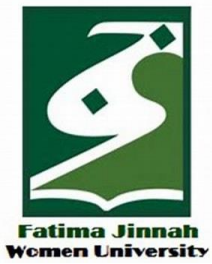
CLOUD COMPUTING

LAB 04



Submitted To:

Engr. Shoaib

Submitted By:

Komal Kashif

BSE V-A

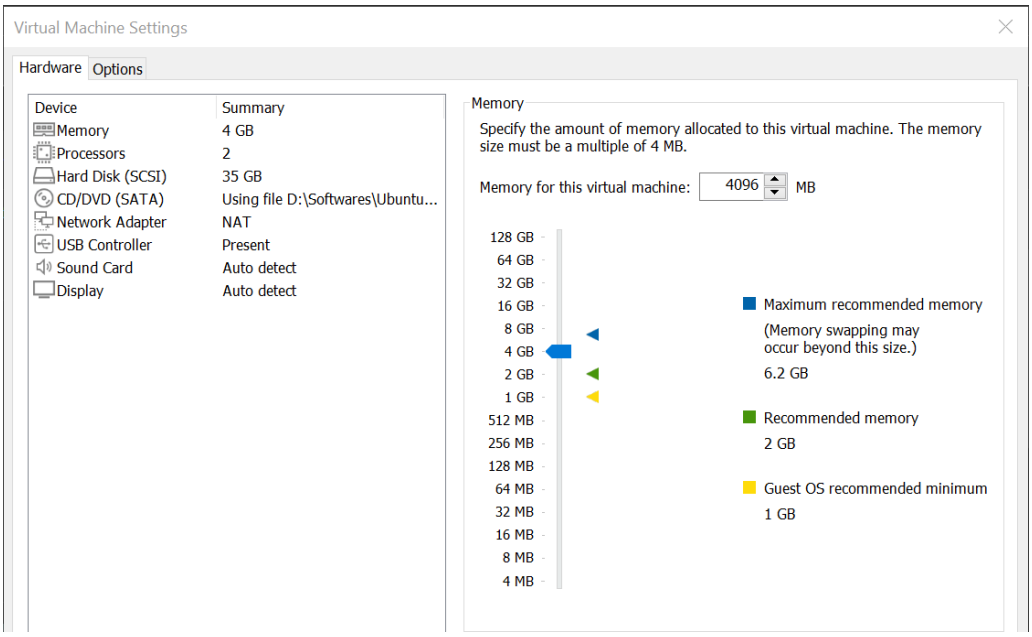
2023-BSE-031

Task 1 – Verify VM resources in VMware

Confirm the VM resources that were allocated in Lab 1.

Steps

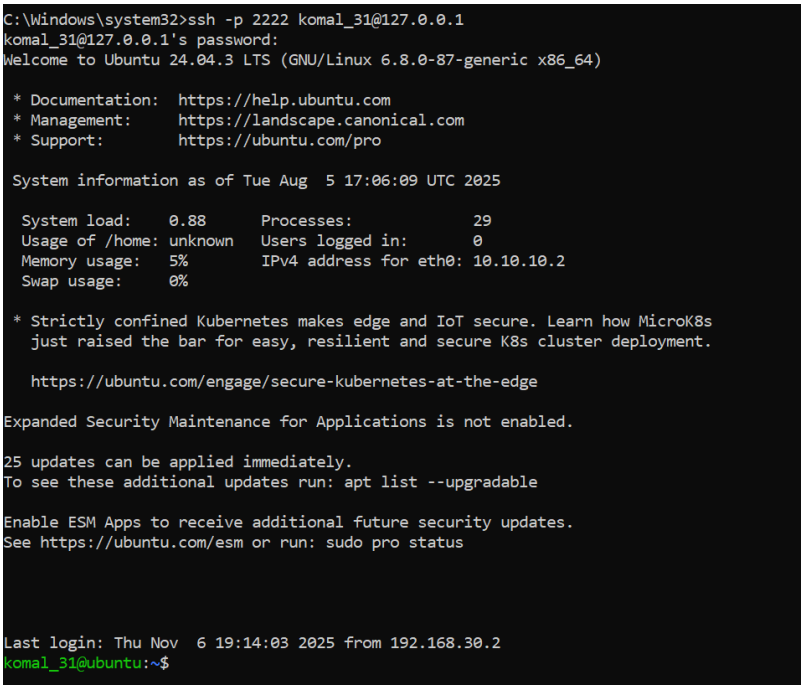
1. Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.
2. Inspect VM settings and note the following (no commands required for GUI): VM name, RAM, CPU, disk, and network adapter type.
3. Take a screenshot of the VM settings window showing RAM, CPU, disk and networking.



Task 2 – Start VM and log in

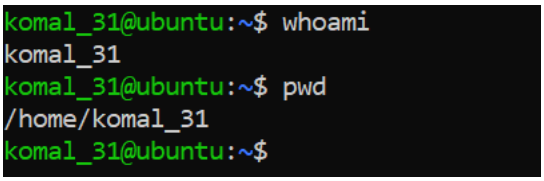
Steps

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



Since my vm couldn't connect to host through ssh username@<ip>, I did it through port forwarding.

