

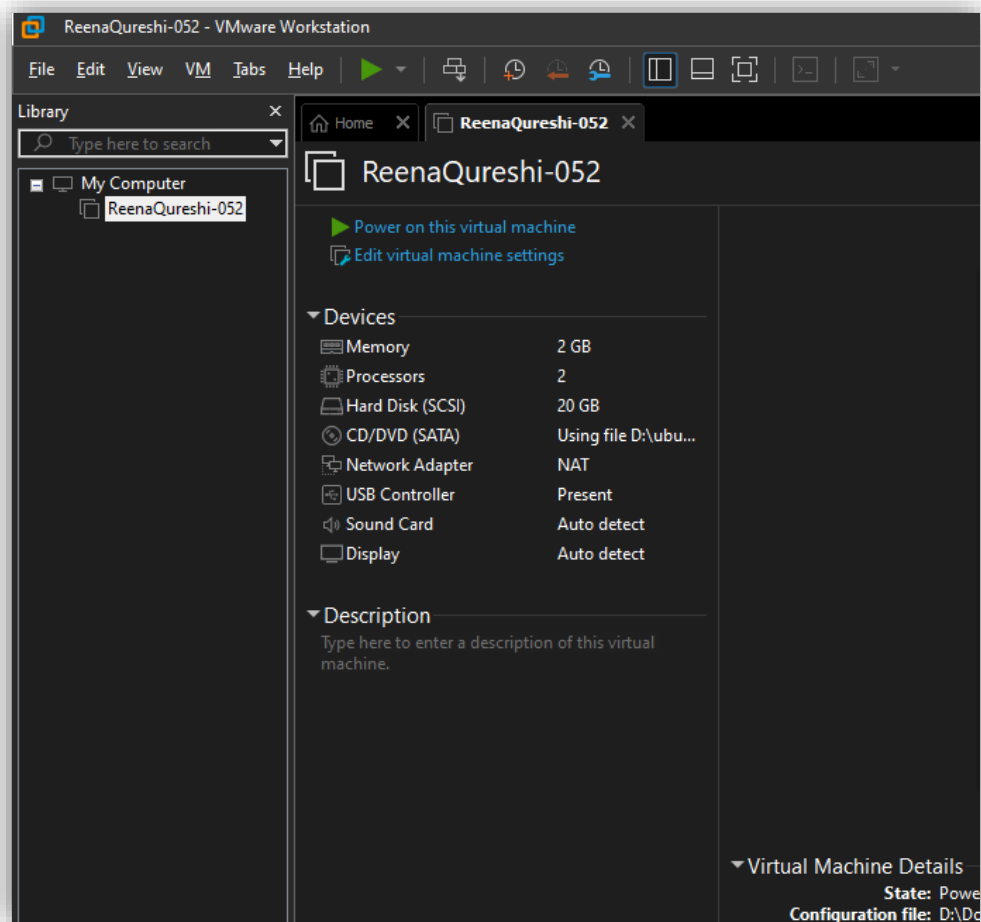
Name : Reena Qureshi

Reg No : 2023-BSE-052

Section : V-B

Lab 4

Task 1 – Verify VM resources in VMware



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

```
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Reena Qureshi> ssh reenaqureshi@192.168.76.129
reenaqureshi@192.168.76.129's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Oct 22 04:25:34 PM UTC 2025

System load:  0.01          Processes:            218
Usage of /:   45.1% of 9.75GB Users logged in:          1
Memory usage: 15%          IPv4 address for ens33: 192.168.76.129
Swap usage:   0%

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Oct 22 16:22:57 2025 from 192.168.76.1
reenaqureshi@reena2904:~$ whoami
reenaqureshi
reenaqureshi@reena2904:~$ pwd
/home/reenaqureshi
reenaqureshi@reena2904:~$
```

```
Last login: Wed Oct 22 16:22:57 2025 from 192.168.76.1
reenaqureshi@reena2904:~$ whoami
reenaqureshi
reenaqureshi@reena2904:~$ pwd
/home/reenaqureshi
reenaqureshi@reena2904:~$
```

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

List root directory contents:

```
valid_lrt forever preferred_lrt forever
reenaquareshi@reena2904:~$ ls -la /
total 1994844
drwxr-xr-x 23 root root      4096 Sep 26 10:09 .
drwxr-xr-x 23 root root      4096 Sep 26 10:09 ..
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 10:09 boot
dr-xr-xr-x  2 root root      4096 Aug  5 23:53 cdrom
drwxr-xr-x 20 root root     4120 Oct 22 16:12 dev
drwxr-xr-x 108 root root     4096 Sep 26 10:17 etc
drwxr-xr-x  3 root root      4096 Sep 26 10:17 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 10:03 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 Oct 22 16:12 proc
drwx----- 3 root root      4096 Oct 22 16:19 root
drwxr-xr-x 29 root root       860 Oct 22 16:25 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 10:17 snap
drwxr-xr-x  2 root root      4096 Aug  5 16:54 srv
-rw-----  1 root root 2042626048 Sep 26 10:09 swap.img
dr-xr-xr-x 13 root root       0 Oct 22 16:12 sys
drwxrwxrwt 15 root root      4096 Oct 22 16:25 tmp
drwxr-xr-x 12 root root      4096 Aug  5 16:54 usr
drwxr-xr-x 13 root root      4096 Sep 26 10:17 var
reenaquareshi@reena2904:~$
```

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

ls -la /bin

```
reenaquareshi@reena2904:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
reenaquareshi@reena2904:~$
```

ls -la /sbin

```
reenaquareshi@reena2904:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
reenaquareshi@reena2904:~$
```

ls -la /usr

```
reenaquareshi@reena2904:~$ 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 10:09 ..
drwxr-xr-x  2 root root 36864 Sep 26 10:09 bin
drwxr-xr-x  2 root root 4096 Apr 22  2024 games
drwxr-xr-x 33 root root 4096 Sep 26 10:06 include
drwxr-xr-x 78 root root 4096 Sep 26 10:09 lib
drwxr-xr-x  2 root root 4096 Aug  5 17:01 lib64
drwxr-xr-x 11 root root 4096 Sep 26 10:08 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x  2 root root 20480 Sep 26 10:10 sbin
drwxr-xr-x 124 root root 4096 Sep 26 10:09 share
drwxr-xr-x  4 root root 4096 Sep 26 10:07 src
reenaquareshi@reena2904:~$
```

ls -la /opt

```
reenaquareshi@reena2904:~$ 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 10:09 ..
reenaquareshi@reena2904:~$
```

