

Fatima Jinnah Women University



Cloud  
Computing  
Lab 4

Submitted By :

Inshal Nasir

Section :

A

Roll No:

38

Submitted To:

Sir Shoaib

## LAB TITLE: Virtualization & Linux Fundamentals

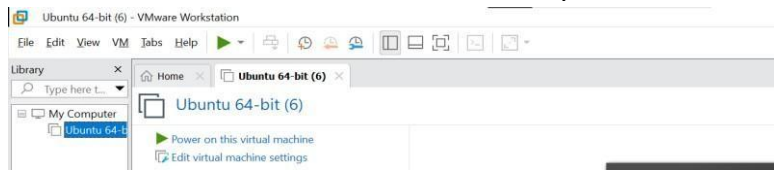
### TASK:

## Task 1: Verify VM resources in VMware

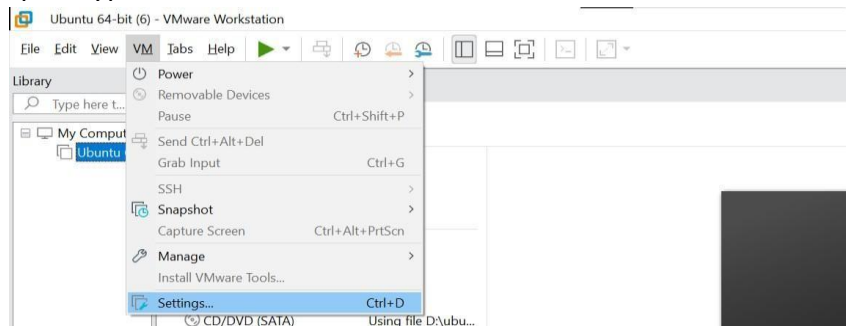
Confirm the VM resources that were allocated in Lab 1.

### Steps

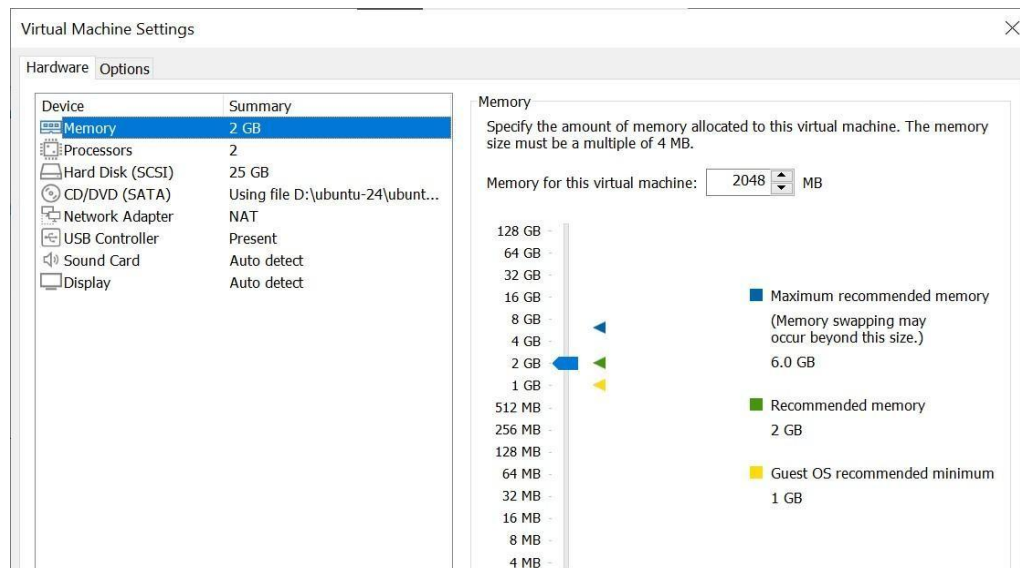
1. Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.



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



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



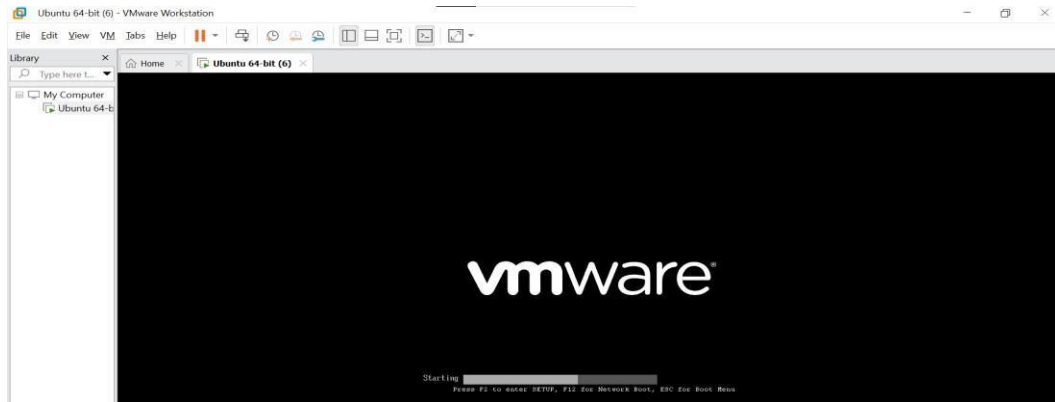
vm\_settings.png

## 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: `ssh student@<vm-ipaddress>`

1. Find the IP address of your Ubuntu Server using “ip addr”

```
ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:0c:29:6a:f6:87 brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 192.168.161.129/24 metric 100 brd 192.168.161.255 scope global dynamic ens33
    valid_lft 1082sec preferred_lft 1082sec
inet6 fe80::20c:29ff:fe6a:f687/64 scope link
    valid_lft forever preferred_lft forever
```

2. Connect via SSH from Windows

```
PS C:\Users\HP> ping 192.168.161.129

Pinging 192.168.161.129 with 32 bytes of data:
Reply from 192.168.161.129: bytes=32 time=1ms TTL=64
Reply from 192.168.161.129: bytes=32 time<1ms TTL=64
Reply from 192.168.161.129: bytes=32 time<1ms TTL=64
Reply from 192.168.161.129: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.161.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

### Enter your password

Use the same password you set up during the Ubuntu Server installation.

