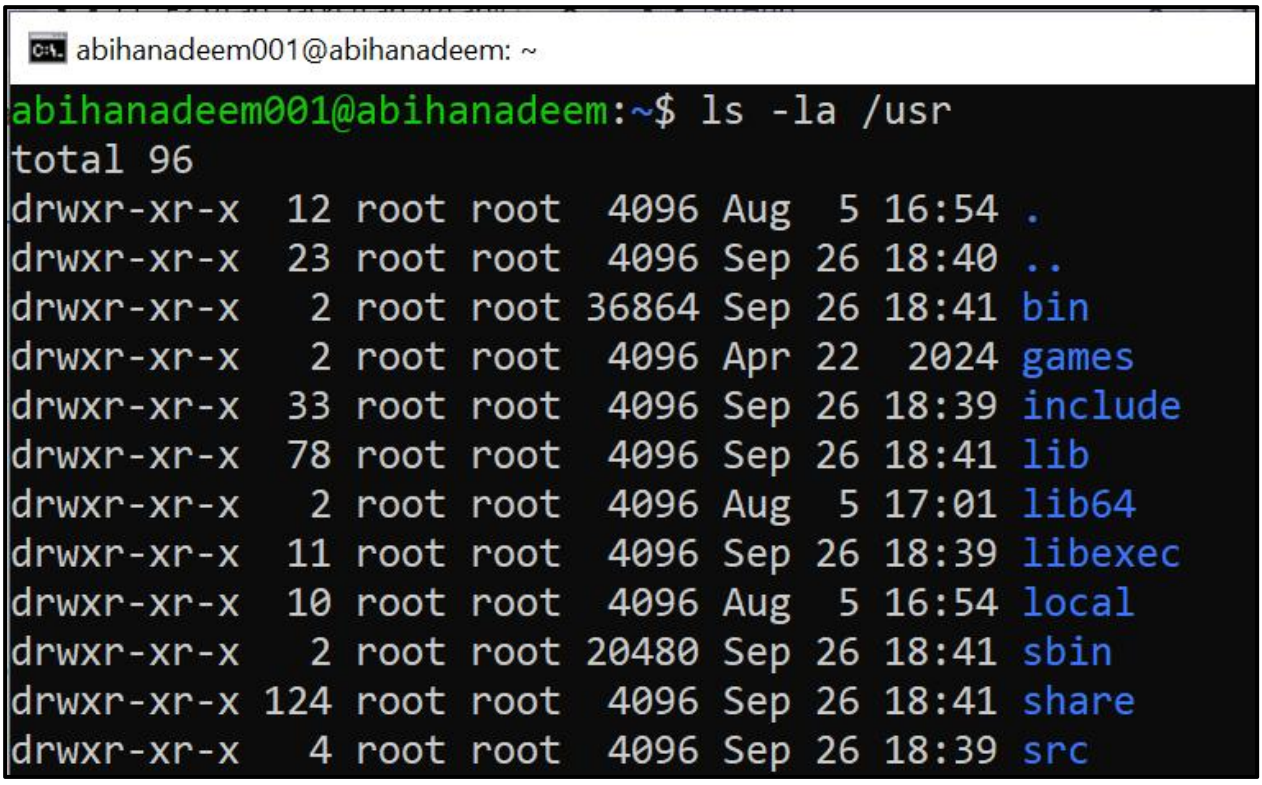
1. List root directory contents:

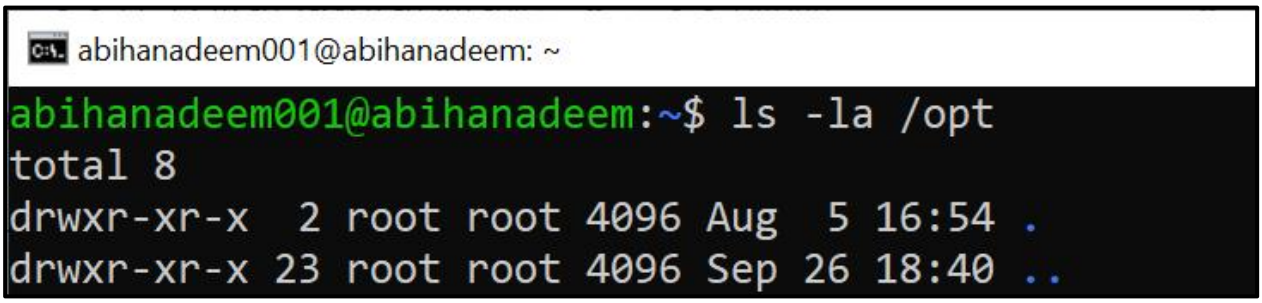
```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /
total 1994844
drwxr-xr-x  23 root root       4096 Sep 26 18:40 .
drwxr-xr-x  23 root root       4096 Sep 26 18:40 ..
lrwxrwxrwx   1 root root          7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x   2 root root       4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x   4 root root       4096 Sep 26 18:41 boot
dr-xr-xr-x   2 root root       4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root       4120 Oct 24  2025 dev
drwxr-xr-x 108 root root       4096 Sep 26 18:46 etc
drwxr-xr-x   3 root root       4096 Sep 26 18:46 home
lrwxrwxrwx   1 root root          7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx   1 root root          9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x   2 root root       4096 Feb 26  2024 lib.usr-is-merged
drwx------   2 root root      16384 Sep 26 18:37 lost+found
drwxr-xr-x   2 root root       4096 Aug  5 16:54 media
drwxr-xr-x   2 root root       4096 Aug  5 16:54 mnt
drwxr-xr-x   2 root root       4096 Aug  5 16:54 opt
dr-xr-xr-x 279 root root          0 Oct 23 15:45 proc
drwx------   3 root root       4096 Aug  5 17:02 root
drwxr-xr-x  29 root root        880 Oct 23 15:56 run
lrwxrwxrwx   1 root root          8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root       4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x   2 root root       4096 Sep 26 18:46 snap
drwxr-xr-x   2 root root       4096 Aug  5 16:54 srv
-rw-------   1 root root 2042626048 Sep 26 18:40 swap.img
dr-xr-xr-x  13 root root          0 Oct 23 15:45 sys
drwxrwxrwt  15 root root       4096 Oct 23 15:55 tmp
drwxr-xr-x  12 root root       4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root       4096 Sep 26 18:46 var
```

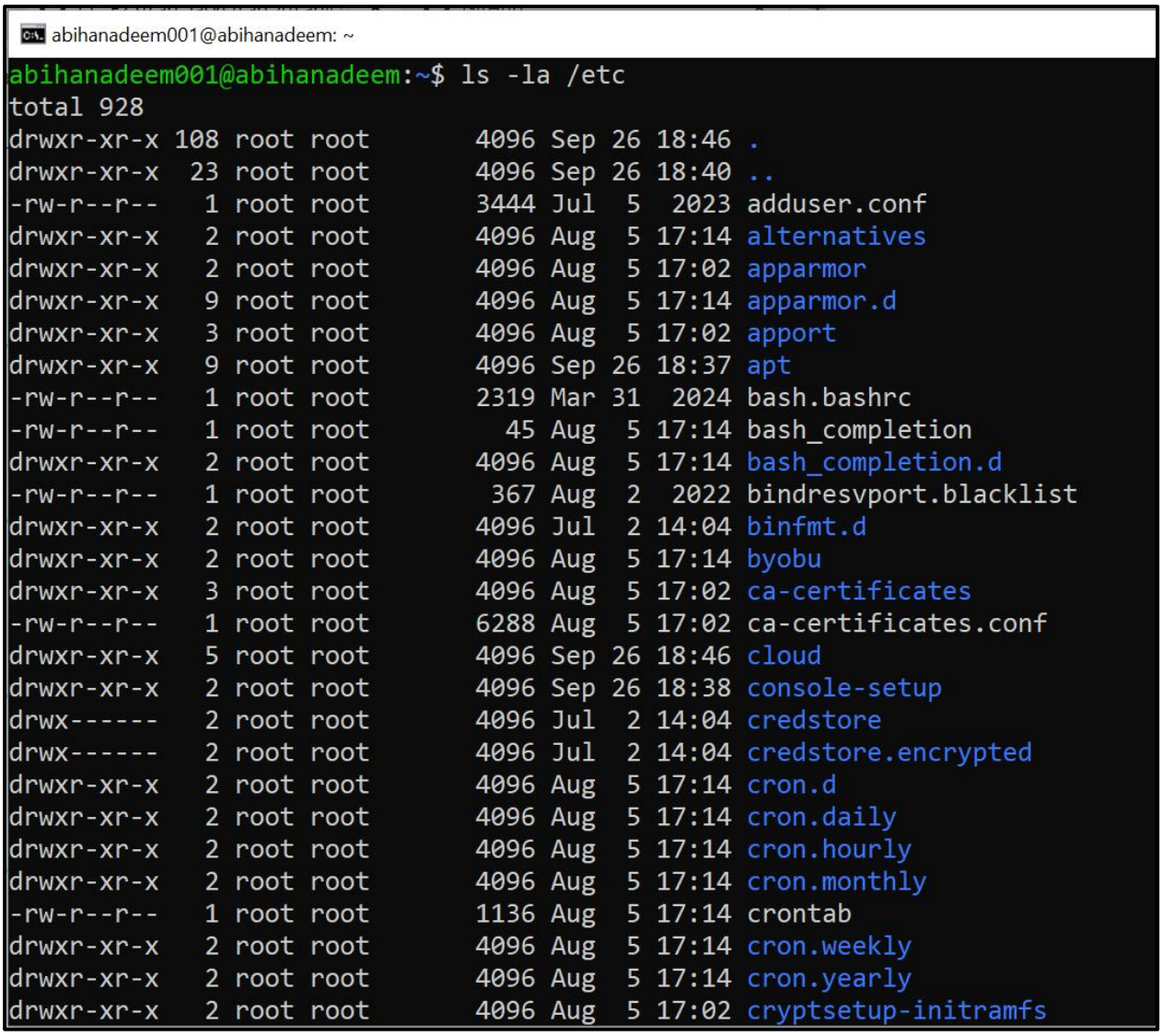
2. Inspect these directories (run each command and screenshot the output):