ls -la /etc

```
reenaquareshi@reena2904:~$ ls -la /etc
total 408
-rw-r--r--  1 root root      0 Sep 26 10:17 subuid
-rw-r--r--  1 root root      0 Aug  5 16:54 subuid-
-rw-r--r--  1 root root  4343 Jun 25 12:42 sudo.conf
-r--r-----  1 root root  1800 Jan 29  2024 sudoers
drwxr-xr-x  2 root root  4096 Aug  5 17:02 sudoers.d
-rw-r--r--  1 root root  9804 Jun 25 12:42 sudo_logsrvd.conf
drwxr-xr-x  2 root root  4096 Aug  5 17:14 supercat
-rw-r--r--  1 root root  2209 Mar 24  2024 sysctl.conf
drwxr-xr-x  2 root root  4096 Aug  5 17:02 sysctl.d
drwxr-xr-x  2 root root  4096 Aug  5 17:14 sysstat
drwxr-xr-x  6 root root  4096 Aug  5 16:49 systemd
drwxr-xr-x  2 root root  4096 Aug  5 17:00 terminfo
drwxr-xr-x  2 root root  4096 Sep 26 10:08 thermalid
-rw-r--r--  1 root root      8 Aug  5 17:02 timezone
drwxr-xr-x  2 root root  4096 Aug  5 17:14 tmpfiles.d
drwxr-xr-x  2 root root  4096 Aug  5 17:14 ubuntu-advantage
-rw-r--r--  1 root root  1260 Jan 27  2023 ucf.conf
drwxr-xr-x  4 root root  4096 Aug  5 17:02 udev
drwxr-xr-x  2 root root  4096 Aug  5 17:14 udisks2
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 update-manager
drwxr-xr-x  2 root root  4096 Aug  5 17:14 update-motd.d
drwxr-xr-x  2 root root  4096 Aug  5 17:14 update-notifier
drwxr-xr-x  2 root root  4096 Sep 26 10:08 UPower
-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.d
lrwxrwxrwx  1 root root    16 Aug  5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x  2 root root  4096 Aug  5 17:14 vim
drwxr-xr-x  4 root root  4096 Aug  5 17:14 vmware-tools
lrwxrwxrwx  1 root root    23 Feb 26  2024 vttrgb -> /etc/alternatives/vttrgb
-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 xdg
drwxr-xr-x  2 root root  4096 Aug  5 17:02 xml
-rw-r--r--  1 root root   460 Aug  5 17:14 zsh_command_not_found
reenaquareshi@reena2904:~$
```

ls -la /dev

```

crw-rw---- 1 root    kvm      10, 124 Oct 22 16:12 udmabuf
crw----- 1 root    root      10, 239 Oct 22 16:12 uhid
crw----- 1 root    root      10, 223 Oct 22 16:12 uinput
crw-rw-rw- 1 root    root        1,   9 Oct 22 16:12 urandom
crw----- 1 root    root      10, 126 Oct 22 16:12 userfaultfd
crw----- 1 root    root      10, 240 Oct 22 16:12 userio
crw-rw---- 1 root    tty        7,   0 Oct 22 16:12 vcs
crw-rw---- 1 root    tty        7,   1 Oct 22 16:12 vcs1
crw-rw---- 1 root    tty        7,   2 Oct 22 16:12 vcs2
crw-rw---- 1 root    tty        7,   3 Oct 22 16:12 vcs3
crw-rw---- 1 root    tty        7,   4 Oct 22 16:12 vcs4
crw-rw---- 1 root    tty        7,   5 Oct 22 16:12 vcs5
crw-rw---- 1 root    tty        7,   6 Oct 22 16:12 vcs6
crw-rw---- 1 root    tty        7, 128 Oct 22 16:12 vcsa
crw-rw---- 1 root    tty        7, 129 Oct 22 16:12 vcsa1
crw-rw---- 1 root    tty        7, 130 Oct 22 16:12 vcsa2
crw-rw---- 1 root    tty        7, 131 Oct 22 16:12 vcsa3
crw-rw---- 1 root    tty        7, 132 Oct 22 16:12 vcsa4
crw-rw---- 1 root    tty        7, 133 Oct 22 16:12 vcsa5
crw-rw---- 1 root    tty        7, 134 Oct 22 16:12 vcsa6
crw-rw---- 1 root    tty        7,  64 Oct 22 16:12 vcsu
crw-rw---- 1 root    tty        7,  65 Oct 22 16:12 vcsu1
crw-rw---- 1 root    tty        7,  66 Oct 22 16:12 vcsu2
crw-rw---- 1 root    tty        7,  67 Oct 22 16:12 vcsu3
crw-rw---- 1 root    tty        7,  68 Oct 22 16:12 vcsu4
crw-rw---- 1 root    tty        7,  69 Oct 22 16:12 vcsu5
crw-rw---- 1 root    tty        7,  70 Oct 22 16:12 vcsu6
drwxr-xr-x 2 root    root      10,  60 Oct 22 16:12 vfio
crw----- 1 root    root      10, 127 Oct 22 16:12 vga_arbiter
crw----- 1 root    root      10, 137 Oct 22 16:12 vhci
crw-rw---- 1 root    kvm      10, 238 Oct 22 16:12 vhost-net
crw-rw---- 1 root    kvm      10, 241 Oct 22 16:12 vhost-vsock
crw----- 1 root    root      10, 122 Oct 22 16:12 vmci
crw-rw-rw- 1 root    root      10, 121 Oct 22 16:12 vsock
crw-rw-rw- 1 root    root        1,   5 Oct 22 16:12 zero
crw----- 1 root    root      10, 249 Oct 22 16:12 zfs

```

ls -la /var

```

reenaquareshi@reena2904:~$ ls -la /var
total 56
drwxr-xr-x 13 root root 4096 Sep 26 10:17 .
drwxr-xr-x 23 root root 4096 Sep 26 10:09 ..
drwxr-xr-x  2 root root 4096 Sep 28 14:19 backups
drwxr-xr-x 16 root root 4096 Oct 22 16:25 cache
drwxrwsrwt  2 root root 4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root 4096 Oct 22 16:25 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 22 16:12 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 22 16:25 tmp
-rw-r--r--  1 root root 208 Aug  5 16:54 .updated
reenaquareshi@reena2904:~$