```

Warning: Permanently added '192.168.161.129' (ED25519) to the list of known hosts.
hajra@192.168.161.129'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 Sat 27 Sep 10:28:45 UTC 2025

System load:  1.46           Processes:           276
Usage of /:   70.2% of 11.21GB Users logged in:       1
Memory usage: 57%           IPv4 address for ens33: 192.168.161.129
Swap usage:   9%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

hajra@ubuntu-lab: $

```

- After logging in, run both commands and capture them together in a single screenshot:  
whoami  
pwd

```

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ whoami
Alli

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ /home/Alli
bash: /home/Alli: No such file or directory

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ pwd
/c/Users/Alli

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$

```

### Task 3: Filesystem exploration — root tree and dotfiles

#### Steps (run inside VM terminal)

- List root directory contents:

ls -la /

```

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ ls -la
total 39593
drwxr-xr-x 1 Alli 197609  0 Nov 15 09:10 ./
drwxr-xr-x 1 Alli 197609  0 Oct 16 00:59 ../
-rw-r--r-- 1 Alli 197609 11439 Nov 20 01:26 .bash_history
drwxr-xr-x 1 Alli 197609  0 Dec 10 2024 .dotnet/
drwxr-xr-x 1 Alli 197609  0 Oct 18 03:51 .git/
-rw-r--r-- 1 Alli 197609 301 Oct 18 02:07 .gitconfig
drwxr-xr-x 1 Alli 197609  0 Dec  5 2024 .gk/
drwxr-xr-x 1 Alli 197609  0 Dec  5 2024 .gnupg/
-rw-r--r-- 1 Alli 197609 20 Oct 18 03:48 .lessht

```

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

ls -la /bin

```

Alli@DESKTOP-KQE4P80 MINGW64 ~ (main)
$ ls -la /bin
total 90304
drwxr-xr-x 1 Alli 197609  0 Oct  8 20:18 ./
drwxr-xr-x 1 Alli 197609  0 Oct  8 20:19 ../
-rwxr-xr-x 1 Alli 197609 77418 Sep 28 21:48 'if.exe'

```

ls -la /sbin

```

lrwxrwxrwx 1 root root 8 Apr 22 2024 /sbin -> usr/sbin
hajra@ubuntu-lab:~$

```

ls -la /usr

```
total 96
drwxr-xr-x 12 root root 4096 Aug  5 16:54 .
drwxr-xr-x 22 root root 4096 Sep 26 21:19 ..
drwxr-xr-x 2 root root 36864 Oct 21 17:19 bin
drwxr-xr-x 2 root root 4096 Apr 22 2024 games
drwxr-xr-x 35 root root 4096 Oct 14 08:07 include
drwxr-xr-x 83 root root 4096 Oct 21 17:20 lib
drwxr-xr-x 2 root root 4096 Sep 26 21:18 lib64
drwxr-xr-x 13 root root 4096 Oct 14 08:06 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x 2 root root 4096 Oct 21 17:10 sbin
drwxr-xr-x 128 root root 4096 Oct 14 08:07 share
drwxr-xr-x 7 root root 4096 Oct 21 17:20 src
hajra@ubuntu-lab:~$
```

ls -la /opt

```
total 16
drwxr-xr-x 4 root root 4096 Sep 26 21:51 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxr-xr-x 2 root root 4096 Sep 26 21:51 cmi
drwxr-xr-x 4 root root 4096 Sep 26 21:51 kontainerd
hajra@ubuntu-lab:~$
```

ls -la /etc

```
drwxr-xr-x 2 root root 4096 Aug  5 17:14 acpi.conf
-rw-r--r-- 1 root root 12813 Mar 27 2021 services
drwxr-xr-x 2 root root 4096 Aug  5 17:02 shadow
-rw-r--r-- 1 root shadow 965 Sep 26 21:49 shadow
-rw-r--r-- 1 root shadow 967 Sep 26 21:38 shadow
-rw-r--r-- 1 root root 148 Aug  5 17:14 shells
drwxr-xr-x 2 root root 4096 Aug  5 16:55 subuid
drwxr-xr-x 6 root root 4096 Aug  5 17:14 subuid
drwxr-xr-x 4 root root 4096 Sep 26 21:58 subuid
drwxr-xr-x 4 root root 4096 Oct 21 17:18 subuid
-rw-r--r-- 1 root root 19 Sep 26 21:38 subgid
-rw-r--r-- 1 root root 0 Aug  5 16:54 subgid
-rw-r--r-- 1 root root 19 Sep 26 21:38 subgid
-rw-r--r-- 1 root root 0 Aug  5 16:54 subgid
-rw-r--r-- 1 root root 4343 Jun 25 12:42 sudo.conf
-rw-r--r-- 1 root root 1000 Jan 29 2024 sudocore
drwxr-xr-x 2 root root 4096 Aug  5 17:02 sudo.conf.d
drwxr-xr-x 1 root root 9884 Jun 25 12:42 sudo_logsrvd.conf
drwxr-xr-x 2 root root 4096 Aug  5 17:14 sysctl.conf
-rw-r--r-- 1 root root 2209 Mar 24 2024 sysctl.conf
drwxr-xr-x 2 root root 4096 Sep 26 21:51 sysctl.conf.d
drwxr-xr-x 2 root root 4096 Aug  5 17:14 sysctl.d
drwxr-xr-x 6 root root 4096 Aug  5 16:49 syslog.conf
drwxr-xr-x 2 root root 4096 Aug  5 17:00 syslog.conf.d
drwxr-xr-x 2 root root 4096 Sep 26 21:19 timezone
-rw-r--r-- 1 root root 8 Aug  5 17:02 timezone
drwxr-xr-x 2 root root 4096 Aug  5 17:14 udev.conf.d
drwxr-xr-x 2 root root 4096 Aug  5 17:14 udev.conf.d.d
drwxr-xr-x 1 root root 1209 Jan 27 2023 ucf.conf
drwxr-xr-x 4 root root 4096 Aug  5 17:02 ucf
drwxr-xr-x 2 root root 4096 Sep 26 21:123 ufw.conf
drwxr-xr-x 3 root root 4096 Aug  5 17:14 ufw
-rw-r--r-- 1 root root 208 Aug  5 16:54 updated
drwxr-xr-x 3 root root 4096 Aug  5 17:02 usbmuxd
drwxr-xr-x 2 root root 4096 Sep 26 21:51 usbmuxd.conf
drwxr-xr-x 2 root root 4096 Aug  5 17:14 usbmuxd.conf.d
drwxr-xr-x 2 root root 4096 Sep 26 21:19 usbmuxd.conf.d
-rw-r--r-- 1 root root 1523 Aug  5 17:14 usb_modeswitch.conf
drwxr-xr-x 2 root root 4096 Aug  5 17:14 usb_modeswitch.conf.d
lrwxrwxrwx 1 root root 16 Aug  5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x 4 root root 4096 Sep 26 21:24 vconsole.conf.d
drwxr-xr-x 4 root root 4096 Oct 21 17:19 vconsole.conf.d
lrwxrwxrwx 1 root root 23 Feb 26 2024 vtvgb -> /etc/alternatives/vtvgb
-rw-r--r-- 1 root root 4942 Aug  5 17:14 wgetrc
drwxr-xr-x 4 root root 4096 Aug  5 17:02 x11
-rw-r--r-- 1 root root 681 Apr  8 2024 xattr.conf
drwxr-xr-x 4 root root 4096 Aug  5 17:02 xattr
drwxr-xr-x 2 root root 4096 Aug  5 17:02 xattr.d
-rw-r--r-- 1 root root 460 Aug  5 17:14 zsh_command_not_found
```

Click inside or press Ctrl+G.

ls -la /dev