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
abihanadeem001@abihanadeem:~$
```

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
```


abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ 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 18:40 ..
drwxr-xr-x   2 root root 36864 Sep 26 18:41 bin
drwxr-xr-x   2 root root 4096 Apr 22 2024 games
drwxr-xr-x 33 root root 4096 Sep 26 18:39 include
drwxr-xr-x 78 root root 4096 Sep 26 18:41 lib
drwxr-xr-x   2 root root 4096 Aug 5 17:01 lib64
drwxr-xr-x 11 root root 4096 Sep 26 18:39 libexec
drwxr-xr-x 10 root root 4096 Aug 5 16:54 local
drwxr-xr-x   2 root root 20480 Sep 26 18:41 sbin
drwxr-xr-x 124 root root 4096 Sep 26 18:41 share
drwxr-xr-x   4 root root 4096 Sep 26 18:39 src


abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /opt
total 8
drwxr-xr-x 2 root root 4096 Aug 5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 26 18:40 ..


abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /etc
total 928
drwxr-xr-x 108 root root   4096 Sep 26 18:46 .
drwxr-xr-x 23 root root   4096 Sep 26 18:40 ..
-rw-r--r--   1 root root   3444 Jul 5 2023 adduser.conf
drwxr-xr-x   2 root root   4096 Aug 5 17:14 alternatives
drwxr-xr-x   2 root root   4096 Aug 5 17:02 apparmor
drwxr-xr-x   9 root root   4096 Aug 5 17:14 apparmor.d
drwxr-xr-x   3 root root   4096 Aug 5 17:02 apport
drwxr-xr-x   9 root root   4096 Sep 26 18:37 apt
-rw-r--r--   1 root root   2319 Mar 31 2024 bash.bashrc
-rw-r--r--   1 root root   45 Aug 5 17:14 bash_completion
drwxr-xr-x   2 root root   4096 Aug 5 17:14 bash_completion.d
-rw-r--r--   1 root root   367 Aug 2 2022 bindresvport.blacklist
drwxr-xr-x   2 root root   4096 Jul 2 14:04 binfmt.d
drwxr-xr-x   2 root root   4096 Aug 5 17:14 byobu
drwxr-xr-x   3 root root   4096 Aug 5 17:02 ca-certificates
-rw-r--r--   1 root root   6288 Aug 5 17:02 ca-certificates.conf
drwxr-xr-x   5 root root   4096 Sep 26 18:46 cloud
drwxr-xr-x   2 root root   4096 Sep 26 18:38 console-setup
drwx------   2 root root   4096 Jul 2 14:04 credstore
drwx------   2 root root   4096 Jul 2 14:04 credstore.encrypted
drwxr-xr-x   2 root root   4096 Aug 5 17:14 cron.d
drwxr-xr-x   2 root root   4096 Aug 5 17:14 cron.daily
drwxr-xr-x   2 root root   4096 Aug 5 17:14 cron.hourly
drwxr-xr-x   2 root root   4096 Aug 5 17:14 cron.monthly
-rw-r--r--   1 root root   1136 Aug 5 17:14 crontab
drwxr-xr-x   2 root root   4096 Aug 5 17:14 cron.weekly
drwxr-xr-x   2 root root   4096 Aug 5 17:14 cron.yearly
drwxr-xr-x   2 root root   4096 Aug 5 17:02 cryptsetup-initramfs

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /dev
total 4
drwxr-xr-x  20 root           root        4120 Oct 24  2025 .
drwxr-xr-x  23 root           root        4096 Sep 26 18:40 ..
crw-r--r--   1 root           root     10, 235 Oct 24  2025 autofs
drwxr-xr-x   2 root           root         320 Oct 24  2025 block
drwxr-xr-x   2 root           root          80 Oct 23 15:45 bsg
crw-rw----   1 root           disk     10, 234 Oct 24  2025 btrfs-control
drwxr-xr-x   3 root           root          60 Oct 23 15:45 bus
lrwxrwxrwx   1 root           root           3 Oct 23 15:45 cdrom -> sr0
drwxr-xr-x   2 root           root        3700 Oct 24  2025 char
crw--w----   1 root           tty        5,   1 Oct 23 15:47 console
lrwxrwxrwx   1 root           root          11 Oct 23 15:45 core -> /proc/kcore
drwxr-xr-x   4 root           root          80 Oct 23 15:45 cpu
crw-------   1 root           root     10, 123 Oct 24  2025 cpu_dma_latency
crw-------   1 root           root     10, 203 Oct 23 15:45 cuse
drwxr-xr-x   9 root           root         180 Oct 23 15:45 disk
brw-rw----   1 root           disk    252,   0 Oct 23 15:45 dm-0
drwxr-xr-x   2 root           root          60 Oct 23 15:45 dma_heap
crw-rw----+  1 root           audio    14,   9 Oct 24  2025 dmmidi
drwxr-xr-x   3 root           root         100 Oct 24  2025 dri
crw-------   1 root           root     10, 125 Oct 24  2025 ecryptfs
crw-rw----   1 root           video    29,   0 Oct 24  2025 fb0
lrwxrwxrwx   1 root           root          13 Oct 23 15:45 fd -> /proc/self/fd
crw-rw-rw-   1 root           root      1,   7 Oct 24  2025 full
crw-rw-rw-   1 root           root     10, 229 Oct 24  2025 fuse
crw-------   1 root           root    241,   0 Oct 23 15:45 hidraw0
crw-------   1 root           root     10, 228 Oct 24  2025 hpet
drwxr-xr-x   2 root           root           0 Oct 23 15:45 hugepages
crw-------   1 root           root     10, 183 Oct 24  2025 hwrng
```

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Sep 26 18:46 .
drwxr-xr-x 23 root root   4096 Sep 26 18:40 ..
drwxr-xr-x  2 root root   4096 Oct  2 03:29 backups
drwxr-xr-x 16 root root   4096 Oct  2 03:29 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct  2 03:29 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 24  2025 log
drwxrwsr-x  2 root mail   4096 Aug  5 16:54 mail
drwxr-xr-x  2 root root   4096 Aug  5 16:54 opt
lrwxrwxrwx  1 root root      4 Aug  5 16:54 run -> /run
drwxr-xr-x  2 root root   4096 May 21 15:46 snap
drwxr-xr-x  4 root root   4096 Aug  5 17:14 spool
drwxrwxrwt  9 root root   4096 Oct 23 15:55 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
```

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 23 15:55 .
drwxr-xr-x 23 root root 4096 Sep 26 18:40 ..
drwxrwxrwt  2 root root 4096 Oct 23 15:45 .font-unix
drwxrwxrwt  2 root root 4096 Oct 23 15:45 .ICE-unix
drwx------  2 root root 4096 Oct 23 15:45 snap-private-tmp
drwx------  3 root root 4096 Oct 23 15:55 systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-fwupd.service-sAHSiC
drwx------  3 root root 4096 Oct 23 15:45 systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-ModemManager.service-NxI4We
drwx------  3 root root 4096 Oct 23 15:45 systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-polkit.service-j3nU4x
drwx------  3 root root 4096 Oct 23 15:45 systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-systemd-logind.service-VUS5uH
drwx------  3 root root 4096 Oct 23 15:45 systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-systemd-resolved.service-pFRJSK
drwx------  3 root root 4096 Oct 23 15:45 systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-systemd-timesyncd.service-DqdTGc
drwx------  3 root root 4096 Oct 23 15:55 systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-upower.service-bX94Ry
drwx------  2 root root 4096 Oct 23 15:46 vmware-root_733-4248680474
drwxrwxrwt  2 root root 4096 Oct 23 15:45 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 23 15:45 .XIM-unix
```

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

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la ~
total 32
drwxr-x--- 4 abihanadeem001 abihanadeem001 4096 Sep 26 19:11 .
drwxr-xr-x 3 root           root           4096 Sep 26 18:46 ..
-rw------- 1 abihanadeem001 abihanadeem001   23 Sep 26 19:32 .bash_history
-rw-r--r-- 1 abihanadeem001 abihanadeem001  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 abihanadeem001 abihanadeem001 3771 Mar 31  2024 .bashrc
drwx------ 2 abihanadeem001 abihanadeem001 4096 Sep 26 18:48 .cache
-rw-r--r-- 1 abihanadeem001 abihanadeem001  807 Mar 31  2024 .profile
drwx------ 2 abihanadeem001 abihanadeem001 4096 Sep 26 19:47 .ssh
```

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. Save that screenshot as: answers_md.png

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ abihanadeem001@abihanadeem:~$ cat ~/answers.md
The /bin directory contains essential system commands and utilities needed for basic system operation even when no other
 file systems are mounted.
The /usr/bin directory holds most of the user-level applications and programs installed by the opearting system package
manager.
Meanwhile /usr/local/bin is reserved for programs manually installed by the system administrator or user keeping them se
parate from system-managed files

abihanadeem001@abihanadeem:~$
```

Task 4 – Essential CLI tasks — navigation and file operations

Steps (inside VM terminal)

1. Create a workspace and navigate:

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ mkdir -p ~/lab4/workspace/python_project
abihanadeem001@abihanadeem:~$
```

```
abihanadeem001@abihanadeem: ~/lab4/workspace/python_project
abihanadeem001@abihanadeem:~$ mkdir -p ~/lab4/workspace/python_project
abihanadeem001@abihanadeem:~$ cd ~/lab4/workspace/python_project
abihanadeem001@abihanadeem:~/lab4/workspace/python_project$
```

```
abihanadeem001@abihanadeem: ~/lab4/workspace/python_project
abihanadeem001@abihanadeem:~/lab4/workspace/python_project$ pwd
/home/abihanadeem001/lab4/workspace/python_project
abihanadeem001@abihanadeem:~/lab4/workspace/python_project$
```

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

```
abihanadeem001@abihanadeem: ~/lab4/workspace/python_project
  GNU nano 7.2                                          README.md *
Lab 4 README
```

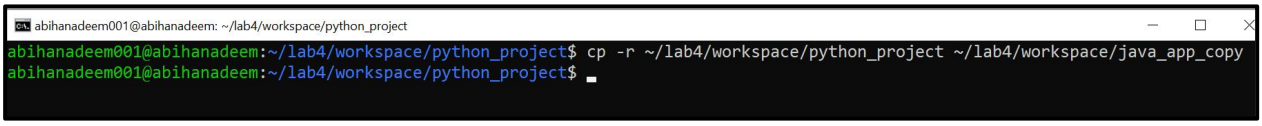
```
abihanadeem001@abihanadeem: ~/lab4/workspace/python_project
  GNU nano 7.2                                            main.py *
print("hello lab4")
```

