CLOUD COMPUTING LAB

Fatima Jinnah
Women University

SUBMITTED TO
SIR WAQAS SALEEM

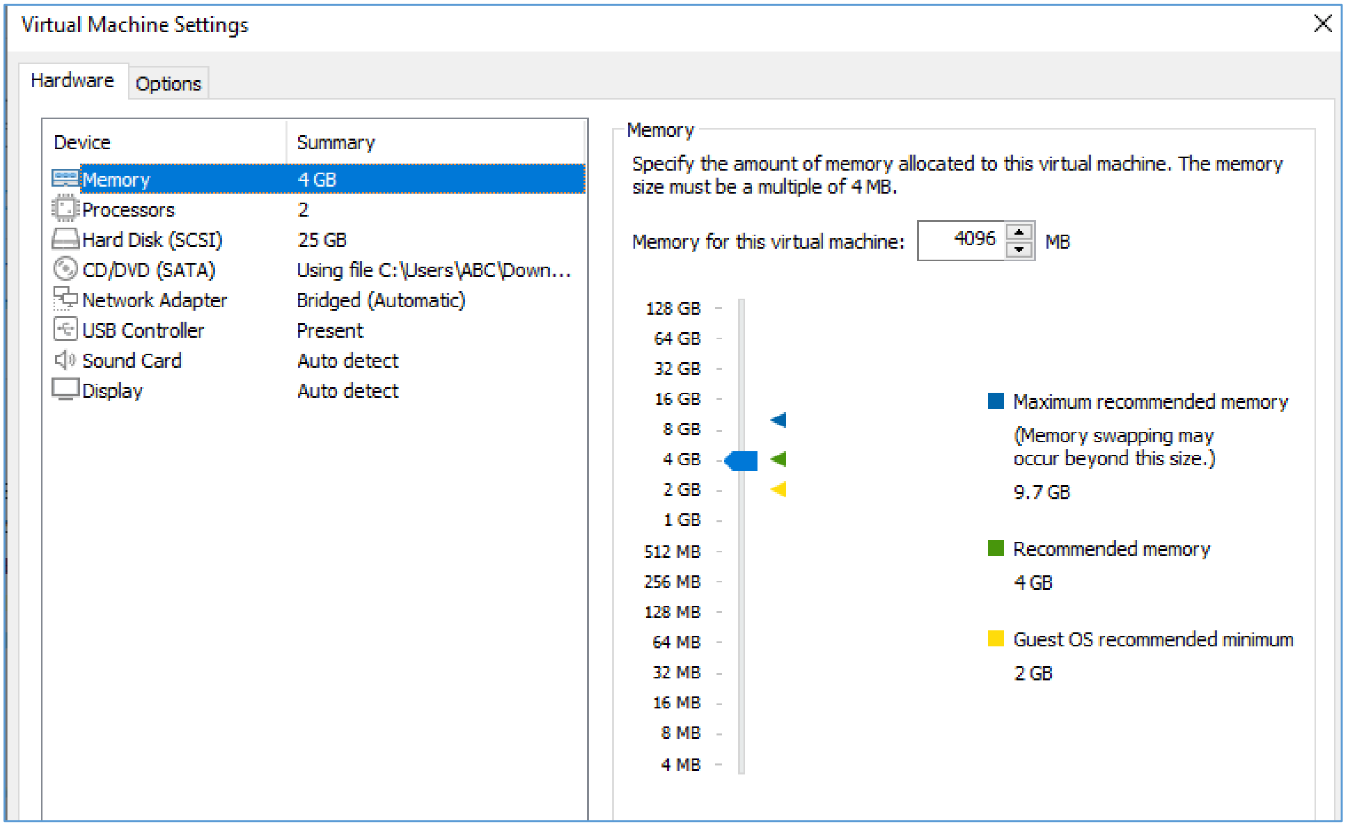
SUBMITTED BY
HAMNA MAHMOOD

2023-BSE-025
BSE V-A

Lab 04

Virtualization & Linux Fundamentals

Task 1 – Verify VM resources in VMware



Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	25 GB
CD/DVD (SATA)	Using file C:\Users\ABC\Down...
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 4096 MB

🟦 Maximum recommended memory

(Memory swapping may occur beyond this size.)

9.7 GB

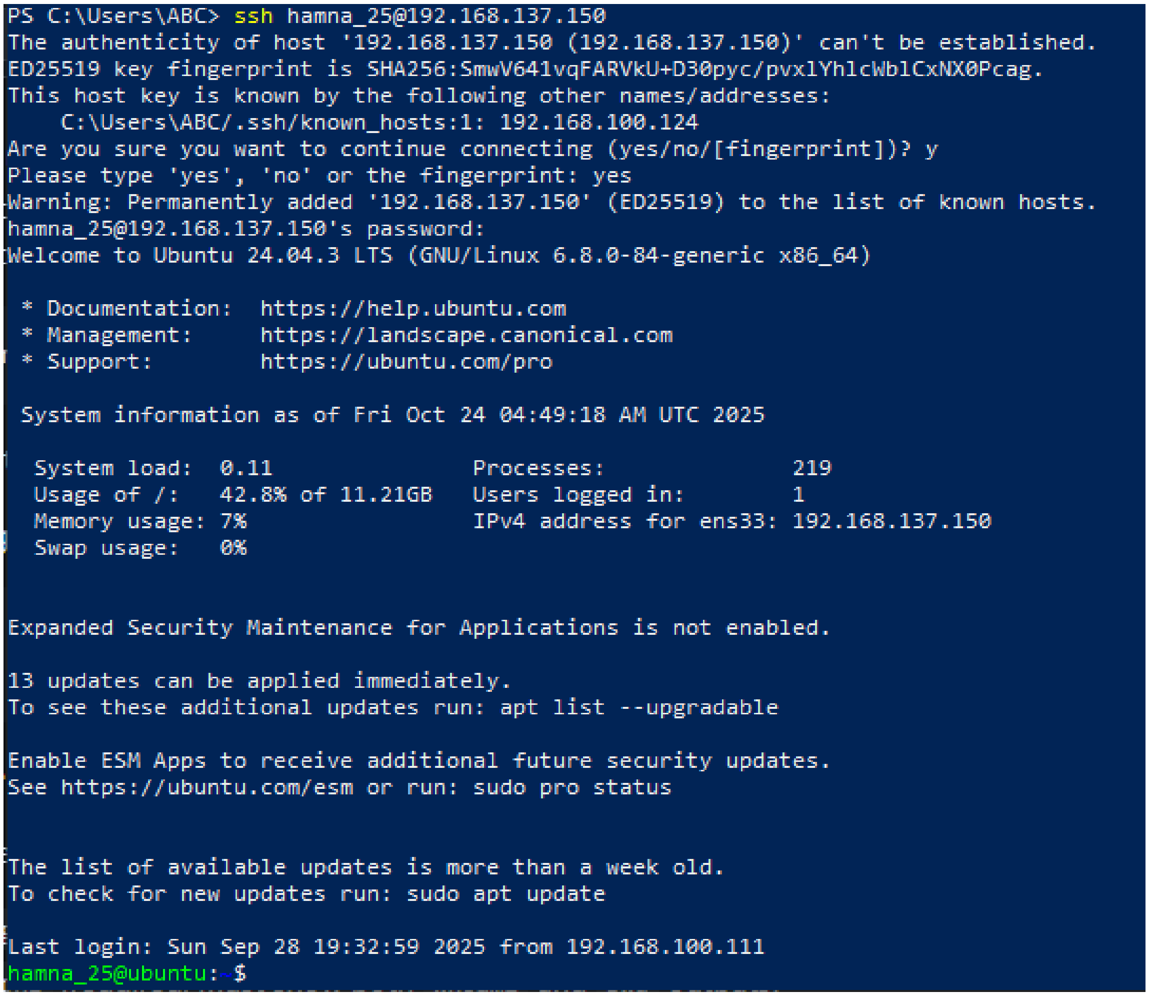
🟩 Recommended memory

4 GB

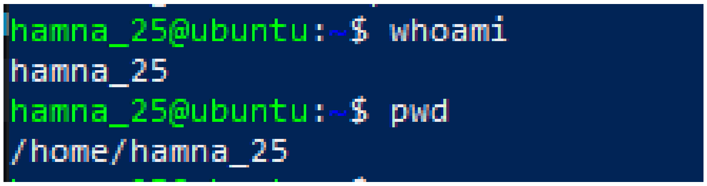
🟨 Guest OS recommended minimum

2 GB

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

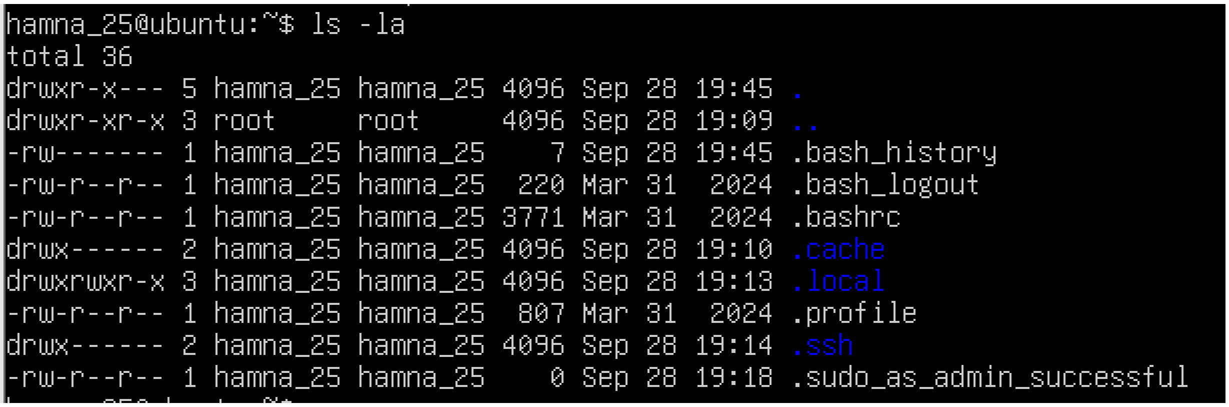


```
PS C:\Users\ABC> ssh hamna_25@192.168.137.150
The authenticity of host '192.168.137.150 (192.168.137.150)' can't be established.
ED25519 key fingerprint is SHA256:SmwV641vqFARVkU+D30pyc/pvxlYhlcWblCxNX0Pcag.
This host key is known by the following other names/addresses:
    C:\Users\ABC/.ssh/known_hosts:1: 192.168.100.124
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.137.150' (ED25519) to the list of known hosts.
hamna_25@192.168.137.150's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-84-generic x86_64)

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

 System information as of Fri Oct 24 04:49:18 AM UTC 2025

  System load:  0.11               Processes:             219
  Usage of /:   42.8% of 11.21GB   Users logged in:       1
  Memory usage: 7%                 IPv4 address for ens33: 192.168.137.150
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

13 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


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

Last login: Sun Sep 28 19:32:59 2025 from 192.168.100.111
hamna_25@ubuntu:~$
```

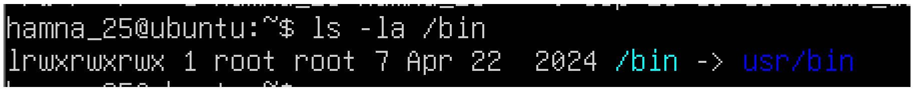


```
hamna_25@ubuntu:~$ whoami
hamna_25
hamna_25@ubuntu:~$ pwd
/home/hamna_25
```

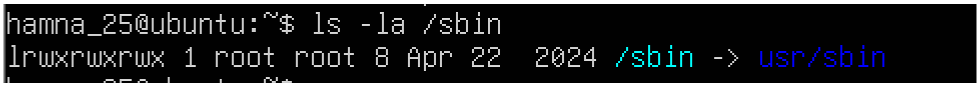
Task 3- Filesystem exploration — root tree and dotfiles



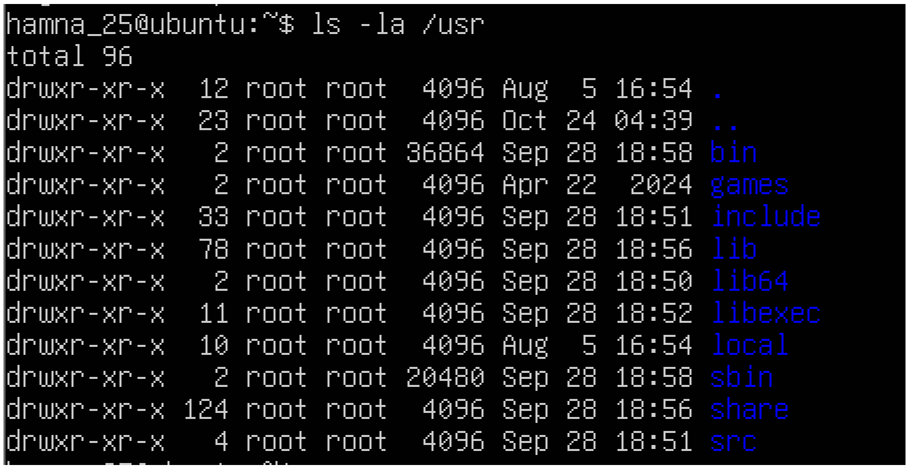
```
hamna_25@ubuntu:~$ ls -la
total 36
drwxr-x--- 5 hamna_25 hamna_25 4096 Sep 28 19:45 .
drwxr-xr-x 3 root     root     4096 Sep 28 19:09 ..
-rw------- 1 hamna_25 hamna_25    7 Sep 28 19:45 .bash_history
-rw-r--r-- 1 hamna_25 hamna_25  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hamna_25 hamna_25 3771 Mar 31  2024 .bashrc
drwx------ 2 hamna_25 hamna_25 4096 Sep 28 19:10 .cache
drwxrwxr-x 3 hamna_25 hamna_25 4096 Sep 28 19:13 .local
-rw-r--r-- 1 hamna_25 hamna_25  807 Mar 31  2024 .profile
drwx------ 2 hamna_25 hamna_25 4096 Sep 28 19:14 .ssh
-rw-r--r-- 1 hamna_25 hamna_25    0 Sep 28 19:18 .sudo_as_admin_successful
```