```
crw-rw---- 1 root dialout 4, 91 Oct 22 20:00 ttyS27
crw-rw---- 1 root dialout 4, 92 Oct 22 20:00 ttyS28
crw-rw---- 1 root dialout 4, 93 Oct 22 20:00 ttyS29
crw-rw---- 1 root dialout 4, 67 Oct 22 20:00 ttyS3
crw-rw---- 1 root dialout 4, 94 Oct 22 20:00 ttyS30
crw-rw---- 1 root dialout 4, 95 Oct 22 20:00 ttyS31
crw-rw---- 1 root dialout 4, 69 Oct 22 20:00 ttyS4
crw-rw---- 1 root dialout 4, 69 Oct 22 20:00 ttyS5
crw-rw---- 1 root dialout 4, 70 Oct 22 20:00 ttyS6
crw-rw---- 1 root dialout 4, 71 Oct 22 20:00 ttyS7
crw-rw---- 1 root dialout 4, 72 Oct 22 20:00 ttyS8
crw-rw---- 1 root dialout 4, 73 Oct 22 20:00 ttyS9
drwxr-xr-x 2 root root 60 Oct 22 20:00
crw-rw---- 1 root kvm 10, 124 Oct 22 20:00 udmabuf
crw-rw---- 1 root root 10, 239 Oct 22 20:00 uhid
crw-rw---- 1 root root 10, 223 Oct 22 20:00 urandom
crw-rw-rw-rw 1 root root 1, 9 Oct 22 20:00 urandom
crw-rw---- 1 root root 10, 126 Oct 22 20:00 userfaultfd
crw-rw---- 1 root root 10, 240 Oct 22 20:00 vcs0
crw-rw---- 1 root tty 7, 0 Oct 22 20:00 vcs1
crw-rw---- 1 root tty 7, 1 Oct 22 20:00 vcs1
crw-rw---- 1 root tty 7, 2 Oct 22 20:00 vcs2
crw-rw---- 1 root tty 7, 3 Oct 22 20:00 vcs3
crw-rw---- 1 root tty 7, 4 Oct 22 20:00 vcs4
crw-rw---- 1 root tty 7, 5 Oct 22 20:00 vcs5
crw-rw---- 1 root tty 7, 6 Oct 22 20:00 vcs5
crw-rw---- 1 root tty 7, 128 Oct 22 20:00 vcsa
crw-rw---- 1 root tty 7, 129 Oct 22 20:00 vcsa1
crw-rw---- 1 root tty 7, 130 Oct 22 20:00 vcsa2
crw-rw---- 1 root tty 7, 131 Oct 22 20:00 vcsa3
crw-rw---- 1 root tty 7, 132 Oct 22 20:00 vcsa4
crw-rw---- 1 root tty 7, 133 Oct 22 20:00 vcsa5
crw-rw---- 1 root tty 7, 134 Oct 22 20:00 vcsa6
crw-rw---- 1 root tty 7, 64 Oct 22 20:00 vcsu
crw-rw---- 1 root tty 7, 65 Oct 22 20:00 vcsu1
crw-rw---- 1 root tty 7, 66 Oct 22 20:00 vcsu2
crw-rw---- 1 root tty 7, 67 Oct 22 20:00 vcsu3
crw-rw---- 1 root tty 7, 68 Oct 22 20:00 vcsu4
crw-rw---- 1 root tty 7, 69 Oct 22 20:00 vcsu5
crw-rw---- 1 root tty 7, 70 Oct 22 20:00 vcsu6
drwxr-xr-x 2 root root 60 Oct 22 20:00
crw-rw---- 1 root root 10, 127 Oct 22 20:00 vga_arbiter
crw-rw---- 1 root root 10, 137 Oct 22 20:00 vhc1
crw-rw---- 1 root kvm 10, 238 Oct 22 20:00 vhost-net
crw-rw---- 1 root kvm 10, 241 Oct 22 20:00 vhost-vsock
crw-rw---- 1 root root 10, 122 Oct 22 20:00 vnet1
crw-rw---- 1 root root 10, 121 Oct 22 20:00 vsock
crw-rw-rw-rw 1 root root 1, 5 Oct 22 20:00 zero
crw-rw---- 1 root root 10, 240 Oct 22 20:00 zfs
haina@ubuntu-lab:~$
```

ls -la /var

```
total 56
drwxr-xr-x 13 root root 4096 Sep 26 21:38 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxr-xr-x 2 root root 4096 Oct 22 00:00 backups
drwxr-xr-x 2 root root 4096 Sep 27 08:39 crash
drwxrwxrwt 2 root root 4096 Aug 5 17:02 cshare
drwxr-xr-x 46 root root 4096 Sep 27 08:39 data
drwxrwxr-x 2 root staff 4096 Apr 22 2024 data1
lrwxrwxrwx 1 root root 9 Aug 5 16:54 lock -> /run/lock
drwxrwxr-x 12 root root 4096 Oct 22 20:00 log
drwxrwxr-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 20 root root 4096 Sep 26 22:00 sbin
drwxr-xr-x 4 root root 4096 Aug 5 17:14 sbin1
drwxrwxrwt 7 root root 4096 Oct 22 20:01 tmp
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated
haina@ubuntu-lab:~$
```

ls -la /tmp

```
total 52
drwxrwxrwt 13 root root 4096 Oct 22 20:11 .
drwxr-xr-x 23 root root 4096 Sep 26 21:19 ..
drwxrwxrwt 2 root root 4096 Oct 22 20:00 .font-unix
drwxrwxrwt 2 root root 4096 Oct 22 20:00 .ICE-unix
drwxrwxrwt 6 root root 4096 Oct 22 20:00 .X11-unix
drwxrwxrwt 3 root root 4096 Oct 22 20:00 .X11-unix
drwxrwxrwt 3 root root 4096 Oct 22 20:00 .X11-unix
drwxrwxrwt 3 root root 4096 Oct 22 20:00 .X11-unix
drwxrwxrwt 2 root root 4096 Oct 22 20:00 .X11-unix
drwxrwxrwt 2 root root 4096 Oct 22 20:00 .X11-unix
drwxrwxrwt 2 root root 4096 Oct 22 20:00 .X11-unix
haina@ubuntu-lab:~$
```

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

ls -la ~