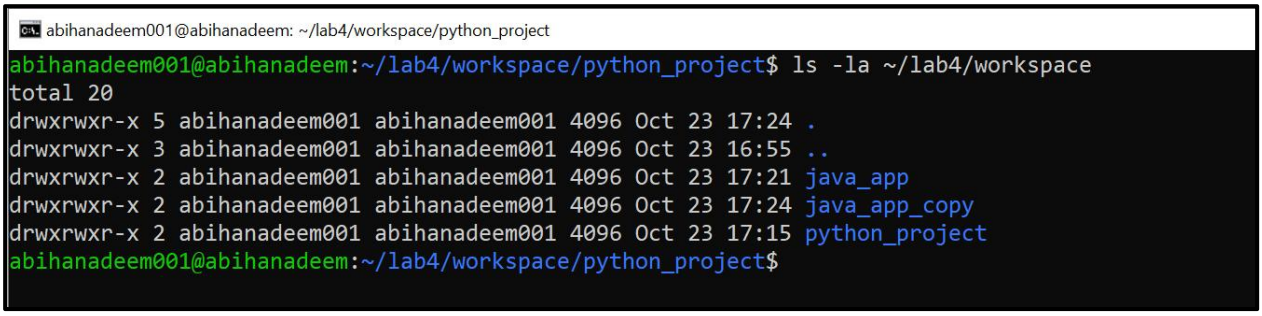
```
abihanadeem001@abihanadeem: ~/lab4/workspace/python_project
  GNU nano 7.2                                              .env *
ENV=lab4
```

3. List files and capture:

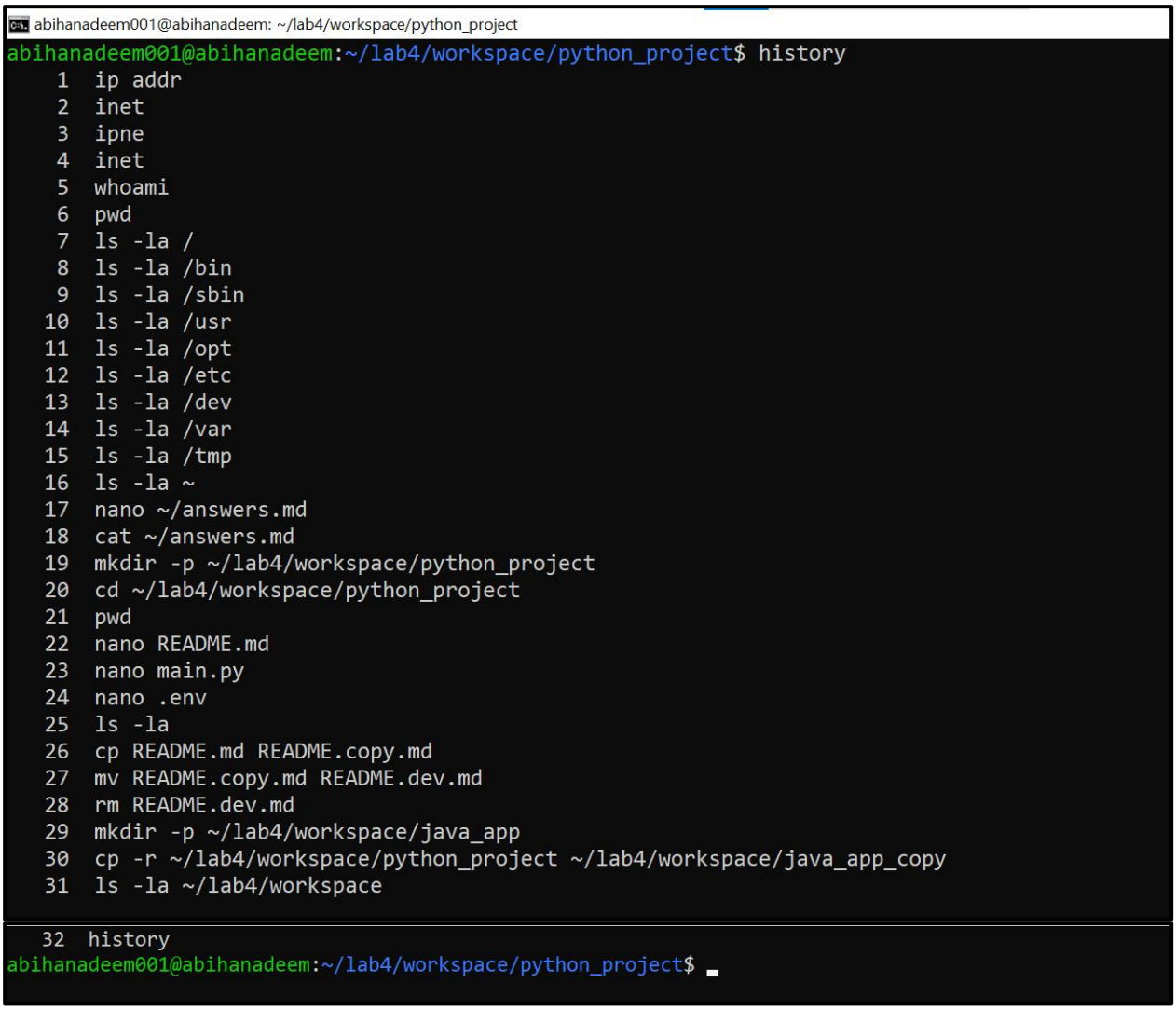
```
abihanadeem001@abihanadeem: ~/lab4/workspace/python_project
abihanadeem001@abihanadeem:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 abihanadeem001 abihanadeem001 4096 Oct 23 17:09 .
drwxrwxr-x 3 abihanadeem001 abihanadeem001 4096 Oct 23 16:55 ..
-rw-rw-r-- 1 abihanadeem001 abihanadeem001   12 Oct 23 17:09 .env
-rw-rw-r-- 1 abihanadeem001 abihanadeem001   21 Oct 23 17:06 main.py
-rw-rw-r-- 1 abihanadeem001 abihanadeem001   14 Oct 23 17:04 README.md
abihanadeem001@abihanadeem:~/lab4/workspace/python_project$
```

4. Copy, move and remove:





5. Use command history and tab completion:

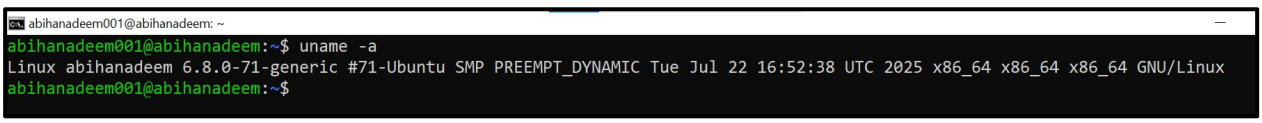


Task 5 – System info, resources & processes

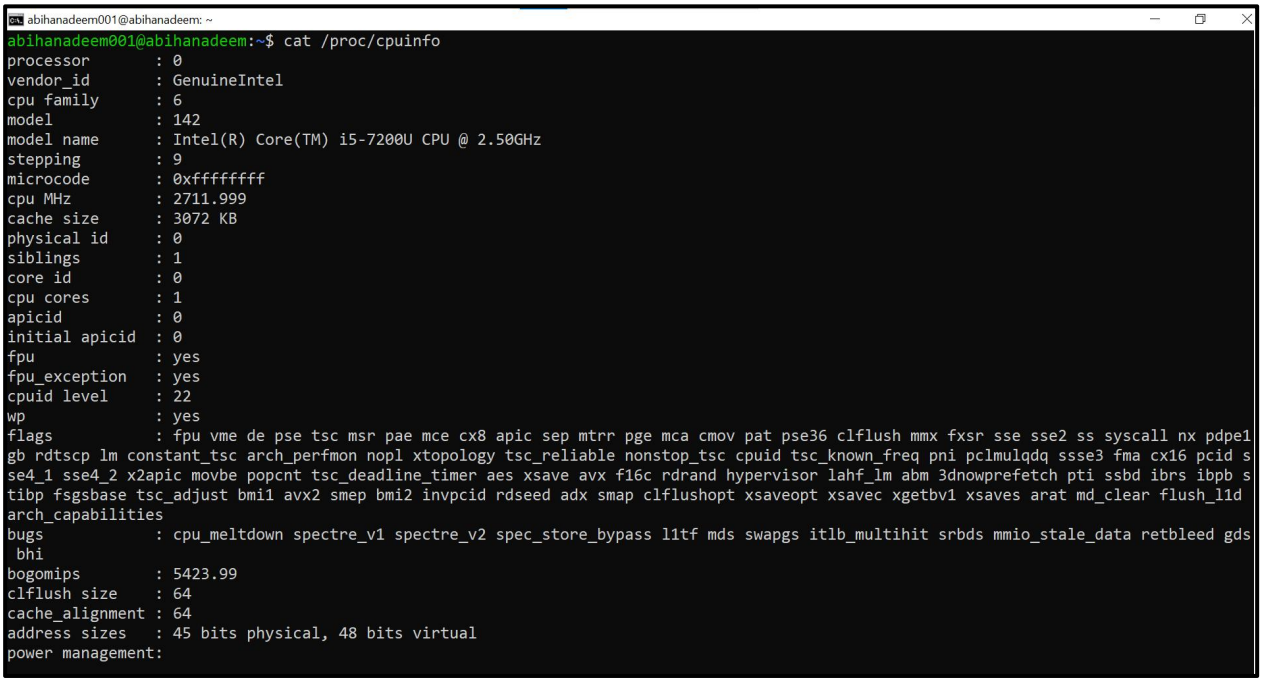
Collect system information and observe processes. Use screenshots only.