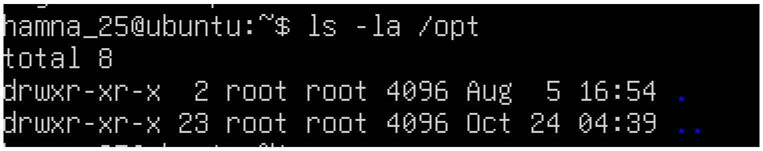
```
hamna_25@ubuntu:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
```



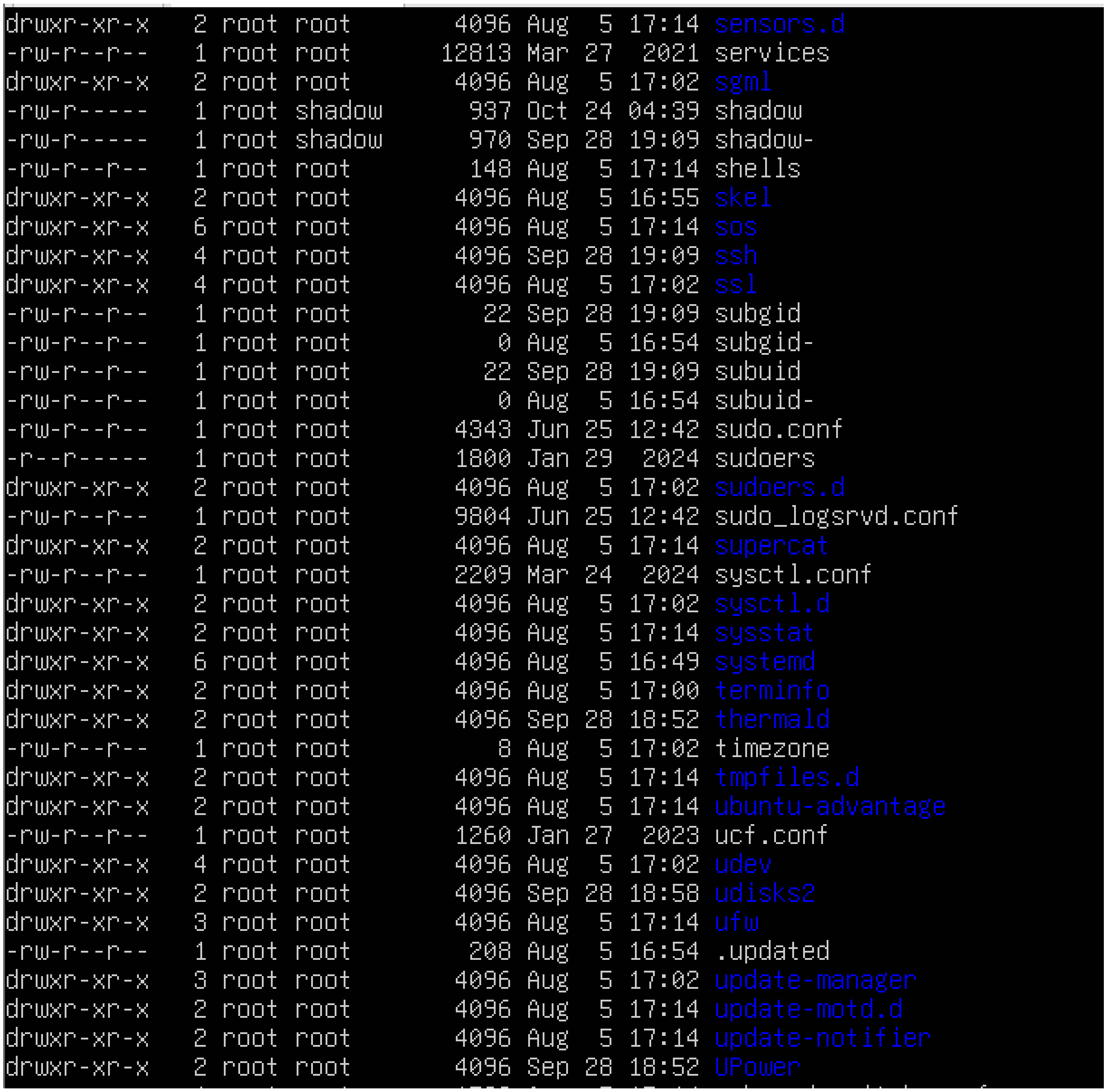
```
hamna_25@ubuntu:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
```



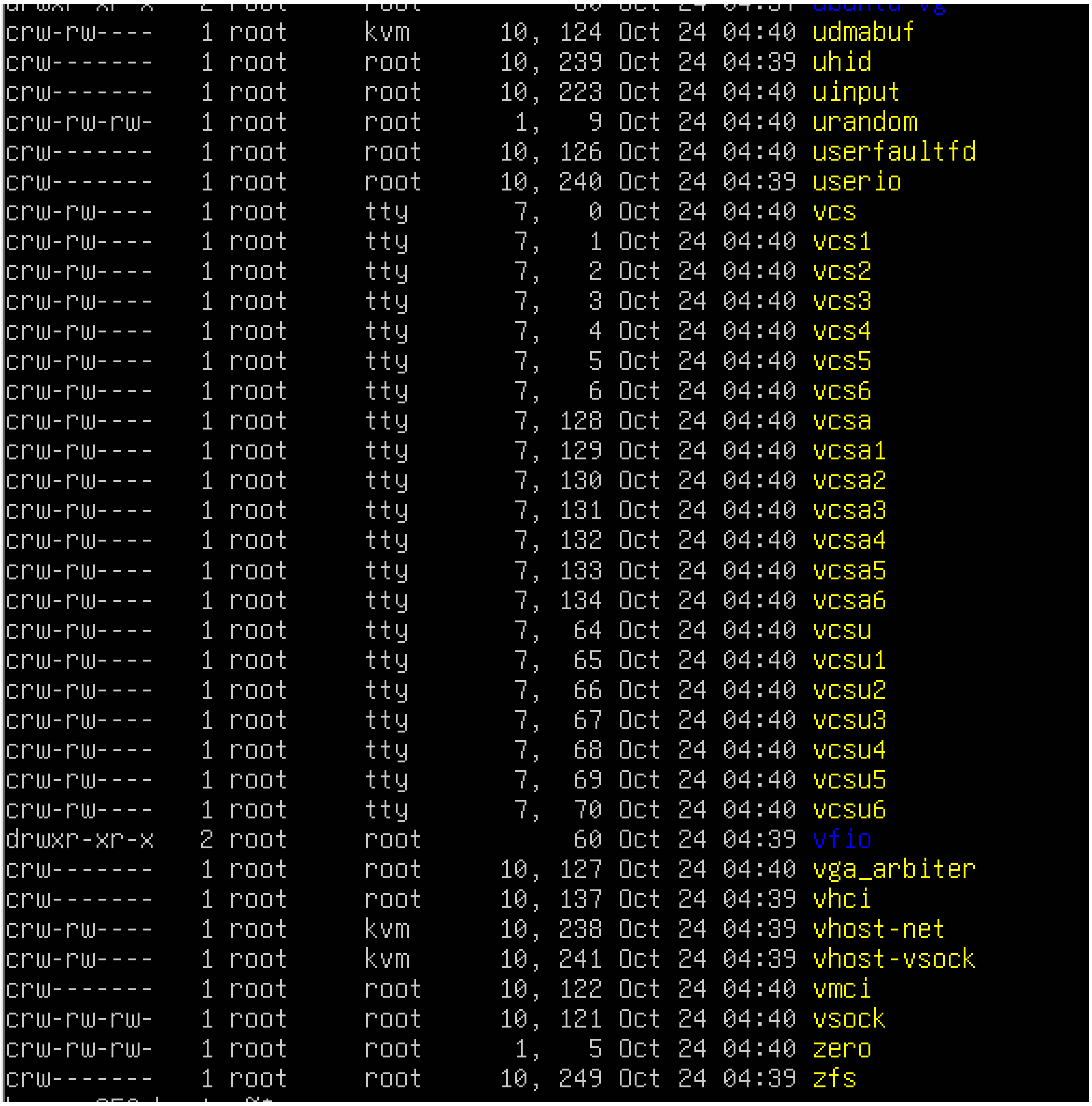
```
hamna_25@ubuntu:~$ ls -la /usr
total 96
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Oct 24 04:39 ..
drwxr-xr-x   2 root root 36864 Sep 28 18:58 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root  4096 Sep 28 18:51 include
drwxr-xr-x  78 root root  4096 Sep 28 18:56 lib
drwxr-xr-x   2 root root  4096 Sep 28 18:50 lib64
drwxr-xr-x  11 root root  4096 Sep 28 18:52 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Sep 28 18:58 sbin
drwxr-xr-x 124 root root  4096 Sep 28 18:56 share
drwxr-xr-x   4 root root  4096 Sep 28 18:51 src
```



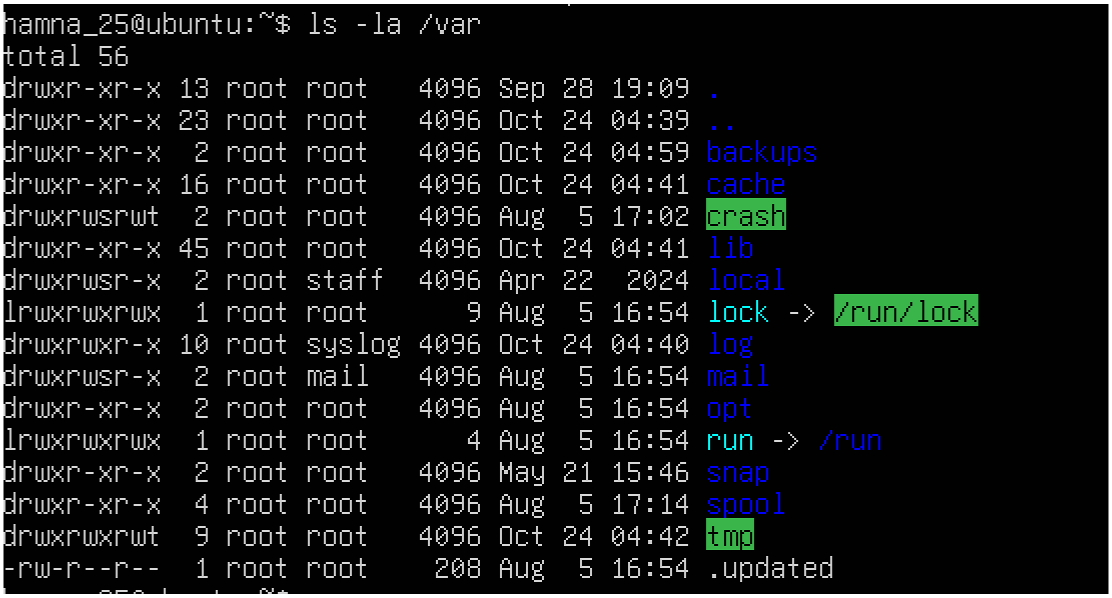
```
hamna_25@ubuntu:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Oct 24 04:39 ..
```



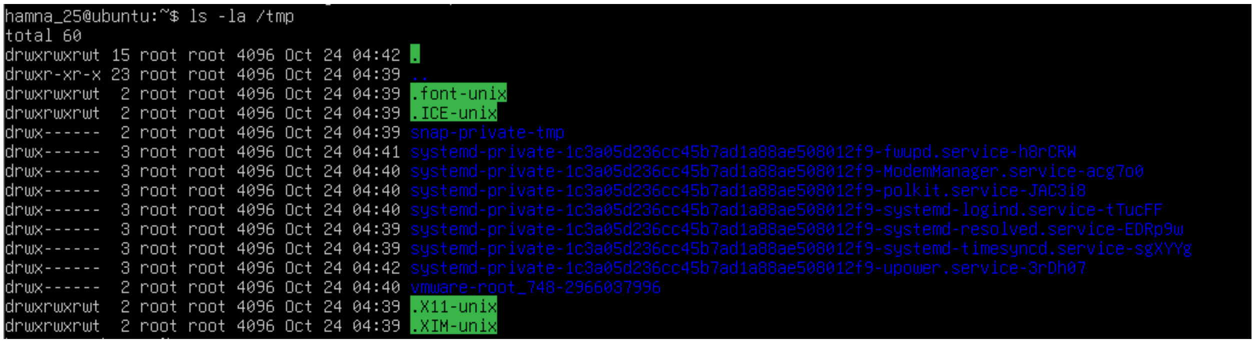
```
drwxr-xr-x   2 root root      4096 Aug  5 17:14 sensors.d
-rw-r--r--   1 root root     12813 Mar 27  2021 services
drwxr-xr-x   2 root root      4096 Aug  5 17:02 sgml
-rw-r-----   1 root shadow     937 Oct 24 04:39 shadow
-rw-r-----   1 root shadow     970 Sep 28 19:09 shadow-
-rw-r--r--   1 root root       148 Aug  5 17:14 shells
drwxr-xr-x   2 root root      4096 Aug  5 16:55 skel
drwxr-xr-x   6 root root      4096 Aug  5 17:14 sos
drwxr-xr-x   4 root root      4096 Sep 28 19:09 ssh
drwxr-xr-x   4 root root      4096 Aug  5 17:02 ssl
-rw-r--r--   1 root root        22 Sep 28 19:09 subgid
-rw-r--r--   1 root root         0 Aug  5 16:54 subgid-
-rw-r--r--   1 root root        22 Sep 28 19:09 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 28 18:52 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 Sep 28 18:58 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 28 18:52 UPower
```