```

ls -la /tmp

```
reenaquareshi@reena2904:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 22 16:25 .
drwxr-xr-x 23 root root 4096 Sep 26 10:09 ..
drwxrwxrwt 2 root root 4096 Oct 22 16:12 .font-unix
drwxrwxrwt 2 root root 4096 Oct 22 16:12 .ICE-unix
drwx----- 2 root root 4096 Oct 22 16:12 snap-private-tmp
drwx----- 3 root root 4096 Oct 22 16:25 systemd-private-b1351901b78a4aff9ef31bbbe399f491-fwupd.service-2DKIts
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-ModemManager.service-1xXnzH
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-polkit.service-n2SQ8R
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-systemd-logind.service-f65Mx6
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-systemd-resolved.service-gNaKAD
drwx----- 3 root root 4096 Oct 22 16:25 systemd-private-b1351901b78a4aff9ef31bbbe399f491-systemd-timesyncd.service-WPovCg
drwx----- 2 root root 4096 Oct 22 16:12 vmware-root_738-2999591909
drwxrwxrwt 2 root root 4096 Oct 22 16:12 .X11-unix
drwxrwxrwt 2 root root 4096 Oct 22 16:12 .XIM-unix
```

ls -la ~

```
drwxrwxrwt 2 root root 4096 Oct 22 16:12 .XIM-unix
reenaquareshi@reena2904:~$ ls -la ~
total 32
drwxr-x--- 4 reenaquareshi reenaquareshi 4096 Oct 22 16:19 .
drwxr-xr-x 3 root root 4096 Sep 26 10:17 ..
-rw----- 1 reenaquareshi reenaquareshi 8 Sep 26 14:05 .bash_history
-rw-r--r-- 1 reenaquareshi reenaquareshi 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 reenaquareshi reenaquareshi 3771 Mar 31 2024 .bashrc
drwx----- 2 reenaquareshi reenaquareshi 4096 Sep 26 10:25 .cache
-rw-r--r-- 1 reenaquareshi reenaquareshi 807 Mar 31 2024 .profile
drwx----- 2 reenaquareshi reenaquareshi 4096 Oct 22 16:16 .ssh
-rw-r--r-- 1 reenaquareshi reenaquareshi 0 Oct 22 16:19 .sudo_as_admin_successful
reenaquareshi@reena2904:~$
```

nano ~/answers.md

```
reenaquareshi@reena2904:~$ cat ~/answers.md
/bin contains essential user binaries needed to boot and run the system
usr/bin contains most installed programs and applications
usr/local/bin stores user compiled or custom software not managed by system package manager
reenaquareshi@reena2904:~$
```

Task 4 – Essential CLI tasks — navigation and file operations

Create a workspace and navigate.

mkdir -p ~/lab4/workspace/python_project

```
reenaquareshi@reena2904:~$ mkdir -p ~/lab4/workspace/python_project
reenaquareshi@reena2904:~$ cd ~/lab4/workspace/python_project
reenaquareshi@reena2904:~/lab4/workspace/python_project$ pwd
/home/reenaquareshi/lab4/workspace/python_project
reenaquareshi@reena2904:~/lab4/workspace/python_project$
```

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

```
Reenaquareshi@052
GNU nano 7.2
LAB 4 README
```

```
ReenaQureshi-052 x
GNU nano 7.2 main.py *
print ("hello lab4")

ReenaQureshi-052 x
GNU nano 7.2 .env *
ENV = lab4_
```

List files and capture:

```
reenaqareshi@reena2904:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 reenaqareshi reenaqareshi 4096 Oct 22 17:25 .
drwxrwxr-x 3 reenaqareshi reenaqareshi 4096 Oct 22 17:15 ..
-rw-rw-r-- 1 reenaqareshi reenaqareshi  11 Oct 22 17:25 .env
-rw-rw-r-- 1 reenaqareshi reenaqareshi  21 Oct 22 17:23 main.py
-rw-rw-r-- 1 reenaqareshi reenaqareshi  13 Oct 22 17:21 README.md
reenaqareshi@reena2904:~/lab4/workspace/python_project$
```

Copy, move and remove:

```
reenaqareshi@reena2904:~/lab4/workspace/python_project$ cp README.md README.copy.md
reenaqareshi@reena2904:~/lab4/workspace/python_project$ cp README.copy.md README.dev.md
reenaqareshi@reena2904:~/lab4/workspace/python_project$ rm README.dev.md
reenaqareshi@reena2904:~/lab4/workspace/python_project$ _
```

mkdir -p ~/lab4/workspace/java_app

```
reenaqareshi@reena2904:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
reenaqareshi@reena2904:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project cp -r ~/lab4/workspace/java_app_copy
target '/home/reenaqareshi/lab4/workspace/java_app_copy': No such file or directory
reenaqareshi@reena2904:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
```

```
reenaqareshi@reena2904:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 16
drwxrwxr-x 4 reenaqareshi reenaqareshi 4096 Oct 22 17:28 .
drwxrwxr-x 3 reenaqareshi reenaqareshi 4096 Oct 22 17:15 ..
drwxrwxr-x 2 reenaqareshi reenaqareshi 4096 Oct 22 17:28 java_app
drwxrwxr-x 2 reenaqareshi reenaqareshi 4096 Oct 22 17:27 python_project
reenaqareshi@reena2904:~/lab4/workspace/python_project$
```

USE COMMAND HISTORY AND TAB COMPLETION

```

reenaqureshi@reena2904:~/lab4/workspace/python_project$ history
1  ip addr
2  ssh reenaqureshi@192.168.76.129
3  sudo systemctl status ssh
4  ip a
5  ls -la /
6  ls -la /bin
7  ls -la /sbin
8  ls -la /usr
9  ls -la /opt
10 ls -la /etc
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 cp README.copy.md README.dev.md
28 rm README.dev.md
29 cd ~/lab4/workspace/java_app
30 mkdir -p ~/lab4/workspace/java_app
31 cp -r ~/lab4/workspace/python_project cp -r ~/lab4/workspace/java_app_copy
32 ls -la ~/lab4/workspace
33 history

```

Task 5 – System info, resources & processes

Kernel and OS:

uname -a

```

reenaqureshi@reena2904:~/lab4/workspace/python_project$ uname -a
Linux reena2904 6.8.0-71-generic #71-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 22 16:52:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
reenaqureshi@reena2904:~/lab4/workspace/python_project$

