FATIMA JINNAH WOMEN UNIVERSITY

Department of Software Engineering

LAB #04

SUBJECT: CLOUD COMPUTING

SUBMITTED TO: SIR MUHAMMAD SHOAIB

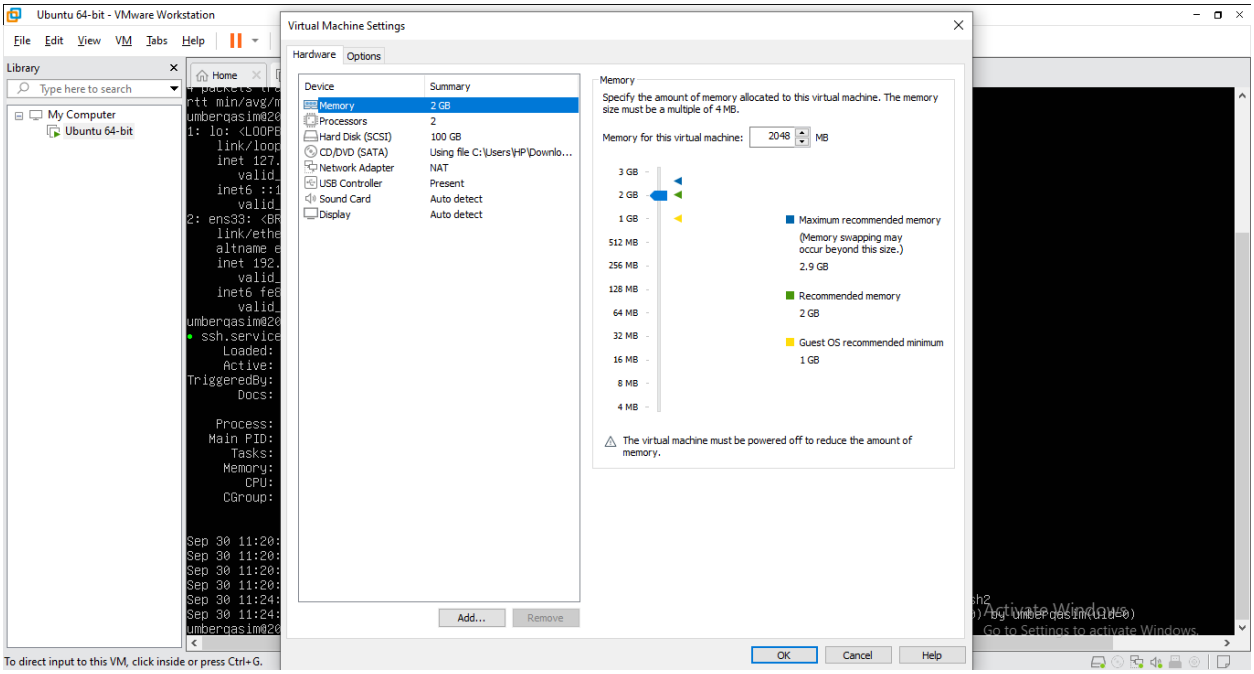
SUBMITTED BY: UMBER QASIM

REGISTRATION NO: 2023-BSE-066

CLASS: BSSE V-B

Virtualization & Linux Fundamentals

Task#01: Verify VM resources in VMware



Task#02: Start VM and log in (use your preferred host terminal method only)

umberqasim@2023-bse-066: ~

```
Microsoft Windows [Version 10.0.19045.6456]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ssh umberqasim@192.168.254.129
umberqasim@192.168.254.129'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 Fri Oct 17 05:14:13 AM UTC 2025

  System load:  0.0               Processes:             222
  Usage of /:   10.5% of 47.93GB  Users logged in:       1
  Memory usage: 20%               IPv4 address for ens33: 192.168.254.129
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

17 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Fri Oct 17 05:07:43 2025 from 192.168.254.1
umberqasim@2023-bse-066:~$
```

```
umberqasim@2023-bse-066:~$ whoami
umberqasim
umberqasim@2023-bse-066:~$ pwd
/home/umberqasim
umberqasim@2023-bse-066:~$
```

Task#03: Filesystem exploration — root tree and dotfiles

List root directory

```
umberqasim@2023-bse-066:~$ ls -la /
total 2097244
drwxr-xr-x  23 root root       4096 Sep 30 03:05 .
drwxr-xr-x  23 root root       4096 Sep 30 03:05 ..
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 Oct 17 04:18 boot
dr-xr-xr-x   2 root root       4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root       4120 Sep 30 11:20 dev
drwxr-xr-x 108 root root       4096 Oct 17 04:16 etc
drwxr-xr-x   3 root root       4096 Sep 30 03:12 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 30 02:57 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 283 root root          0 Sep 30 11:19 proc
drwx------   3 root root       4096 Oct 17 04:54 root
drwxr-xr-x  31 root root       1000 Oct 17 05:14 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 30 03:12 snap
drwxr-xr-x   2 root root       4096 Aug  5 16:54 srv
-rw-------   1 root root 2147483648 Sep 30 03:05 swap.img
dr-xr-xr-x  13 root root          0 Sep 30 11:19 sys
drwxrwxrwt  16 root root       4096 Oct 17 04:17 tmp
drwxr-xr-x  12 root root       4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root       4096 Sep 30 03:12 var
```