Steps (inside VM terminal)

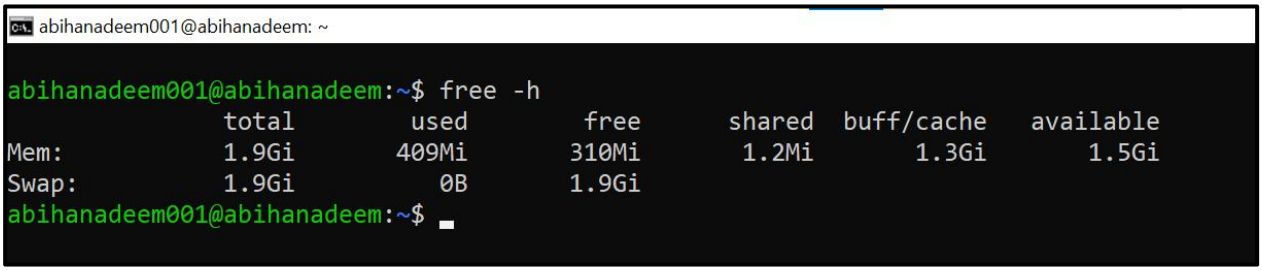
1. Kernel and OS:



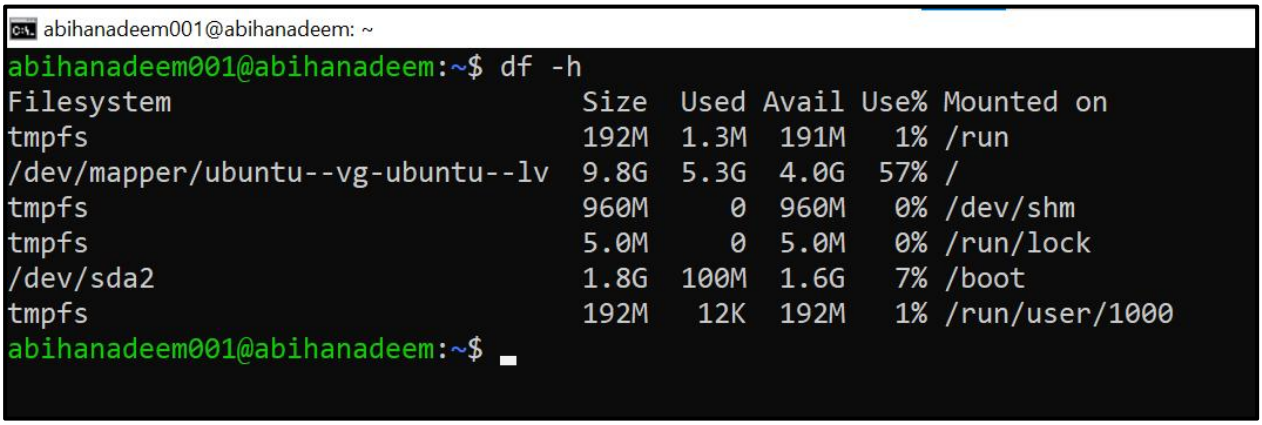
2. CPU (ensure model name visible):



3. Memory:

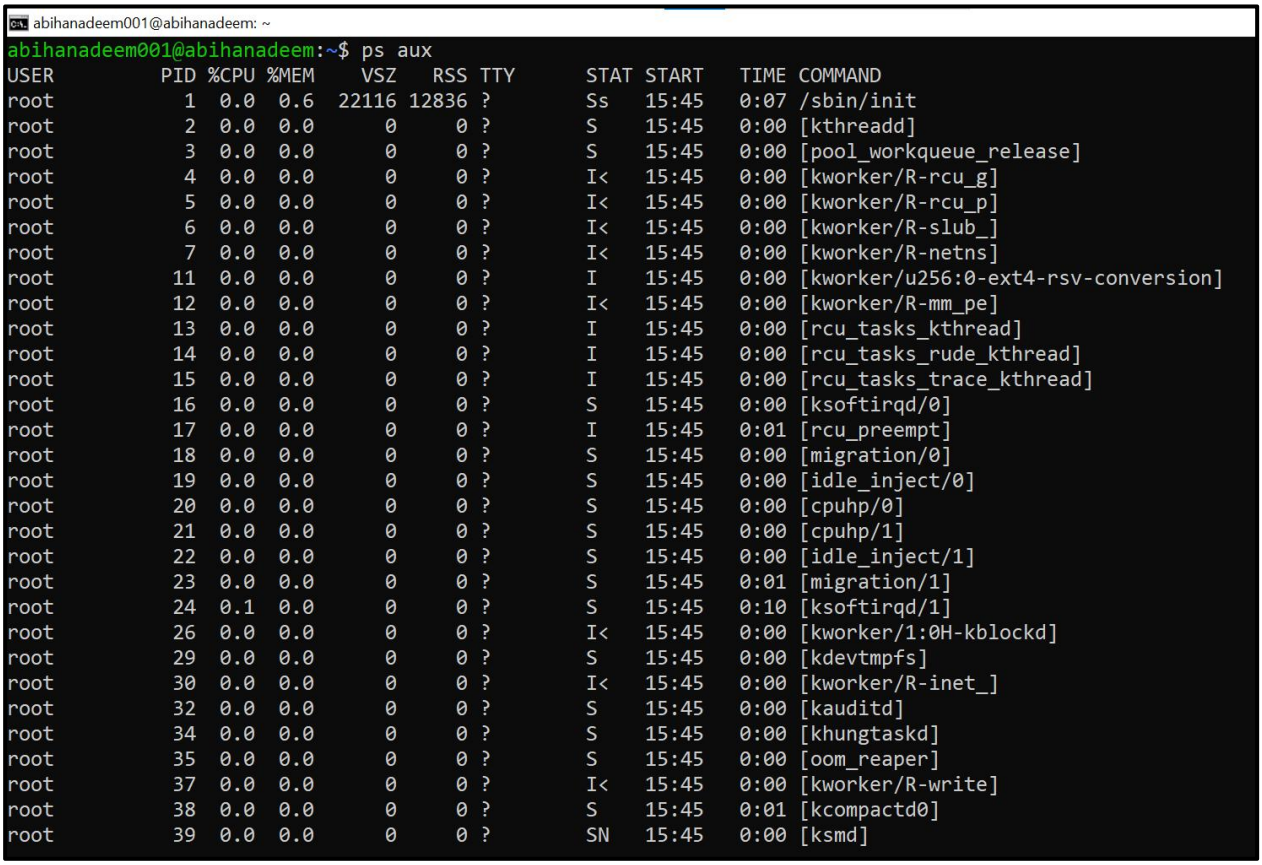


4. Disk:



5. View OS release information:

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

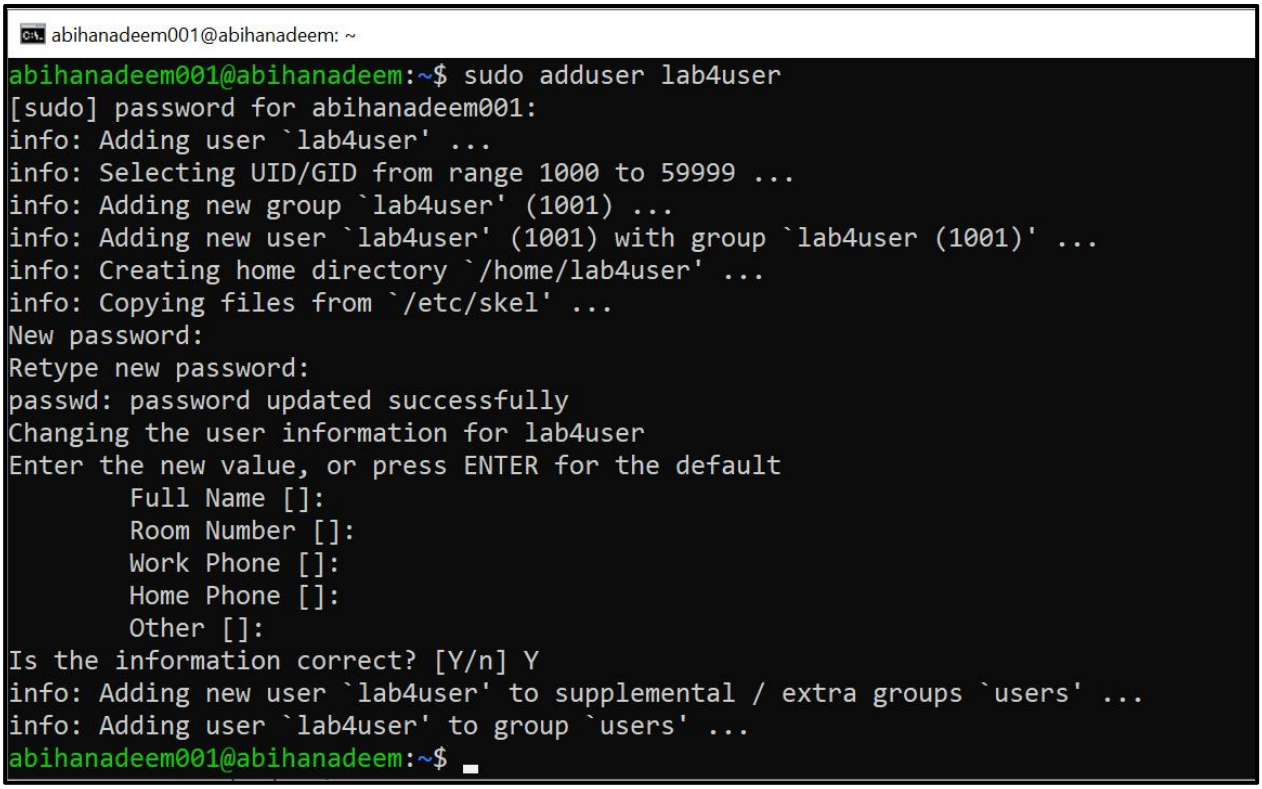


Task 6 – Users and account verification (no sudo group change)

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

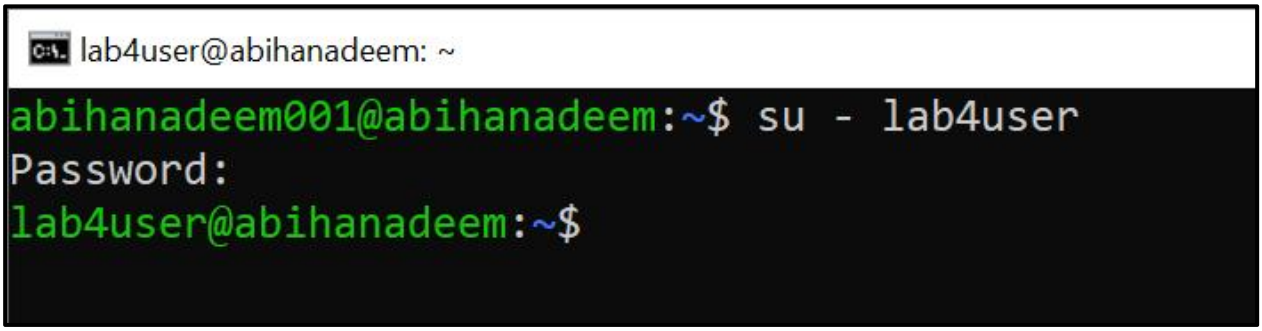
Steps (inside VM terminal)