```

CPU (ensure model name visible):

cat /proc/cpuinfo


```

ReenaQureshi-052
uc_rnd and hyper_vision lah_f_lm pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust smep arat md_clear flush_l1d arch_capabilities
bugs : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_unknown retbleed bhi
bogomips : 5183.18
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 : 58
model name : Intel(R) Core(TM) i5-3320M CPU @ 2.60GHz
stepping : 9
microcode : 0x21
cpu MHz : 2591.593
cache size : 3072 KB
physical id : 2
siblings : 1
core id : 0
cpu cores : 1
apicid : 2
initial apicid : 2
fpu : yes
fpu_exception : yes
cpuid level : 13
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx rdtscp lm con
rfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 cx16 pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer
6c rdrand hypervisor lahf_lm pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust smep arat md_clear flush_l1d arch_capabilities
bugs : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_unknown retbleed bhi
bogomips : 5183.18
clflush_size : 64
cache_alignment : 64
address sizes : 45 bits physical, 48 bits virtual
power management:

reenaqureshi@reena2904:~/lab4/workspace/python_project$

```

Memory:

```

reenaqureshi@reena2904:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:            1.9Gi       376Mi       1.3Gi       1.2Mi       333Mi       1.5Gi
Swap:           1.9Gi         0B       1.9Gi

```

Disk:

```

reenaqureshi@reena2904:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:            1.9Gi       376Mi       1.3Gi       1.2Mi       333Mi       1.5Gi
Swap:           1.9Gi         0B       1.9Gi
reenaqureshi@reena2904:~/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 9.8G  4.5G  4.9G  48% /
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

```

View OS release information:

cat /etc/os-release

```

reenaqureshi@reena2904:~/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
reenaqureshi@reena2904:~/lab4/workspace/python_project$

```

Processes (show top lines of ps output):

```
root      820  0.0  0.6 468952 13568 ?        Ssl  16:12   0:00 /usr/libexec/udisks2/udisksd
syslog    847  0.0  0.2 222508  5888 ?        Ssl  16:12   0:00 /usr/sbin/rsyslogd -n -iNONE
root      852  0.0  0.0      0      0 ?        S    16:12   0:00 [irq/16-vmwgfx]
root      857  0.0  0.0      0      0 ?        I<   16:12   0:00 [kworker/R-ttm]
root      860  0.0  0.1   6824  2816 ?        Ss   16:12   0:00 /usr/sbin/cron -f -P
root      875  0.0  1.1 109692 22912 ?        Ssl  16:12   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgra
root      881  0.0  0.6 392028 12928 ?        Ssl  16:12   0:00 /usr/sbin/ModemManager
root      983  0.0  0.2   6940  4736 tty1    Ss   16:12   0:00 /bin/login -p --
root     1405  0.0  0.0      0      0 ?        S    16:13   0:00 [psimon]
reenaqu+ 1407  0.0  0.5 20088 11136 ?        Ss   16:13   0:00 /usr/lib/systemd/systemd --user
reenaqu+ 1408  0.0  0.1 21152  3648 ?        S    16:13   0:00 (sd-pam)
reenaqu+ 1417  0.0  0.2   8656  5248 tty1    S    16:13   0:00 -bash
root     1464  0.0  0.0      0      0 ?        I<   16:13   0:00 [kworker/R-tls-s]
root     1470  0.0  0.4 12020  7936 ?        Ss   16:14   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root     1495  0.0  0.0      0      0 ?        I    16:20   0:00 [kworker/u257:0-events_power_efficient]
root     1568  0.0  0.0      0      0 ?        I<   16:23   0:00 [kworker/0:0H]
root     1572  0.0  0.5 14964 10496 ?        Ss   16:25   0:00 sshd: reenaqureshi [priv]
root     1580  0.0  2.1 595032 43244 ?        Ssl  16:25   0:03 /usr/libexec/fwupd/fwupd
root     1587  0.0  0.4 313996 8960 ?        Ssl  16:25   0:00 /usr/libexec/upowerd
root     1628  0.0  0.1 81380  2952 ?        Ss   16:25   0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket -
reenaqu+ 1682  0.0  0.3 14964  6980 ?        S    16:25   0:00 sshd: reenaqureshi@pts/0
reenaqu+ 1683  0.0  0.2   8648  5504 pts/0    Ss+  16:25   0:00 -bash
root     1698  0.0  0.0      0      0 ?        I    16:27   0:00 [kworker/u257:1-events_power_efficient]
root     1865  0.0  0.0      0      0 ?        I    16:55   0:00 [kworker/u258:4-events_power_efficient]
root     1885  0.8  0.0      0      0 ?        I    17:05   0:15 [kworker/1:2-mpt_poll_0]
root     1894  0.0  0.0      0      0 ?        I    17:13   0:00 [kworker/u258:0-events_unbound]
root     1900  0.6  0.0      0      0 ?        I    17:16   0:07 [kworker/0:0-events]
root     1907  2.2  0.0      0      0 ?        I    17:20   0:21 [kworker/0:1-events]
root     1909  0.6  0.0      0      0 ?        I    17:22   0:05 [kworker/1:1-events]
root     1916  0.0  0.0      0      0 ?        I    17:25   0:00 [kworker/u258:2-events_power_efficient]
root     1918  0.0  0.0      0      0 ?        I    17:26   0:00 [kworker/u257:2-events_unbound]
reenaqu+ 1940  3.0  0.2 10884  4480 tty1    R+   17:36   0:00 ps aux
reenaqureshi@reena2904:~/lab4/workspace/python_project$
```

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

Create a new user named lab4user:

sudo adduser lab4user

```
reenaqureshi@reena2904:~$ sudo adduser lab4user
[sudo] password for reenaqureshi:
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 []: lab4user
  Room Number []: 100
  Work Phone []: 0300567543
  Home Phone []: 05123445
  Other []: 456
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
reenaqureshi@reena2904:~$
```

Verify the user entry:

getent passwd lab4user

```
reenaqureshi@reena2904:~$ getent passwd lab4user
lab4user:x:1001:1001:lab4user,100,0300567543,05123445,456:/home/lab4user:/bin/bash
reenaqureshi@reena2904:~$
```

Switch to the new user to verify login:

`su - lab4user`

```
reenaqureshi@reena2904:~$ su - lab4user
Password:
lab4user@reena2904:~$
```

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@reena2904:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@reena2904:~$
```

Return to the original user:

`exit`