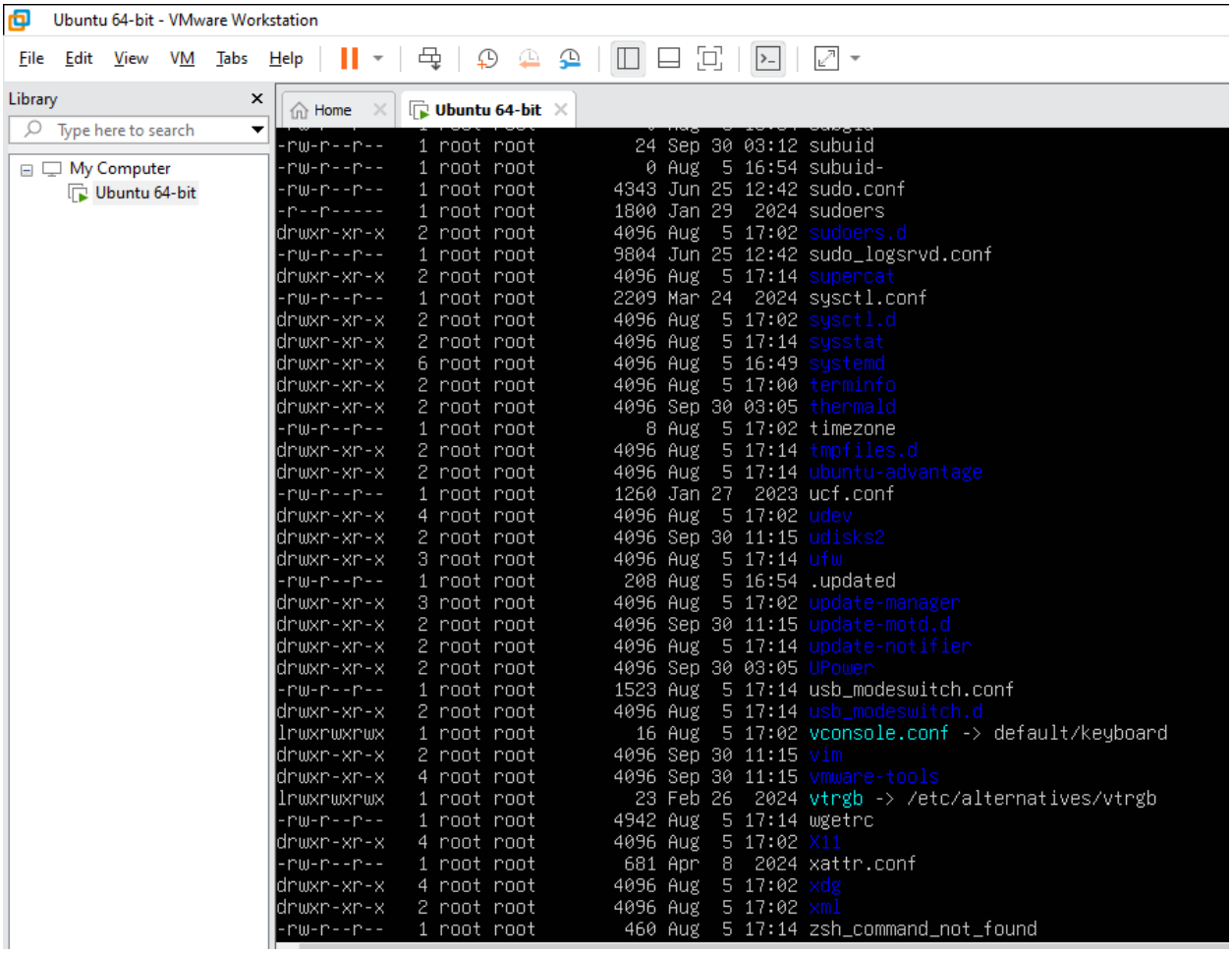
Explore key directories

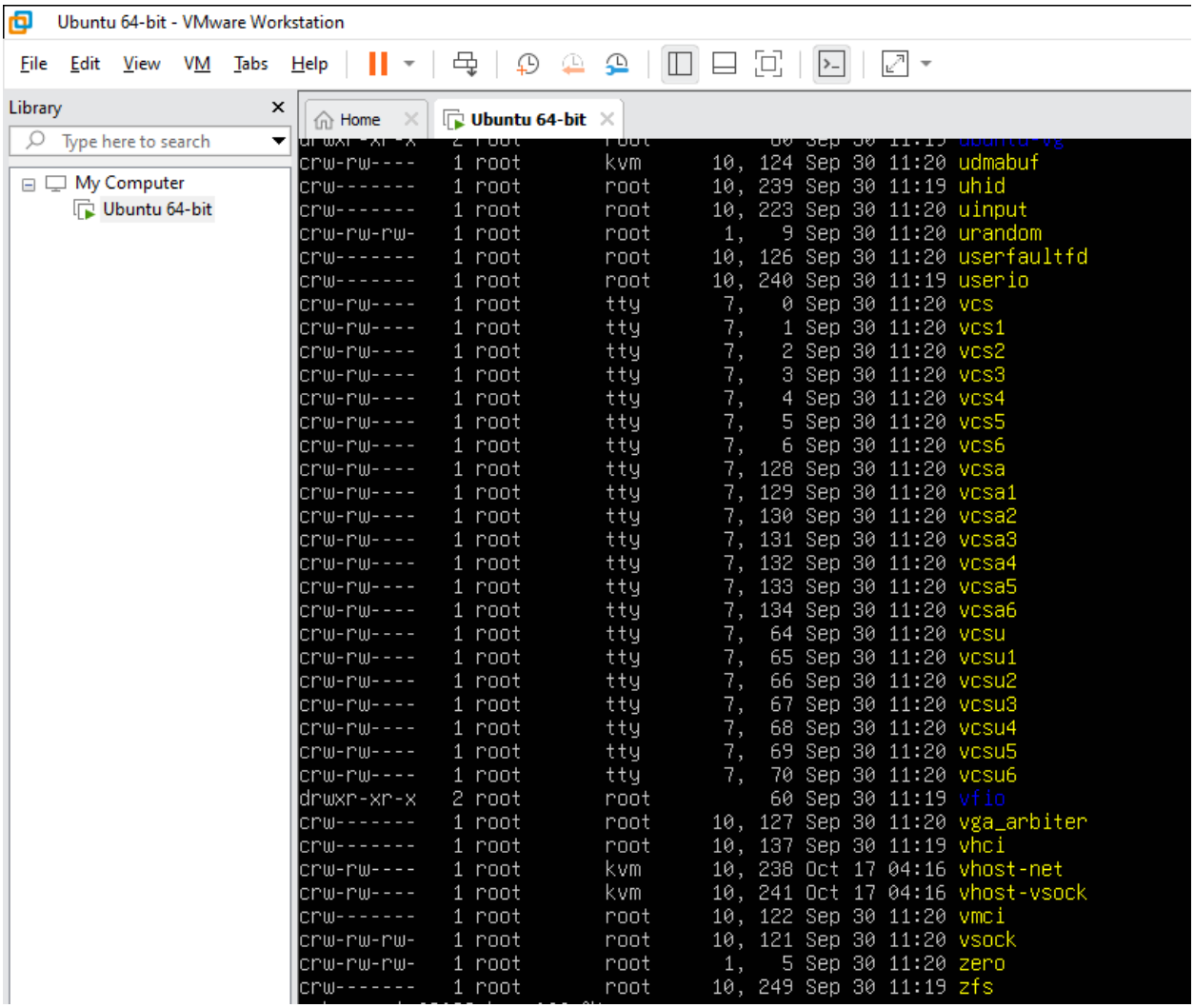
```
umberqasim@2023-bse-066:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
```

```
umberqasim@2023-bse-066:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
```

```
umberqasim@2023-bse-066:~$ ls -la /usr
total 108
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Sep 30 03:05 ..
drwxr-xr-x   2 root root 36864 Oct 17 04:17 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root 16384 Sep 30 11:13 include
drwxr-xr-x  79 root root  4096 Oct 17 04:18 lib
drwxr-xr-x   2 root root  4096 Sep 30 11:13 lib64
drwxr-xr-x  11 root root  4096 Sep 30 03:05 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Oct 17 04:17 sbin
drwxr-xr-x 124 root root  4096 Sep 30 05:21 share
drwxr-xr-x   6 root root  4096 Oct 17 04:18 src
```

```
umberqasim@2023-bse-066:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..
```