1. Create a new user named lab4user:

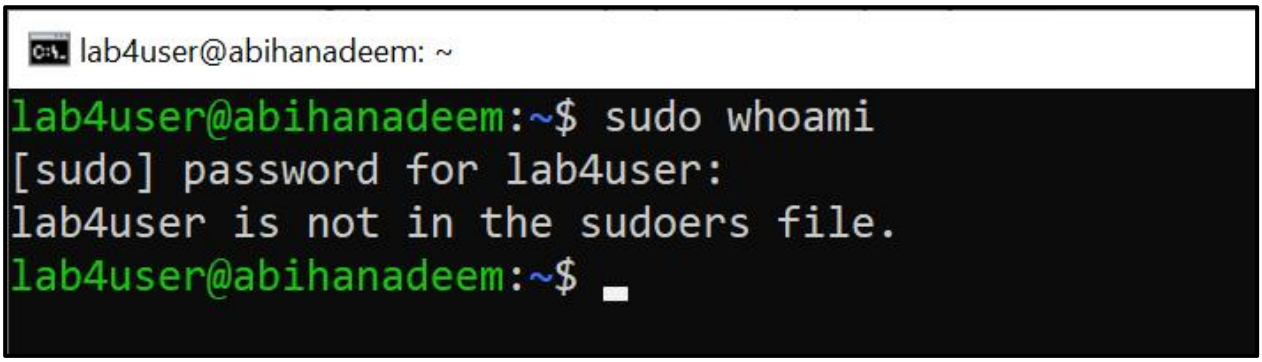


2. Verify the user entry:

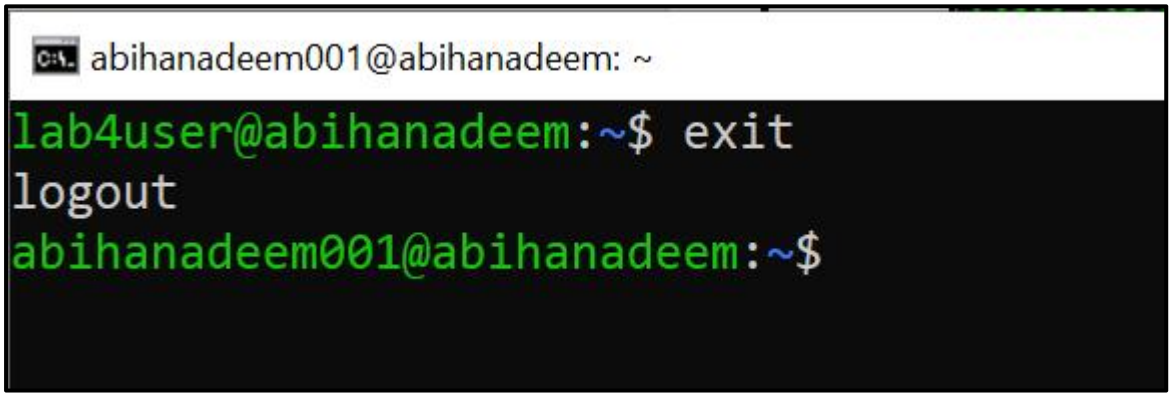
3. Switch to the new user to verify login:



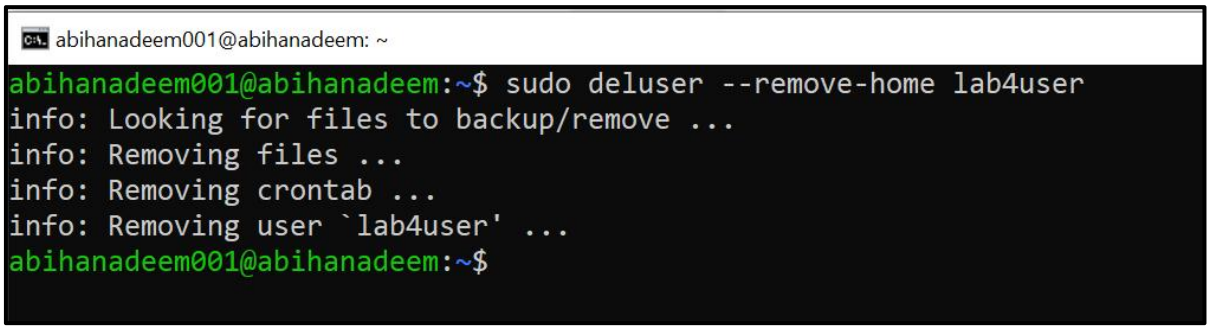
4. From the new user you may attempt a sudo command to show that sudo is not available for this account (expected failure), e.g.:



5. Return to the original user:



6. (Optional) Remove the test user when finished:



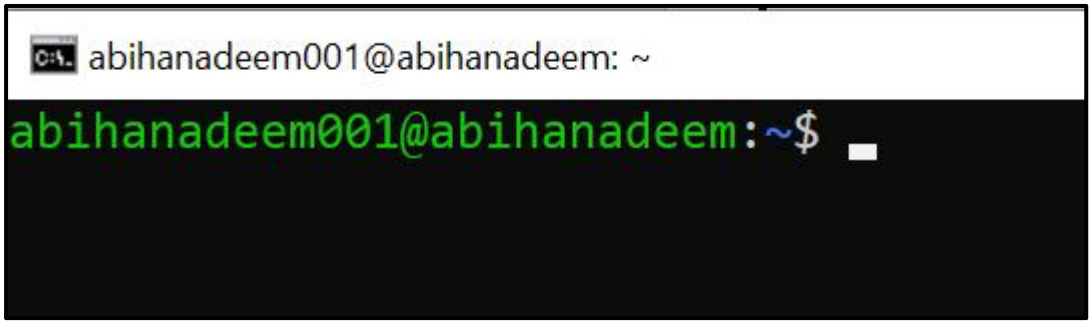
Exam Evaluation Questions

1. Remote Access Verification (Cyber Login Check)

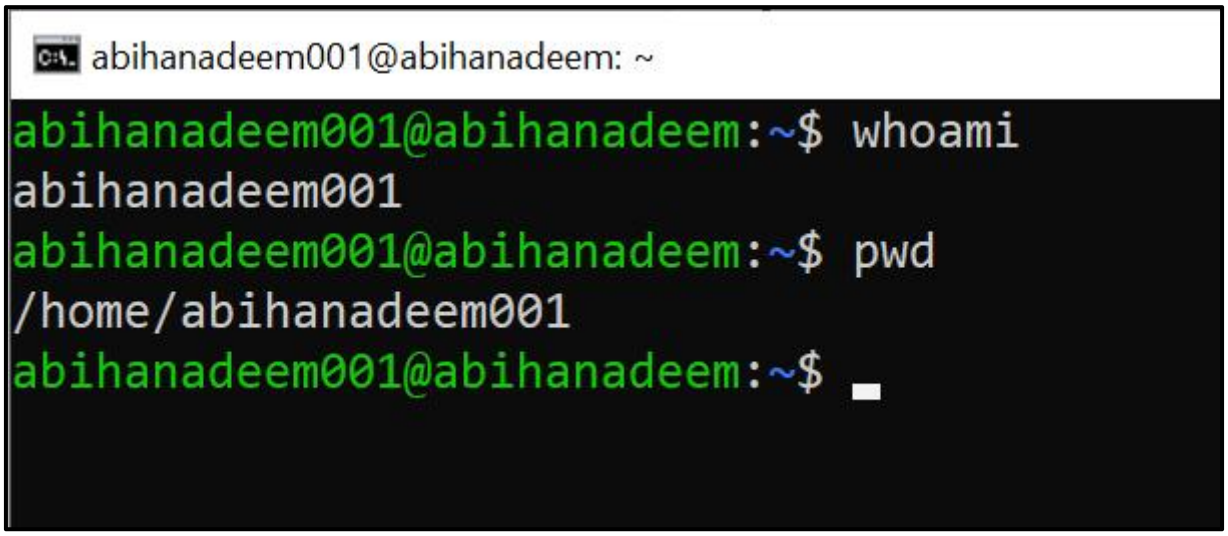
Scenario:
You are part of a SOC (Security Operations Center) investigating unauthorized access to a Linux server hosted on VMware. Prove you can securely connect and verify your identity.

Steps:

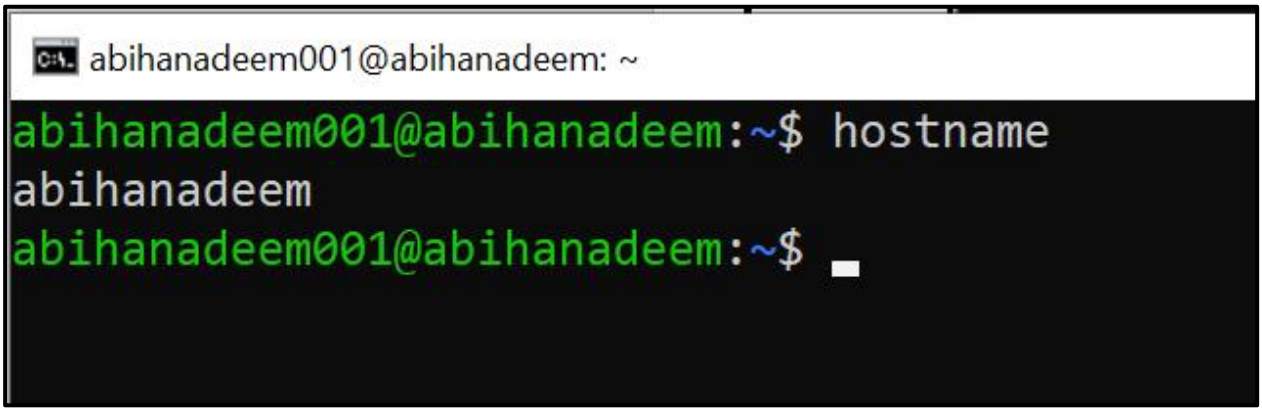
1. Connect to the Ubuntu VM remotely from your host terminal.
    - Screenshot as Q1_remote_connection.png



2. Verify your current user and home directory path.
    - Screenshot as Q1_user_verification.png



3. Confirm you are connected to the correct host machine.
    - Screenshot as Q1_host_confirmation.png



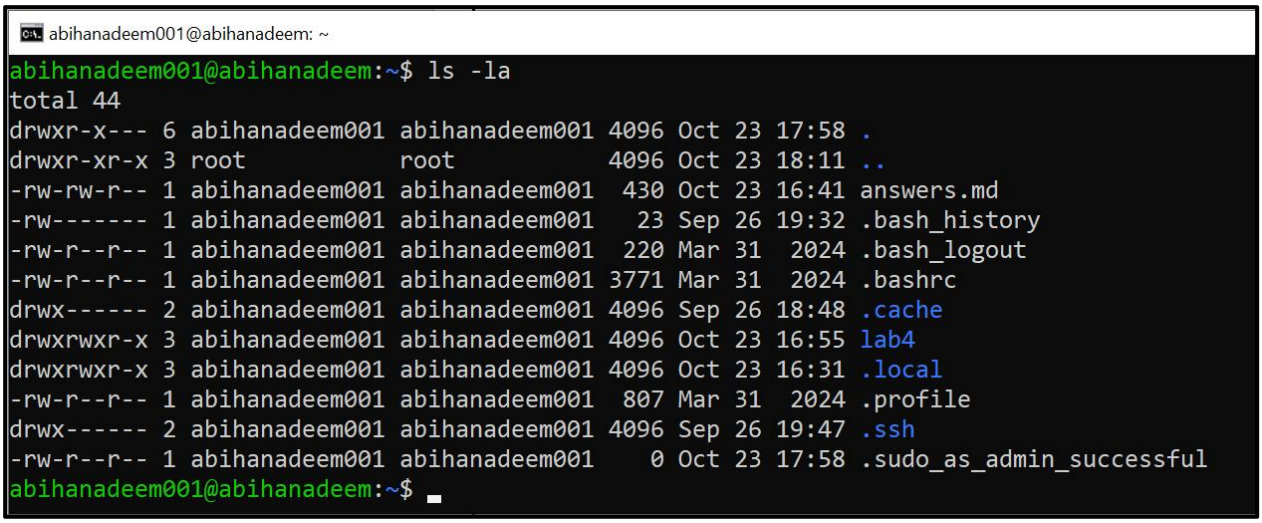
2. Filesystem Inspection for Forensic Evidence