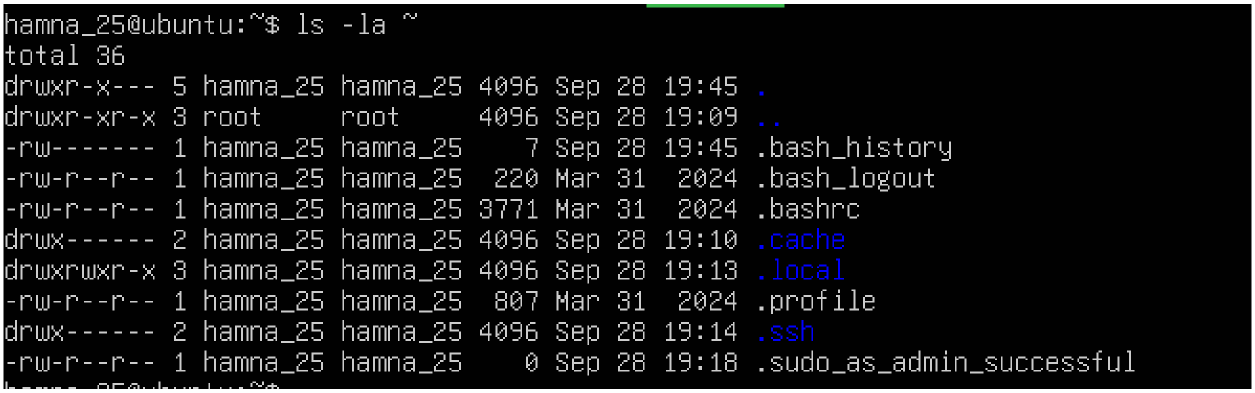
```
drwxr-xr-x   2 root     root          80 Oct 24 04:37 ubuntu-vg
crw-rw----   1 root     kvm      10, 124 Oct 24 04:40 udmabuf
crw-------   1 root     root     10, 239 Oct 24 04:39 uhid
crw-------   1 root     root     10, 223 Oct 24 04:40 uinput
crw-rw-rw-   1 root     root      1,   9 Oct 24 04:40 urandom
crw-------   1 root     root     10, 126 Oct 24 04:40 userfaultfd
crw-------   1 root     root     10, 240 Oct 24 04:39 userio
crw-rw----   1 root     tty       7,   0 Oct 24 04:40 vcs
crw-rw----   1 root     tty       7,   1 Oct 24 04:40 vcs1
crw-rw----   1 root     tty       7,   2 Oct 24 04:40 vcs2
crw-rw----   1 root     tty       7,   3 Oct 24 04:40 vcs3
crw-rw----   1 root     tty       7,   4 Oct 24 04:40 vcs4
crw-rw----   1 root     tty       7,   5 Oct 24 04:40 vcs5
crw-rw----   1 root     tty       7,   6 Oct 24 04:40 vcs6
crw-rw----   1 root     tty       7, 128 Oct 24 04:40 vcsa
crw-rw----   1 root     tty       7, 129 Oct 24 04:40 vcsa1
crw-rw----   1 root     tty       7, 130 Oct 24 04:40 vcsa2
crw-rw----   1 root     tty       7, 131 Oct 24 04:40 vcsa3
crw-rw----   1 root     tty       7, 132 Oct 24 04:40 vcsa4
crw-rw----   1 root     tty       7, 133 Oct 24 04:40 vcsa5
crw-rw----   1 root     tty       7, 134 Oct 24 04:40 vcsa6
crw-rw----   1 root     tty       7,  64 Oct 24 04:40 vcsu
crw-rw----   1 root     tty       7,  65 Oct 24 04:40 vcsu1
crw-rw----   1 root     tty       7,  66 Oct 24 04:40 vcsu2
crw-rw----   1 root     tty       7,  67 Oct 24 04:40 vcsu3
crw-rw----   1 root     tty       7,  68 Oct 24 04:40 vcsu4
crw-rw----   1 root     tty       7,  69 Oct 24 04:40 vcsu5
crw-rw----   1 root     tty       7,  70 Oct 24 04:40 vcsu6
drwxr-xr-x   2 root     root          60 Oct 24 04:39 vfio
crw-------   1 root     root     10, 127 Oct 24 04:40 vga_arbiter
crw-------   1 root     root     10, 137 Oct 24 04:39 vhci
crw-rw----   1 root     kvm      10, 238 Oct 24 04:39 vhost-net
crw-rw----   1 root     kvm      10, 241 Oct 24 04:39 vhost-vsock
crw-------   1 root     root     10, 122 Oct 24 04:40 vmci
crw-rw-rw-   1 root     root     10, 121 Oct 24 04:40 vsock
crw-rw-rw-   1 root     root      1,   5 Oct 24 04:40 zero
crw-------   1 root     root     10, 249 Oct 24 04:39 zfs
```



```
hamna_25@ubuntu:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Sep 28 19:09 .
drwxr-xr-x 23 root root   4096 Oct 24 04:39 ..
drwxr-xr-x  2 root root   4096 Oct 24 04:59 backups
drwxr-xr-x 16 root root   4096 Oct 24 04:41 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct 24 04:41 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 24 04:40 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 24 04:42 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
```

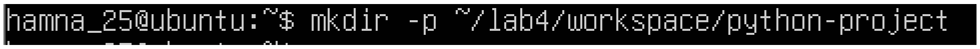


```
hamna_25@ubuntu:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 24 04:42 .
drwxr-xr-x 23 root root 4096 Oct 24 04:39 ..
drwxrwxrwt  2 root root 4096 Oct 24 04:39 .font-unix
drwxrwxrwt  2 root root 4096 Oct 24 04:39 .ICE-unix
drwx------  2 root root 4096 Oct 24 04:39 snap-private-tmp
drwx------  3 root root 4096 Oct 24 04:41 systemd-private-1c3a05d236cc45b7ad1a88ae508012f9-fwupd.service-h8rCRW
drwx------  3 root root 4096 Oct 24 04:40 systemd-private-1c3a05d236cc45b7ad1a88ae508012f9-ModemManager.service-acg7o0
drwx------  3 root root 4096 Oct 24 04:40 systemd-private-1c3a05d236cc45b7ad1a88ae508012f9-polkit.service-JAC3i8
drwx------  3 root root 4096 Oct 24 04:40 systemd-private-1c3a05d236cc45b7ad1a88ae508012f9-systemd-logind.service-tTucFF
drwx------  3 root root 4096 Oct 24 04:39 systemd-private-1c3a05d236cc45b7ad1a88ae508012f9-systemd-resolved.service-EDRp9w
drwx------  3 root root 4096 Oct 24 04:39 systemd-private-1c3a05d236cc45b7ad1a88ae508012f9-systemd-timesyncd.service-sgXYYg
drwx------  3 root root 4096 Oct 24 04:42 systemd-private-1c3a05d236cc45b7ad1a88ae508012f9-upower.service-3rDh07
drwx------  2 root root 4096 Oct 24 04:40 vmware-root_748-2966037996
drwxrwxrwt  2 root root 4096 Oct 24 04:39 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 24 04:39 .XIM-unix
```

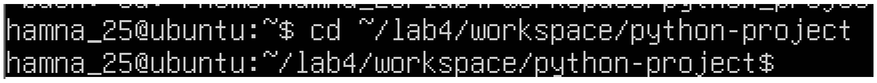


```
hamna_25@ubuntu:~$ ls -la ~
total 36
drwxr-x--- 5 hamna_25 hamna_25 4096 Sep 28 19:45 .
drwxr-xr-x 3 root     root     4096 Sep 28 19:09 ..
-rw------- 1 hamna_25 hamna_25    7 Sep 28 19:45 .bash_history
-rw-r--r-- 1 hamna_25 hamna_25  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hamna_25 hamna_25 3771 Mar 31  2024 .bashrc
drwx------ 2 hamna_25 hamna_25 4096 Sep 28 19:10 .cache
drwxrwxr-x 3 hamna_25 hamna_25 4096 Sep 28 19:13 .local
-rw-r--r-- 1 hamna_25 hamna_25  807 Mar 31  2024 .profile
drwx------ 2 hamna_25 hamna_25 4096 Sep 28 19:14 .ssh
-rw-r--r-- 1 hamna_25 hamna_25    0 Sep 28 19:18 .sudo_as_admin_successful
```

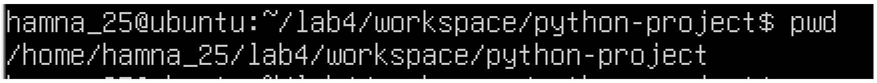
Task 4 – Essential CLI tasks — navigation and file operations



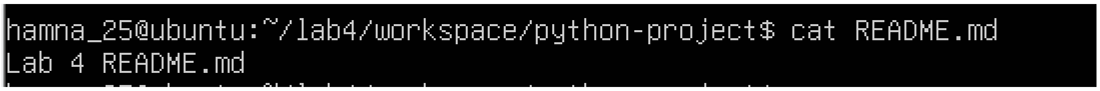
```
hamna_25@ubuntu:~$ mkdir -p ~/lab4/workspace/python-project
```



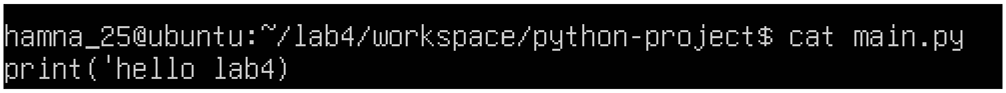
```
hamna_25@ubuntu:~$ cd ~/lab4/workspace/python-project
hamna_25@ubuntu:~/lab4/workspace/python-project$
```



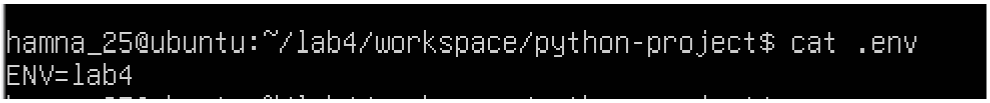
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ pwd
/home/hamna_25/lab4/workspace/python-project
```



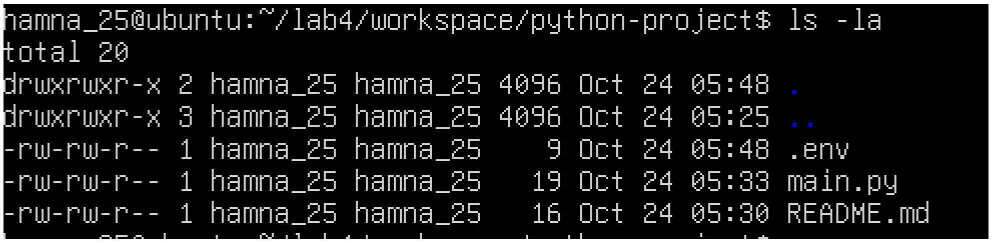
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ cat README.md
Lab 4 README.md
```



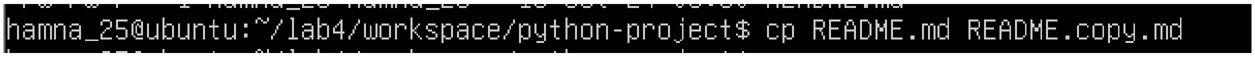
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ cat main.py
print('hello lab4)
```



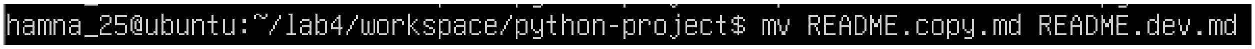
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ cat .env
ENV=lab4
```



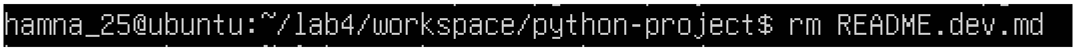
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ ls -la
total 20
drwxrwxr-x 2 hamna_25 hamna_25 4096 Oct 24 05:48 .
drwxrwxr-x 3 hamna_25 hamna_25 4096 Oct 24 05:25 ..
-rw-rw-r-- 1 hamna_25 hamna_25    9 Oct 24 05:48 .env
-rw-rw-r-- 1 hamna_25 hamna_25   19 Oct 24 05:33 main.py
-rw-rw-r-- 1 hamna_25 hamna_25   16 Oct 24 05:30 README.md
```



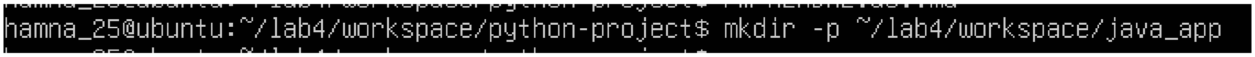
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ cp README.md README.copy.md
```



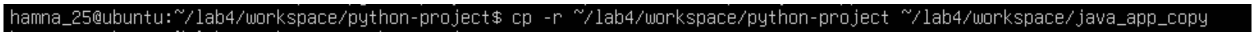
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ mv README.copy.md README.dev.md
```



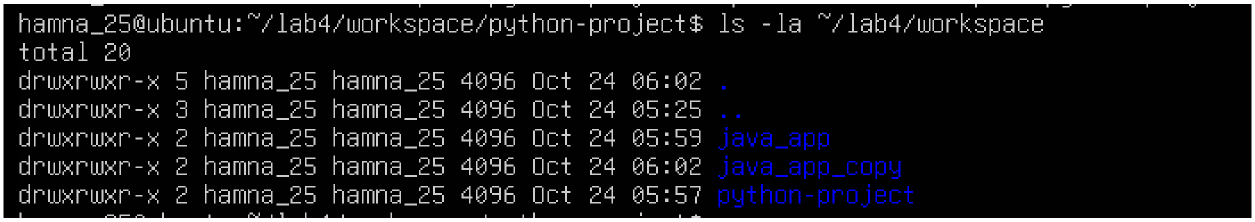
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ rm README.dev.md
```



```
hamna_25@ubuntu:~/lab4/workspace/python-project$ mkdir -p ~/lab4/workspace/java_app
```

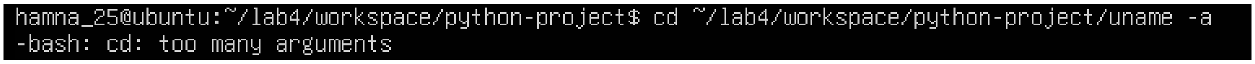


```
hamna_25@ubuntu:~/lab4/workspace/python-project$ cp -r ~/lab4/workspace/python-project ~/lab4/workspace/java_app_copy
```