```
ReenaQureshi-052 x
reenaqureshi@reena2904:~$
```

(Optional) Remove the test user when finished:

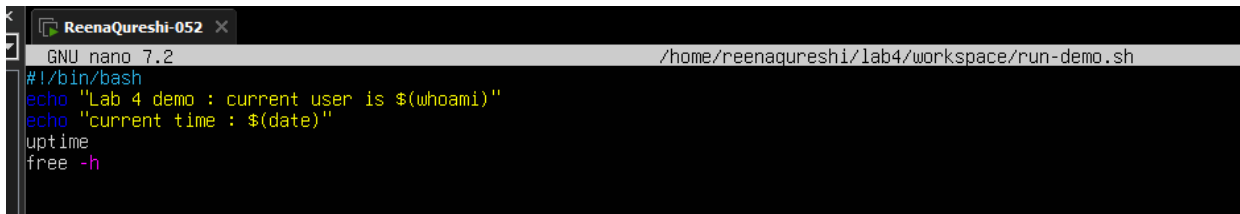
`sudo deluser --remove-home lab4user`

```
ReenaQureshi-052 x
reenaqureshi@reena2904:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
reenaqureshi@reena2904:~$ _
```

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

Open an editor to create the script:

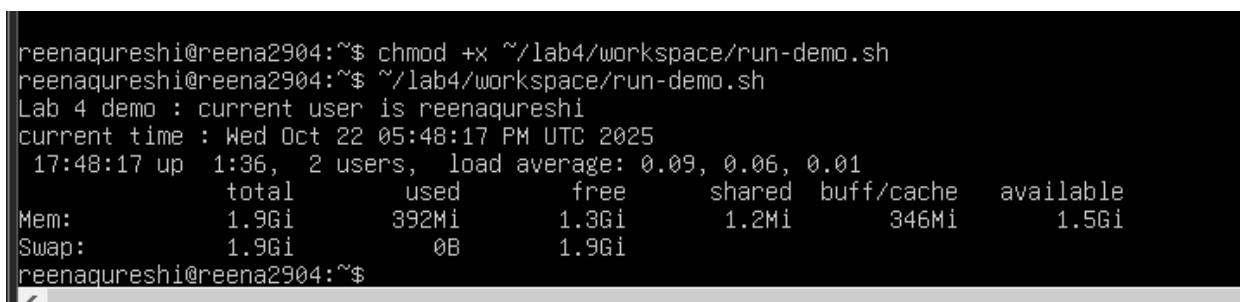
nano ~/lab4/workspace/run-demo.sh

A screenshot of a terminal window with a nano editor. The window title is 'ReenaQureshi-052'. The editor shows the following text:

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

Make the script executable:

Run the script as your regular user:

A screenshot of a terminal window showing the execution of the script. The user 'reenaqaureshi' runs 'chmod +x ~/lab4/workspace/run-demo.sh' and then './~/lab4/workspace/run-demo.sh'. The output is:

```
reenaqaureshi@reena2904:~$ chmod +x ~/lab4/workspace/run-demo.sh
reenaqaureshi@reena2904:~$ ./~/lab4/workspace/run-demo.sh
Lab 4 demo : current user is reenaqaureshi
current time : Wed Oct 22 05:48:17 PM UTC 2025
 17:48:17 up 1:36, 2 users, load average: 0.09, 0.06, 0.01
Mem:          total        used        free      shared  buff/cache   available
Swap:         1.9Gi         392Mi       1.3Gi         1.2Mi       346Mi       1.5Gi
reenaqaureshi@reena2904:~$
```

Exam Evaluation Questions

1. Remote Access Verification (Cyber Login Check)

Steps:

Connect to the Ubuntu VM remotely from your host terminal.

Try the new cross-platform PowerShell <https://aka.ms/pscore6>

```
PS C:\Users\Reena Qureshi> ssh reenaqureshi@192.168.76.129
reenaqureshi@192.168.76.129's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro
```

System information as of Wed Oct 22 04:25:34 PM UTC 2025

```
System load:  0.01      Processes:            218
Usage of /:   45.1% of 9.75GB Users logged in:          1
Memory usage: 15%      IPv4 address for ens33: 192.168.76.129
Swap usage:   0%
```

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`

The list of available updates is more than a week old.
To check for new updates run: `sudo apt update`

Last login: Wed Oct 22 16:22:57 2025 from 192.168.76.1

```
reenaqureshi@reena2904:~$ whoami
reenaqureshi
reenaqureshi@reena2904:~$ pwd
/home/reenaqureshi
reenaqureshi@reena2904:~$
```

VERIFY YOUR CURRENT USER AND HOME DIRECTORY PATH

```
Last login: Wed Oct 22 16:22:57 2025 from 192.168.76.1
reenaqureshi@reena2904:~$ whoami
reenaqureshi
reenaqureshi@reena2904:~$ pwd
/home/reenaqureshi
reenaqureshi@reena2904:~$
```

CONFIRM YOU ARE CONNECTED TO THE CORRECT HOST MACHINE

```
Ubuntu 24.04.3 LTS reena2904 tty1
reena2904 login: reenaqureshi
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Oct 22 06:05:25 PM UTC 2025

System load:  0.01               Processes:            223
Usage of /:   45.3% of 9.75GB    Users logged in:     1
Memory usage: 14%               IPv4 address for ens33: 192.168.76.129
Swap usage:   0%

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

2. Filesystem Inspection for Forensic Evidence

Steps:

Display the contents of the root directory.

```
reenaqureshi@reena2904:~$ ls -la /
total 1994844
drwxr-xr-x 23 root root      4096 Sep 26 10:09 .
drwxr-xr-x 23 root root      4096 Sep 26 10:09 ..
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 10:09 boot
dr-xr-xr-x  2 root root      4096 Aug  5 23:53 cdrom
drwxr-xr-x 20 root root     4120 Oct 22 16:12 dev
drwxr-xr-x 108 root root     4096 Sep 26 10:17 etc
drwxr-xr-x  3 root root      4096 Sep 26 10:17 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 10:03 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 Oct 22 16:12 proc
drwx----- 3 root root      4096 Oct 22 16:19 root
drwxr-xr-x 29 root root       860 Oct 22 16:25 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 10:17 snap
drwxr-xr-x  2 root root      4096 Aug  5 16:54 srv
-rw-----  1 root root 2042626048 Sep 26 10:09 swap.img
dr-xr-xr-x 13 root root         0 Oct 22 16:12 sys
drwxrwxrwt 15 root root      4096 Oct 22 16:25 tmp
drwxr-xr-x 12 root root      4096 Aug  5 16:54 usr
drwxr-xr-x 13 root root      4096 Sep 26 10:17 var
```

Display the OS version and release information

```
reenaquareshi@reena2904:~$ 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
reenaquareshi@reena2904:~$ _
```