Scenario:

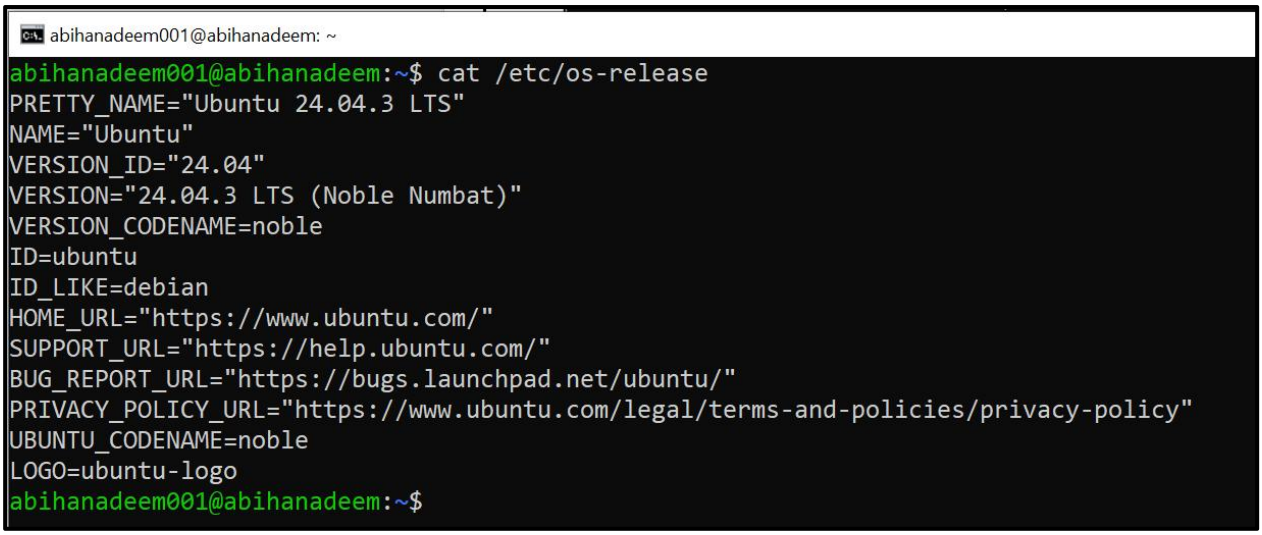
The incident response team suspects malicious files in system directories. You must explore the filesystem to locate and document the system's structure.

Steps:

1. Display the contents of the root directory.
    - Screenshot as Q2_root_listing.png



2. Display the OS version and release information.
    - Screenshot as Q2_os_version.png



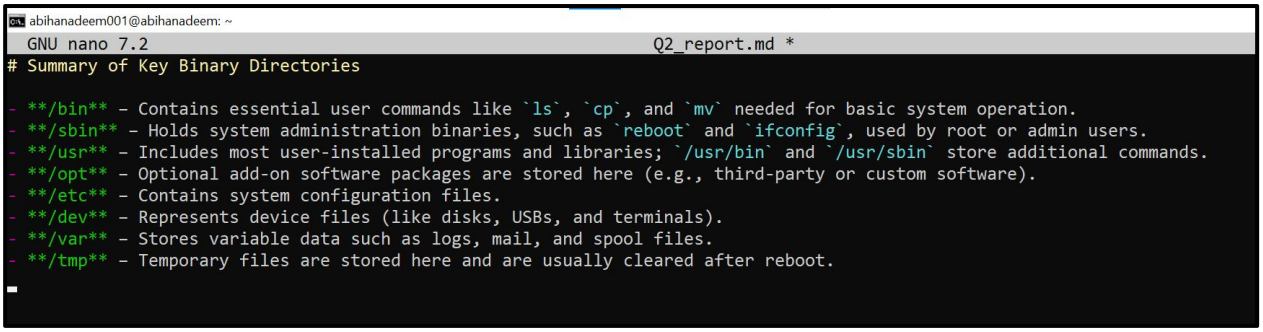
3. Explore and record directory listings for /bin, /sbin, /usr, /opt, /etc, /dev, /var, and /tmp.
    - Screenshot as Q2_directory_evidence.png

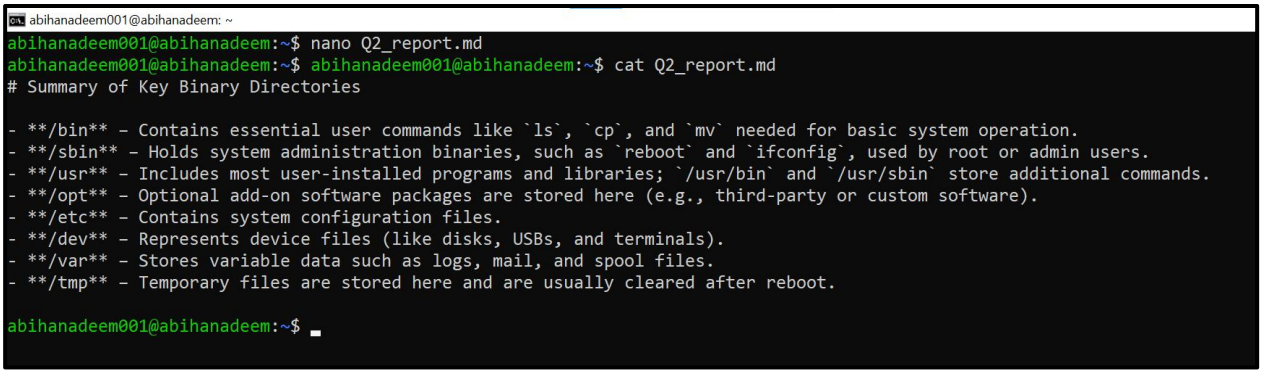
```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls /bin | head -n 2
[
aa-enabled
abihanadeem001@abihanadeem:~$ ls /sbin | head -n 2
aa-load
aa-remove-unknown
abihanadeem001@abihanadeem:~$ ls /usr | head -n 2
bin
games
abihanadeem001@abihanadeem:~$ ls /opt | head -n 2
abihanadeem001@abihanadeem:~$ ls /etc | head -n 2
adduser.conf
alternatives
abihanadeem001@abihanadeem:~$ ls /dev | head -n 2
autofs
block
abihanadeem001@abihanadeem:~$ ls /var | head -n 2
backups
cache
abihanadeem001@abihanadeem:~$ ls /tmp | head -n 2
snap-private-tmp
systemd-private-da0258f4edd04fd5ac9e78aa00941ac9-fwupd.service-sAHSiC
abihanadeem001@abihanadeem:~$
```