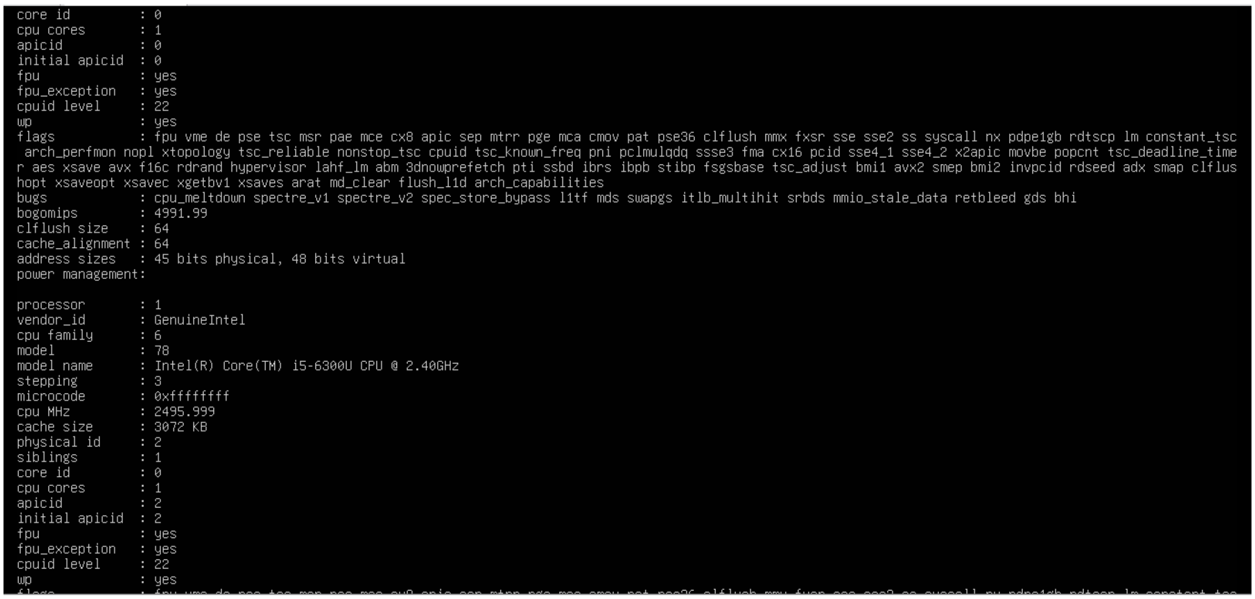


```
hamna_25@ubuntu:~/lab4/workspace/python-project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 hamna_25 hamna_25 4096 Oct 24 06:02 .
drwxrwxr-x 3 hamna_25 hamna_25 4096 Oct 24 05:25 ..
drwxrwxr-x 2 hamna_25 hamna_25 4096 Oct 24 05:59 java_app
drwxrwxr-x 2 hamna_25 hamna_25 4096 Oct 24 06:02 java_app_copy
drwxrwxr-x 2 hamna_25 hamna_25 4096 Oct 24 05:57 python-project
```

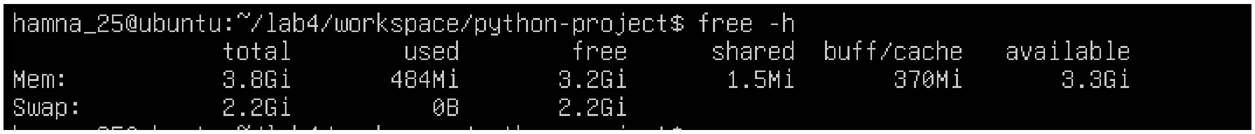
Task 5 – System info, resources & processes



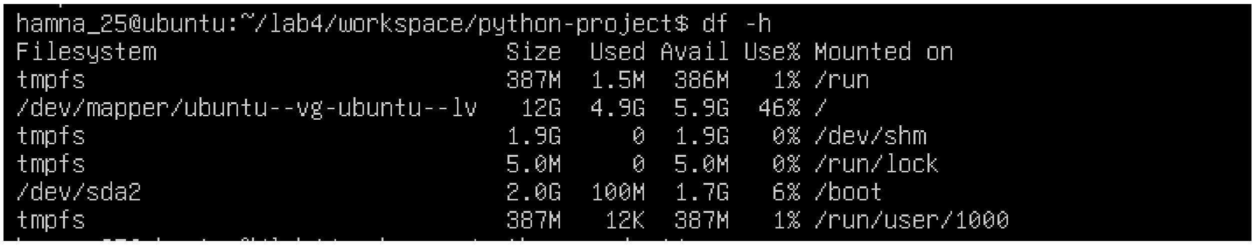
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ cd ~/lab4/workspace/python-project/uname -a
-bash: cd: too many arguments
```



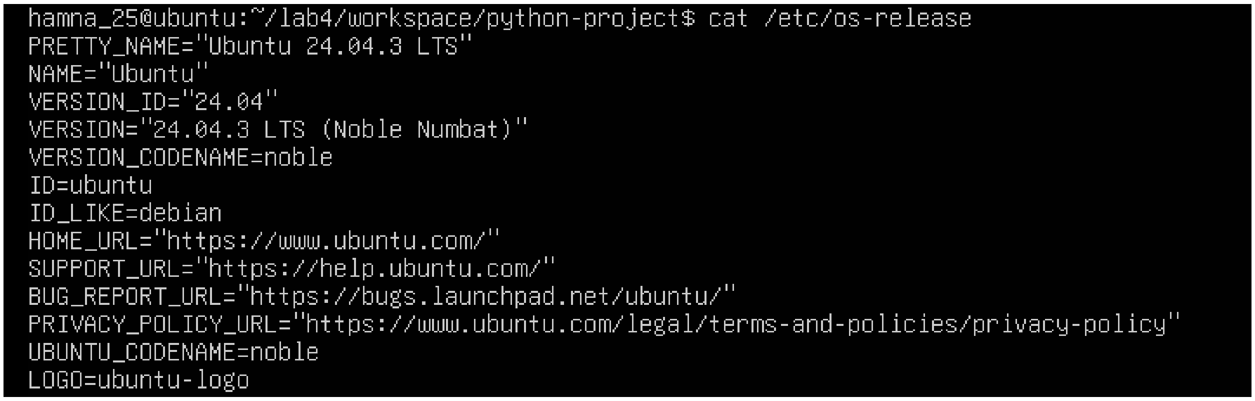
```
core id         : 0
cpu cores       : 1
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx 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:

processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 78
model name      : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
stepping        : 3
microcode       : 0xffffffff
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
```



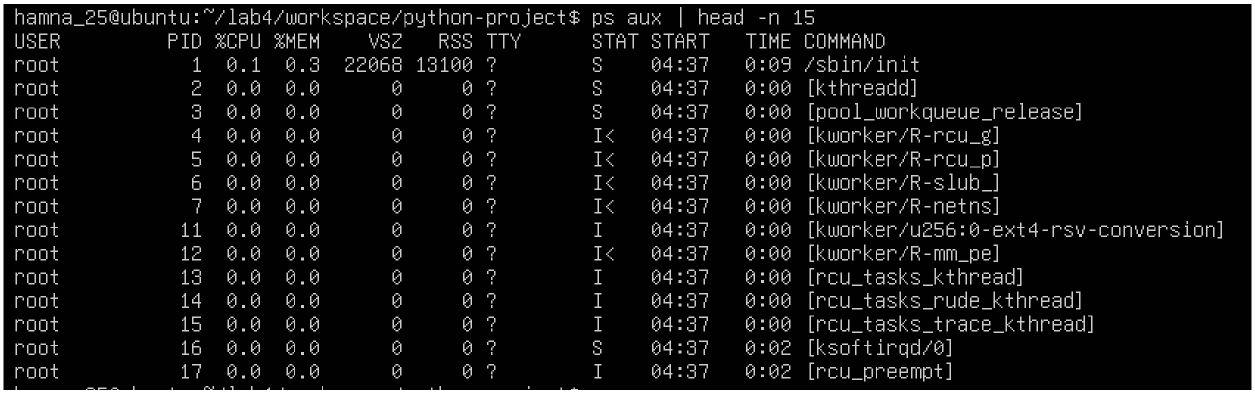
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       484Mi       3.2Gi       1.5Mi       370Mi       3.3Gi
Swap:          2.2Gi          0B       2.2Gi
```



```
hamna_25@ubuntu:~/lab4/workspace/python-project$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              387M  1.5M  386M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   12G  4.9G  5.9G  46% /
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
```

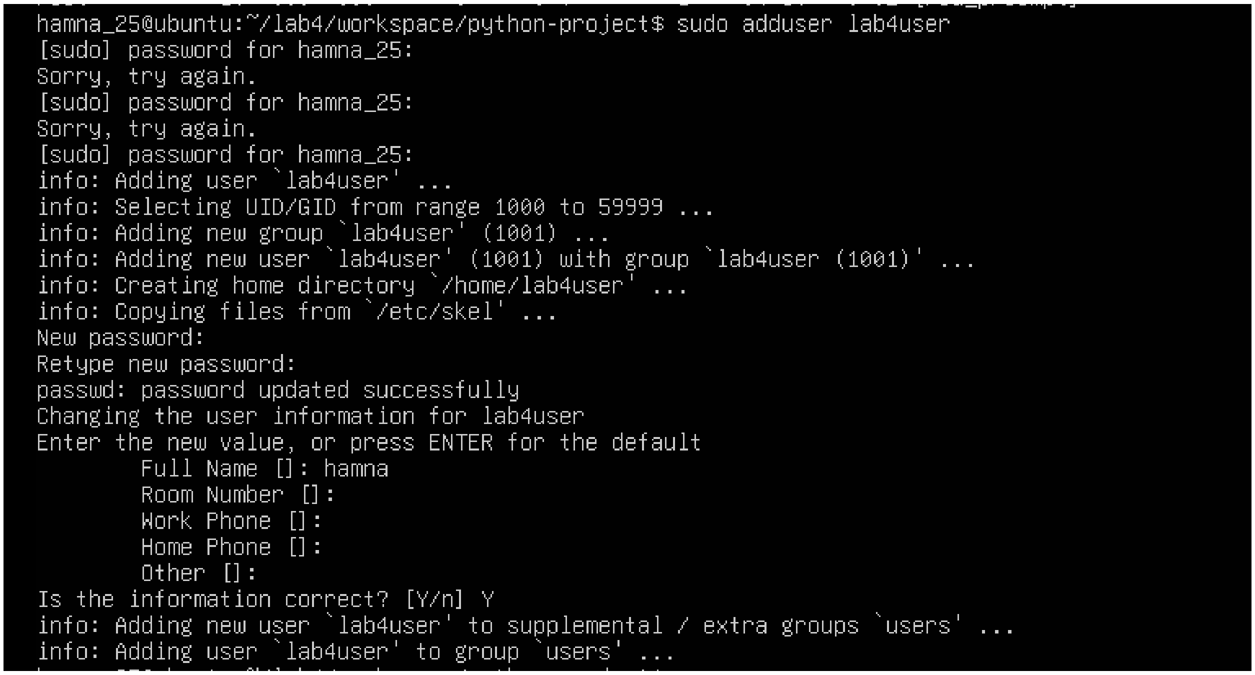


```
hamna_25@ubuntu:~/lab4/workspace/python-project$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

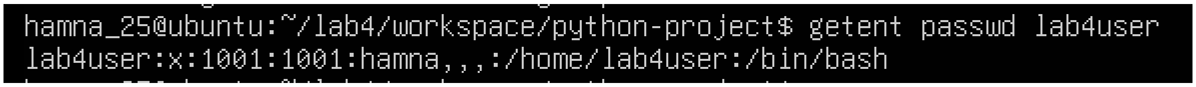


```
hamna_25@ubuntu:~/lab4/workspace/python-project$ ps aux | head -n 15
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.3  22068 13100 ?        S    04:37   0:09 /sbin/init
root           2  0.0  0.0      0     0 ?        S    04:37   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    04:37   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   04:37   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   04:37   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   04:37   0:00 [kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   04:37   0:00 [kworker/R-netns]
root          11  0.0  0.0      0     0 ?        I    04:37   0:00 [kworker/u256:0-ext4-rsv-conversion]
root          12  0.0  0.0      0     0 ?        I<   04:37   0:00 [kworker/R-mm_pe]
root          13  0.0  0.0      0     0 ?        I    04:37   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    04:37   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    04:37   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    04:37   0:02 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    04:37   0:02 [rcu_preempt]
```

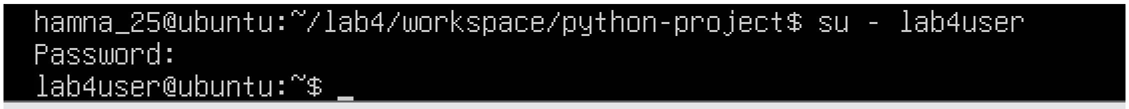
Task 6 – Users and account verification (no sudo group change)



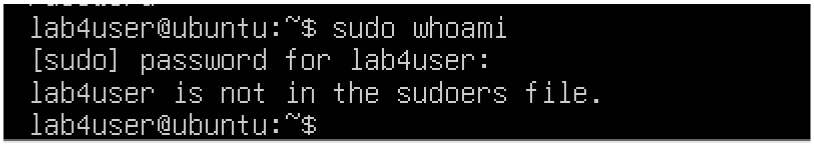
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ sudo adduser lab4user
[sudo] password for hamna_25:
Sorry, try again.
[sudo] password for hamna_25:
Sorry, try again.
[sudo] password for hamna_25:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new 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 []: hamna
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
```



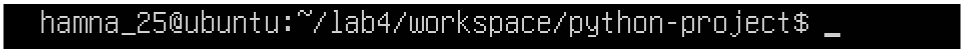
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ getent passwd lab4user
lab4user:x:1001:1001:hamna,,,:/home/lab4user:/bin/bash
```



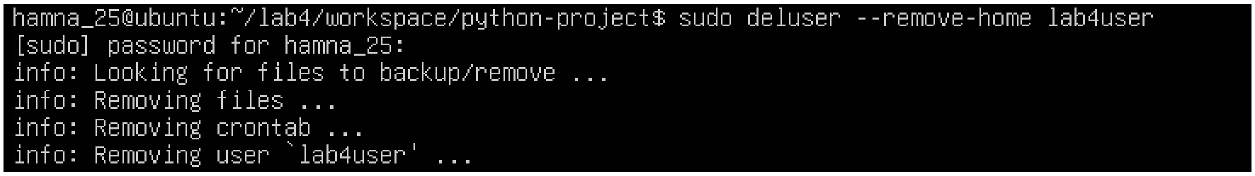
```
hamna_25@ubuntu:~/lab4/workspace/python-project$ su - lab4user
Password:
lab4user@ubuntu:~$ _
```



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

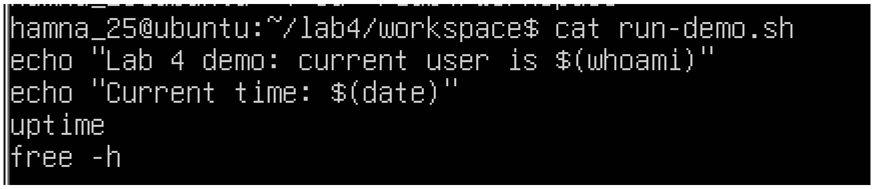