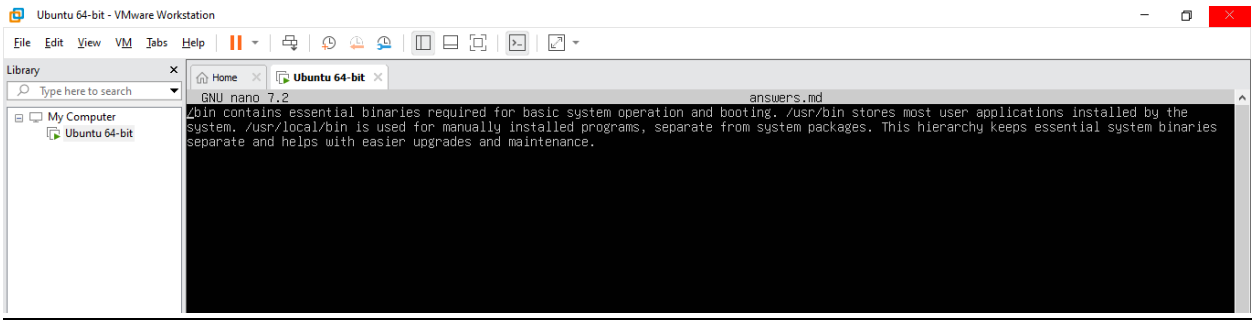



```
umberqasim@2023-bse-066:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Sep 30 03:12 .
drwxr-xr-x 23 root root   4096 Sep 30 03:05 ..
drwxr-xr-x  2 root root   4096 Oct 19 07:09 backups
drwxr-xr-x 16 root root   4096 Sep 30 05:06 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Sep 30 05:06 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 19 07:09 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 19 07:12 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
```

```
umberqasim@2023-bse-066:~$ ls -la /tmp
total 64
drwxrwxrwt 16 root root 4096 Oct 19 07:12 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..
drwxrwxrwt  2 root root 4096 Sep 30 11:19 .font-unix
drwxrwxrwt  2 root root 4096 Sep 30 11:19 .ICE-unix
drwx------  2 root root 4096 Sep 30 11:19 snap-private-tmp
drwx------  3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-fwupd.service-70ZtQF
drwx------  3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-ModemManager.service-7qmoT9
drwx------  3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-polkit.service-M5032n
drwx------  3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-logind.service-YwgFeh
drwx------  3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-resolved.service-qWrVZf
drwx------  3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-timesyncd.service-BwRz3V
drwx------  3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-upower.service-Uwp0A2
drwx------  2 root root 4096 Oct 17 04:16 vmware-root_3320-2999004153
drwx------  2 root root 4096 Sep 30 11:20 vmware-root_741-4248811580
drwxrwxrwt  2 root root 4096 Sep 30 11:19 .X11-unix
drwxrwxrwt  2 root root 4096 Sep 30 11:19 .XIM-unix
```



```
umberqasim@2023-bse-066:~$ ls -la ~
total 36
drwxr-x--- 4 umberqasim umberqasim 4096 Oct  2 12:23 .
drwxr-xr-x 3 root       root       4096 Sep 30 03:12 ..
-rw------- 1 umberqasim umberqasim  429 Oct 17 05:13 .bash_history
-rw-r--r-- 1 umberqasim umberqasim  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 umberqasim umberqasim 3771 Mar 31  2024 .bashrc
drwx------ 2 umberqasim umberqasim 4096 Sep 30 03:17 .cache
-rw------- 1 umberqasim umberqasim   20 Oct  2 12:23 .lesshst
-rw-r--r-- 1 umberqasim umberqasim  807 Mar 31  2024 .profile
drwx------ 2 umberqasim umberqasim 4096 Sep 30 05:47 .ssh
-rw-r--r-- 1 umberqasim umberqasim    0 Sep 30 05:14 .sudo_as_admin_successful
```



Task#04: Essential CLI tasks — navigation and file operations

Creating Workspace

```
umberqasim@2023-bse-066:~$ mkdir -p ~/lab4/workspace/python_project
```

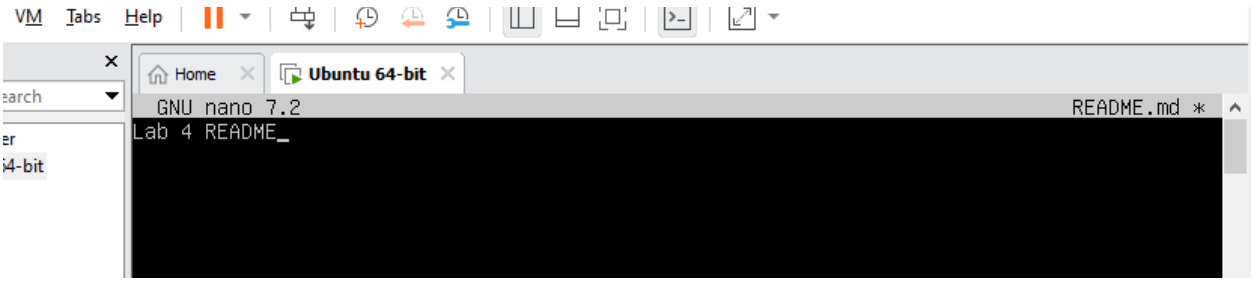
Navigating

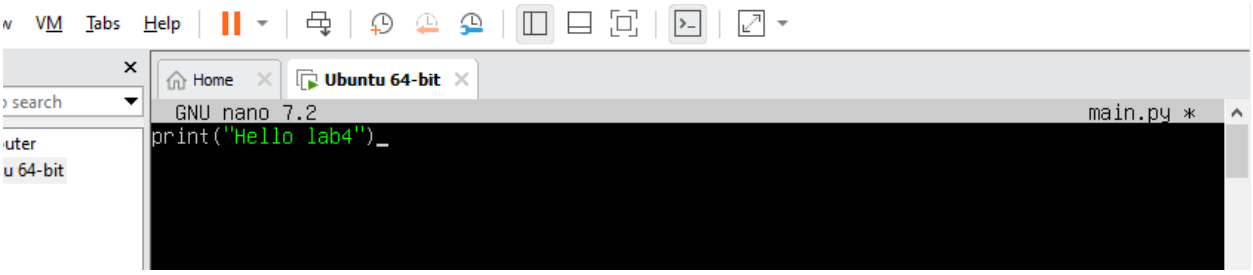
```
umberqasim@2023-bse-066:~$ cd ~/lab4/workspace/python_project
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ _
```

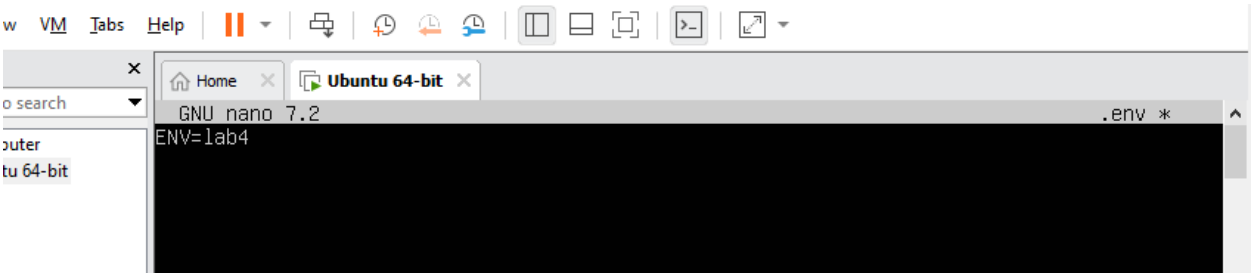
Current directory check

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ pwd
/home/umberqasim/lab4/workspace/python_project
```

Creating files







List files

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 umberqasim umberqasim 4096 Oct 23 12:15 .
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 12:05 ..
-rw-rw-r-- 1 umberqasim umberqasim    9 Oct 23 12:15 .env
-rw-rw-r-- 1 umberqasim umberqasim   20 Oct 23 12:14 main.py
-rw-rw-r-- 1 umberqasim umberqasim   13 Oct 23 12:12 README.md
umberqasim@2023-bse-066:~/lab4/workspace/python_project$
```

Copy README.md

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ cp README.md README.copy.md
```

Move (rename) copied file

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ mv README.copy.md README.dev.md
```

Delete that file

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ rm README.dev.md
```

Create another folder (for Java)

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
```