```
$ ls -la $HOME
total 39593
drwxr-xr-x 1 Alli 197609 0 Nov 15 09:10 ./
drwxr-xr-x 1 Alli 197609 0 Oct 16 00:59 ../
-rw-r--r-- 1 Alli 197609 11439 Nov 20 01:26 .bash_history
drwxr-xr-x 1 Alli 197609 0 Dec 10 2024 .dotnet/
drwxr-xr-x 1 Alli 197609 0 Oct 18 03:51 .git/
-rw-r--r-- 1 Alli 197609 301 Oct 18 02:07 .gitconfig
drwxr-xr-x 1 Alli 197609 0 Dec 5 2024 .gk/
drwxr-xr-x 1 Alli 197609 0 Dec 5 2024 .gnupg/
-rw-r--r-- 1 Alli 197609 20 Oct 18 03:48 .lessht
-rw-r--r-- 1 Alli 197609 174 May 29 2025 .packetracer
drwxr-xr-x 1 Alli 197609 0 Jan 15 2025 .spss/
```

4. Write a short paragraph (3–5 sentences) that explains the difference between /bin, /usr/bin and /usr/local/bin.

Open your editor:

iano ~/answers.md





Added the text “**Lab 4 README**” and saved the file. nano

main.py

```
GNU nano 7.2 main.py *
print ('hello lab4')
```

Added the Python code: `print("hello lab4")` and saved the file.

nano .env

```
GNU nano 7.2 .env *
ENV = lab4_
```

Added the line **ENV=lab4** and saved the file.

### 3. List Files

ls -la

```
total 20
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:14 .
drwxrwxr-x 3 hajra hajra 4096 Oct 23 13:11 ..
-rw-rw-r-- 1 hajra hajra 11 Oct 23 14:14 .env
-rw-rw-r-- 1 hajra hajra 21 Oct 23 14:11 main.py
-rw-rw-r-- 1 hajra hajra 13 Oct 23 14:07 README.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

Displayed all files, including hidden ones, in the current directory.

### 4. Copy, Move, and Remove Files `cp README.md`

README.copy.md

```
lab4/workspace/python_project$ cp README.md README.md.copy.md
lab4/workspace/python_project$
```

Created a copy of the README file.

mv README.copy.md README.dev.md

```
//lab4/workspace/python_project$ mv README.md.copy.md README.dev.md
//lab4/workspace/python_project$
```

Renamed (moved) the copied file.

rm README.dev.md

Copied the entire Python project directory recursively.

ls -la ~/lab4/workspace

```
total 16
drwxrwxr-x 4 hajra hajra 4096 Oct 23 14:34 .
drwxrwxr-x 3 hajra hajra 4096 Oct 23 13:11 ..
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:34 java_app_copy
drwxrwxr-x 2 hajra hajra 4096 Oct 23 14:27 python_project
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

Verified the copied directories.

### 5. Work with Directories

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

```
lab4/workspace/python_project$ mkdir -p $HOME/lab4/workspace/java_app
lab4/workspace/python_project$
```

Created another directory for a Java app.

cp -r ~/lab4/workspace/python\_project ~/lab4/workspace/java\_app\_copy

```
//lab4/workspace/python_project$ cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/java_app_copy
//lab4/workspace/python_project$
```



## 6. Use Command History and Tab Completion

History

```
1 ls -la $HOME
2 nano $HOME/answers.md
3 cat $HOME/answers.md
4 mkdir -p $HOME/lab4/workspace/python_project
5 cd $HOME/lab4/workspace/python_project
6 pwd
7 nano README.md
8 nano main.py
9 nano .env
10 ls -la
11 cd README.md README.md.copy.md
12 mv README.copy.md README.dev.md
13 mv README.md.copy.md README.dev.md
14 rm README.dev.md
15 mkdir -p $HOME/lab4/workspace/java_app
16 cp -r $HOME/lab4/workspace/python_project $HOME/lab4/workspace/java_app_copy
17 ls -la $HOME/lab4/workspace
18 history
ha ira@ubuntu-lab:~/lab4/workspace/python_project$
```

Displayed a list of previously executed commands.

- Demonstrated tab completion by typing part of a file or directory name and pressing **Tab** to autocomplete it.

```
print ('hello lab4')
```

## Task 5: System info, resources & processes

Collect system information and observe processes. Use screenshots only.

Steps (inside VM terminal)


1. Kernel and OS:

uname -a

```
~/lab4/workspace/python_project$ uname -a
6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
~/lab4/workspace/python_project$
```

2. CPU (ensure model name visible):

cat /proc/cpuinfo



```
core id       : 0
cpu cores     : 1
apicid        : 0
initial apicid : 0
fpu           : yes
fpu_exception : yes
cpuid level   : 22
wp            : yes
flags         : fpu vme de pse tsc mtr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc
arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe pconfig tsc_deadline_timer
r_nes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflush
nopl xsaveopt xsavec xgetbv1 xsaues arat md_clear flush_l1d arch_capabilities
bugs         : cpu_mitigation_spectre_v1 spectre_v2 spec_store_bypass l1tf mds swaps itlb_multihit srbds mmio_stale_data retbleed gds bhi
bogomips      : 3791.99
clflush size  : 64
cache_alignment : 64
address sizes  : 45 bits physical, 48 bits virtual
power management:

processor      : 1
vendor_id      : GenuineIntel
cpu family     : 6
model          : 142
model name     : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
stepping       : 10
microcode      : 0xffffffff
cpu mhz        : 1895.997
cache size     : 6144 KB
physical id    : 2
siblings       : 1
cpu cores      : 0
apicid         : 2
initial apicid : 2
fpu            : yes
fpu_exception  : yes
cpuid level    : 22
wp             : yes
flags          : fpu vme de pse tsc mtr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc
arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe pconfig tsc_deadline_timer
r_nes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflush
nopl xsaveopt xsavec xgetbv1 xsaues arat md_clear flush_l1d arch_capabilities
bugs         : cpu_mitigation_spectre_v1 spectre_v2 spec_store_bypass l1tf mds swaps itlb_multihit srbds mmio_stale_data retbleed gds bhi
bogomips      : 3791.99
clflush size  : 64
cache_alignment : 64
address sizes  : 45 bits physical, 48 bits virtual
power management:

ha ira@ubuntu-lab:~/lab4/workspace/python_project$
```

1. click inside or press Ctrl+G.

3. Memory: free -h

```
ha ira@ubuntu-lab:~/lab4/workspace/python_project$ free -h
              total        used        free      shared  buff/cache   available
Mem:          1.9Gi          1.2Gi          132Mi          12Mi          734Mi          667Mi
Swap:         2.0Gi          223Mi          1.8Gi
```

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