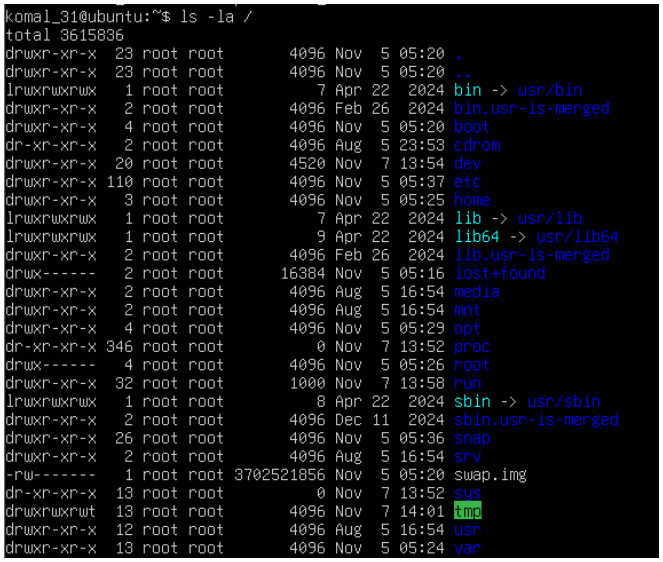
3. After logging in, run both commands and capture them together in a single screenshot:
   whoami
   pwd



Task 3 – Filesystem exploration — root tree and dotfiles

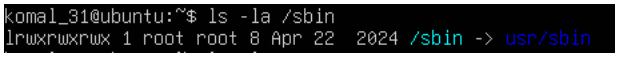
Steps (run inside VM terminal)

1. List root directory contents:

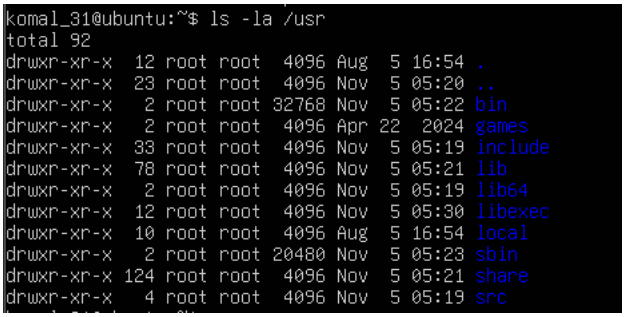


2. Inspect these directories:
   - ls -la /bin

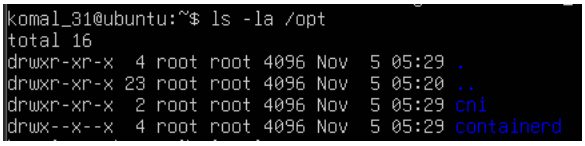
   - ls -la /sbin



   - ls -la /usr



   - ls -la /opt



- ls -la /etc

```
komal_31@ubuntu:~$ ls -la /etc
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 Nov  5 05:20 thermald
-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 Nov  5 05:22 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 Nov  5 05:26 update-motd.d
drwxr-xr-x   2 root root       4096 Aug  5 17:14 update-notifier
drwxr-xr-x   2 root root       4096 Nov  5 05:20 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 Nov  5 05:22 vim
drwxr-xr-x   4 root root       4096 Nov  5 05:22 vmware-tools
lrwxrwxrwx   1 root root         23 Feb 26  2024 vtrgb -> /etc/alternatives/vtrgb
-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
```

- ls -la /dev

```
komal_31@ubuntu:~$ ls -la /dev
crw-rw----   1 root     tty       7,   5 Nov  7 13:53 vcs5
crw-rw----   1 root     tty       7,   6 Nov  7 13:53 vcs6
crw-rw----   1 root     tty       7, 128 Nov  7 13:53 vcsa
crw-rw----   1 root     tty       7, 129 Nov  7 13:53 vcsa1
crw-rw----   1 root     tty       7, 130 Nov  7 13:53 vcsa2
crw-rw----   1 root     tty       7, 131 Nov  7 13:53 vcsa3
crw-rw----   1 root     tty       7, 132 Nov  7 13:53 vcsa4
crw-rw----   1 root     tty       7, 133 Nov  7 13:53 vcsa5
crw-rw----   1 root     tty       7, 134 Nov  7 13:53 vcsa6
crw-rw----   1 root     tty       7,  64 Nov  7 13:53 vcsu
crw-rw----   1 root     tty       7,  65 Nov  7 13:53 vcsu1
crw-rw----   1 root     tty       7,  66 Nov  7 13:53 vcsu2
crw-rw----   1 root     tty       7,  67 Nov  7 13:53 vcsu3
crw-rw----   1 root     tty       7,  68 Nov  7 13:53 vcsu4
crw-rw----   1 root     tty       7,  69 Nov  7 13:53 vcsu5
crw-rw----   1 root     tty       7,  70 Nov  7 13:53 vcsu6
drwxr-xr-x   2 root     root          60 Nov  7 13:52 vfio
crw-------   1 root     root     10, 127 Nov  7 13:53 vga_arbiter
crw-------   1 root     root     10, 137 Nov  7 13:52 vhci
crw-rw----   1 root     kvm      10, 238 Nov  7 13:52 vhost-net
crw-rw----   1 root     kvm      10, 241 Nov  7 13:52 vhost-vsock
crw-------   1 root     root     10, 122 Nov  7 13:53 vmci
crw-rw-rw-   1 root     root     10, 121 Nov  7 13:53 vsock
crw-rw-rw-   1 root     root      1,   5 Nov  7 13:53 zero
crw-------   1 root     root     10, 249 Nov  7 13:52 zfs
```