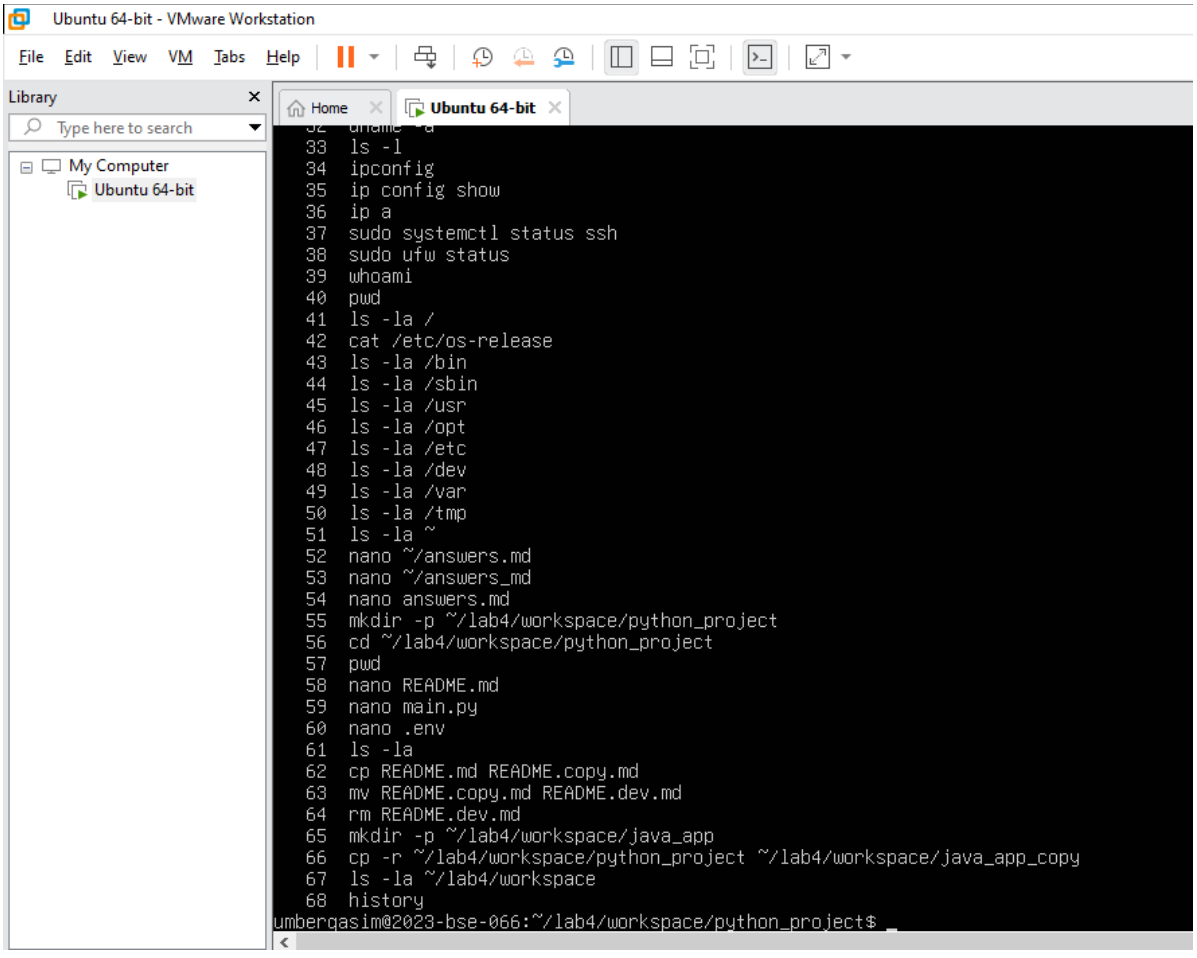
Copy entire python_project folder

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
```

Verify copy

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 umberqasim umberqasim 4096 Oct 23 12:29 .
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 12:05 ..
drwxrwxr-x 2 umberqasim umberqasim 4096 Oct 23 12:25 java_app
drwxrwxr-x 2 umberqasim umberqasim 4096 Oct 23 12:29 java_app_copy
drwxrwxr-x 2 umberqasim umberqasim 4096 Oct 23 12:22 python_project
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ _
```

Show command history



Demonstrate tab completion

Before tab:

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ cd ~/lab4/workspace/p_
```

After tab:

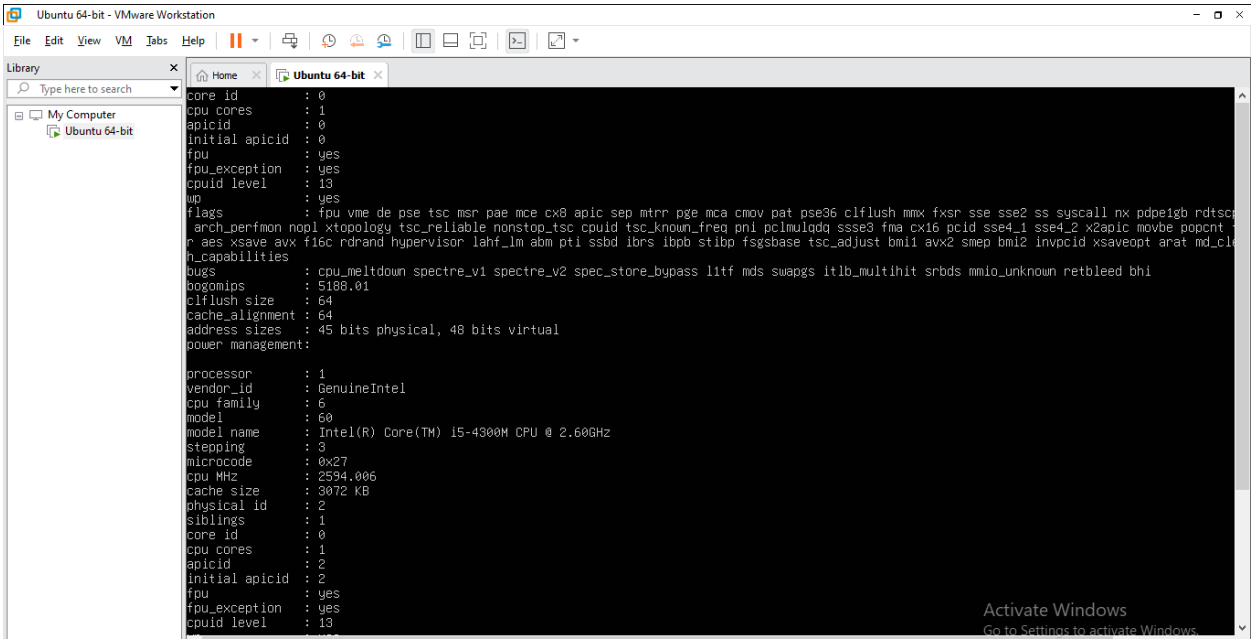
```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ cd ~/lab4/workspace/python_project/_
```

Task#05: System info, resources & processes

Kernel and OS info

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ uname -a
Linux 2023-bse-066 6.8.0-84-generic #84-Ubuntu SMP PREEMPT_DYNAMIC Fri Sep  5 22:36:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

CPU details



Memory information

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       437Mi       576Mi       920Ki       1.1Gi       1.4Gi
Swap:          2.0Gi       780Ki       2.0Gi
```