```

root      0.00 0.00 0.1 1259496 2220 ? S    12:24 0:00 httpd -d /snap/nextcloud/50464 -k start -DFOREGROUND
root      4987 0.0 0.1 1259496 2356 ? S    12:24 0:00 httpd -d /snap/nextcloud/50464 -k start -DFOREGROUND
root      5496 0.0 0.1 8408 3456 ? Ss   12:24 0:00 bash /usr/bin/systemd/511/run-cluster-agent-with-args
ha.jaira  5630 0.0 0.0 20464 8132 ? Ss   12:24 0:00 /usr/lib/systemd/systemd --user
ha.jaira  5632 0.0 0.0 21148 1852 ? S    12:24 0:00 (sd-pam)
ha.jaira  5634 0.0 0.0 8656 4496 ttyL S    12:24 0:00 --bash
ha.jaira  5704 0.0 0.3 1259494 1612 ? Ss   12:24 0:00 /usr/bin/microk8s/5511/bin/cncluster-agent -v-bind 0.0.0.0:25000 --keyfile /var/snap/
root      5985 1.0 1.5 2300568 31132 ? Ssl  12:24 1:50 /usr/bin/microk8s/5511/bin/containerd --config /var/snap/microk8s/5511/args/containerd.toml -ro
root      6204 0.0 0.1 1545400 31028 ? Ss   12:12 0:00 /usr/bin/microk8s/5511/adbelittle - scheduler-args files:/var/snap/microk8s/5511/args/Audel
root      7140 0.3 0.4 1234156 8380 ? Sl    12:24 0:33 /usr/bin/microk8s/5511/bin/containerd-shim-runc-v2 -namespace k8s.io -id c4e7879b4dc6b1845e94b8
ss535     7229 0.0 0.0 1234156 8380 ? Ss   12:24 0:00 /pause
root      7294 0.0 0.3 1234142 6940 ? Sl    12:25 0:00 /usr/bin/microk8s/5511/bin/containerd-shim-runc-v2 -namespace k8s.io -id f1af57bd78de6f55ee774952
ss535     7608 0.0 0.0 1028 120 ? Ss   12:25 0:00 /pause
root      7610 0.4 0.4 1234142 6956 ? Sl    12:25 0:00 /usr/bin/microk8s/5511/bin/containerd-shim-runc-v2 -namespace k8s.io -id 9070e5c3fa2edabdd7e07c5b
ss535     7670 0.0 0.0 1028 120 ? Ss   12:25 0:00 /pause
root      7728 0.2 1.0 764656 20364 ? SSl  12:25 0:24 /coredns -conf /etc/coredns/Corefile
root      7790 0.0 1.5 1276704 31300 ? Ssl  12:25 0:00 /usr/bin/kube-apiserver --etcd-servers https://127.0.0.1:2379
root      8389 0.0 0.0 4476 1152 ? Ss   12:25 0:00 /usr/local/bin/runc/unsvdr -P /etc/service/enabled
root      8637 0.0 0.0 4324 1152 ? Ss   12:25 0:00 runcsv allocate-tunnel-address
root      8638 0.0 0.0 4324 1152 ? Ss   12:25 0:00 runcsv felix
root      8639 0.0 0.0 4324 1152 ? Ss   12:25 0:00 runcsv nvidia-status-reporter
root      8640 0.0 0.0 4324 1152 ? Ss   12:25 0:00 runcsv cil
root      8641 0.0 0.0 4324 1280 ? Ss   12:25 0:00 runcsv monitor-addresses
root      8642 0.0 0.0 4324 1280 ? Ss   12:25 0:00 calico-node -allocate-tunnel-addrs
root      8643 0.0 2.8 1794220 56160 ? Sl    12:25 0:01 calico-node -status-reporter
root      8644 0.0 2.7 1794476 55800 ? Sl    12:25 0:01 calico-node -monitor-token
root      8646 7 3.5 2317200 4984 ? Ss   12:25 0:34 calico-node -felix
root      8647 0.0 2.8 1794476 55752 ? Sl    12:25 0:01 calico-node -monitor-addresses
root      8650 0.0 0.0 0 0 ? Ss   12:57 0:00 [kworker/0:0H-blockd]
root      112669 0.0 0.0 0 0 ? Ic    12:55 0:00 [kworker/0:1s-blkio]
root      113204 0.0 1.9 478476 30364 ? SSl  12:57 0:01 /usr/libexec/faultd/faultd
root      113205 0.0 0.4 31406 856 ? Ss   12:57 0:00 /usr/libexec/Poweraid
root      148689 0.0 0.0 0 0 ? Ic    13:05 0:00 [kworker/1:0H]
root      347870 0.0 0.0 0 0 ? Ss   13:06 0:00 [kworker/u257:1-flush-252:0]
root      537636 0.0 0.0 0 0 ? I    14:28 0:00 [kworker/u258:0-wr-lteback]
root      538250 0.0 0.0 0 0 ? I    14:39 0:00 [kworker/u257:2-fush-252:0]
root      545537 0.0 0.0 0 0 ? I    14:57 0:00 [kworker/1:1-events]
root      681389 0.0 0.0 0 0 ? I    15:00 0:00 [kworker/u258:3-events_power_efficient]
root      684235 0.3 0.0 0 0 ? I    15:01 0:02 [kworker/v0:1-events]
root      693359 0.0 0.0 0 0 ? I    15:01 0:00 [kworker/1:2-events]
root      698137 0.0 0.0 0 0 ? I    15:04 0:00 [kworker/u257:3-events_unbound]
root      709739 0.0 0.0 0 0 ? I    15:06 0:00 [kworker/0:0-events]
root      711863 0.0 0.0 0 0 ? I    15:06 0:00 [kworker/u258:1-unrlteback]
root      713791 0.4 0.0 0 0 ? I    15:08 0:01 [kworker/1:0-events]
root      724181 0.0 0.0 4556 1536 ? S    15:09 0:00 sleep 6m
root      733079 0.0 0.0 0 0 ? I    15:11 0:00 [kworker/v0:2-events]
root      737692 0.0 0.0 0 0 ? I    15:12 0:00 [kworker/u257:1-f-lush-252:0]
root      740675 0.0 0.0 5940 1664 ? S    15:13 0:00 sleep 5
root      740900 1050 0.2 12312 5120 ttyL R+   15:13 0:00 ps aux
ls /dev/shm/lib-7/lsst-workspace/ncp/ncp_daemon.py

```

M, click inside or press Ctrl+G.

```

Mem:          total      used      free      shared  buff/cache   available
Swap:         2.0Gi      223Mi      1.8Gi
ha/ja@ubuntu-lab:~/lab4/workspace/python_projects$ df -h
Filesystem      Size      Used Avail Use% Mounted on
tmpfs            192M      1.6M  191M   1% /run
/dev/mapper/ubunt
vg-ubuntu--lv   12G      11G   343M  97% /
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     20K   192M   1% /run/user/1000
shm              64M      0     64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/ce047894ba4dc681485046b884d
81bfef7c1524cd31f3f71c0866562f5474/shm 64M      0     64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/907a05c3fa2edab7e07c5bb55
f734ead19372884c9de10e7c3258af5f4114e6/shm 64M      0     64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/1fa57bb780d67f58e774952f1e
a158625b771458a25531d41300447ba423a7/shm 64M      0     64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/1fa57bb780d67f58e774952f1e
ha/ja@ubuntu-lab:~/lab4/workspace/python_projects$

```

#### 4. View OS release information:

```
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
ba1ca@ubuntu:lab$ cd ~/lab4/workspace/puthon_projects$
```

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

## Steps (inside VM terminal)

1. Create a new user named lab4user:

```
sudo adduser lab4user
```

```

info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1002) ...
info: Adding new user `lab4user' (1002) with group `lab4user (1002)' ...
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 []: hajra
    Room Number []: twenty two
    Work Phone []: 03two7-5007883
    Home Phone []: 03two7-5007883
    Other []: nil
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
hajra@ubuntu-lab:~/lab4/workspace/python_project$

```

2. Verify the user entry:

```
getent passwd lab4user
```

```

lab4user:x:1002:1002:hajra,twenty two,03two7-5007883,03two7-5007883,nil:/home/lab4user:/bin/bash
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _

```

3. Switch to the new user to verify login:

```
su - lab4user
```

```

Password:
lab4user@ubuntu-lab:~$ _

```

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.:

```
sudo whoami
```

```

lab4user@ubuntu-lab:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu-lab:~$ _

```

5. Return to the original user:

[Exit](#)

```
~/lab4/workspace/python_project$ _
```

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

```
sudo deluser --remove-home lab4user
```

```

hajra@ubuntu-lab:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
[sudo] password for hajra:
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _

```

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

### **Steps (inside VM)**

1. Open an editor to create the script:

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

```
~/lab4/workspace/python_project$ nano $HOME/lab4/workspace/python_project/run-demo.sh
```

- Type the following lines into the editor (manually or paste), save and exit:

```
#!/bin/bash
echo "Lab 4 demo: current user is
$(whoami)" echo "Current time: $(date)"
uptime free -h
```

```
GNU nano 7.2 /home/hajra/lab4/workspace/python_project/run-demo.sh *
#!/bin/bash
echo "Lab 4 demo: current user is $(whoami)"
echo "Current time: $(date)"
uptime
free -h_
```

2. Make the script executable:

```
chmod +x ~/lab4/workspace/run-demo.sh
```

```
~/lab4/workspace/python_project$ chmod +x ~/lab4/workspace/python_project/run-demo.sh
~/lab4/workspace/python_project$ _
```

3. Run the script as your regular user:

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

```
Lab 4 demo: current user is $(whoami)
Current time: $(date)
19:02:29 up 6:39, 1 user, load average: 0.78, 0.74, 0.76
Mem:      total      used      free      shared  buff/cache   available
Swap:     1.9Gi      1.2Gi      111Mi      740Ki      730Mi      652Mi
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

4. Optionally run it with sudo:

```
sudo ~/lab4/workspace/run-demo.sh
```

```
[sudo] password for hajra:
Lab 4 demo: current user is $(whoami)
Current time: $(date)
19:03:47 up 6:41, 1 user, load average: 0.57, 0.66, 0.73
Mem:      total      used      free      shared  buff/cache   available
Swap:     1.9Gi      1.2Gi      128Mi      824Ki      731Mi      671Mi
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

## 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:

```
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 Sat 27 Sep 10:28:45 UTC 2025

System load:  1.46           Processes:           276
Usage of /:   70.2% of 11.21GB Users logged in:       1
Memory usage: 57%           IPv4 address for ens33: 192.168.161.129
Swap usage:   9%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

hajra@ubuntu-lab: $
```

2. Verify your current user and home directory path.

```
A111@DESKTOP-KQE4P80 MINGW64 - (main)
$ whoami
A111
A111@DESKTOP-KQE4P80 MINGW64 - (main)
$ /home/A111
bash: /home/A111: No such file or directory
```

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

```
ubuntu-lab
```

## 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.

```
total 44
drwxr-xr-x  4 hajra hajra 4096 Sep 26 22:08 .
drwxr-xr-x  3 root  root  4096 Sep 26 21:38 ..
-rw-r--r--  1 hajra hajra 220  Mar 31  2024 .bash_logout
-rw-r--r--  1 hajra hajra 3771 Mar 31  2024 .bashrc
drwx-----  2 hajra hajra 4096 Sep 26 21:40 .cache
-rw-----  1 hajra hajra  20 Sep 26 22:08 .lessht
-rw-r--r--  1 hajra hajra 807  Mar 31  2024 .profile
drwx-----  2 hajra hajra 4096 Sep 26 22:00 .ssh
-rw-r--r--  1 hajra hajra  10 Sep 26 21:48 .sudo_as_admin_successful
-rw-r--r--  1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$
```

Display the OS version and release information.

```
~/lab4/workspace/python_project$ uname -a
6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
~/lab4/workspace/python_project$
```

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



```

Home x Ubuntu 64-bit (6) x
Insecure 1 root root 7 Apr 22 2024 /bin -> usr/bin
Insecure 1 root root 8 Apr 22 2024 /sbin -> usr/sbin

/duf
total 4
drwxr-xr-x 20 root root 4096 Oct 23 12:23 .
drwxr-xr-x 23 root root 4096 Sep 26 21:13 ..
crw-rw-rw- 1 root root 10, 235 Oct 23 12:23 autofs
drwxr-xr-x 2 root root 70 Oct 23 12:23 blkio
drwxr-xr-x 2 root root 80 Oct 23 12:22 bsg
crw-rw-rw- 1 root disk 10, 224 Oct 23 12:22 btrfs-control
drwxr-xr-x 3 root root 60 Oct 23 12:22 bus
Insecure 1 root root 0 Oct 23 12:23 cdrom -> sro
drwxr-xr-x 2 root root 3740 Oct 23 12:22 cgroup
crw-rw-rw- 1 root tty 5, 1 Oct 23 12:23 console
Insecure 1 root root 11 Oct 23 12:22 core -> /proc/kcore
drwxr-xr-x 4 root root 80 Oct 23 12:23 cpu
crw-rw-rw- 1 root root 10, 129 Oct 23 12:23 csw_dma_latency
crw-rw-rw- 1 root root 10, 283 Oct 23 12:23 cusp
drwxr-xr-x 10 root root 200 Oct 23 12:23 disk
drwxr-xr-x 1 root disk 252, 0 Oct 23 12:23 dma
drwxr-xr-x 2 root root 60 Oct 23 12:22 dma_heap
crw-rw-rw- 1 root audio 14, 9 Oct 23 12:23 dmidev
drwxr-xr-x 3 root root 100 Oct 23 12:23 dmi
crw-rw-rw- 1 root root 10, 125 Oct 23 12:23 ecmvttfs
drwxr-xr-x 1 root video 23, 0 Oct 23 12:23 fb
Insecure 1 root root 13 Oct 23 12:22 fd -> /proc/self/fd
crw-rw-rw- 1 root root 1, 7 Oct 23 12:23 full
crw-rw-rw- 1 root root 10, 229 Oct 23 12:23 fuse
crw-rw-rw- 1 root root 241, 0 Oct 23 12:23 hidraw
crw-rw-rw- 1 root root 10, 230 Oct 23 12:23 hpet
drwxr-xr-x 2 root root 0 Oct 23 12:23 hugepages
crw-rw-rw- 1 root root 10, 189 Oct 23 12:23 hwrng
Insecure 1 root root 12 Oct 23 12:23 initctl -> /run/initctl
drwxr-xr-x 4 root root 200 Oct 23 12:23 input
crw-rw-rw- 1 root root 1, 11 Oct 23 12:23 kmsg
Insecure 1 root root 0 Oct 23 12:22 log -> /run/systemd/journal/dev-log
drwxr-xr-x 1 root disk 7, 0 Oct 23 12:23 loop0
brw-rw-rw- 1 root disk 7, 1 Oct 23 12:23 loop1
brw-rw-rw- 1 root disk 7, 10 Oct 23 12:23 loop10
brw-rw-rw- 1 root disk 7, 11 Oct 23 12:23 loop11
brw-rw-rw- 1 root disk 7, 12 Oct 23 12:23 loop12
brw-rw-rw- 1 root disk 7, 13 Oct 23 12:23 loop13
brw-rw-rw- 1 root disk 7, 14 Oct 23 12:23 loop14
brw-rw-rw- 1 root disk 7, 15 Oct 23 12:23 loop15
brw-rw-rw- 1 root disk 7, 16 Oct 23 12:23 loop16
brw-rw-rw- 1 root disk 7, 17 Oct 23 12:23 loop17
brw-rw-rw- 1 root disk 7, 18 Oct 23 12:23 loop18
brw-rw-rw- 1 root disk 7, 19 Oct 23 12:23 loop19

```

3. Display all hidden files in your home directory.