```
hamna_25@ubuntu:~/lab4/workspace/python-project$ _
```

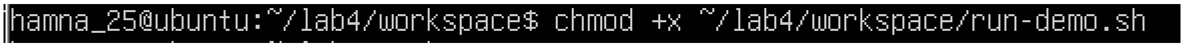


```
hamna_25@ubuntu:~/lab4/workspace/python-project$ sudo deluser --remove-home lab4user
[sudo] password for hamna_25:
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
```

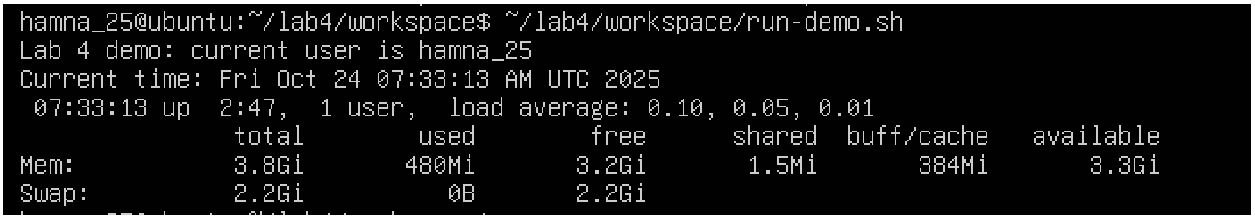
Bonus Task 7 – Create a small demo script using an editor and run it



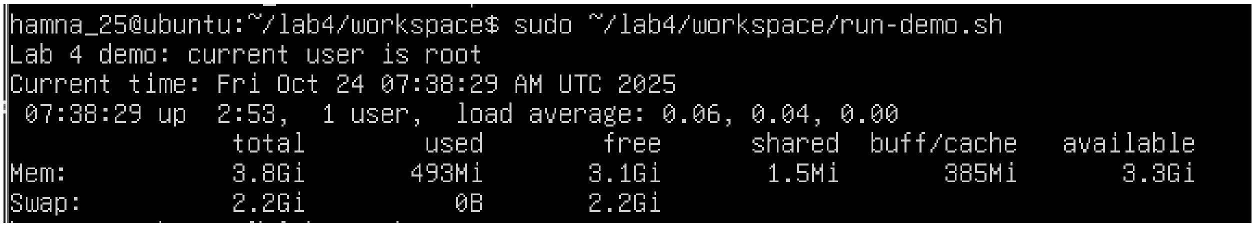
```
hamna_25@ubuntu:~/lab4/workspace$ cat run-demo.sh
echo "Lab 4 demo: current user is $(whoami)"
echo "Current time: $(date)"
uptime
free -h
```



```
hamna_25@ubuntu:~/lab4/workspace$ chmod +x ~/lab4/workspace/run-demo.sh
```



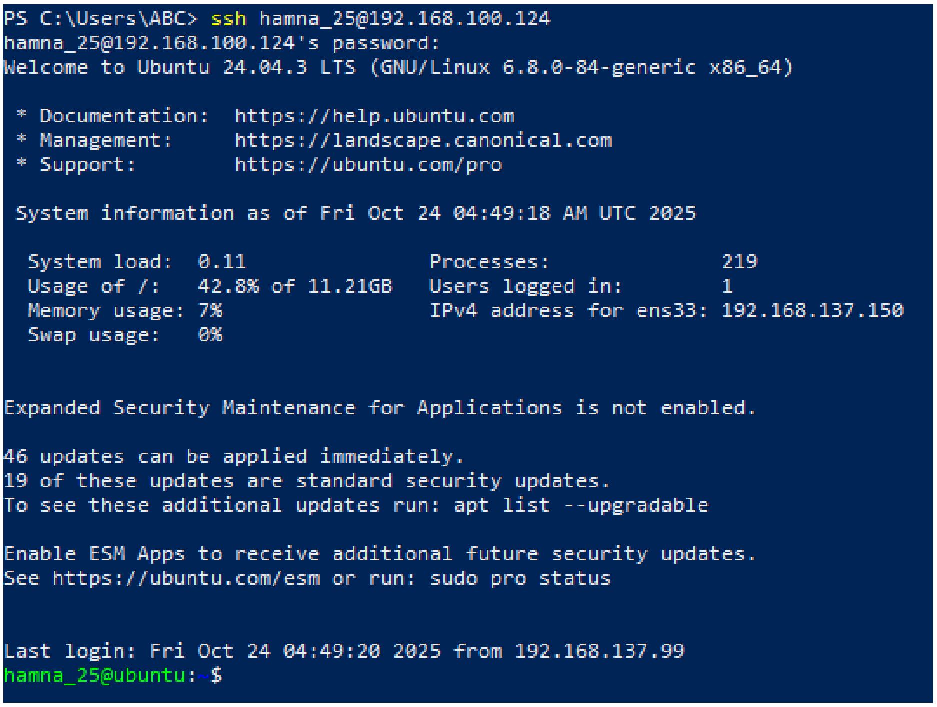
```
hamna_25@ubuntu:~/lab4/workspace$ ~/lab4/workspace/run-demo.sh
Lab 4 demo: current user is hamna_25
Current time: Fri Oct 24 07:33:13 AM UTC 2025
 07:33:13 up  2:47,  1 user,  load average: 0.10, 0.05, 0.01
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       480Mi       3.2Gi       1.5Mi       384Mi       3.3Gi
Swap:          2.2Gi          0B       2.2Gi
```



```
hamna_25@ubuntu:~/lab4/workspace$ sudo ~/lab4/workspace/run-demo.sh
Lab 4 demo: current user is root
Current time: Fri Oct 24 07:38:29 AM UTC 2025
 07:38:29 up  2:53,  1 user,  load average: 0.06, 0.04, 0.00
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       493Mi       3.1Gi       1.5Mi       385Mi       3.3Gi
Swap:          2.2Gi          0B       2.2Gi
```

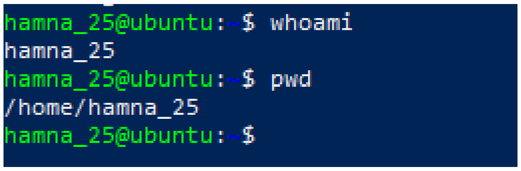
Exam Evaluation Questions

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



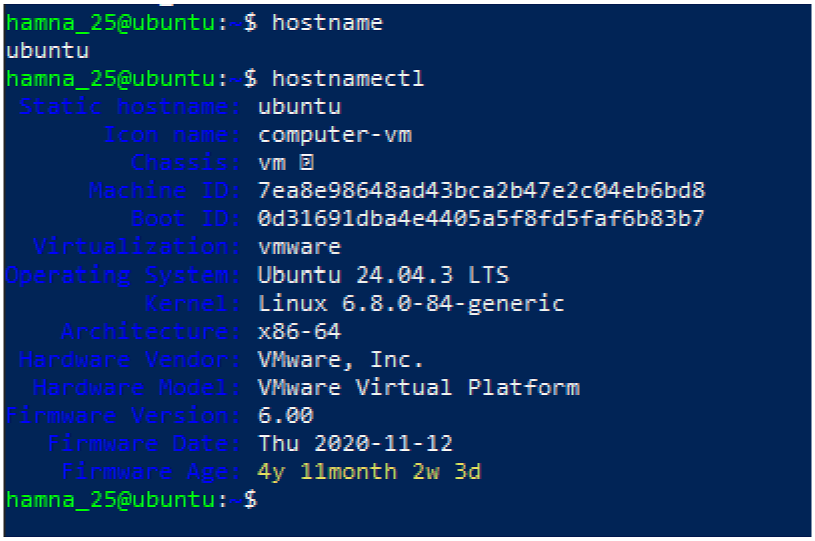
```
PS C:\Users\ABC> ssh hamna_25@192.168.100.124
hamna_25@192.168.100.124's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-84-generic x86_64)

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

 System information as of Fri Oct 24 04:49:18 AM UTC 2025

  System load:  0.11               Processes:             219
  Usage of /:   42.8% of 11.21GB   Users logged in:       1
  Memory usage: 7%                 IPv4 address for ens33: 192.168.137.150
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

46 updates can be applied immediately.
19 of these updates are standard security updates.
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: Fri Oct 24 04:49:20 2025 from 192.168.137.99
hamna_25@ubuntu:~$
```

Verify your current user and home directory path.



```
hamna_25@ubuntu:~$ whoami
hamna_25
hamna_25@ubuntu:~$ pwd
/home/hamna_25
hamna_25@ubuntu:~$
```

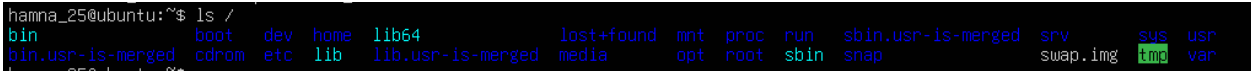
Confirm you are connected to the correct host machine.



```
hamna_25@ubuntu:~$ hostname
ubuntu
hamna_25@ubuntu:~$ hostnamectl
 Static hostname: ubuntu
       Icon name: computer-vm
         Chassis: vm ⊡
      Machine ID: 7ea8e98648ad43bca2b47e2c04eb6bd8
         Boot ID: 0d31691dba4e4405a5f8fd5faf6b83b7
  Virtualization: vmware
Operating System: Ubuntu 24.04.3 LTS
          Kernel: Linux 6.8.0-84-generic
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
Firmware Version: 6.00
   Firmware Date: Thu 2020-11-12
    Firmware Age: 4y 11month 2w 3d
hamna_25@ubuntu:~$
```

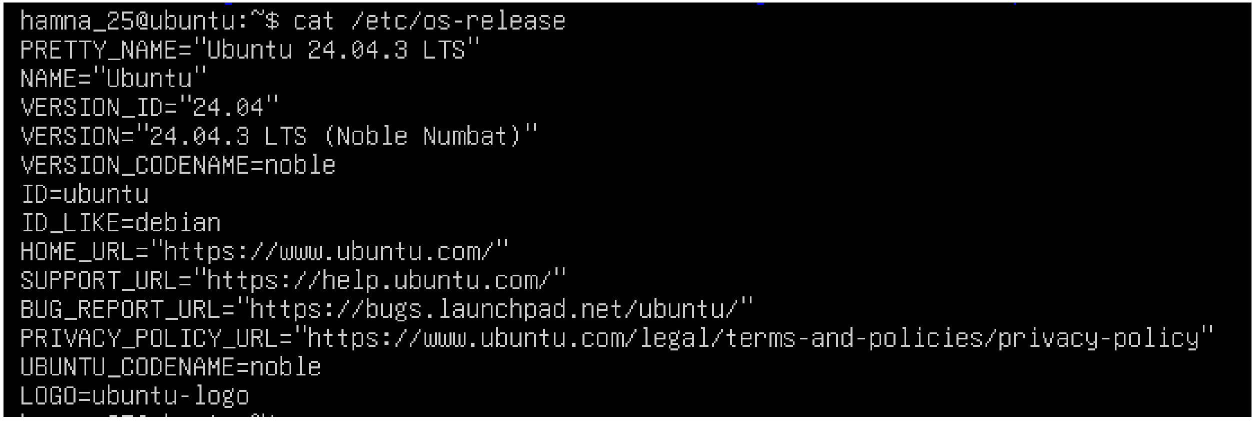
2. Filesystem Inspection for Forensic Evidence

Display the contents of the root directory



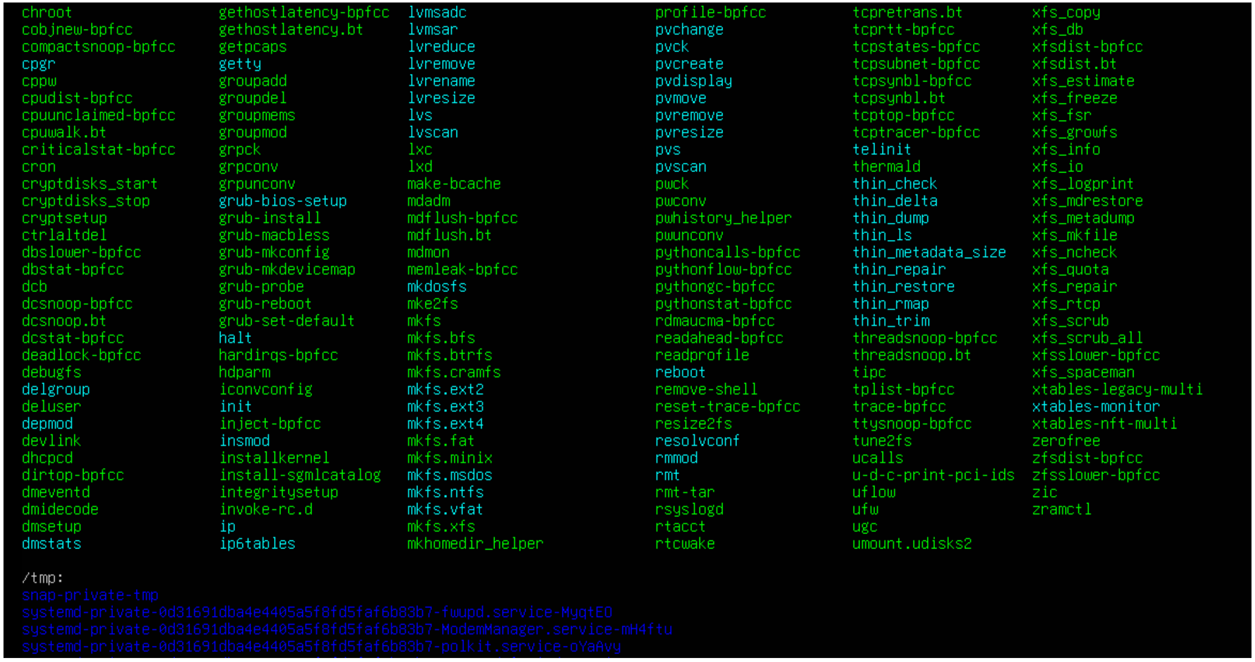
```
hamna_25@ubuntu:~$ ls /
bin                boot   dev  home  lib64              lost+found  mnt  proc  run   sbin.usr-is-merged  srv       sys  usr
bin.usr-is-merged  cdrom  etc  lib   lib.usr-is-merged  media       opt  root  sbin  snap                swap.img  tmp  var
```

Display the OS version and release information.



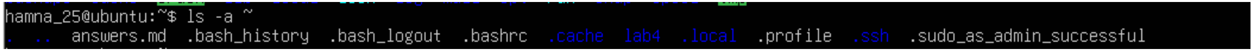
```
hamna_25@ubuntu:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