- ls -la /var

```
komal_31@ubuntu:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Nov  5 05:24 .
drwxr-xr-x 23 root root   4096 Nov  5 05:20 ..
drwxr-xr-x  2 root root   4096 Nov  6 18:46 backups
drwxr-xr-x 16 root root   4096 Nov  5 06:21 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 46 root root   4096 Nov  5 06:13 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 12 root syslog 4096 Nov  7 13:54 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 25 root root   4096 Nov  5 05:36 snap
drwxr-xr-x  4 root root   4096 Aug  5 17:14 spool
drwxrwxrwt  7 root root   4096 Nov  7 13:53 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
```

- ls -la /tmp

```
komal_31@ubuntu:~$ ls -la /tmp
total 52
drwxrwxrwt 13 root root 4096 Nov  7 14:39 .
drwxr-xr-x 23 root root 4096 Nov  5 05:20 ..
drwxrwxrwt  2 root root 4096 Nov  7 13:52 .font-unix
drwxrwxrwt  2 root root 4096 Nov  7 13:52 .ICE-unix
drwx------ 11 root root 4096 Nov  7 13:54 snap-private-tmp
drwx------  3 root root 4096 Nov  7 13:54 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-ModemManager.service-7u5DFA
drwx------  3 root root 4096 Nov  7 13:54 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-polkit.service-qu5c7L
drwx------  3 root root 4096 Nov  7 13:54 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-systemd-logind.service-2Ba2yh
drwx------  3 root root 4096 Nov  7 13:52 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-systemd-resolved.service-2n0NKA
drwx------  3 root root 4096 Nov  7 13:52 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-systemd-timesyncd.service-Ok751M
drwx------  2 root root 4096 Nov  7 13:53 vmware-root_845-4021653450
drwxrwxrwt  2 root root 4096 Nov  7 13:52 .X11-unix
drwxrwxrwt  2 root root 4096 Nov  7 13:52 .XIM-unix
```

3. List your home directory and show hidden (dot) files:
   ls -la ~

```
komal_31@ubuntu:~$ ls -la ~
total 32
drwxr-x--- 4 komal_31 komal_31 4096 Nov  5 06:56 .
drwxr-xr-x 3 root     root     4096 Nov  5 05:25 ..
-rw------- 1 komal_31 komal_31  180 Nov  7 14:22 .bash_history
-rw-r--r-- 1 komal_31 komal_31  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 komal_31 komal_31 3771 Mar 31  2024 .bashrc
drwx------ 2 komal_31 komal_31 4096 Nov  5 06:21 .cache
-rw-r--r-- 1 komal_31 komal_31  807 Mar 31  2024 .profile
drwx------ 2 komal_31 komal_31 4096 Nov  5 05:37 .ssh
-rw-r--r-- 1 komal_31 komal_31    0 Nov  5 06:56 .sudo_as_admin_successful
```

4. Write a short paragraph (3–5 sentences) that explains the difference between /bin, /usr/bin and /usr/local/bin. Open your editor:
   nano ~/answers.md

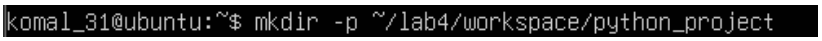
- Type the paragraph in the editor, save and exit.
- After saving, open the editor display (or show the file) and capture a screenshot of the paragraph.

```
komal_31@ubuntu:~$ nano ~ /answers.md
komal_31@ubuntu:~$ cat ~/answers.md
In Linux, /bin contains essential system commands needed for booting and repair,
 /usr/bin holds standard user programs installed by the system,
and /usr/local/bin stores custom software installed manually by the user or administrator.
```

Task 4 – Essential CLI tasks — navigation and file operations

Steps (inside VM terminal)

1. Create a workspace and navigate:
   - mkdir -p ~/lab4/workspace/python_project

   - cd ~/lab4/workspace/python_project

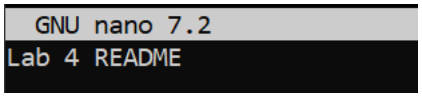
     

   - pwd

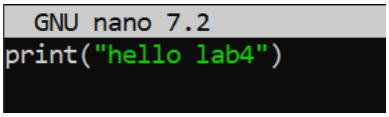
2. Create files using an editor (open each editor session and save a screenshot showing content):
   - nano README.md

     Inside nano add: Lab 4 README and save.

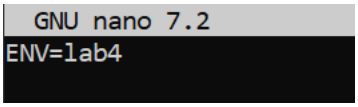
   - nano main.py

     Inside nano add: print("hello lab4") and save.

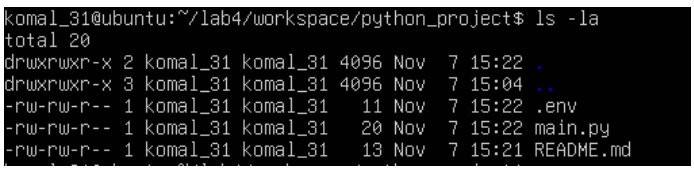
   - nano .env

     Inside nano add: ENV=lab4 and save.