```

total 48
drwxr-xr-x 5 hajra hajra 4096 Oct 23 04:41
drwxr-xr-x 3 root root 4096 Sep 26 21:38
-rw-rw-rw- 1 hajra hajra 220 Mar 31 2024 .bash_logout
-rw-rw-rw- 1 hajra hajra 3771 Mar 31 2024 .bashrc
drwx----- 2 hajra hajra 4096 Sep 26 21:40 .cache
drwxrwxr-x 2 hajra hajra 4096 Oct 23 04:41 .lesshst
-rw-rw-rw- 1 hajra hajra 20 Sep 26 22:08 .profile
drwx----- 2 hajra hajra 4096 Sep 26 22:00 .ssh
-rw-rw-rw- 1 hajra hajra 0 Sep 26 21:48 .sudo_as_admin_successful
-rw-rw-rw- 1 hajra hajra 9839 Sep 26 22:06 'systemctl status ssh'
hajra@ubuntu-lab:~$

```

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

1. Go to your **home directory** (or your lab workspace folder):

cd ~ or cd ~/lab4/workspace

```
~$ cd ~/lab4/workspace
```

2. Create and open a new Markdown file using **nano editor**:

nano report.md

```
~/lab4/workspace$ nano report.md_
```

3. Inside nano, type your short summary.

```

<!--System Directory Summary-->
- **/bin** - contains essential user command binaries (like ls, cp, mv)
- **/sbin** - Contain system binaries used mainly by the root user for system admi
- **/usr** - Contains user-installed programs, libraries, and documentation.
- **/opt** - Used for optional or third-party software.
- **/etc** - Contains configuration files for the system and installed services.
- **/dev** - Contains device files representing hardware devices.
- **/var** - Contains variable data such as logs, caches, and spool files.
- **tmp** - Temporary files created by running processes.

hajra@ubuntu-lab:~/lab4/workspace$

```

```

GNU nano 7.2 report.md *
<!--System Directory Summary-->
- **/bin** - contains essential user command binaries (like ls, cp, mv)
- **/sbin** - Contain system binaries used mainly by the root user for system admi
- **/usr** - Contains user-installed programs, libraries, and documentation.
- **/opt** - Used for optional or third-party software.
- **/etc** - Contains configuration files for the system and installed services.
- **/dev** - Contains device files representing hardware devices.
- **/var** - Contains variable data such as logs, caches, and spool files.
- **tmp** - Temporary files created by running processes.

```

4. When done, **save and exit nano**.

### 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.

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ pwd
/home/hajra/lab4/workspace/python_project
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ ls -ls
total 20
drwxr-xr-x 2 hajra hajra 4096 Oct 23 14:14
-rw-r--r-- 1 hajra hajra 4096 Oct 23 14:11
-rw-r--r-- 1 hajra hajra 11 Oct 23 14:14 .env
-rw-r--r-- 1 hajra hajra 51 Oct 23 14:11 main.py
-rw-r--r-- 1 hajra hajra 13 Oct 23 14:07 README.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

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

```
cp README.md README.copy.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$ cp README.md README.md.copy.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$
Created a copy of the README file.
mv README.copy.md README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$ mv README.md.copy.md README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$
Renamed (moved) the copied file.
rm README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$ rm README.dev.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$
Deleted the renamed file.
```

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

```
mkdir -p ~/lab4/workspace/java_app
hajra@ubuntu-lab:~/lab4/workspace/python_project$ mkdir -p $HOME/lab4/workspace/java_app
hajra@ubuntu-lab:~/lab4/workspace/python_project$
Created another directory for a Java app.
cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
hajra@ubuntu-lab:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project $HOME/lab4/workspace/java_app_copy
hajra@ubuntu-lab:~/lab4/workspace/python_project$
Copied the entire Python project directory recursively.
ls -ls ~/lab4/workspace
total 16
drwxr-xr-x 4 hajra hajra 4096 Oct 23 14:14
drwxr-xr-x 2 hajra hajra 4096 Oct 23 14:14
drwxr-xr-x 2 hajra hajra 4096 Oct 23 14:14
-rw-r--r-- 1 hajra hajra 13 Oct 23 14:07 README.md
hajra@ubuntu-lab:~/lab4/workspace/python_project$
Verified the copied directories.
```

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ history
1  ls -ls
2  cp README.md README.copy.md
3  mv README.copy.md README.dev.md
4  rm README.dev.md
5  mkdir -p ~/lab4/workspace/java_app
6  cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
7  ls -ls ~/lab4/workspace
8  history
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

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

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ cat main.py
print ("hello lab4")
```

#### 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.

```
hajra@ubuntu-lab:~/lab4/workspace/python_project$ uname -a
Linux ubuntu-lab 6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
hajra@ubuntu-lab:~/lab4/workspace/python_project$
```