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



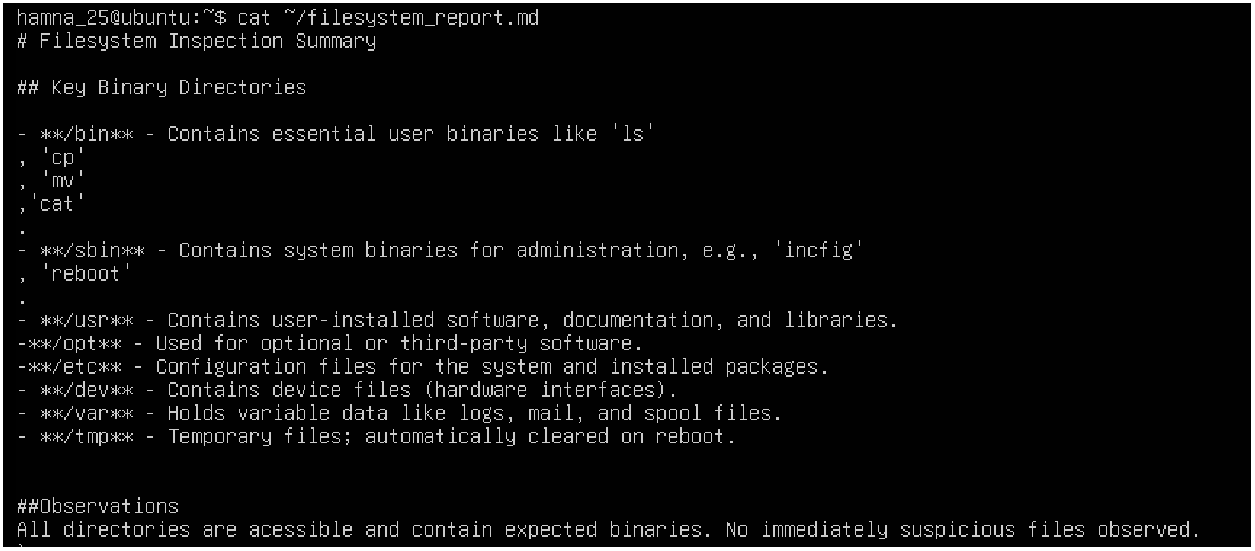
```
chroot                 gethostlatency-bpfcc  lvmsadc                      profile-bpfcc          tcpretrans.bt        xfs_copy
cobjnew-bpfcc          gethostlatency.bt     lvmsar                       pvchange               tcprtt-bpfcc         xfs_db
compactsnoop-bpfcc     getpcaps              lvreduce                     pvck                   tcpstates-bpfcc      xfsdist-bpfcc
cpgr                   getty                 lvremove                     pvcreate               tcpsubnet-bpfcc      xfsdist.bt
cppw                   groupadd              lvrename                     pvdisplay              tcpsynbl-bpfcc       xfs_estimate
cpudist-bpfcc          groupdel              lvresize                     pvmove                 tcpsynbl.bt          xfs_freeze
cpuunclaimed-bpfcc     groupmems             lvs                          pvremove               tcptop-bpfcc         xfs_fsr
cpuwalk.bt             groupmod              lvscan                       pvresize               tcptracer-bpfcc      xfs_growfs
criticalstat-bpfcc     grpck                 lxc                          pvs                    telinit              xfs_info
cron                   grpconv               lxd                          pvscan                 thermald             xfs_io
cryptdisks_start       grpunconv             make-bcache                  pwck                   thin_check           xfs_logprint
cryptdisks_stop        grub-bios-setup       mdadm                        pwconv                 thin_delta           xfs_mdrestore
cryptsetup             grub-install          mdflush-bpfcc                pwhistory_helper       thin_dump            xfs_metadump
ctrlaltdel             grub-macbless         mdflush.bt                   pwunconv               thin_ls              xfs_mkfile
dbslower-bpfcc         grub-mkconfig         mdmon                        pythoncalls-bpfcc      thin_metadata_size   xfs_ncheck
dbstat-bpfcc           grub-mkdevicemap      memleak-bpfcc                pythonflow-bpfcc       thin_repair          xfs_quota
dcb                    grub-probe            mkdosfs                      pythongc-bpfcc         thin_restore         xfs_repair
dcsnoop-bpfcc          grub-reboot           mke2fs                       pythonstat-bpfcc       thin_rmap            xfs_rtcp
dcsnoop.bt             grub-set-default      mkfs                         rdmaucma-bpfcc         thin_trim            xfs_scrub
dcstat-bpfcc           halt                  mkfs.bfs                     readahead-bpfcc        threadsnoop-bpfcc    xfs_scrub_all
deadlock-bpfcc         hardirqs-bpfcc        mkfs.btrfs                   readprofile            threadsnoop.bt       xfsslower-bpfcc
debugfs                hdparm                mkfs.cramfs                  reboot                 tipc                 xfs_spaceman
delgroup               iconvconfig           mkfs.ext2                    remove-shell           tplist-bpfcc         xtables-legacy-multi
deluser                init                  mkfs.ext3                    reset-trace-bpfcc      trace-bpfcc          xtables-monitor
depmod                 inject-bpfcc          mkfs.ext4                    resize2fs              ttysnoop-bpfcc       xtables-nft-multi
devlink                insmod                mkfs.fat                     resolvconf             tune2fs              zerofree
dhcpcd                 installkernel         mkfs.minix                   rmmod                  ucalls               zfsdist-bpfcc
dirtop-bpfcc           install-sgmlcatalog   mkfs.msdos                   rmt                    u-d-c-print-pci-ids  zfsslower-bpfcc
dmeventd               integritysetup        mkfs.ntfs                    rmt-tar                uflow                zic
dmidecode              invoke-rc.d           mkfs.vfat                    rsyslogd               ufw                  zramctl
dmsetup                ip                    mkfs.xfs                     rtacct                 ugc
dmstats                ip6tables             mkhomedir_helper             rtcwake                umount.udisks2

/tmp:
snap-private-tmp
systemd-private-0d31691dba4e4405a5f8fd5faf6b83b7-fwupd.service-MyqtEO
systemd-private-0d31691dba4e4405a5f8fd5faf6b83b7-ModemManager.service-mH4ftu
systemd-private-0d31691dba4e4405a5f8fd5faf6b83b7-polkit.service-oYaAvy
```

Display all hidden files in your home directory.



```
hamna_25@ubuntu:~$ ls -a ~
.  ..  answers.md  .bash_history  .bash_logout  .bashrc  .cache  lab4  .local  .profile  .ssh  .sudo_as_admin_successful
```

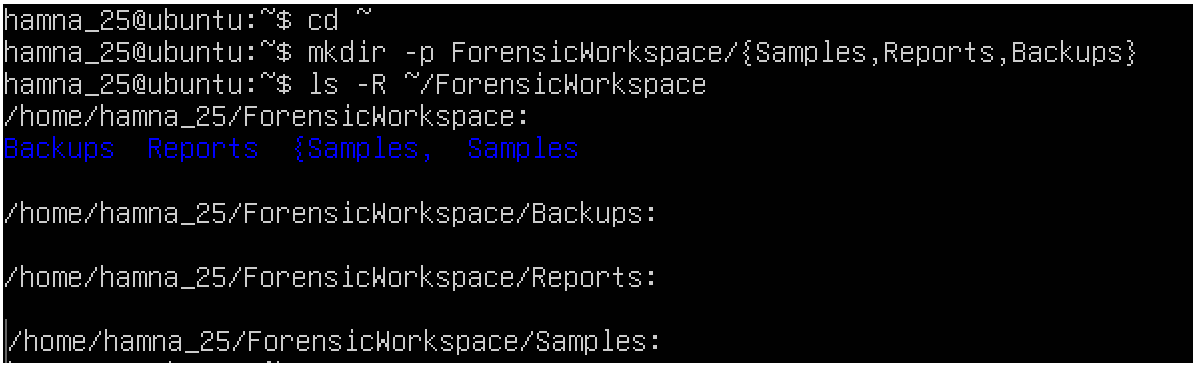
Create a markdown file summarizing your findings on key binary directories.



```
hamna_25@ubuntu:~$ cat ~/filesystem_report.md
# Filesystem Inspection Summary

## Key Binary Directories

- **/bin** - Contains essential user binaries like 'ls'
, 'cp'
, 'mv'
,'cat'
.
- **/sbin** - Contains system binaries for administration, e.g., 'incfig'
, 'reboot'
.
- **/usr** - Contains user-installed software, documentation, and libraries.
-**/opt** - Used for optional or third-party software.
-**/etc** - Configuration files for the system and installed packages.
- **/dev** - Contains device files (hardware interfaces).
- **/var** - Holds variable data like logs, mail, and spool files.
- **/tmp** - Temporary files; automatically cleared on reboot.


##Observations
All directories are acessible and contain expected binaries. No immediately suspicious files observed.
```

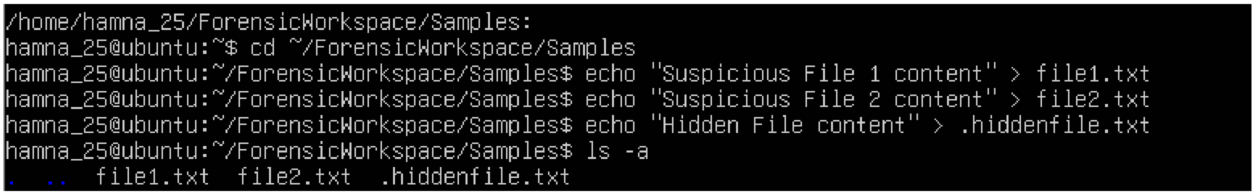
3. Evidence handling & File Operations

Create a structured folder hierarchy under your home directory for analysis.



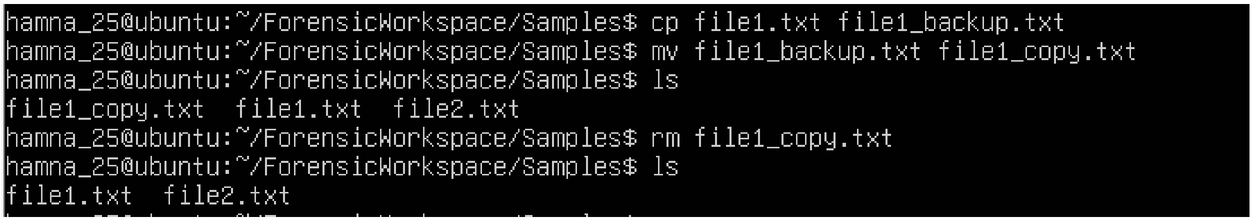
```
hamna_25@ubuntu:~$ cd ~
hamna_25@ubuntu:~$ mkdir -p ForensicWorkspace/{Samples,Reports,Backups}
hamna_25@ubuntu:~$ ls -R ~/ForensicWorkspace
/home/hamna_25/ForensicWorkspace:
Backups  Reports  {Samples,  Samples

/home/hamna_25/ForensicWorkspace/Backups:

/home/hamna_25/ForensicWorkspace/Reports:

/home/hamna_25/ForensicWorkspace/Samples:
```

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



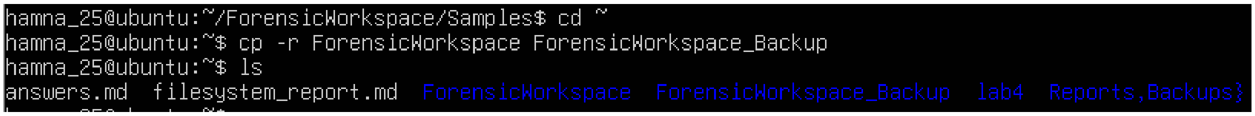
```
/home/hamna_25/ForensicWorkspace/Samples:
hamna_25@ubuntu:~$ cd ~/ForensicWorkspace/Samples
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ echo "Suspicious File 1 content" > file1.txt
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ echo "Suspicious File 2 content" > file2.txt
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ echo "Hidden File content" > .hiddenfile.txt
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ ls -a
.  ..  file1.txt  file2.txt  .hiddenfile.txt
```

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



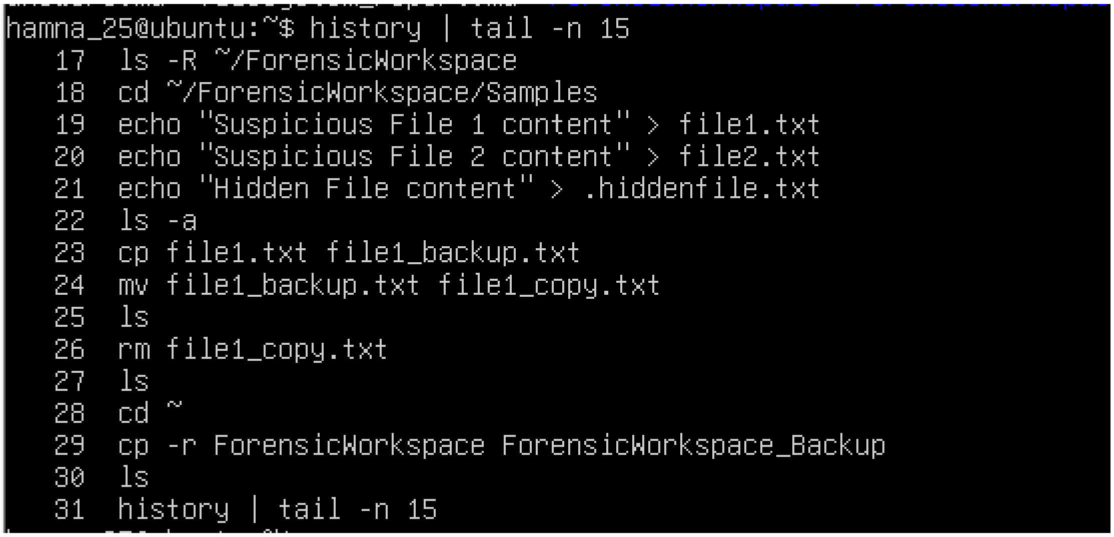
```
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ cp file1.txt file1_backup.txt
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ mv file1_backup.txt file1_copy.txt
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ ls
file1_copy.txt  file1.txt  file2.txt
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ rm file1_copy.txt
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ ls
file1.txt  file2.txt
```

Copy the entire workspace as an evidence backup folder.