3. List files and capture:

   ls -la

4. Copy, move and remove:

   - cp README.md README.copy.md

```
komal_31@ubuntu:~/lab4/workspace/python_project$ cp README.md README.md.copy.md
komal_31@ubuntu:~/lab4/workspace/python_project$
```

   - mv README.copy.md README.dev.md

```
komal_31@ubuntu:~/lab4/workspace/python_project$ mv README.md.copy.md README.dev.md
komal_31@ubuntu:~/lab4/workspace/python_project$
```

   - rm README.dev.md

```
komal_31@ubuntu:~/lab4/workspace/python_project$ rm README.dev.md
komal_31@ubuntu:~/lab4/workspace/python_project$
```

   - mkdir -p ~/lab4/workspace/java_app

```
komal_31@ubuntu:~/lab4/workspace/python_project$ mkdir -p ~/lab/workspace/java_app
komal_31@ubuntu:~/lab4/workspace/python_project$
```

   - cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy

```
komal_31@ubuntu:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
komal_31@ubuntu:~/lab4/workspace/python_project$
```

   - ls -la ~/lab4/workspace

```
komal_31@ubuntu:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 16
drwxrwxr-x 4 komal_31 komal_31 4096 Nov  7 15:32 .
drwxrwxr-x 3 komal_31 komal_31 4096 Nov  7 15:04 ..
drwxrwxr-x 2 komal_31 komal_31 4096 Nov  7 15:32 java_app_copy
drwxrwxr-x 2 komal_31 komal_31 4096 Nov  7 15:27 python_project
```

5. Use command history and tab completion:

   - history

```
komal_31@ubuntu:~/lab4/workspace/python_project$ history
    1  ip a
    2  apt list --upgradeable
    3  sudo apt update
    4  sudo apt --fix-broken install
    5  sudo systemctl restart NetworkManager
    6  ls /etc/netplan
    7  cat /etc/netplan/50-cloud-init.yaml
    8  ip a
    9  ls -la /
   10  ls -la /bin
   11  ls -la /sbin
   12  ls -la /usr
   13  ls -la /opt
   14  ls -la /etc
   15  ls -la /opt
   16  ls -la /dev
   17  ls -la /var
   18  ls -la /tmp
   19  ls -la~
   20  ls -la ~
   21  nano~/answers.md
   22  nano ~ /answers.md
   23  cat ~/answers.md
   24  mkdir -p ~/lab4/workspace/python_project
   25  cd  ~/lab4/workspace/python_project
   26  pwd
   27  nano README.md
   28  ls -la
   29  nano README.md
   30  cat README.md
   31  ls -la
   32  cp README.md README.md.copy.md
   33  mv README.md.copy.md README.dev.md
   34  rm README.dev.md
   35  mkdir -p ~/lab/workspace/java_app
   36  cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
   37  ls -la ~/lab4/workspace
   38  history
```

- Demonstrate tab completion (type partial name and press Tab) and capture that action as tab_completion.png.

```
komal_31@ubuntu:~/lab4/workspace/python_project$ cat main.py
print('hello lab4')
```

Task 5 – System info, resources & processes

Steps (inside VM terminal)

1. Kernel and OS:

   uname -a

```
komal_31@ubuntu:~$ uname -a
Linux ubuntu 6.8.0-87-generic #88-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 09:28:41 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

2. CPU (ensure model name visible):

   cat /proc/cpuinfo

```
processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 78
model name      : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
stepping        : 3
microcode       : 0xf0
cpu MHz         : 2495.999
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     : 22
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 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 popcnt tsc_deadline_time
r aes 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 clflus
hopt xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_l1d arch_capabilities
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_stale_data retbleed gds bhi
bogomips        : 4991.99
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:
```

3. Memory:

   free -h

```
komal_31@ubuntu:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       2.3Gi       254Mi       3.7Mi       1.5Gi       1.5Gi
Swap:          3.4Gi       218Mi       3.2Gi
```

4. Disk:

   df -h

```
komal_31@ubuntu:~$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              387M  2.0M  385M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   17G   12G  3.6G  77% /
tmpfs                              1.9G     0  1.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          2.0G  100M  1.7G   6% /boot
tmpfs                              387M   12K  387M   1% /run/user/1000
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/ac47d52793c3bac5cd51794010
63ad6274340be397b0b37f751daf0ad6440168/shm
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/610018f4ec97749b91d025c56f
245fdb56ab989cc7bf4c946b20e22da8214030/shm
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/bf81875e88ef6cdd41ac7ef3f4
55e534ce316858f5ae8982cd4ba0898924fd92/shm
```

5. View OS release information:

   cat /etc/os-release