Explore and record directory listings for /bin, /sbin

ls -la /bin

```
reenaquareshi@reena2904:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
reenaquareshi@reena2904:~$
```

ls -la /sbin

```
reenaquareshi@reena2904:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
reenaquareshi@reena2904:~$
```

ls -la /usr

```
reenaquareshi@reena2904:~$ 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 10:09 ..
drwxr-xr-x  2 root root 36864 Sep 26 10:09 bin
drwxr-xr-x  2 root root 4096 Apr 22  2024 games
drwxr-xr-x 33 root root 4096 Sep 26 10:06 include
drwxr-xr-x 78 root root 4096 Sep 26 10:09 lib
drwxr-xr-x  2 root root 4096 Aug  5 17:01 lib64
drwxr-xr-x 11 root root 4096 Sep 26 10:08 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x  2 root root 20480 Sep 26 10:10 sbin
drwxr-xr-x 124 root root 4096 Sep 26 10:09 share
drwxr-xr-x  4 root root 4096 Sep 26 10:07 src
reenaquareshi@reena2904:~$
```

ls -la /opt

```
reenaquareshi@reena2904:~$ 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 10:09 ..
reenaquareshi@reena2904:~$
```

ls -la /etc

```

reena@reena2904:~$ ls -la /dev
crw-rw-rw- 1 root root 10, 124 Oct 22 16:12 udmabuf
crw-rw-rw- 1 root root 10, 239 Oct 22 16:12 uhid
crw-rw-rw- 1 root root 10, 223 Oct 22 16:12 uinput
crw-rw-rw- 1 root root 1, 9 Oct 22 16:12 urandom
crw-rw-rw- 1 root root 10, 126 Oct 22 16:12 userfaultfd
crw-rw-rw- 1 root root 10, 240 Oct 22 16:12 userio
crw-rw-rw- 1 root tty 7, 0 Oct 22 16:12 vcs
crw-rw-rw- 1 root tty 7, 1 Oct 22 16:12 vcs1
crw-rw-rw- 1 root tty 7, 2 Oct 22 16:12 vcs2
crw-rw-rw- 1 root tty 7, 3 Oct 22 16:12 vcs3
crw-rw-rw- 1 root tty 7, 4 Oct 22 16:12 vcs4
crw-rw-rw- 1 root tty 7, 5 Oct 22 16:12 vcs5
crw-rw-rw- 1 root tty 7, 6 Oct 22 16:12 vcs6
crw-rw-rw- 1 root tty 7, 128 Oct 22 16:12 vcsa
crw-rw-rw- 1 root tty 7, 129 Oct 22 16:12 vcsa1
crw-rw-rw- 1 root tty 7, 130 Oct 22 16:12 vcsa2
crw-rw-rw- 1 root tty 7, 131 Oct 22 16:12 vcsa3
crw-rw-rw- 1 root tty 7, 132 Oct 22 16:12 vcsa4
crw-rw-rw- 1 root tty 7, 133 Oct 22 16:12 vcsa5
crw-rw-rw- 1 root tty 7, 134 Oct 22 16:12 vcsa6
crw-rw-rw- 1 root tty 7, 64 Oct 22 16:12 vcsu
crw-rw-rw- 1 root tty 7, 65 Oct 22 16:12 vcsu1
crw-rw-rw- 1 root tty 7, 66 Oct 22 16:12 vcsu2
crw-rw-rw- 1 root tty 7, 67 Oct 22 16:12 vcsu3
crw-rw-rw- 1 root tty 7, 68 Oct 22 16:12 vcsu4
crw-rw-rw- 1 root tty 7, 69 Oct 22 16:12 vcsu5
crw-rw-rw- 1 root tty 7, 70 Oct 22 16:12 vcsu6
drwxr-xr-x 2 root root 10, 60 Oct 22 16:12 vfiio
crw-rw-rw- 1 root root 10, 127 Oct 22 16:12 vga_arbiter
crw-rw-rw- 1 root root 10, 137 Oct 22 16:12 vhci
crw-rw-rw- 1 root kvm 10, 238 Oct 22 16:12 vhost-net
crw-rw-rw- 1 root kvm 10, 241 Oct 22 16:12 vhost-vsock
crw-rw-rw- 1 root root 10, 122 Oct 22 16:12 vmci
crw-rw-rw- 1 root root 10, 121 Oct 22 16:12 vsock
crw-rw-rw- 1 root root 1, 5 Oct 22 16:12 zero
crw-rw-rw- 1 root root 10, 249 Oct 22 16:12 zfs

```

ls -la /dev

```

reena@reena2904:~$ ls -la /dev
crw-rw-rw- 1 root root 10, 124 Oct 22 16:12 udmabuf
crw-rw-rw- 1 root root 10, 239 Oct 22 16:12 uhid
crw-rw-rw- 1 root root 10, 223 Oct 22 16:12 uinput
crw-rw-rw- 1 root root 1, 9 Oct 22 16:12 urandom
crw-rw-rw- 1 root root 10, 126 Oct 22 16:12 userfaultfd
crw-rw-rw- 1 root root 10, 240 Oct 22 16:12 userio
crw-rw-rw- 1 root tty 7, 0 Oct 22 16:12 vcs
crw-rw-rw- 1 root tty 7, 1 Oct 22 16:12 vcs1
crw-rw-rw- 1 root tty 7, 2 Oct 22 16:12 vcs2
crw-rw-rw- 1 root tty 7, 3 Oct 22 16:12 vcs3
crw-rw-rw- 1 root tty 7, 4 Oct 22 16:12 vcs4
crw-rw-rw- 1 root tty 7, 5 Oct 22 16:12 vcs5
crw-rw-rw- 1 root tty 7, 6 Oct 22 16:12 vcs6
crw-rw-rw- 1 root tty 7, 128 Oct 22 16:12 vcsa
crw-rw-rw- 1 root tty 7, 129 Oct 22 16:12 vcsa1
crw-rw-rw- 1 root tty 7, 130 Oct 22 16:12 vcsa2
crw-rw-rw- 1 root tty 7, 131 Oct 22 16:12 vcsa3
crw-rw-rw- 1 root tty 7, 132 Oct 22 16:12 vcsa4
crw-rw-rw- 1 root tty 7, 133 Oct 22 16:12 vcsa5
crw-rw-rw- 1 root tty 7, 134 Oct 22 16:12 vcsa6
crw-rw-rw- 1 root tty 7, 64 Oct 22 16:12 vcsu
crw-rw-rw- 1 root tty 7, 65 Oct 22 16:12 vcsu1
crw-rw-rw- 1 root tty 7, 66 Oct 22 16:12 vcsu2
crw-rw-rw- 1 root tty 7, 67 Oct 22 16:12 vcsu3
crw-rw-rw- 1 root tty 7, 68 Oct 22 16:12 vcsu4
crw-rw-rw- 1 root tty 7, 69 Oct 22 16:12 vcsu5
crw-rw-rw- 1 root tty 7, 70 Oct 22 16:12 vcsu6
drwxr-xr-x 2 root root 10, 60 Oct 22 16:12 vfiio
crw-rw-rw- 1 root root 10, 127 Oct 22 16:12 vga_arbiter
crw-rw-rw- 1 root root 10, 137 Oct 22 16:12 vhci
crw-rw-rw- 1 root kvm 10, 238 Oct 22 16:12 vhost-net
crw-rw-rw- 1 root kvm 10, 241 Oct 22 16:12 vhost-vsock
crw-rw-rw- 1 root root 10, 122 Oct 22 16:12 vmci
crw-rw-rw- 1 root root 10, 121 Oct 22 16:12 vsock
crw-rw-rw- 1 root root 1, 5 Oct 22 16:12 zero
crw-rw-rw- 1 root root 10, 249 Oct 22 16:12 zfs