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

```
Mem:                total        used        free        shared    buff/cache    available
Swap:              2.0Gi          30Mi        2.0Gi
hajra@ubuntu-lab:~$ df -h
Filesystem          Size  Used Avail Use% Mounted on
tmpfs               192M  1.5M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 12G   11G  335M  97% /
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   20K  192M   1% /run/user/1000
hajra@ubuntu-lab:~$
```



root	4986	0.0	0.1	1258496	2228	?	S1	12:24	0:00	httpd -d /snap/nextcloud/26464 -k start -DFOREGROUND
root	4987	0.0	0.1	1258496	2228	?	S1	12:24	0:00	httpd -d /snap/nextcloud/26464 -k start -DFOREGROUND
root	5496	0.0	0.1	8440	3456	?	Ss	12:24	0:02	bash /snap/microk8s/8511/run-cluster-agent-with-args
hajra	5630	0.0	0.4	26640	6192	?	Ss	12:24	0:01	/usr/lib/systemd/systemd --user
hajra	5632	0.0	0.0	21140	1852	?	S	12:24	0:00	(sd-ran)
hajra	5634	0.0	0.2	8656	4096	ttul	S	12:24	0:00	-bash
root	5729	0.0	0.3	1258884	7672	?	S1	12:24	0:04	/snap/microk8s/8511/bin/cluster-agent cluster-agent --bind 0.0.0.0:25000 --keyfile /var/snap/
root	5985	1.0	1.5	2309568	31192	?	Ss1	12:24	1:50	/snap/microk8s/8511/bin/containerd --config /var/snap/microk8s/8511/args/containerd.toml --no
root	6269	7.2	16.1	1546420	318220	?	Ss1	12:24	12:12	/snap/microk8s/8511/kubelite --scheduler-args-files /var/snap/microk8s/8511/args/kube-schedule
root	7140	0.3	0.4	1234156	6380	?	S1	12:24	0:33	/snap/microk8s/8511/bin/containerd-shim-runc-v2 --namespace k8s.io -id ce847834b0d5618485948
65535	7229	0.0	0.0	1820	128	?	Ss	12:24	0:00	/pause
root	7568	0.0	0.3	1234412	6380	?	S1	12:25	0:03	/snap/microk8s/8511/bin/containerd-shim-runc-v2 --namespace k8s.io -id 1fa57b0780d67f58e774952
65535	7680	0.0	0.0	1820	128	?	Ss	12:25	0:00	/pause
root	7639	0.3	0.4	1234412	6552	?	S1	12:25	0:33	/snap/microk8s/8511/bin/containerd-shim-runc-v2 --namespace k8s.io -id 9e7095c3fa2edabd7e07c5b
65535	7670	0.0	0.0	1820	128	?	Ss	12:25	0:00	/pause
root	7728	0.2	1.0	764656	20364	?	Ss1	12:25	0:24	/coredns -conf /etc/coredns/Corefile
lxd	7788	0.3	1.5	1276780	31880	?	Ss1	12:25	0:05	/usr/bin/lxc/controllers
root	8389	0.0	0.0	4476	1152	?	Ss	12:25	0:00	/usr/local/bin/runcvdir -P /etc/service/enabled
root	8637	0.0	0.0	4324	1152	?	Ss	12:25	0:00	runcv allocate-tunnel-addr
root	8638	0.0	0.0	4324	1152	?	Ss	12:25	0:00	runcv felix
root	8639	0.0	0.0	4324	1152	?	Ss	12:25	0:00	runcv node-status-reporter
root	8640	0.0	0.0	4324	1152	?	Ss	12:25	0:00	runcv cni
root	8641	0.0	0.0	4324	1152	?	Ss	12:25	0:00	runcv monitor-addresses
root	8642	0.0	2.9	1794476	58192	?	S1	12:25	0:01	calico-node -allocate-tunnel-addr
root	8643	0.0	2.0	1794220	56160	?	S1	12:25	0:01	calico-node -status-reporter
root	8644	0.0	2.7	1794476	55000	?	S1	12:25	0:01	calico-node -monitor-token
root	8646	2.7	3.5	2237380	68964	?	S1	12:25	0:34	calico-node -felix
root	8647	0.0	2.0	1794476	55192	?	S1	12:25	0:01	calico-node -monitor-addresses
root	48430	0.0	0.0	0	0	?	IC	12:37	0:04	[kworker/0:0h-kblockd]
root	115363	0.0	0.0	0	0	?	IC	12:52	0:00	[kworker/0:15-c]
root	119204	0.0	1.9	478476	38364	?	Ss1	12:57	0:01	/usr/libexec/fuupd/fuupd
root	119202	0.0	0.4	314000	6960	?	Ss1	12:57	0:00	/usr/libexec/upowerd
root	149609	0.0	0.0	0	0	?	IC	13:00	0:00	[kworker/1:0u]
root	347306	0.0	0.0	0	0	?	I	13:48	0:00	[kworker/u257:0-flush-252:0]
root	527626	0.0	0.0	0	0	?	I	14:28	0:00	[kworker/u257:0-writeback]
root	590250	0.0	0.0	0	0	?	I	14:39	0:00	[kworker/u257:2-flush-252:0]
root	666337	0.2	0.0	0	0	?	I	14:57	0:02	[kworker/1:1-events]
root	681389	0.0	0.0	0	0	?	I	15:00	0:00	[kworker/u257:3-events_power_efficient]
root	684235	0.3	0.0	0	0	?	I	15:01	0:02	[kworker/0:1-events]
root	693388	0.0	0.0	0	0	?	I	15:03	0:00	[kworker/1:2-events]
root	698137	0.0	0.0	0	0	?	I	15:04	0:00	[kworker/u257:3-events_unbound]
root	709790	0.1	0.0	0	0	?	I	15:06	0:00	[kworker/0:0-events]
root	711803	0.0	0.0	0	0	?	I	15:06	0:00	[kworker/u257:1-writeback]
root	719791	0.4	0.0	0	0	?	I	15:08	0:01	[kworker/1:0-events]
root	724101	0.0	0.0	4556	1536	?	S	15:09	0:00	sleep 5s
root	733879	0.0	0.0	0	0	?	I	15:11	0:00	[kworker/0:2-events]
root	737692	0.0	0.0	0	0	?	I	15:12	0:00	[kworker/u257:1-flush-252:0]
root	740076	0.0	0.0	5340	1664	?	S	15:12	0:00	sleep 5
hajra	740909	1050	0.2	12312	5120	ttul	R+	15:13	0:00	ps aux

h@ubuntu-lab:~/lab4/workspace/python\_projects\$

## 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.

```

info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1002) ...
info: Adding new user `lab4user' (1002) with group `lab4user (1002)' ...
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 []: hajra
  Room Number []: twenty two
  Work Phone []: 03two7-5007883
  Home Phone []: 03two7-5007883
  Other []: nil
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
hajra@ubuntu-lab:~/lab4/workspace/python_projects$

```

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

```

lab4user:x:1002:1002:hajra, twenty two, 03two7-5007883, 03two7-5007883, nil:/home/lab4user:/bin/bash
hajra@ubuntu-lab:~/lab4/workspace/python_projects$

```

3. Log in as lab4user and confirm successful login.

```

Password:
lab4user@ubuntu-lab:~$

```

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

```

lab4user@ubuntu-lab:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu-lab:~$

```

5. Switch back to your main analyst account.

```

~/lab4/workspace/python_projects$

```

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

```
info: Looking for files to backup/remove ...  
info: Removing files ...  
info: Removing crontab ...  
info: Removing user 'lab4user' ...  
hajra@ubuntu-lab:~/lab4/workspace/python_project$ _
```