```
komal_31@ubuntu:~$ 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
```

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

   ps aux

Some of the running processes are:

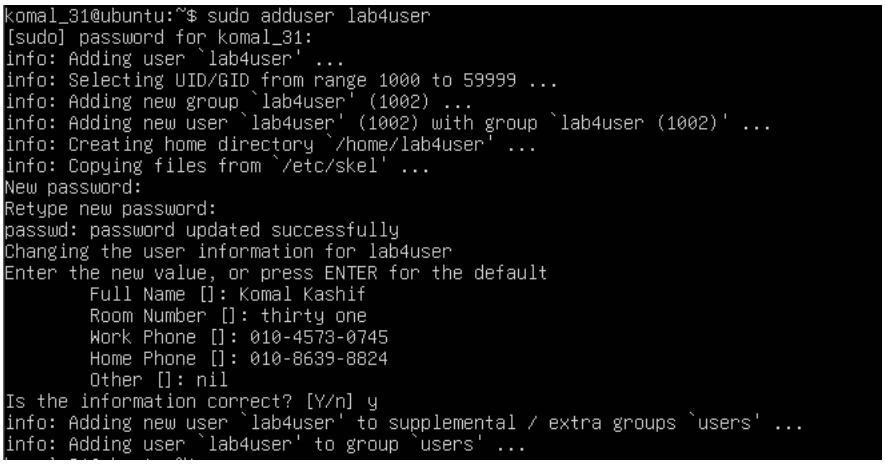
```
komal_31  409310  0.0  0.1  15092  6848 ?        S    14:50   0:02 sshd: komal_31@pts/0
komal_31  409315  0.0  0.1   8648  5632 pts/0    Ss+  14:50   0:00 -bash
root      519537  0.0  0.0      0     0 ?        I    15:03   0:00 [kworker/u258:0-events_power_efficient]
root      525589  0.0  0.0      0     0 ?        I    15:04   0:00 [kworker/u257:1-flush-252:0]
root      546719  0.0  0.0      0     0 ?        I<   15:06   0:00 [kworker/1:2H]
root      615144  0.0  0.0      0     0 ?        I    15:13   0:00 [kworker/u257:2-events_power_efficient]
root      817021  0.0  0.0      0     0 ?        I    15:34   0:00 [kworker/u258:3-events_power_efficient]
root      833017  0.0  0.0      0     0 ?        I<   15:35   0:00 [kworker/0:0H]
root      842033  0.0  0.0      0     0 ?        I<   15:36   0:00 [kworker/R-tls-s]
root      917261  0.0  0.0      0     0 ?        I    15:44   0:00 [kworker/u258:4-events_unbound]
root      951618  0.0  0.0      0     0 ?        I    15:47   0:00 [kworker/u257:0-events_freezable_power_]
root      953474  0.0  0.0      0     0 ?        I    15:47   0:01 [kworker/1:1-events]
root     1005177  0.0  0.0      0     0 ?        I    15:52   0:00 [kworker/1:2-cgroup_destroy]
root     1009283  0.0  0.0      0     0 ?        I    15:53   0:00 [kworker/u257:3-events_power_efficient]
root     1014336  0.0  0.0      0     0 ?        I<   15:53   0:00 [kworker/0:1H-kblockd]
root     1020623  0.0  0.0      0     0 ?        I    15:54   0:00 [kworker/0:1-events]
root     1076155  0.1  0.0      0     0 ?        I    16:00   0:00 [kworker/0:0-cgroup_destroy]
root     1095362  0.0  0.0      0     0 ?        I    16:02   0:00 [kworker/u258:1-events_unbound]
root     1109361  0.1  0.0      0     0 ?        I    16:03   0:00 [kworker/1:0-events]
root     1112890  0.0  0.0   4556  1536 ?        S    16:04   0:00 sleep 5m
root     1128470  0.0  0.0      0     0 ?        I    16:06   0:00 [kworker/0:2-cgroup_destroy]
root     1143544  8.3  0.0   9824  2560 ?        Ss   16:07   0:00 /bin/bash /snap/wekan/1999/bin/wekan-control
root     1144197  0.0  0.0   5948  1792 ?        S    16:07   0:00 sleep 5
root     1144249  0.0  0.0   4556  1536 ?        S    16:07   0:00 sleep 1
root     1144490  0.0  0.0   4556  1536 ?        S    16:07   0:00 sleep 1
root     1144607  121  1.0 923332 41452 ?        Rl   16:07   0:00 /snap/wekan/1999/bin/node --stack-size=65500 main.js
komal_31 1144616  200  0.1  12312  5120 tty1     R+   16:07   0:00 ps aux
```

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

Steps (inside VM terminal)

1. Create a new user named lab4user:

   sudo adduser lab4user



2. Verify the user entry:

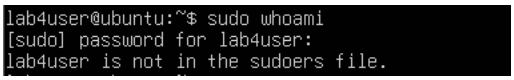
   getent passwd lab4user

3. Switch to the new user to verify login:

   su - lab4user

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



5. Return to the original user:

   exit

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

   sudo deluser --remove-home lab4user

```
komal_31@ubuntu:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
komal_31@ubuntu:~$ _
```

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

   - 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/komal_
#!/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

```
komal_31@ubuntu:~$ chmod +x ~/lab4/workspace/run-demo.sh
komal_31@ubuntu:~$ _
```

3. Run the script as your regular user:

   ~/lab4/workspace/run-demo.sh

```
komal_31@ubuntu:~$ ~/lab4/workspace/run-demo.sh
Lab 4 demo: current user is komal_31
Current time: Fri Nov  7 04:51:26 PM UTC 2025
 16:51:26 up  2:58,  2 users,  load average: 3.70, 3.72, 3.19
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       2.2Gi       353Mi       3.3Mi       1.5Gi       1.6Gi
Swap:          3.4Gi       220Mi       3.2Gi
```

4. Optionally run it with sudo:

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