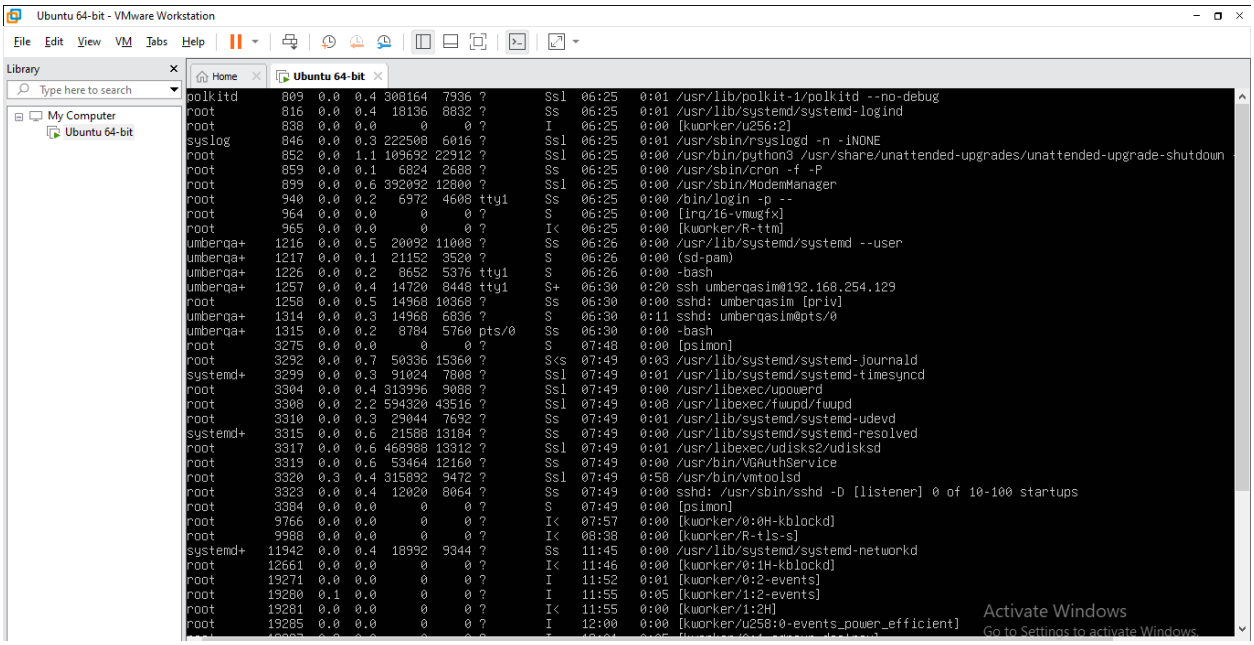
Disk information

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              192M  1.3M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   48G  5.1G   41G  12% /
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   12K  192M   1% /run/user/1000
```

OS release version

```
umberqasim@2023-bse-066:~/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
```

Running processes



<u>Task#06:</u> Users and account verification (no sudo group change)

Create new user

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ sudo adduser lab4user
[sudo] password for umberqasim:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
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 []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
```

Verify user entry

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ getent passwd lab4user
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
```

Switch to new user

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ su - lab4user
Password:
lab4user@2023-bse-066:~$ _
```

Verify that sudo is not allowed

```
lab4user@2023-bse-066:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
```

Return to original user

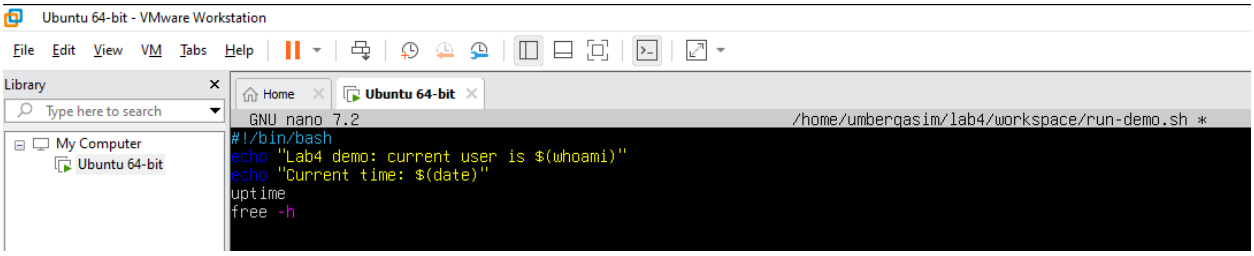
```
lab4user@2023-bse-066:~$ exit
logout
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/python_project
```

Remove test user (cleanup)

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
[sudo] password for umberqasim:
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
umberqasim@2023-bse-066:~/lab4/workspace/python_project$
```

Bonus Task#07: Create a small demo script using an editor and run it

Creating script using nano



Make script executable

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ chmod +x ~/lab4/workspace/run-demo.sh
```

Run script like a normal user

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ~/lab4/workspace/run-demo.sh
Lab4 demo: current user is umberqasim
Current time: Thu Oct 23 02:18:09 PM UTC 2025
 14:18:09 up  7:51,  2 users,  load average: 0.06, 0.05, 0.00
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       435Mi       554Mi       924Ki       1.1Gi       1.5Gi
Swap:          2.0Gi       780Ki       2.0Gi
```

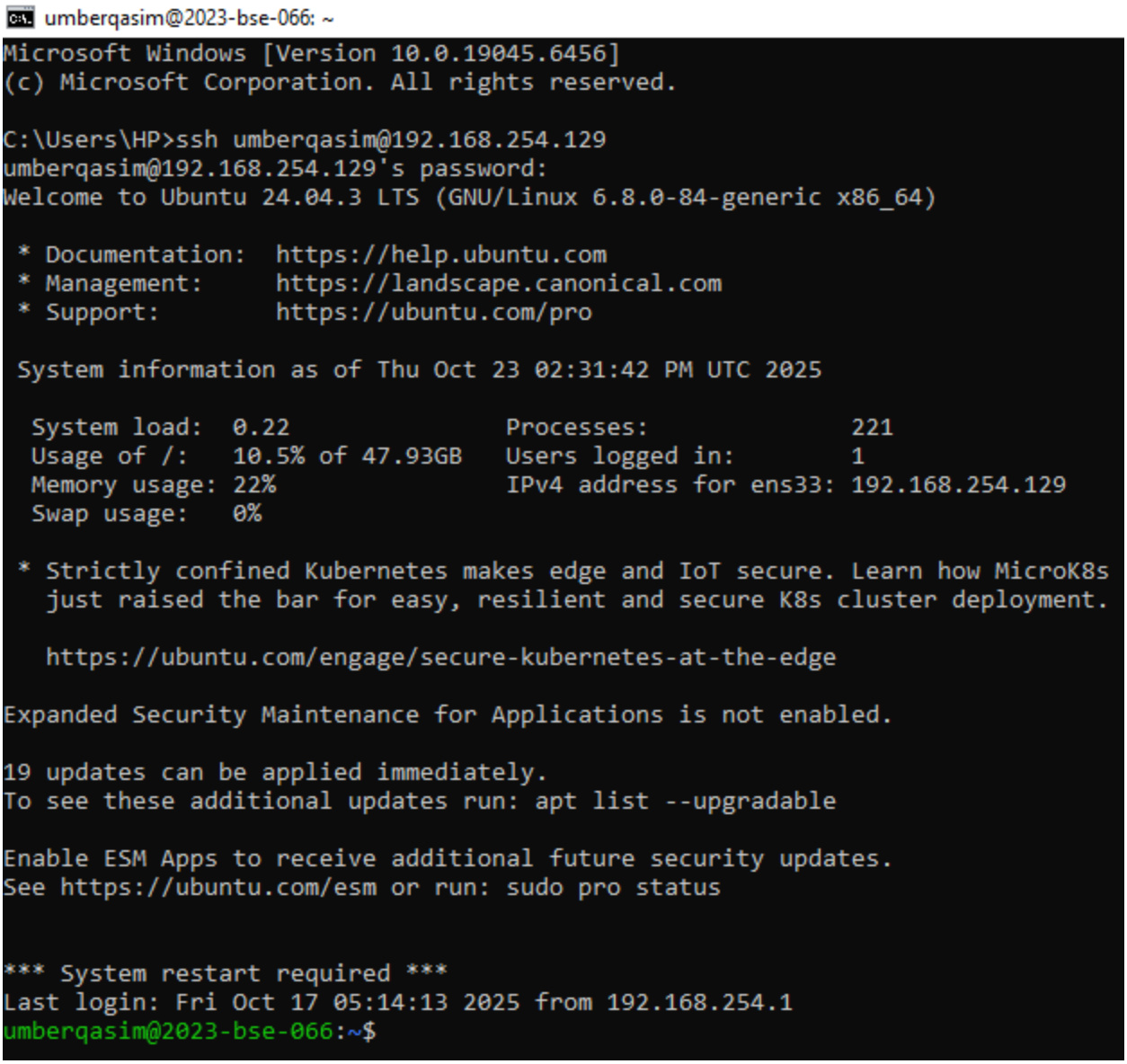
Run with sudo

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ sudo ~/lab4/workspace/run-demo.sh
[sudo] password for umberqasim:
Lab4 demo: current user is root
Current time: Thu Oct 23 02:19:34 PM UTC 2025
 14:19:34 up  7:53,  2 users,  load average: 0.01, 0.03, 0.00
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       436Mi       553Mi       924Ki       1.1Gi       1.4Gi
Swap:          2.0Gi       780Ki       2.0Gi
```