```


ls -la /var

```
reenaqureshi@reena2904:~$ ls -la /var
total 56
drwxr-xr-x 13 root root 4096 Sep 26 10:17 .
drwxr-xr-x 23 root root 4096 Sep 26 10:09 ..
drwxr-xr-x  2 root root 4096 Sep 28 14:19 backups
drwxr-xr-x 16 root root 4096 Oct 22 16:25 cache
drwxrwsrwt  2 root root 4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root 4096 Oct 22 16:25 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 22 16:12 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 22 16:25 tmp
-rw-r--r--  1 root root 208 Aug  5 16:54 .updated
reenaqureshi@reena2904:~$
```

ls -la /tmp

```
reenaqureshi@reena2904:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 22 16:25 .
drwxr-xr-x 23 root root 4096 Sep 26 10:09 ..
drwxrwxrwt  2 root root 4096 Oct 22 16:12 .font-unix
drwxrwxrwt  2 root root 4096 Oct 22 16:12 .ICE-unix
drwx----- 2 root root 4096 Oct 22 16:12 snap-private-tmp
drwx----- 3 root root 4096 Oct 22 16:25 systemd-private-b1351901b78a4aff9ef31bbbe399f491-fwupd.service-20KIts
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-ModemManager.service-1xXnzH
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-polkit.service-n2S08R
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-systemd-logind.service-f65MX6
drwx----- 3 root root 4096 Oct 22 16:12 systemd-private-b1351901b78a4aff9ef31bbbe399f491-systemd-resolved.service-gNaKAD
drwx----- 3 root root 4096 Oct 22 16:25 systemd-private-b1351901b78a4aff9ef31bbbe399f491-systemd-timesyncd.service-WP0VCg
drwx----- 3 root root 4096 Oct 22 16:25 systemd-private-b1351901b78a4aff9ef31bbbe399f491-upower.service-Lss44X
drwx----- 2 root root 4096 Oct 22 16:12 vmware-root_738-2999591909
drwxrwxrwt  2 root root 4096 Oct 22 16:12 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 22 16:12 .XIM-unix
```

Display all hidden files in your home directory.

```
reenaqureshi@reena2904:~$ ls -la ~
total 32
drwxr-xr-x  4 reenaqureshi reenaqureshi 4096 Oct 22 16:19 .
drwxr-xr-x  3 root         root         4096 Sep 26 10:17 ..
-rw-----  1 reenaqureshi reenaqureshi   8 Sep 26 14:05 .bash_history
-rw-r--r--  1 reenaqureshi reenaqureshi 220 Mar 31 2024 .bash_logout
-rw-r--r--  1 reenaqureshi reenaqureshi 3771 Mar 31 2024 .bashrc
drwx-----  2 reenaqureshi reenaqureshi 4096 Sep 26 10:25 .cache
-rw-r--r--  1 reenaqureshi reenaqureshi 807 Mar 31 2024 .profile
drwx-----  2 reenaqureshi reenaqureshi 4096 Oct 22 16:16 .ssh
-rw-r--r--  1 reenaqureshi reenaqureshi   0 Oct 22 16:19 .sudo_as_admin_successful
reenaqureshi@reena2904:~$
```

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

```
reenaqareshi@reena2904:~$ cat ~/answers.md
/bin contains essential user binaries needed to boot and run the system
usr/bin contains most installed programs and applicaions
usr/local/bin stores user compiled or custom software not managed by system package manager
reenaqareshi@reena2904:~$
```

Evidence Handling & File Operations

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



The image shows three terminal windows. The first window, titled 'ReenaQureshi-052', shows the nano editor editing 'LAB 4 README'. The second window, also titled 'ReenaQureshi-052', shows the nano editor editing 'main.py *' with the content 'print ("hello lab4")'. The third window, titled 'ReenaQureshi-052', shows the nano editor editing '.hiddenfile' with the content 'secret data'.

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

```
reenaqareshi@reena2904:~/lab4/workspace/python_project$ cp README.md README.copy.md
reenaqareshi@reena2904:~/lab4/workspace/python_project$ cp README.copy.md README.dev.md
reenaqareshi@reena2904:~/lab4/workspace/python_project$ rm README.dev.md
reenaqareshi@reena2904:~/lab4/workspace/python_project$
```

Copy the entire workspace as an evidence backup folder.

```
naqareshi@reena2904:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
naqareshi@reena2904:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project cp -r ~/lab4/workspace/java_app_copy
target '/home/reenaqareshi/lab4/workspace/java_app_copy': No such file or directory
naqareshi@reena2904:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
```

Display your command history to document all actions performed.

```

reenaqureshi@reena2904:~/lab4/workspace/python_project$ history
 1 ip addr
 2 ssh reenaqureshi@192.168.76.129
 3 sudo systemctl status ssh
 4 ip a
 5 ls -la /
 6 ls -la /bin
 7 ls -la /sbin
 8 ls -la /usr
 9 ls -la /opt
10 ls -la /etc
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 cp README.copy.md README.dev.md
28 rm README.dev.md
29 cd ~/lab4/workspace/java_app
30 mkdir -p ~/lab4/workspace/java_app
31 cp -r ~/lab4/workspace/python_project cp -r ~/lab4/workspace/java_app_copy
32 ls -la ~/lab4/workspace
33 history