```
komal_31@ubuntu:~$ sudo ~/lab4/workspace/run-demo.sh
[sudo] password for komal_31:
Lab 4 demo: current user is root
Current time: Fri Nov  7 04:53:03 PM UTC 2025
 16:53:03 up  3:00,  2 users,  load average: 4.20, 3.98, 3.34
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       2.2Gi       309Mi       3.3Mi       1.5Gi       1.5Gi
Swap:          3.4Gi       220Mi       3.2Gi
```

EXAM EVALUATION QUESTIONS

1. Remote Access Verification (Cyber Login Check)

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

Steps:

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

```
C:\Windows\system32>ssh -p 2222 komal_31@127.0.0.1
komal_31@127.0.0.1's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

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

 System information as of Tue Aug  5 17:06:09 UTC 2025

  System load:    0.88      Processes:             29
  Usage of /home: unknown   Users logged in:       0
  Memory usage:   5%        IPv4 address for eth0: 10.10.10.2
  Swap usage:     0%

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

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

Expanded Security Maintenance for Applications is not enabled.

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

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



Last login: Thu Nov  6 19:14:03 2025 from 192.168.30.2
komal_31@ubuntu:~$
```

2. Verify your current user and home directory path.

```
komal_31@ubuntu:~$ whoami
komal_31
komal_31@ubuntu:~$ pwd
/home/komal_31
komal_31@ubuntu:~$
```

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

```
komal_31@ubuntu:~$ hostname
ubuntu
```

2. Filesystem Inspection for Forensic Evidence

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

Steps:

1. Display the contents of the root directory.catc

```
komal_31@ubuntu:~$ ls -la
total 60
drwxr-x--- 7 komal_31 komal_31 4096 Nov  7 15:29 .
drwxr-xr-x 3 root     root     4096 Nov  7 16:26 ..
-rw-rw-r-- 1 komal_31 komal_31  238 Nov  7 14:54 answers.md
-rw------- 1 komal_31 komal_31  180 Nov  7 14:22 .bash_history
-rw-r--r-- 1 komal_31 komal_31  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 komal_31 komal_31 3771 Mar 31  2024 .bashrc
drwx------ 2 komal_31 komal_31 4096 Nov  5 06:21 .cache
-rw-rw-r-- 1 komal_31 komal_31   11 Nov  7 15:14 .env
drwxrwxr-x 3 komal_31 komal_31 4096 Nov  7 15:29 lab
drwxrwxr-x 3 komal_31 komal_31 4096 Nov  7 15:04 lab4
drwxrwxr-x 3 komal_31 komal_31 4096 Nov  7 14:44 .local
-rw-rw-r-- 1 komal_31 komal_31   22 Nov  7 15:13 main.py
-rw-r--r-- 1 komal_31 komal_31  807 Mar 31  2024 .profile
-rw-rw-r-- 1 komal_31 komal_31   14 Nov  7 15:11 README.md
drwx------ 2 komal_31 komal_31 4096 Nov  5 05:37 .ssh
-rw-r--r-- 1 komal_31 komal_31    0 Nov  5 06:56 .sudo_as_admin_successful
```

2. Display the OS version and release information.

```
komal_31@ubuntu:~$ 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
```

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

   For this step, save all the listings in one file directory_listings.txt using:

   ls -l /bin >> ~/directory_listings.txt

   And same for all the files.

   Then, run

   cat ~/directory_listings.txt

```
komal_31@ubuntu:~$ cat ~/directory_listings.txt
total 44
drwxr-xr-x  2 root root   4096 Nov  6 18:46 backups
drwxr-xr-x 16 root root   4096 Nov  5 06:21 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 46 root root   4096 Nov  5 06:13 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 12 root syslog 4096 Nov  7 13:54 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 25 root root   4096 Nov  5 05:36 snap
drwxr-xr-x  4 root root   4096 Aug  5 17:14 spool
drwxrwxrwt  9 root root   4096 Nov  7 14:59 tmp
total 36
drwx------ 11 root root 4096 Nov  7 13:54 snap-private-tmp
drwx------  3 root root 4096 Nov  7 14:43 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-fwupd.service-n2s3to
drwx------  3 root root 4096 Nov  7 13:54 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-ModemManager.service-7u5DFA
drwx------  3 root root 4096 Nov  7 13:54 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-polkit.service-qu5c7L
drwx------  3 root root 4096 Nov  7 13:54 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-systemd-logind.service-2Ba2yh
drwx------  3 root root 4096 Nov  7 13:52 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-systemd-resolved.service-2n0NKA
drwx------  3 root root 4096 Nov  7 13:52 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-systemd-timesyncd.service-Ok751M
drwx------  3 root root 4096 Nov  7 14:43 systemd-private-060b5bd33e7440518e1f53ff5c3d28ed-upower.service-24Td4u
drwx------  2 root root 4096 Nov  7 13:53 vmware-root_845-4021653450
```

4. Display all hidden files in your home directory.