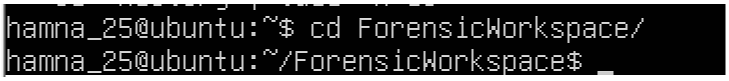
```
hamna_25@ubuntu:~/ForensicWorkspace/Samples$ cd ~
hamna_25@ubuntu:~$ cp -r ForensicWorkspace ForensicWorkspace_Backup
hamna_25@ubuntu:~$ ls
answers.md  filesystem_report.md  ForensicWorkspace  ForensicWorkspace_Backup  lab4  Reports,Backups}
```

Display your command history to document all actions performed.



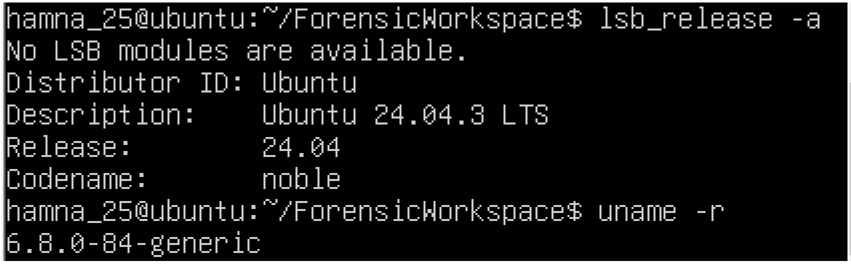
```
hamna_25@ubuntu:~$ history | tail -n 15
   17  ls -R ~/ForensicWorkspace
   18  cd ~/ForensicWorkspace/Samples
   19  echo "Suspicious File 1 content" > file1.txt
   20  echo "Suspicious File 2 content" > file2.txt
   21  echo "Hidden File content" > .hiddenfile.txt
   22  ls -a
   23  cp file1.txt file1_backup.txt
   24  mv file1_backup.txt file1_copy.txt
   25  ls
   26  rm file1_copy.txt
   27  ls
   28  cd ~
   29  cp -r ForensicWorkspace ForensicWorkspace_Backup
   30  ls
   31  history | tail -n 15
```

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



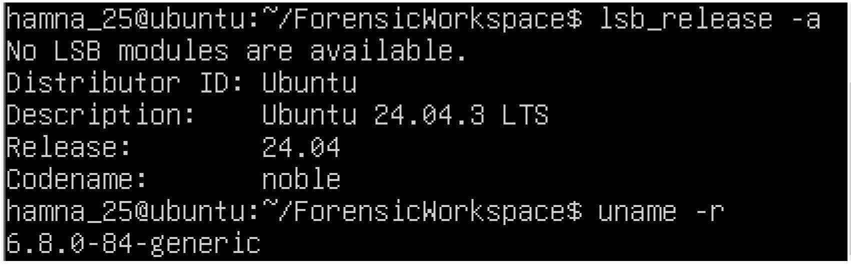
```
hamna_25@ubuntu:~$ cd ForensicWorkspace/
hamna_25@ubuntu:~/ForensicWorkspace$ _
```

4. **System Profiling and Process Monitoring**
   Display the system's OS and kernel version for the investigation report.

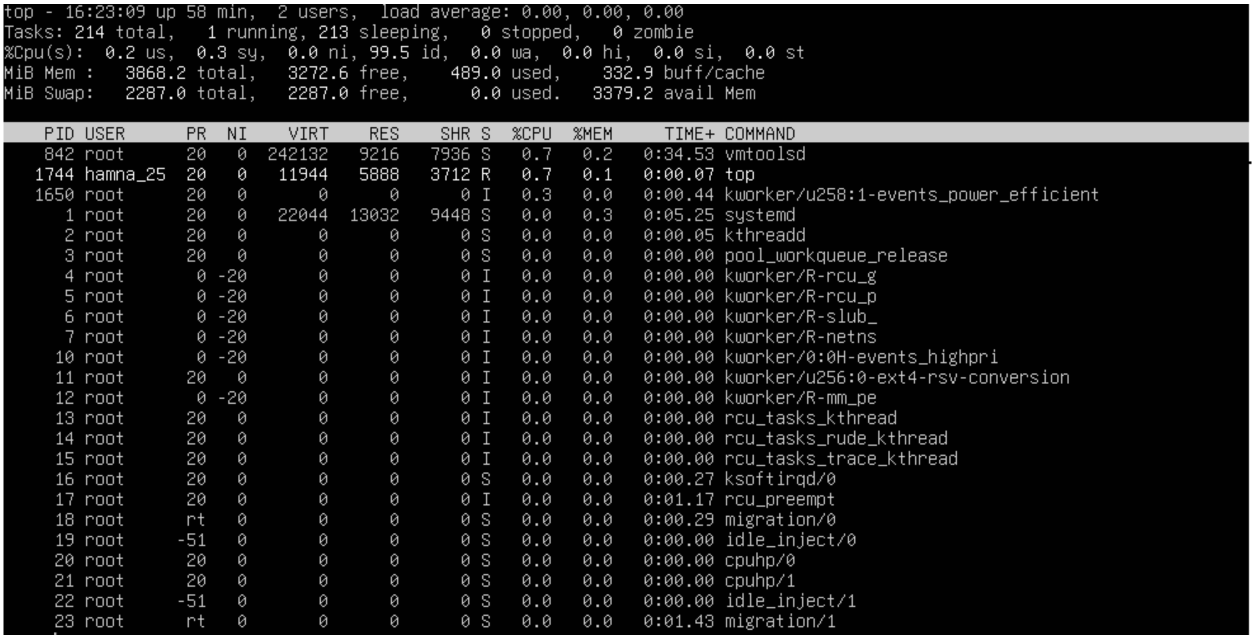


```
hamna_25@ubuntu:~/ForensicWorkspace$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.3 LTS
Release:        24.04
Codename:       noble
hamna_25@ubuntu:~/ForensicWorkspace$ uname -r
6.8.0-84-generic
```

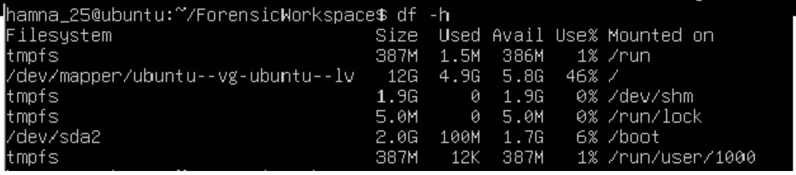
Display CPU, memory, and disk usage information.



```
hamna_25@ubuntu:~/ForensicWorkspace$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.3 LTS
Release:        24.04
Codename:       noble
hamna_25@ubuntu:~/ForensicWorkspace$ uname -r
6.8.0-84-generic
```

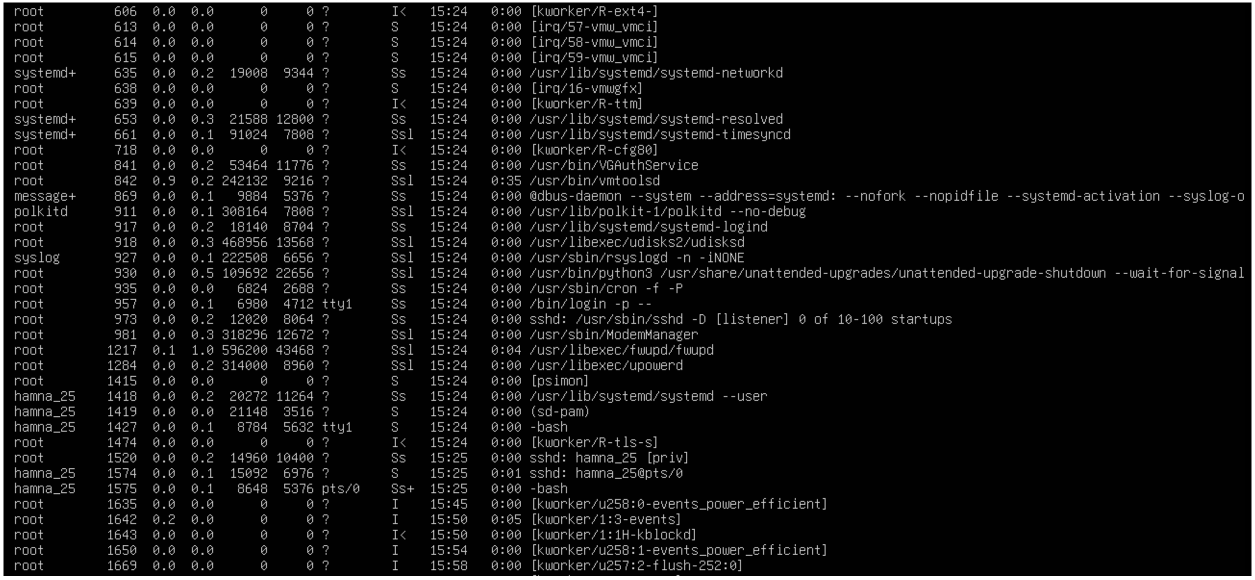


```
top - 16:23:09 up 58 min,  2 users,  load average: 0.00, 0.00, 0.00
Tasks: 214 total,   1 running, 213 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.2 us,  0.3 sy,  0.0 ni, 99.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3868.2 total,   3272.6 free,    489.0 used,    332.9 buff/cache
MiB Swap:   2287.0 total,   2287.0 free,      0.0 used.   3379.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    842 root      20   0  242132   9216   7936 S   0.7   0.2   0:34.53 vmtoolsd
   1744 hamna_25  20   0   11944   5888   3712 R   0.7   0.1   0:00.07 top
   1650 root      20   0       0      0      0 I   0.3   0.0   0:00.44 kworker/u258:1-events_power_efficient
      1 root      20   0   22044  13032   9448 S   0.0   0.3   0:05.25 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.05 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_g
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_p
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-slub_
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-netns
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/u256:0-ext4-rsv-conversion
     12 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-mm_pe
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     14 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.27 ksoftirqd/0
     17 root      20   0       0      0      0 I   0.0   0.0   0:01.17 rcu_preempt
     18 root      rt   0       0      0      0 S   0.0   0.0   0:00.29 migration/0
     19 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     21 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     22 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/1
     23 root      rt   0       0      0      0 S   0.0   0.0   0:01.43 migration/1
```



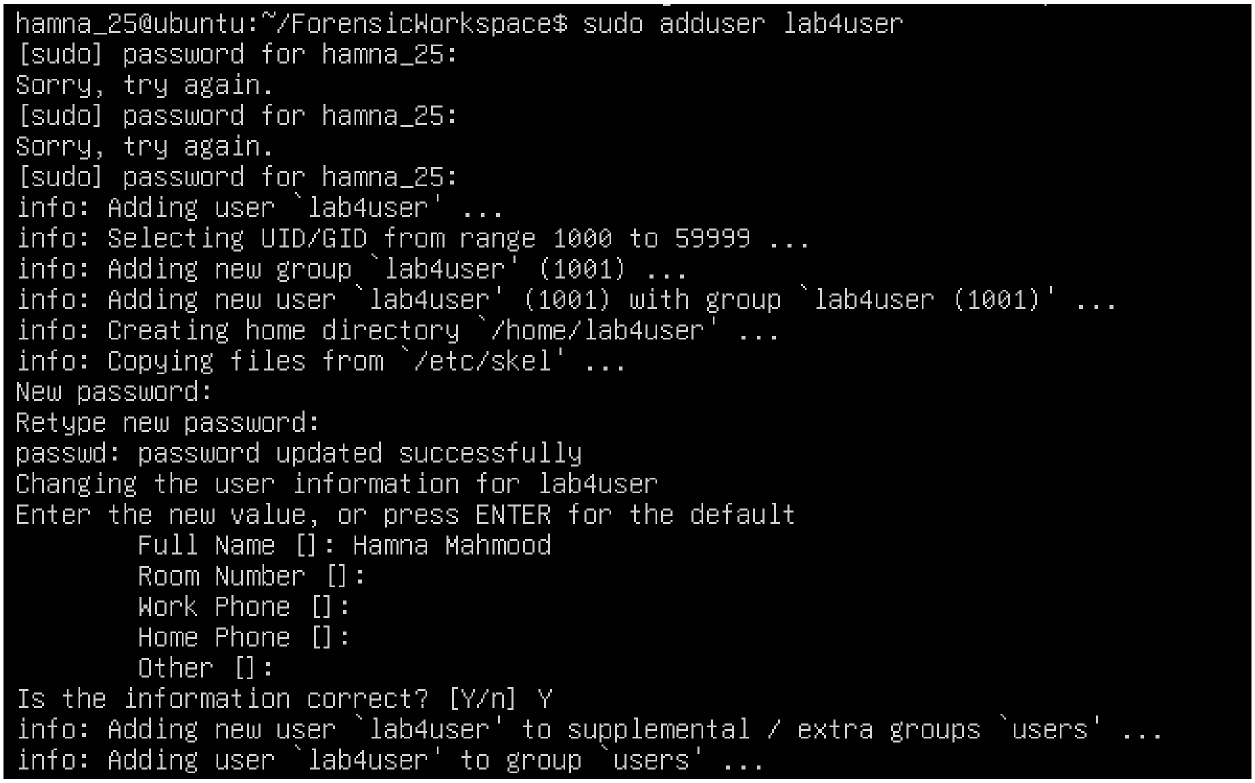
```
hamna_25@ubuntu:~/ForensicWorkspace$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              387M  1.5M  386M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   12G  4.9G  5.8G  46% /
tmpfs                              1.9G     0  1.9G   0% /dev/shm
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
```

Display all active running processes to identify suspicious activity.