4. Display all hidden files in your home directory.
    - Screenshot as Q2_hidden_files.png

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ls -la ~
total 44
drwxr-x--- 6 abihanadeem001 abihanadeem001 4096 Oct 23 17:58 .
drwxr-xr-x 3 root           root           4096 Oct 23 18:11 ..
-rw-rw-r-- 1 abihanadeem001 abihanadeem001  430 Oct 23 16:41 answers.md
-rw------- 1 abihanadeem001 abihanadeem001   23 Sep 26 19:32 .bash_history
-rw-r--r-- 1 abihanadeem001 abihanadeem001  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 abihanadeem001 abihanadeem001 3771 Mar 31  2024 .bashrc
drwx------ 2 abihanadeem001 abihanadeem001 4096 Sep 26 18:48 .cache
drwxrwxr-x 3 abihanadeem001 abihanadeem001 4096 Oct 23 16:55 lab4
drwxrwxr-x 3 abihanadeem001 abihanadeem001 4096 Oct 23 16:31 .local
-rw-r--r-- 1 abihanadeem001 abihanadeem001  807 Mar 31  2024 .profile
drwx------ 2 abihanadeem001 abihanadeem001 4096 Sep 26 19:47 .ssh
-rw-r--r-- 1 abihanadeem001 abihanadeem001    0 Oct 23 17:58 .sudo_as_admin_successful
abihanadeem001@abihanadeem:~$
```

5. Create a markdown file summarizing your findings on key binary directories.
    - Screenshot as Q2_report_file.png



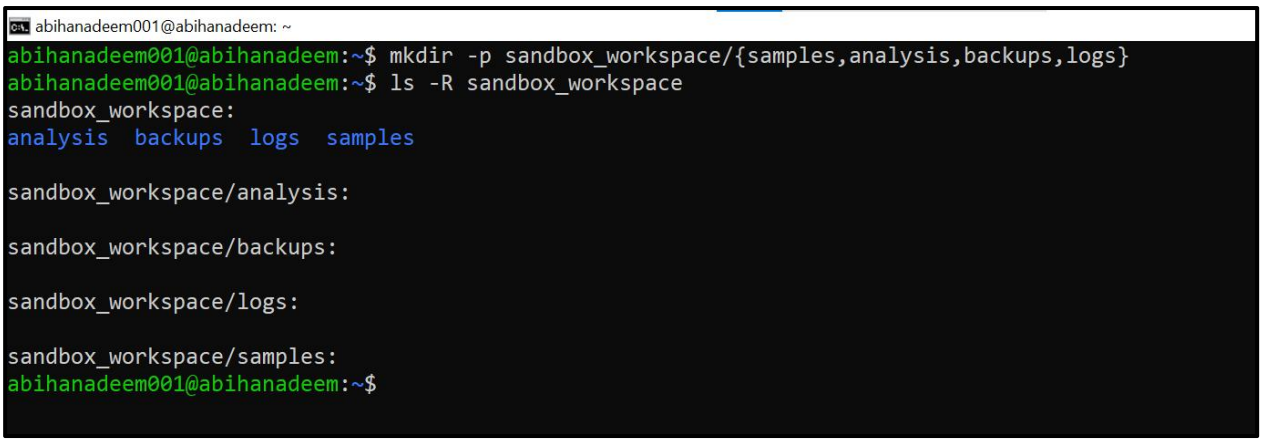


3. Evidence Handling & File Operations

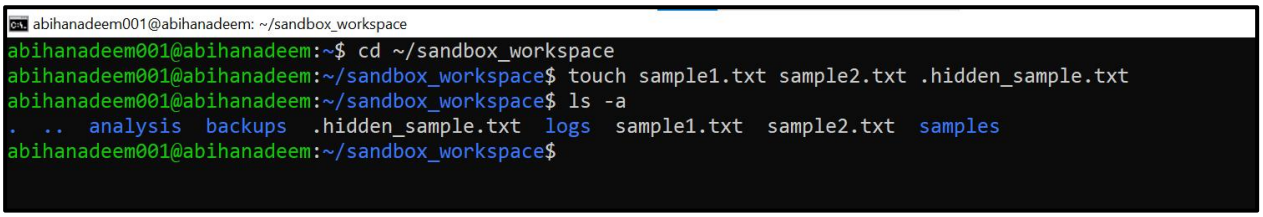
You are creating a sandbox environment to safely analyze and handle suspicious files collected from a compromised system.

Steps:

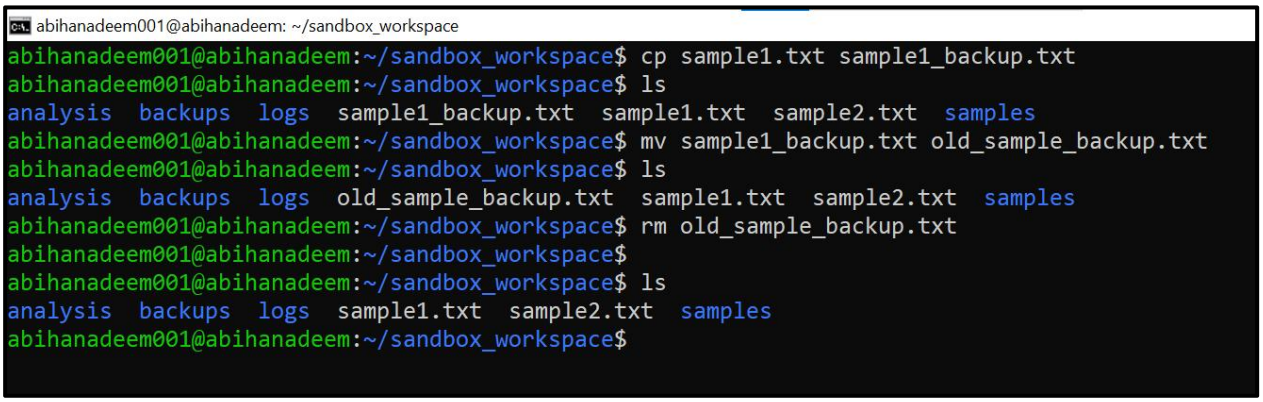
1. Create a structured folder hierarchy under your home directory for analysis.
    - Screenshot as Q3_workspace_created.png



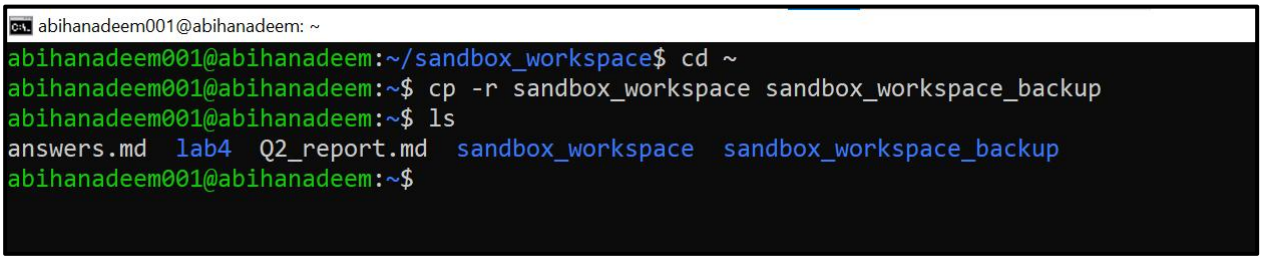
2. Create three text files, including one hidden file, in your workspace.
    - Screenshot as Q3_files_created.png



3. Create a backup copy of one file, rename it, and then delete it after verification.
    - Screenshot as Q3_backup_handling.png



4. Copy the entire workspace as an evidence backup folder.
    - Screenshot as Q3_workspace_backup.png
    -



5. Display your command history to document all actions performed.
    - Screenshot as Q3_command_history.png

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ history
    1  ip addr
    2  inet
    3  ipne
    4  inet
    5  whoami
    6  pwd
    7  ls -la /
    8  ls -la /bin
    9  ls -la /sbin
   10  ls -la /usr
   11  ls -la /opt
   12  ls -la /etc
   13  ls -la /dev
   14  ls -la /var
   15  ls -la /tmp
   16  ls -la ~
   17  nano ~/answers.md
   18  cat ~/answers.md
   19  mkdir -p ~/lab4/workspace/python_project
   20  cd ~/lab4/workspace/python_project
   21  pwd
   22  nano README.md
   23  nano main.py
   24  nano .env
   25  ls -la
   26  cp README.md README.copy.md
   27  mv README.copy.md README.dev.md
   28  rm README.dev.md
   29  mkdir -p ~/lab4/workspace/java_app
   30  cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
   31  ls -la ~/lab4/workspace
```

```
abihanadeem001@abihanadeem: ~
   58  cat /etc/os-release
   59  ls /bin
   60  ls /bin | head -n 2
   61  ls /sbin | head -n 2
   62  ls /usr | head -n 2
   63  ls /opt | head -n 2
   64  ls /etc | head -n 2
   65  ls /dev | head -n 2
   66  ls /var | head -n 2
   67  ls /tmp | head -n 2
   68  ls -la ~
   69  nano Q2_reportmd
   70  nano Q2_report.md
   71  cat Q2_report.md
   72  mkdir -p sandbox_workspace/{samples,analysis,backups,logs}
   73  tree sandbox_workspace
   74  mkdir -p sandbox_workspace/{samples,analysis,backups,logs}
   75  ls -R sandbox_workspace
   76  cd ~/sandbox_workspace
   77  touch sample1.txt sample2.txt .hidden_sample.txt
   78  ls -a
   79  cp sample1.txt sample1_backup.txt
   80  ls
   81  mv sample1_backup.txt old_sample_backup.txt
   82  ls
   83  rm old_sample_backup.txt
   84  ls
   85  cd ~
   86  cp -r sandbox_workspace sandbox_workspace_backup
   87  ls
   88  history
abihanadeem001@abihanadeem:~$
```

6. Demonstrate Linux auto-completion by typing a partial command or filename.
    - Screenshot as Q3_autocomplete.png

```
abihanadeem001@abihanadeem: ~/sandbox_workspace
abihanadeem001@abihanadeem:~/sandbox_workspace$ cat sample
cat: sample: No such file or directory
abihanadeem001@abihanadeem:~/sandbox_workspace$
```

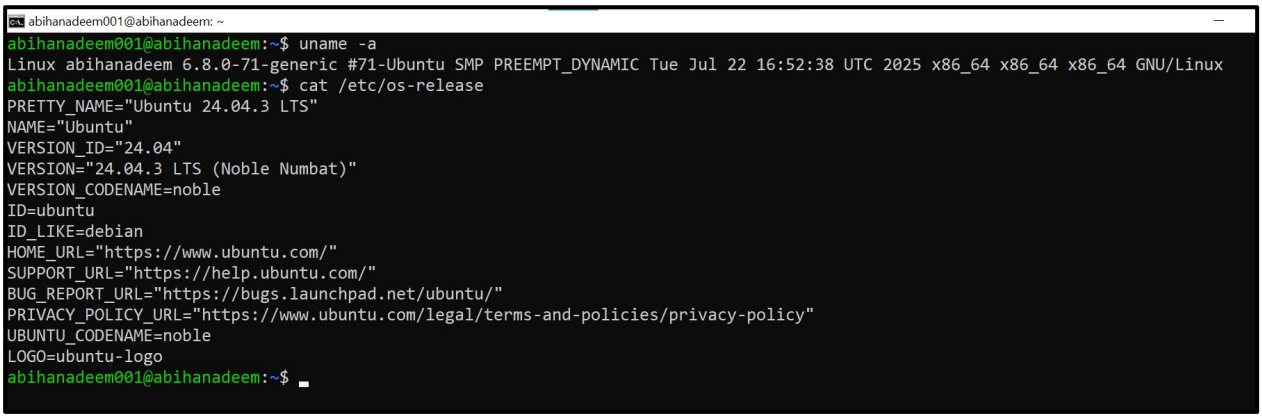
4. System Profiling and Process Monitoring

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



2. Display CPU, memory, and disk usage information.
    - Screenshot as Q4_resource_info.png

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ cat /proc/cpuinfo | head 10
head: cannot open '10' for reading: No such file or directory
abihanadeem001@abihanadeem:~$ cat /proc/cpuinfo | head -10
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 142
model name      : Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz
stepping        : 9
microcode       : 0xffffffff
cpu MHz         : 2711.999
cache size      : 3072 KB
physical id     : 0
abihanadeem001@abihanadeem:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       413Mi       290Mi       1.3Mi       1.4Gi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
abihanadeem001@abihanadeem:~$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              192M  1.3M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  9.8G  5.3G  4.0G  58% /
tmpfs                              960M     0  960M   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.8G  100M  1.6G   7% /boot
tmpfs                              192M   12K  192M   1% /run/user/1000
abihanadeem001@abihanadeem:~$
```

3. Display all active running processes to identify suspicious activity.
    - Screenshot as Q4_process_list.png