```
komal_31@ubuntu:~$ ls -la
total 88
drwxr-x--- 7 komal_31 komal_31  4096 Nov  7 17:11 .
drwxr-xr-x 3 root     root      4096 Nov  7 16:26 ..
-rw-rw-r-- 1 komal_31 komal_31   238 Nov  7 14:54 answers.md
-rw------- 1 komal_31 komal_31   180 Nov  7 14:22 .bash_history
-rw-r--r-- 1 komal_31 komal_31   220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 komal_31 komal_31  3771 Mar 31  2024 .bashrc
drwx------ 2 komal_31 komal_31  4096 Nov  5 06:21 .cache
-rw-rw-r-- 1 komal_31 komal_31 27301 Nov  7 17:13 directory_listings.txt
-rw-rw-r-- 1 komal_31 komal_31    11 Nov  7 15:14 .env
drwxrwxr-x 3 komal_31 komal_31  4096 Nov  7 15:29 lab
drwxrwxr-x 3 komal_31 komal_31  4096 Nov  7 15:04 lab4
drwxrwxr-x 3 komal_31 komal_31  4096 Nov  7 14:44 .local
-rw-rw-r-- 1 komal_31 komal_31    22 Nov  7 15:13 main.py
-rw-r--r-- 1 komal_31 komal_31   807 Mar 31  2024 .profile
-rw-rw-r-- 1 komal_31 komal_31    14 Nov  7 15:11 README.md
drwx------ 2 komal_31 komal_31  4096 Nov  5 05:37 .ssh
-rw-r--r-- 1 komal_31 komal_31     0 Nov  5 06:56 .sudo_as_admin_successful
```

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

   For this step, create a file report.md in /lab4/workspace. Add summary to report.md by:

   nano report.md

   Then, run

   cat report.md

```
komal_31@ubuntu:~$ cd ~/lab4/workspace
komal_31@ubuntu:~/lab4/workspace$ cat report.md
/bin - Contains essential user command binaries needed for basic system operation.
/sbin - Holds system administration binaries used mainly by the root user.
/usr - Stores user programs, libraries, and documentation installed by the system.
/opt - Contains optional or third-party software packages.
/etc - Houses system-wide configuration files.
/dev - Contains device files that represent hardware and virtual devices.
/var - Stores variable data like logs, caches, and spool files.
/tmp - Used for temporary files created by users and application.
```

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.

```
komal_31@ubuntu:~$ mkdir -p ~/sandbox/analysis/samples
komal_31@ubuntu:~$
```

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

```
komal_31@ubuntu:~$ mkdir -p ~/sandbox/analysis/samples
komal_31@ubuntu:~$ cd ~/sandbox/analysis/samples
komal_31@ubuntu:~/sandbox/analysis/samples$ touch file1.txt file2.txt .hiddenfile.txt
komal_31@ubuntu:~/sandbox/analysis/samples$ ls -la
total 8
drwxrwxr-x 2 komal_31 komal_31 4096 Nov  7 17:46 .
drwxrwxr-x 3 komal_31 komal_31 4096 Nov  7 17:44 ..
-rw-rw-r-- 1 komal_31 komal_31    0 Nov  7 17:46 file1.txt
-rw-rw-r-- 1 komal_31 komal_31    0 Nov  7 17:46 file2.txt
-rw-rw-r-- 1 komal_31 komal_31    0 Nov  7 17:46 .hiddenfile.txt
```

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

```
komal_31@ubuntu:~/sandbox/analysis/samples$ cp file1.txt file1_backup.txt
komal_31@ubuntu:~/sandbox/analysis/samples$ mv file1_backup.txt verified_backup.txt
komal_31@ubuntu:~/sandbox/analysis/samples$ ls
file1.txt  file2.txt  verified_backup.txt
komal_31@ubuntu:~/sandbox/analysis/samples$ rm verified_backup.txt
komal_31@ubuntu:~/sandbox/analysis/samples$ ls
file1.txt  file2.txt
```

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

```
komal_31@ubuntu:~/sandbox/analysis/samples$ cd ~
komal_31@ubuntu:~$ cp -r sandbox sandbox_backup
komal_31@ubuntu:~$ ls -R | grep sandbox
sandbox
sandbox_backup
./sandbox:
./sandbox/analysis:
./sandbox/analysis/samples:
./sandbox_backup:
./sandbox_backup/analysis:
./sandbox_backup/analysis/samples:
```

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

```
komal_31@ubuntu:~$ history | tail -n 20
   64  ls -la
   65  cd ~/lab4/workspace
   66  cat report.md
   67  pwd
   68  cd
   69  mkdir -p ~/sandbox/analysis/samples
   70  cd ~/sandbox/analysis/samples
   71  touch file1.txt file2.txt .hiddenfile.txt
   72  ls -la
   73  cp file1.txt file1_backup.txt
   74  mv file1_backuup.txt verified_backup.txt
   75  mv file1_backup.txt verified_backup.txt
   76  ls
   77  rm verified_backup.txt
   78  ls
   79  cd ~
   80  cp -r sandbox sandbox_backup
   81  ls -R | grep sandbox
   82  history | -n 20
   83  history | tail -n 20
```

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

```
komal_31@ubuntu:~$ cd sand
-bash: cd: sand: No such file or directory
```

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.