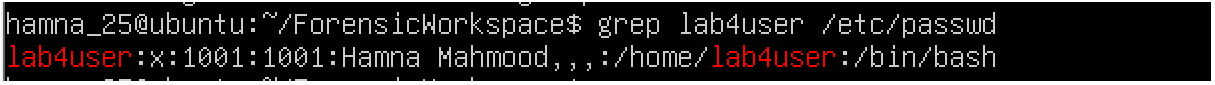
```
root         606  0.0  0.0      0     0 ?        I<   15:24   0:00 [kworker/R-ext4-]
root         613  0.0  0.0      0     0 ?        S    15:24   0:00 [irq/57-vmw_vmci]
root         614  0.0  0.0      0     0 ?        S    15:24   0:00 [irq/58-vmw_vmci]
root         615  0.0  0.0      0     0 ?        S    15:24   0:00 [irq/59-vmw_vmci]
systemd+     635  0.0  0.2  19008  9344 ?        Ss   15:24   0:00 /usr/lib/systemd/systemd-networkd
root         638  0.0  0.0      0     0 ?        S    15:24   0:00 [irq/16-vmwgfx]
root         639  0.0  0.0      0     0 ?        I<   15:24   0:00 [kworker/R-ttm]
systemd+     653  0.0  0.3  21588 12800 ?        Ss   15:24   0:00 /usr/lib/systemd/systemd-resolved
systemd+     661  0.0  0.1  91024  7808 ?        Ssl  15:24   0:00 /usr/lib/systemd/systemd-timesyncd
root         718  0.0  0.0      0     0 ?        I<   15:24   0:00 [kworker/R-cfg80]
root         841  0.0  0.2  53464 11776 ?        Ss   15:24   0:00 /usr/bin/VGAuthService
root         842  0.9  0.2 242132  9216 ?        Ssl  15:24   0:35 /usr/bin/vmtoolsd
message+     869  0.0  0.1   9884  5376 ?        Ss   15:24   0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-o
polkitd      911  0.0  0.1 308164  7808 ?        Ssl  15:24   0:00 /usr/lib/polkit-1/polkitd --no-debug
root         917  0.0  0.2  18140  8704 ?        Ss   15:24   0:00 /usr/lib/systemd/systemd-logind
root         918  0.0  0.3 468956 13568 ?        Ssl  15:24   0:00 /usr/libexec/udisks2/udisksd
syslog       927  0.0  0.1 222508  6656 ?        Ssl  15:24   0:00 /usr/sbin/rsyslogd -n -iNONE
root         930  0.0  0.5 109692 22656 ?        Ssl  15:24   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root         935  0.0  0.0   6824  2688 ?        Ss   15:24   0:00 /usr/sbin/cron -f -P
root         957  0.0  0.1   6980  4712 tty1     Ss   15:24   0:00 /bin/login -p --
root         973  0.0  0.2  12020  8064 ?        Ss   15:24   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root         981  0.0  0.3 318296 12672 ?        Ssl  15:24   0:00 /usr/sbin/ModemManager
root        1217  0.1  1.0 596200 43468 ?        Ssl  15:24   0:04 /usr/libexec/fwupd/fwupd
root        1284  0.0  0.2 314000  8960 ?        Ssl  15:24   0:00 /usr/libexec/upowerd
root        1415  0.0  0.0      0     0 ?        S    15:24   0:00 [psimon]
hamna_25    1418  0.0  0.2  20272 11264 ?        Ss   15:24   0:00 /usr/lib/systemd/systemd --user
hamna_25    1419  0.0  0.0  21148  3516 ?        S    15:24   0:00 (sd-pam)
hamna_25    1427  0.0  0.1   8784  5632 tty1     S    15:24   0:00 -bash
root        1474  0.0  0.0      0     0 ?        I<   15:24   0:00 [kworker/R-tls-s]
root        1520  0.0  0.2  14960 10400 ?        Ss   15:25   0:00 sshd: hamna_25 [priv]
hamna_25    1574  0.0  0.1  15092  6976 ?        S    15:25   0:01 sshd: hamna_25@pts/0
hamna_25    1575  0.0  0.1   8648  5376 pts/0    Ss+  15:25   0:00 -bash
root        1635  0.0  0.0      0     0 ?        I    15:45   0:00 [kworker/u258:0-events_power_efficient]
root        1642  0.2  0.0      0     0 ?        I    15:50   0:05 [kworker/1:3-events]
root        1643  0.0  0.0      0     0 ?        I<   15:50   0:00 [kworker/1:1H-kblockd]
root        1650  0.0  0.0      0     0 ?        I    15:54   0:00 [kworker/u258:1-events_power_efficient]
root        1669  0.0  0.0      0     0 ?        I    15:58   0:00 [kworker/u257:2-flush-252:0]
```

5. **User Account Audit & Privilege Escalation Simulation**
   Create a new test user named lab4user.



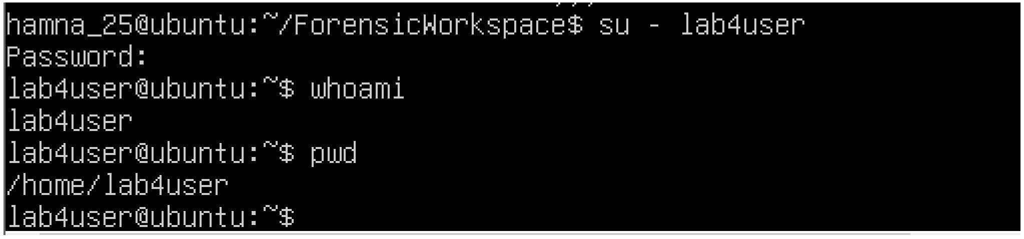
```
hamna_25@ubuntu:~/ForensicWorkspace$ sudo adduser lab4user
[sudo] password for hamna_25:
Sorry, try again.
[sudo] password for hamna_25:
Sorry, try again.
[sudo] password for hamna_25:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (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 []: Hamna Mahmood
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
```

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



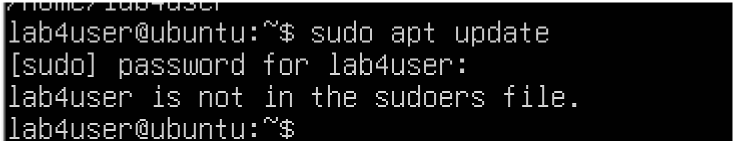
```
hamna_25@ubuntu:~/ForensicWorkspace$ grep lab4user /etc/passwd
lab4user:x:1001:1001:Hamna Mahmood,,,:/home/lab4user:/bin/bash
```

Log in as lab4user and confirm successful login.



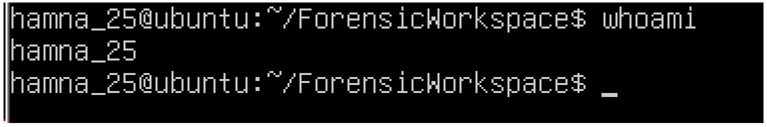
```
hamna_25@ubuntu:~/ForensicWorkspace$ su - lab4user
Password:
lab4user@ubuntu:~$ whoami
lab4user
lab4user@ubuntu:~$ pwd
/home/lab4user
lab4user@ubuntu:~$
```

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



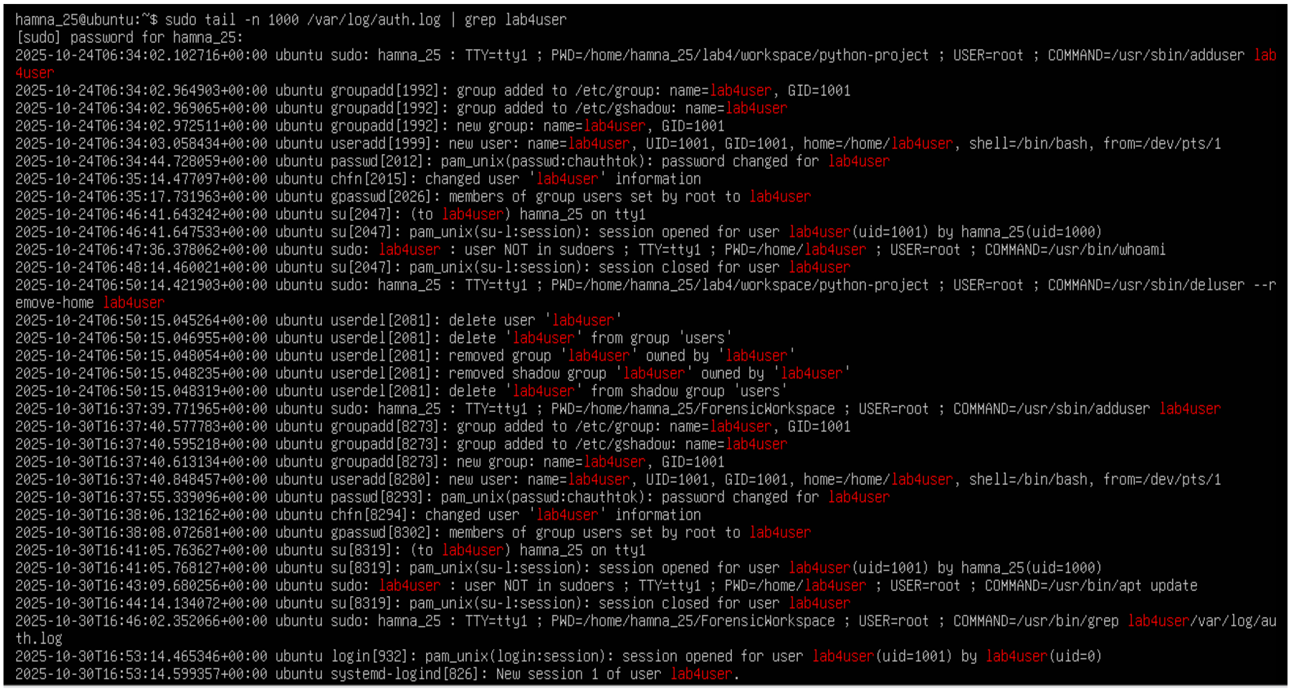
```
lab4user@ubuntu:~$ sudo apt update
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu:~$
```

Switch back to your main analyst account.



```
hamna_25@ubuntu:~/ForensicWorkspace$ whoami
hamna_25
hamna_25@ubuntu:~/ForensicWorkspace$ _
```

Inspect the system authentication logs located at /var/log/auth.log to determine whether the lab4user account attempted any logins (successful or failed).



```
hamna_25@ubuntu:~$ sudo tail -n 1000 /var/log/auth.log | grep lab4user
[sudo] password for hamna_25:
2025-10-24T06:34:02.102716+00:00 ubuntu sudo: hamna_25 : TTY=tty1 ; PWD=/home/hamna_25/lab4/workspace/python-project ; USER=root ; COMMAND=/usr/sbin/adduser lab
4user
2025-10-24T06:34:02.964903+00:00 ubuntu groupadd[1992]: group added to /etc/group: name=lab4user, GID=1001
2025-10-24T06:34:02.969065+00:00 ubuntu groupadd[1992]: group added to /etc/gshadow: name=lab4user
2025-10-24T06:34:02.972511+00:00 ubuntu groupadd[1992]: new group: name=lab4user, GID=1001
2025-10-24T06:34:03.058434+00:00 ubuntu useradd[1999]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/bin/bash, from=/dev/pts/1
2025-10-24T06:34:44.728059+00:00 ubuntu passwd[2012]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-24T06:35:14.477097+00:00 ubuntu chfn[2015]: changed user 'lab4user' information
2025-10-24T06:35:17.731963+00:00 ubuntu gpasswd[2026]: members of group users set by root to lab4user
2025-10-24T06:46:41.643242+00:00 ubuntu su[2047]: (to lab4user) hamna_25 on tty1
2025-10-24T06:46:41.647533+00:00 ubuntu su[2047]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by hamna_25(uid=1000)
2025-10-24T06:47:36.378062+00:00 ubuntu sudo: lab4user : user NOT in sudoers ; TTY=tty1 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/whoami
2025-10-24T06:48:14.460021+00:00 ubuntu su[2047]: pam_unix(su-l:session): session closed for user lab4user
2025-10-24T06:50:14.421903+00:00 ubuntu sudo: hamna_25 : TTY=tty1 ; PWD=/home/hamna_25/lab4/workspace/python-project ; USER=root ; COMMAND=/usr/sbin/deluser --r
emove-home lab4user
2025-10-24T06:50:15.045264+00:00 ubuntu userdel[2081]: delete user 'lab4user'
2025-10-24T06:50:15.046955+00:00 ubuntu userdel[2081]: delete 'lab4user' from group 'users'
2025-10-24T06:50:15.048054+00:00 ubuntu userdel[2081]: removed group 'lab4user' owned by 'lab4user'
2025-10-24T06:50:15.048235+00:00 ubuntu userdel[2081]: removed shadow group 'lab4user' owned by 'lab4user'
2025-10-24T06:50:15.048319+00:00 ubuntu userdel[2081]: delete 'lab4user' from shadow group 'users'
2025-10-30T16:37:39.771965+00:00 ubuntu sudo: hamna_25 : TTY=tty1 ; PWD=/home/hamna_25/ForensicWorkspace ; USER=root ; COMMAND=/usr/sbin/adduser lab4user
2025-10-30T16:37:40.577783+00:00 ubuntu groupadd[8273]: group added to /etc/group: name=lab4user, GID=1001
2025-10-30T16:37:40.595218+00:00 ubuntu groupadd[8273]: group added to /etc/gshadow: name=lab4user
2025-10-30T16:37:40.613134+00:00 ubuntu groupadd[8273]: new group: name=lab4user, GID=1001
2025-10-30T16:37:40.848457+00:00 ubuntu useradd[8280]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/bin/bash, from=/dev/pts/1
2025-10-30T16:37:55.339096+00:00 ubuntu passwd[8293]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-30T16:38:06.132162+00:00 ubuntu chfn[8294]: changed user 'lab4user' information
2025-10-30T16:38:08.072681+00:00 ubuntu gpasswd[8302]: members of group users set by root to lab4user
2025-10-30T16:41:05.763627+00:00 ubuntu su[8319]: (to lab4user) hamna_25 on tty1
2025-10-30T16:41:05.768127+00:00 ubuntu su[8319]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by hamna_25(uid=1000)
2025-10-30T16:43:09.680256+00:00 ubuntu sudo: lab4user : user NOT in sudoers ; TTY=tty1 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/apt update
2025-10-30T16:44:14.134072+00:00 ubuntu su[8319]: pam_unix(su-l:session): session closed for user lab4user
2025-10-30T16:46:02.352066+00:00 ubuntu sudo: hamna_25 : TTY=tty1 ; PWD=/home/hamna_25/ForensicWorkspace ; USER=root ; COMMAND=/usr/bin/grep lab4user/var/log/au
th.log
2025-10-30T16:53:14.465346+00:00 ubuntu login[932]: pam_unix(login:session): session opened for user lab4user(uid=1001) by lab4user(uid=0)
2025-10-30T16:53:14.599357+00:00 ubuntu systemd-logind[826]: New session 1 of user lab4user.
```