```
abihanadeem001@abihanadeem: ~
abihanadeem001@abihanadeem:~$ ps aux | head -20
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.6  22116 12836 ?        Ss   15:45   0:07 /sbin/init
root           2  0.0  0.0      0     0 ?        S    15:45   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    15:45   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   15:45   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   15:45   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   15:45   0:00 [kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   15:45   0:00 [kworker/R-netns]
root          11  0.0  0.0      0     0 ?        I    15:45   0:00 [kworker/u256:0-ext4-rsv-conversion]
root          12  0.0  0.0      0     0 ?        I<   15:45   0:00 [kworker/R-mm_pe]
root          13  0.0  0.0      0     0 ?        I    15:45   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    15:45   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    15:45   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    15:45   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    15:45   0:01 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    15:45   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    15:45   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    15:45   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    15:45   0:00 [cpuhp/1]
root          22  0.0  0.0      0     0 ?        S    15:45   0:00 [idle_inject/1]
abihanadeem001@abihanadeem:~$
```

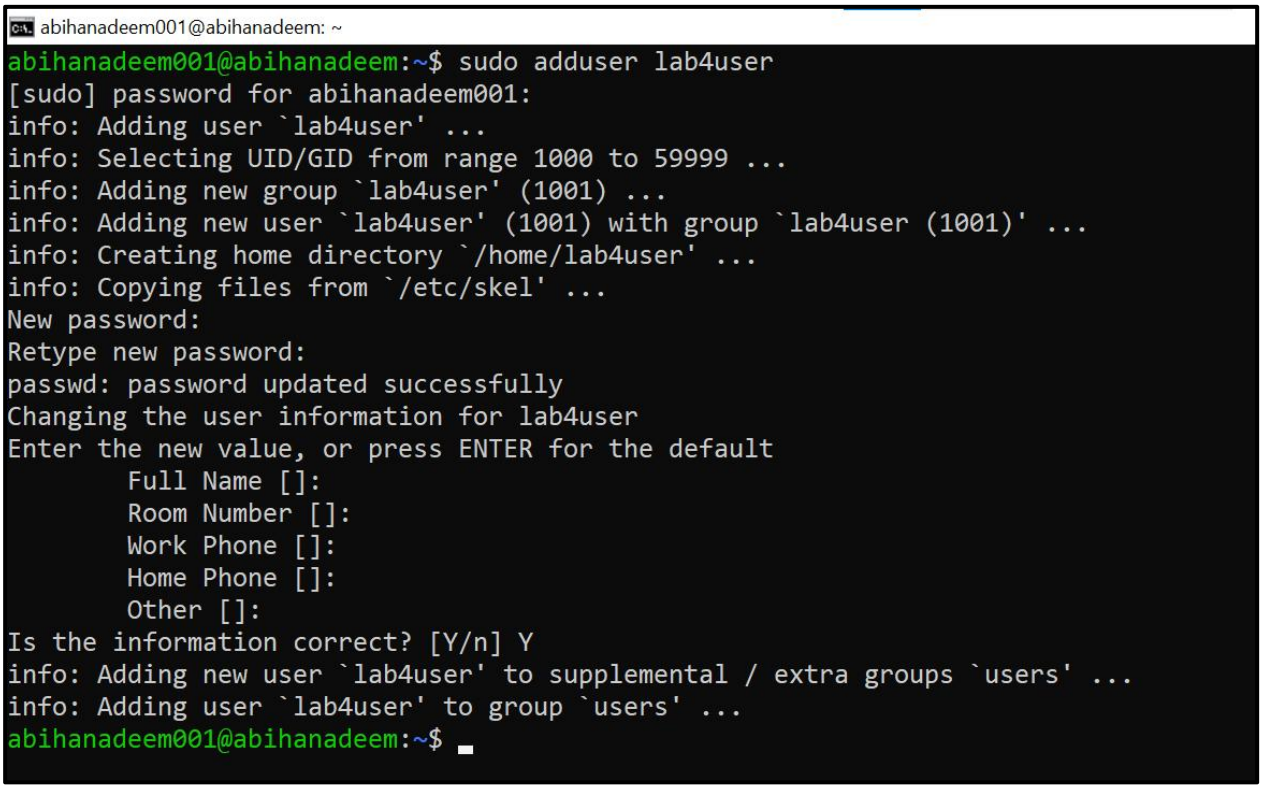
5. User Account Audit & Privilege Escalation Simulation

Scenario:

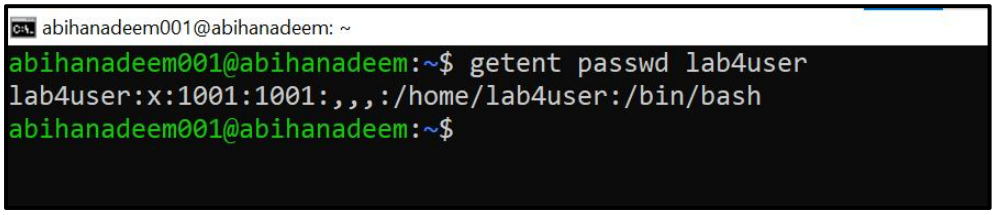
You are performing a **user activity audit** on a compromised Linux server.
The SOC suspects a newly created account (lab4user) may have been used for unauthorized access.
Your task is to simulate the account creation, perform privilege tests, and analyze authentication logs for forensic evidence.

Steps:

1. Create a new test user named lab4user.
    - Screenshot as Q5_user_created.png

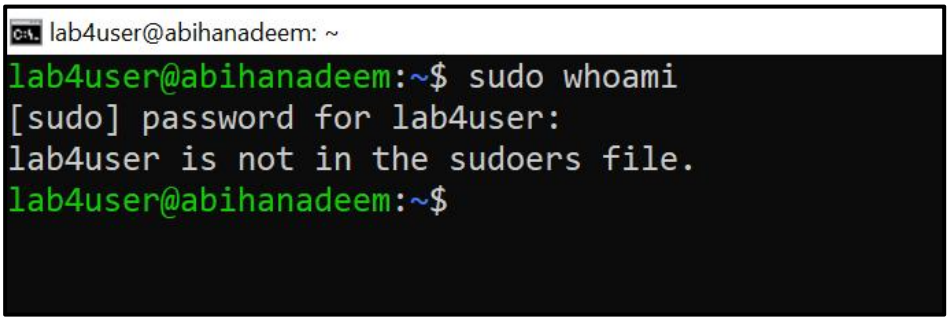


2. Verify that the new user record exists in the system's user database.
    - Screenshot as Q5_user_verified.png

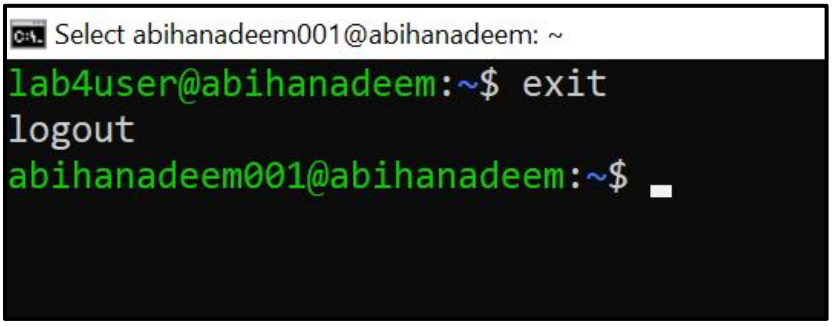


3. Log in as lab4user and confirm successful login.
    - Screenshot as Q5_user_login.png

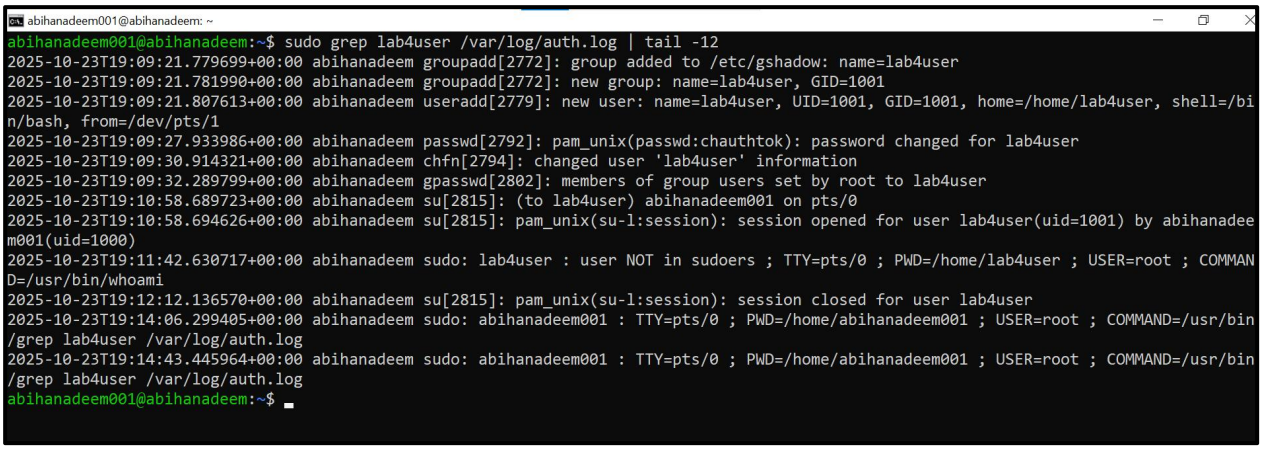
4. Attempt to run an administrative command as lab4user (expect permission denied).
    - Screenshot as Q5_permission_denied.png



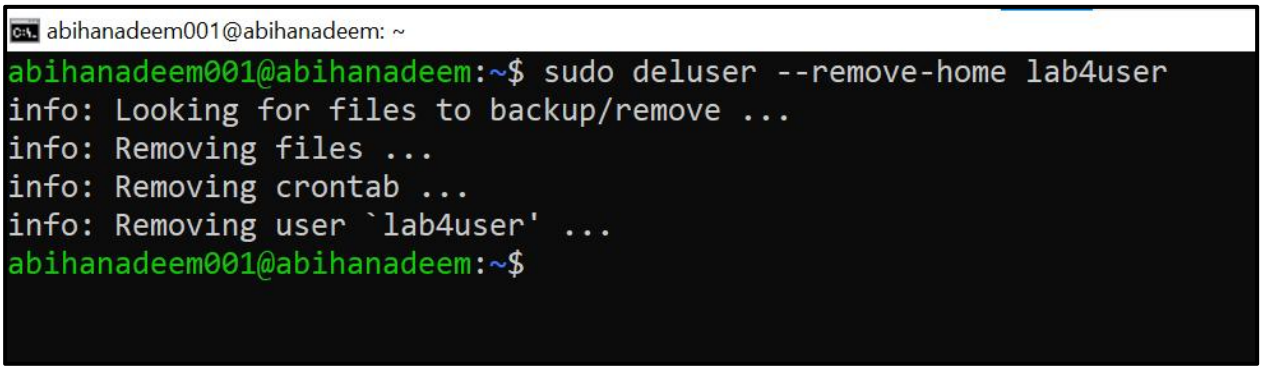
5. Switch back to your main analyst account.
    - Screenshot as Q5_switch_back.png



6. 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



7. (Optional) Remove the lab4user account after the audit and verify deletion.
    - Screenshot as Q5_user_removed.png



****