Exam Evaluation Questions

I. Remote Access Verification (Cyber Login Check)

Connect remotely from your host (Windows CMD)



Verify current user and home directory

```
umberqasim@2023-bse-066:~$ whoami
umberqasim
umberqasim@2023-bse-066:~$ pwd
/home/umberqasim
umberqasim@2023-bse-066:~$
```

Confirm correct host machine

```
umberqasim@2023-bse-066:~$ hostname
2023-bse-066
umberqasim@2023-bse-066:~$
```

II. Filesystem Inspection for Forensic Evidence

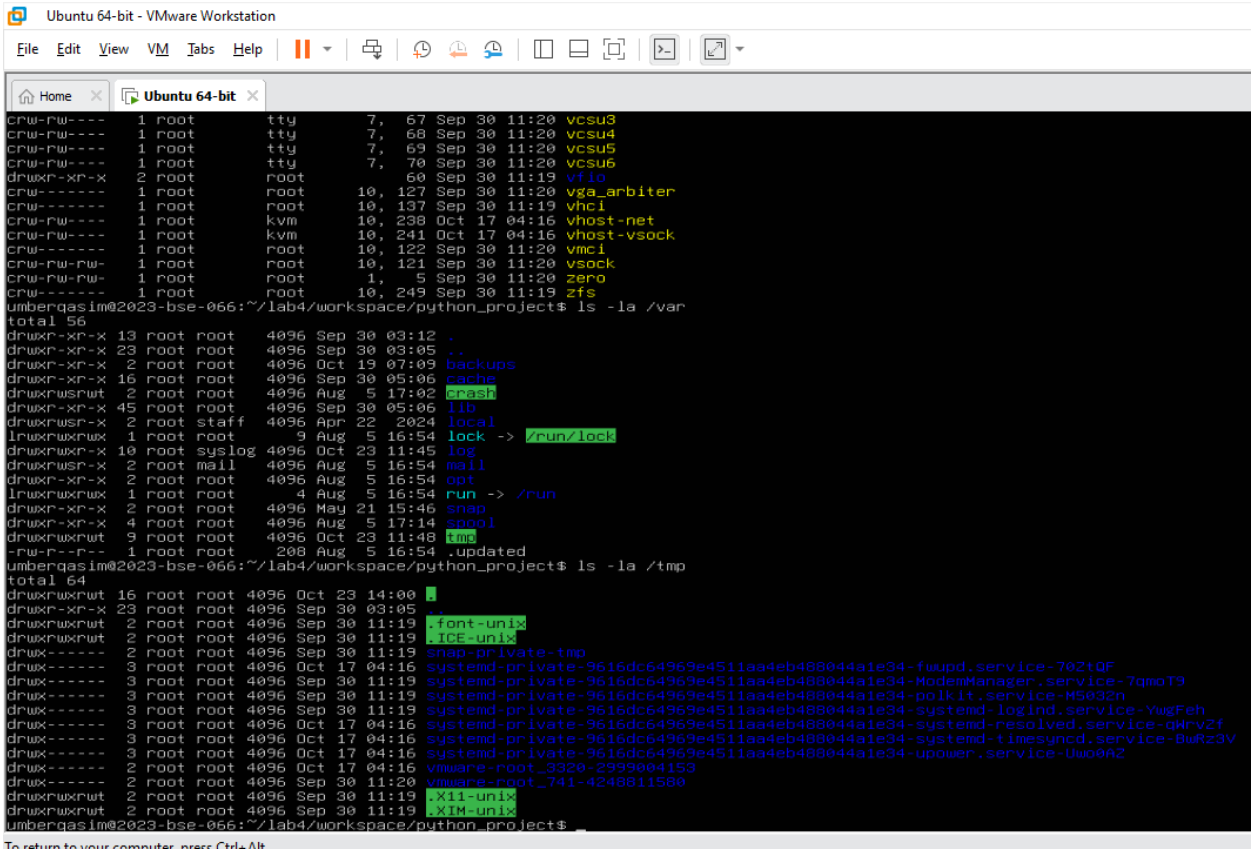
Root directory contents

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la /
total 2097244
drwxr-xr-x  23 root root       4096 Sep 30 03:05 .
drwxr-xr-x  23 root root       4096 Sep 30 03:05 ..
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 Oct 23 11:49 boot
dr-xr-xr-x   2 root root       4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root       4120 Sep 30 11:20 dev
drwxr-xr-x 108 root root       4096 Oct 23 13:25 etc
drwxr-xr-x   3 root root       4096 Oct 23 13:25 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 30 02:57 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 281 root root          0 Sep 30 11:19 proc
drwx------   3 root root       4096 Oct 17 04:54 root
drwxr-xr-x  31 root root       1020 Oct 23 14:31 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 30 03:12 snap
drwxr-xr-x   2 root root       4096 Aug  5 16:54 srv
-rw-------   1 root root 2147483648 Sep 30 03:05 swap.img
dr-xr-xr-x  13 root root          0 Oct 17 05:18 sys
drwxrwxrwt  16 root root       4096 Oct 23 14:00 tmp
drwxr-xr-x  12 root root       4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root       4096 Sep 30 03:12 var
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ _
```

OS version and release info

```
umberqasim@2023-bse-066:~/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
```

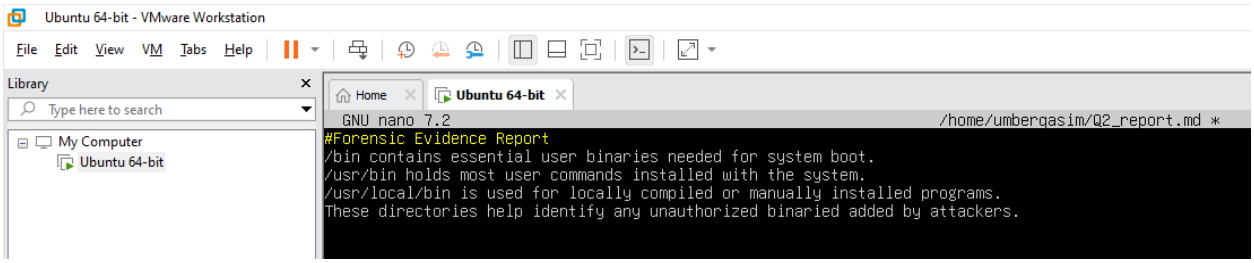
Explore important system directories



Hidden files in your home directory

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la ~
total 48
drwxr-x--- 6 umberqasim umberqasim 4096 Oct 23 12:05 .
drwxr-xr-x 3 root       root       4096 Oct 23 13:25 ..
-rw-rw-r-- 1 umberqasim umberqasim  338 Oct 23 11:52 answers.md
-rw------- 1 umberqasim umberqasim  440 Oct 19 07:44 .bash_history
-rw-r--r-- 1 umberqasim umberqasim  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 umberqasim umberqasim 3771 Mar 31  2024 .bashrc
drwx------ 2 umberqasim umberqasim 4096 Sep 30 03:17 .cache
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 12:05 lab4
-rw------- 1 umberqasim umberqasim   20 Oct  2 12:23 .lesshst
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 19 07:22 .local
-rw-r--r-- 1 umberqasim umberqasim  807 Mar 31  2024 .profile
drwx------ 2 umberqasim umberqasim 4096 Sep 30 05:47 .ssh
-rw-r--r-- 1 umberqasim umberqasim    0 Sep 30 05:14 .sudo_as_admin_successful
```