```
komal_31@ubuntu:~$ 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
komal_31@ubuntu:~$ uname -r
6.8.0-87-generic
```

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

```
                        tant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2a
                        pic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase t
                        sc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_l1d arch_capabilit
                        ies
Virtualization features:
  Hypervisor vendor:     VMware
  Virtualization type:   full
Caches (sum of all):
  L1d:                   64 KiB (2 instances)
  L1i:                   64 KiB (2 instances)
  L2:                    512 KiB (2 instances)
  L3:                    6 MiB (2 instances)
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0,1
Vulnerabilities:
  Gather data sampling:  Unknown: Dependent on hypervisor status
  Itlb multihit:         KVM: Mitigation: VMX unsupported
  L1tf:                  Mitigation; PTE Inversion
  Mds:                   Mitigation; Clear CPU buffers; SMT Host state unknown
  Meltdown:              Mitigation; PTI
  Mmio stale data:       Mitigation; Clear CPU buffers; SMT Host state unknown
  Reg file data sampling: Not affected
  Retbleed:              Mitigation; IBRS
  Spec rstack overflow:  Not affected
  Spec store bypass:     Mitigation; Speculative Store Bypass disabled via prctl
  Spectre v1:            Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:            Mitigation; IBRS; IBPB conditional; STIBP disabled; RSB filling; PBRSB-eIBRS Not affected; BHI SW loop, KVM SW loop
  Srbds:                 Unknown: Dependent on hypervisor status
  Tsx async abort:       Not affected
  Vmscape:               Not affected
komal_31@ubuntu:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       2.2Gi       292Mi       2.2Mi       1.5Gi       1.5Gi
Swap:          3.4Gi       224Mi       3.2Gi
komal_31@ubuntu:~$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              387M  2.0M  385M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   17G   12G  3.5G  78% /
tmpfs                              1.9G     0  1.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          2.0G  100M  1.7G   6% /boot
tmpfs                              387M   12K  387M   1% /run/user/1000
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/ac47d52793c3bac5cd51794010
63ad6274340be397b0b37f751daf0ad6440168/shm
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/610018f4ec97749b91d025c56f
245fdb56ab989cc7bf4c946b20e22da8214030/shm
shm                                 64M     0   64M   0% /var/snap/microk8s/common/run/containerd/io.containerd.grpc.v1.cri/sandboxes/bf81875e88ef6cdd41ac7ef3f4
55e534ce316858f5ae8982cd4ba0898924fd92/shm
```

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

```
root     1879699  0.1  0.0      0     0 ?        I<   17:41   0:02 [kworker/0:2H-kblockd]
root     1915131  0.2  0.0      0     0 ?        I    17:46   0:02 [kworker/0:0-mpt_poll_0]
root     1920035  0.0  0.0      0     0 ?        I    17:47   0:00 [kworker/u257:4-events_power_efficient]
root     1924226  0.0  0.0      0     0 ?        I    17:48   0:00 [kworker/1:1-cgroup_destroy]
root     1974613  0.0  0.0      0     0 ?        I    17:55   0:00 [kworker/1:0-events]
root     1981490  0.0  0.0      0     0 ?        I    17:56   0:00 [kworker/u257:0-flush-252:0]
root     1983632  0.0  0.0      0     0 ?        I    17:56   0:00 [kworker/u257:3-events_power_efficient]
root     1994487  0.0  0.0      0     0 ?        I<   17:58   0:00 [kworker/1:1H-kblockd]
root     1995084  0.0  0.0      0     0 ?        I    17:58   0:00 [kworker/0:2-events]
root     2006801  0.0  0.0      0     0 ?        I<   18:00   0:00 [kworker/0:0H]
root     2017608  0.2  0.0      0     0 ?        I    18:01   0:00 [kworker/1:2-events]
root     2028735  0.0  0.0      0     0 ?        I    18:03   0:00 [kworker/0:1-events]
root     2039653  0.0  0.0   4556  1664 ?        S    18:04   0:00 sleep 5m
root     2040338  0.0  0.0      0     0 ?        I    18:04   0:00 [kworker/u258:3-flush-252:0]
root     2049903  4.2  0.0   9824  2688 ?        Ss   18:06   0:00 /bin/bash /snap/wekan/1999/bin/wekan-control
root     2051109  103  3.5 1313952 141152 ?      Rl   18:06   0:07 /snap/wekan/1999/bin/node --stack-size=65500 main.js
root     2051289  0.0  0.0   5948  1792 ?        S    18:06   0:00 sleep 5
root     2051525  0.0  0.0   4556  1536 ?        S    18:06   0:00 sleep 1
komal_31 2051526  500  0.1  12312  5120 tty1     R+   18:06   0:00 ps aux
```

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.

```
komal_31@ubuntu:~$ sudo adduser lab4user
[sudo] password for komal_31:
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 []: Komal Kashif
        Room Number []: thirty one
        Work Phone []: 010-4573-0745
        Home Phone []: 010-8639-8824
        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' ...
```

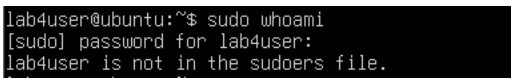
2. Verify that the new user record exists in the system's user database.

```
komal_31@ubuntu:~$ getent passwd lab4user
lab4user:x:1002:1002:Komal Kashif,thirty one,010-4573-0745,010-8639-8824,nil:/home/lab4user:/bin/bash
```

3. Log in as lab4user and confirm successful login.

```
komal_31@ubuntu:~$ su - lab4user
Password:
lab4user@ubuntu:~$ _
```

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



5. Switch back to your main analyst account.

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