```

4. System Profiling and Process Monitoring

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

```

reenaqureshi@reena2904:~/lab4/workspace/python_project$ uname -a
Linux reena2904 6.8.0-71-generic #71-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 22 16:52:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
reenaqureshi@reena2904:~/lab4/workspace/python_project$

```

Display CPU, memory, and disk usage information

```

ReenaQureshi-052
vc_l1 and hyper visor : lahf_lm pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust smep arat md_clear flush_l1d arch_capabilities
bugs : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_unknown retbleed bhi
bogomips : 5183.18
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 : 58
model name : Intel(R) Core(TM) i5-3320M CPU @ 2.60GHz
stepping : 9
microcode : 0x21
cpu MHz : 2591.593
cache size : 3072 KB
physical id : 2
siblings : 1
core id : 0
cpu cores : 1
apicid : 2
initial apicid : 2
fpu : yes
fpu_exception : yes
cpuid level : 13
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx rdtscp lm constant
rfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 cx16 pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer
6c rdrand hypervisor lahf_lm pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust smep arat md_clear flush_l1d arch_capabilities
bugs : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_unknown retbleed bhi
bogomips : 5183.18
clflush_size : 64
cache_alignment : 64
address sizes : 45 bits physical, 48 bits virtual
power management:

reenaqureshi@reena2904:~/lab4/workspace/python_project$

```

```

reenaqureshi@reena2904:~/lab4/workspace/python_project$ free -h
              total        used        free      shared  buff/cache   available
Mem:          1.9Gi          376Mi        1.3Gi         1.2Mi        333Mi        1.5Gi
Swap:         1.9Gi           0B          1.9Gi

```

```

reenaqureshi@reena2904:~/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 9.8G  4.5G  4.9G  48% /
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

```

Display all active running processes to identify suspicious activity.

```

root      820  0.0  0.6 468952 13568 ?      Ssl 16:12  0:00 /usr/libexec/udisks2/udisksd
syslog    847  0.0  0.2 222508  5888 ?      Ssl 16:12  0:00 /usr/sbin/rsyslogd -n -iNONE
root      852  0.0  0.0  0 0 ?      S   16:12  0:00 [irq/16-vmwfx]
root      857  0.0  0.0  0 0 ?      I<  16:12  0:00 [kworker/R-rtm]
root      860  0.0  0.1  6824 2816 ?      Ss  16:12  0:00 /usr/sbin/cron -f -P
root      875  0.0  1.1 109632 22912 ?      Ssl 16:12  0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgr
root      881  0.0  0.6 392028 12928 ?      Ssl 16:12  0:00 /usr/sbin/ModemManager
root      983  0.0  0.2  6940 4736 tty1    Ss  16:12  0:00 /bin/login -p --
root     1405  0.0  0.0  0 0 ?      S   16:13  0:00 [psimon]
reenaqua+ 1407  0.0  0.5 20088 11136 ?      Ss  16:13  0:00 /usr/lib/systemd/systemd --user
reenaqua+ 1408  0.0  0.1 21152 3648 ?      S   16:13  0:00 (sd-pam)
reenaqua+ 1417  0.0  0.2  8656 5248 tty1    S   16:13  0:00 -bash
root     1464  0.0  0.0  0 0 ?      I<  16:13  0:00 [kworker/R-tls-s]
root     1470  0.0  0.4 12020 7936 ?      Ss  16:14  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root     1495  0.0  0.0  0 0 ?      I   16:20  0:00 [kworker/u257:0-events_power_efficient]
root     1568  0.0  0.0  0 0 ?      I<  16:23  0:00 [kworker/0:0H]
root     1572  0.0  0.5 14964 10496 ?      Ss  16:25  0:00 sshd: reenaqureshi [priv]
root     1580  0.0  2.1 595032 43244 ?      Ssl 16:25  0:03 /usr/libexec/fwupd/fwupd
root     1587  0.0  0.4 313996 8960 ?      Ssl 16:25  0:00 /usr/libexec/upowerd
root     1628  0.0  0.1 81380 2952 ?      Ss  16:25  0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket -
reenaqua+ 1682  0.0  0.3 14964 6980 ?      S   16:25  0:00 sshd: reenaqureshi@pts/0
reenaqua+ 1683  0.0  0.2  8648 5504 pts/0   Ss+  16:25  0:00 -bash
root     1698  0.0  0.0  0 0 ?      I   16:27  0:00 [kworker/u257:1-events_power_efficient]
root     1865  0.0  0.0  0 0 ?      I   16:55  0:00 [kworker/u258:4-events_power_efficient]
root     1885  0.0  0.0  0 0 ?      I   17:05  0:15 [kworker/1:2-mpt_poll_0]
root     1894  0.0  0.0  0 0 ?      I   17:13  0:00 [kworker/u258:0-events_unbound]
root     1900  0.6  0.0  0 0 ?      I   17:16  0:07 [kworker/0:0-events]
root     1907  2.2  0.0  0 0 ?      I   17:20  0:21 [kworker/0:1-events]
root     1909  0.6  0.0  0 0 ?      I   17:22  0:05 [kworker/1:1-events]
root     1916  0.0  0.0  0 0 ?      I   17:25  0:00 [kworker/u258:2-events_power_efficient]
root     1918  0.0  0.0  0 0 ?      I   17:26  0:00 [kworker/u257:2-events_unbound]
reenaqua+ 1940  300  0.2 10884 4480 tty1    R+  17:36  0:00 ps aux
reenaqureshi@reena2904:~/lab4/workspace/python_project$

```

User Account Audit & Privilege Escalation Simulation

Create a new test user named lab4user.

```

reenaqureshi@reena2904:~$ sudo adduser lab4user
[sudo] password for reenaqureshi:
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 []: lab4user
  Room Number []: 100
  Work Phone []: 0300567543
  Home Phone []: 05123445
  Other []: 456
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
reenaqureshi@reena2904:~$

```

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

```

reenaqureshi@reena2904:~$ getent passwd lab4user
lab4user:x:1001:1001:lab4user,100,0300567543,05123445,456:/home/lab4user:/bin/bash
reenaqureshi@reena2904:~$

```

Log in as lab4user and confirm successful login.

```

reenaqureshi@reena2904:~$ su - lab4user
Password:
lab4user@reena2904:~$

```

Attempt to run an administrative command as lab4user (expect permission

```
lab4user@reena2904:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@reena2904:~$
```

Switch back to your main analyst account.

```
ReenaQureshi-052 x
reenaqaureshi@reena2904:~$
```

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

```
ReenaQureshi-052 x
reenaqaureshi@reena2904:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
reenaqaureshi@reena2904:~$ _
```