Create a file summarizing /bin, /usr/bin, and /usr/local/bin differences:



III. Evidence Handling & File Operations

Create a structured workspace

```
umberqasim@2023-bse-066:~$ mkdir -p ~/analysis/evidence/suspicious_files
```

Create text files (including one hidden)

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ ls -la
total 20
drwxrwxr-x 2 umberqasim umberqasim 4096 Oct 23 16:39 .
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 16:35 ..
-rw-rw-r-- 1 umberqasim umberqasim   22 Oct 23 16:39 .hidden_note.txt
-rw-rw-r-- 1 umberqasim umberqasim   34 Oct 23 16:38 log.txt
-rw-rw-r-- 1 umberqasim umberqasim   37 Oct 23 16:37 report.txt
```

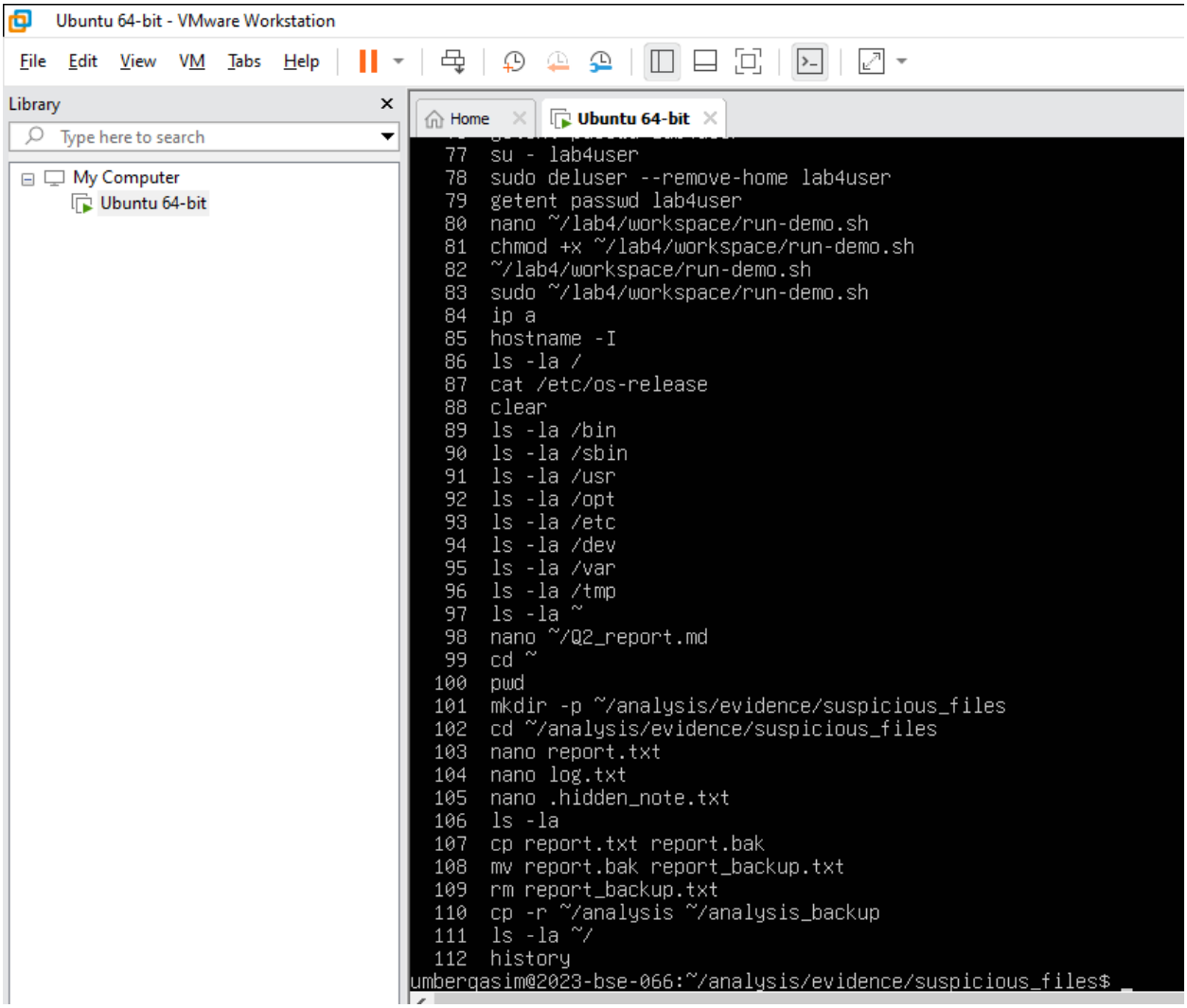
Backup, rename, delete

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ cp report.txt report.bak
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ mv report.bak report_backup.txt
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ rm report_backup.txt
```

Copy entire workspace as a backup

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ ls -la ~/
total 60
drwxr-x--- 8 umberqasim umberqasim 4096 Oct 23 16:43 .
drwxr-xr-x 3 root       root       4096 Oct 23 13:25 ..
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 16:35 analysis
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 16:43 analysis_backup
-rw-rw-r-- 1 umberqasim umberqasim  338 Oct 23 11:52 answers.md
-rw------- 1 umberqasim umberqasim  440 Oct 19 07:44 .bash_history
-rw-r--r-- 1 umberqasim umberqasim  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 umberqasim umberqasim 3771 Mar 31  2024 .bashrc
drwx------ 2 umberqasim umberqasim 4096 Sep 30 03:17 .cache
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 12:05 lab4
-rw------- 1 umberqasim umberqasim   20 Oct  2 12:23 .lesshst
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 19 07:22 .local
-rw-r--r-- 1 umberqasim umberqasim  807 Mar 31  2024 .profile
-rw-rw-r-- 1 umberqasim umberqasim  303 Oct 23 16:28 Q2_report.md
drwx------ 2 umberqasim umberqasim 4096 Sep 30 05:47 .ssh
-rw-r--r-- 1 umberqasim umberqasim    0 Sep 30 05:14 .sudo_as_admin_successful
```

Show command history



Demonstrate auto-completion

Before tab:

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ cd ~/anal_
```

After tab:

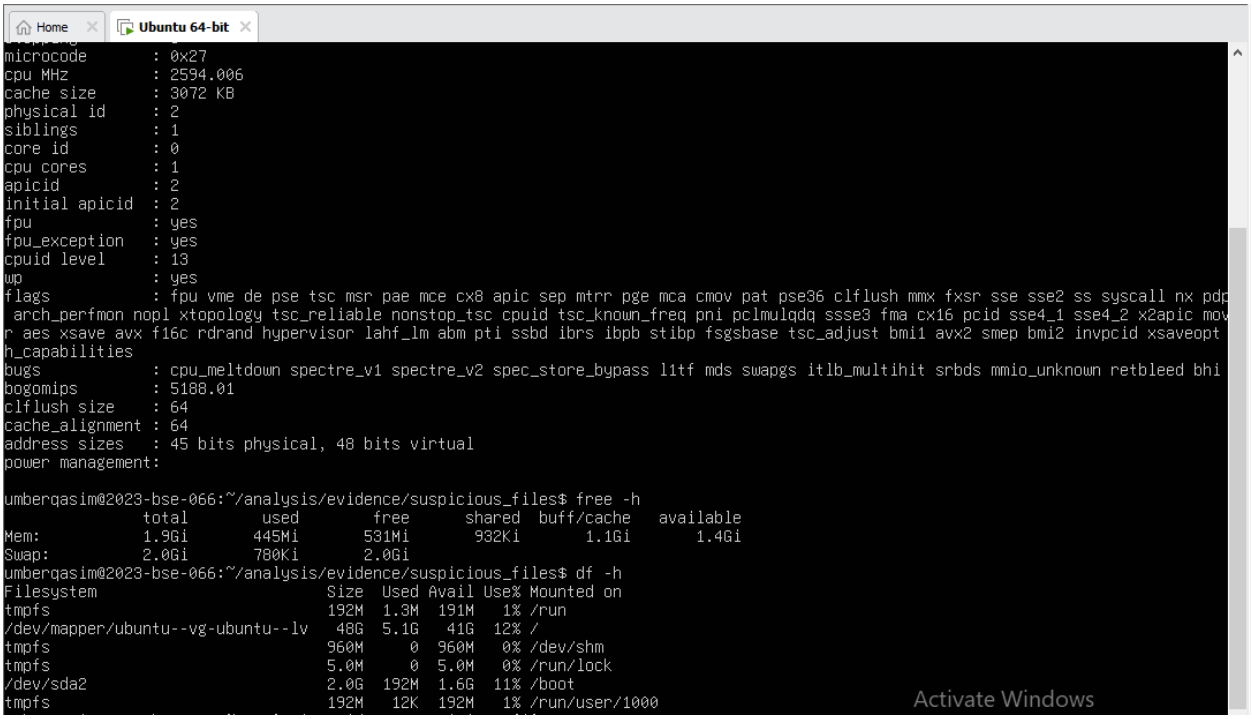
```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ cd ~/analysis
```

IV. System Profiling and Process Monitoring

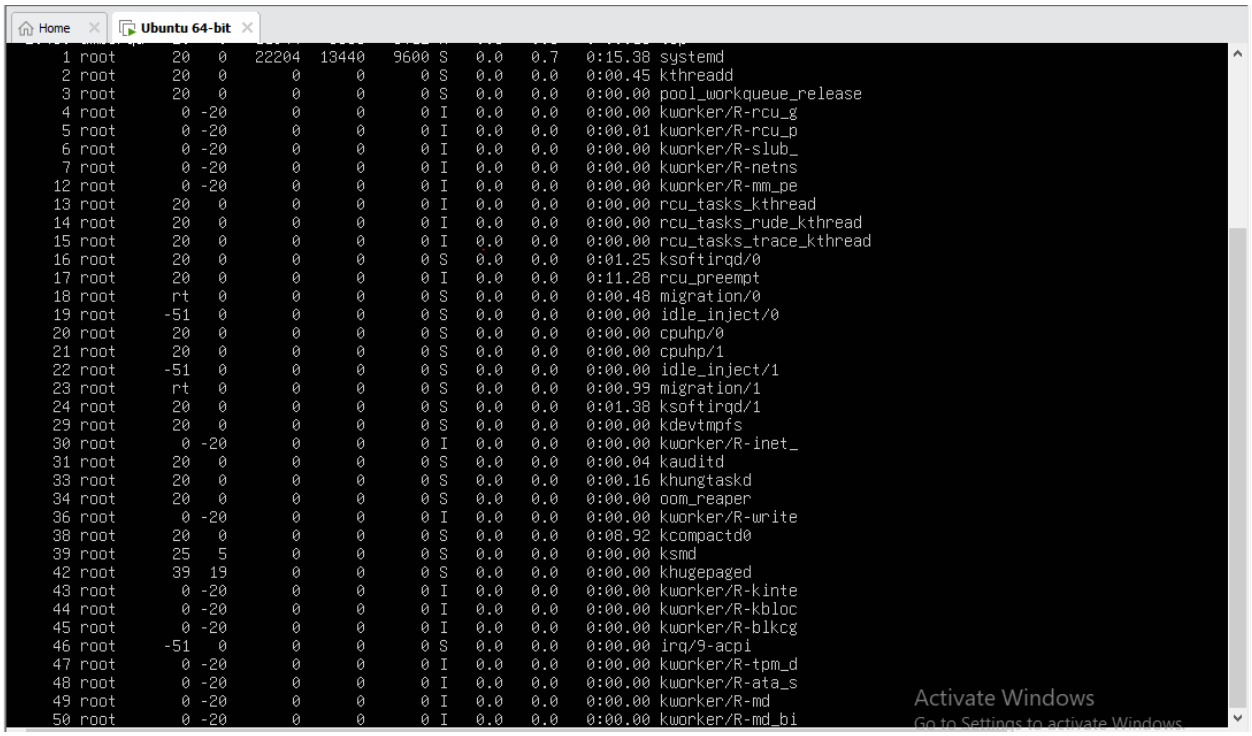
Display OS and kernel version

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ uname -a
Linux 2023-bse-066 6.8.0-84-generic #84-Ubuntu SMP PREEMPT_DYNAMIC Fri Sep  5 22:36:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ 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
```


Display CPU, memory, and disk usage



Display all active processes



V. User Account Audit & Privilege Escalation Simulation

Create a new test user

```
umberqasim@2023-bse-066:~$ sudo adduser lab4user
[sudo] password for umberqasim:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
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 []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
```

Verify user record in system database

```
umberqasim@2023-bse-066:~$ grep 'lab4user' /etc/passwd
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
```

Log in as lab4user

```
umberqasim@2023-bse-066:~$ su - lab4user
Password:
lab4user@2023-bse-066:~$
```

Try an administrative command

```
lab4user@2023-bse-066:~$ sudo apt update
[sudo] password for lab4user:
lab4user is not in the sudoers file.
```

Switch back to your main analyst account

```
lab4user@2023-bse-066:~$ exit
logout
umberqasim@2023-bse-066:~$ _
```

Inspect authentication logs

```
umberqasim@2023-bse-066:~$ sudo grep lab4user /var/log/auth.log
2025-10-26T11:06:17.364898+00:00 2023-bse-066 sudo: umberqasim : TTY=pts/0 ; PWD=/home/umberqasim ; USER=root ; COMMAND=/usr/sbin/add
2025-10-26T11:06:17.742893+00:00 2023-bse-066 groupadd[21389]: group added to /etc/group: name=lab4user, GID=1001
2025-10-26T11:06:17.746351+00:00 2023-bse-066 groupadd[21389]: group added to /etc/gshadow: name=lab4user
2025-10-26T11:06:17.749525+00:00 2023-bse-066 groupadd[21389]: new group: name=lab4user, GID=1001
2025-10-26T11:06:17.798384+00:00 2023-bse-066 useradd[21396]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell
2025-10-26T11:07:07.062546+00:00 2023-bse-066 passwd[21409]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-26T11:07:10.060256+00:00 2023-bse-066 chfn[21412]: changed user 'lab4user' information
2025-10-26T11:07:12.219421+00:00 2023-bse-066 gpasswd[21420]: members of group users set by root to lab4user
2025-10-26T11:11:38.430645+00:00 2023-bse-066 su[21436]: (to lab4user) umberqasim on pts/0
2025-10-26T11:11:38.432731+00:00 2023-bse-066 su[21436]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by umberq
2025-10-26T11:13:16.668859+00:00 2023-bse-066 sudo: lab4user : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/lab4user ; USER=root ; COM
2025-10-26T11:14:07.893328+00:00 2023-bse-066 su[21436]: pam_unix(su-l:session): session closed for user lab4user
2025-10-26T11:16:35.144431+00:00 2023-bse-066 sudo: umberqasim : TTY=pts/0 ; PWD=/home/umberqasim ; USER=root ; COMMAND=/usr/bin/grep
```


Remove the test user

```
umberqasim@2023-bse-066:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
umberqasim@2023-bse-066:~$ grep 'lab4user' /etc/passwd
```