Fatima Jinnah Women University

Opening Portals of Excellence Through Higher Education

DEPARTMENT OF SOFTWARE ENGINEERING

LAB#4

SUBMITTED TO:

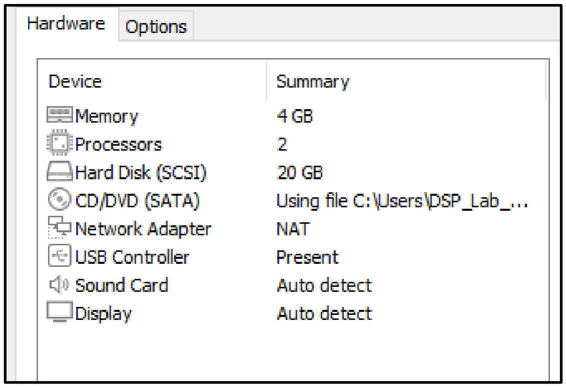
ENGR. MUHAMMAD SHOAIB

ENGR. WAQAS SALEEM

SUBMITTED BY: NEHA AMJAD

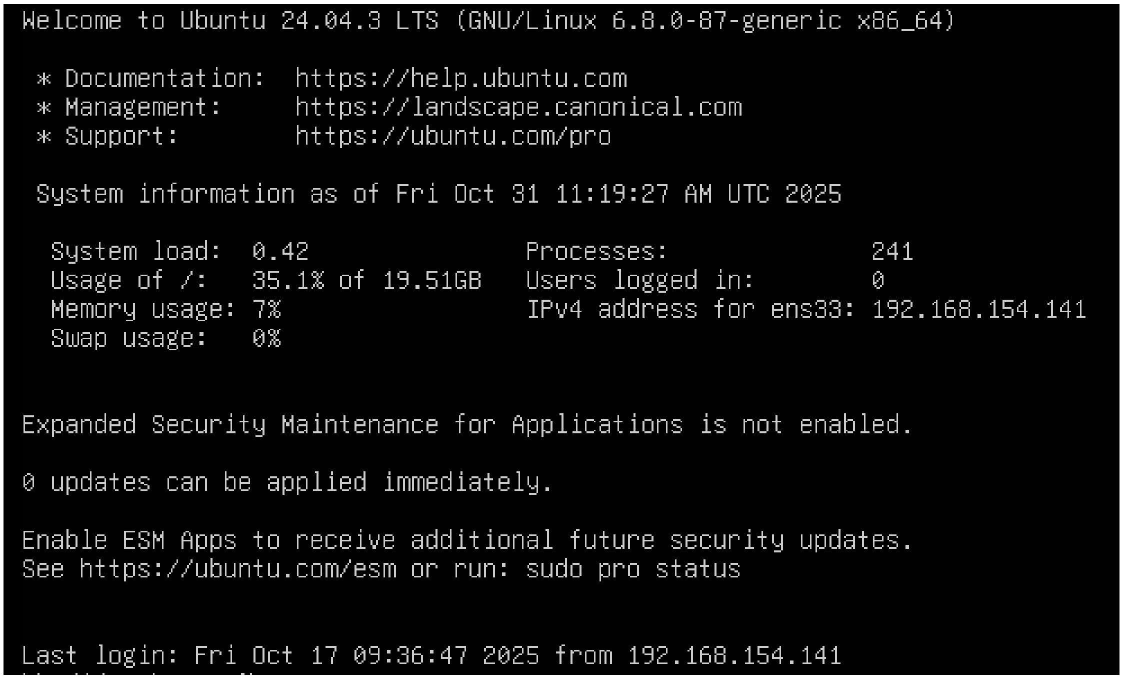
REG NO: 2021-BSE-024

Task 1: Verify VM resources in VMware

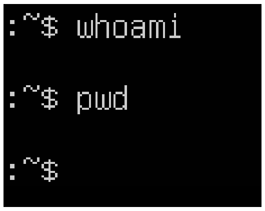


Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\Users\DSP_Lab_...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

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

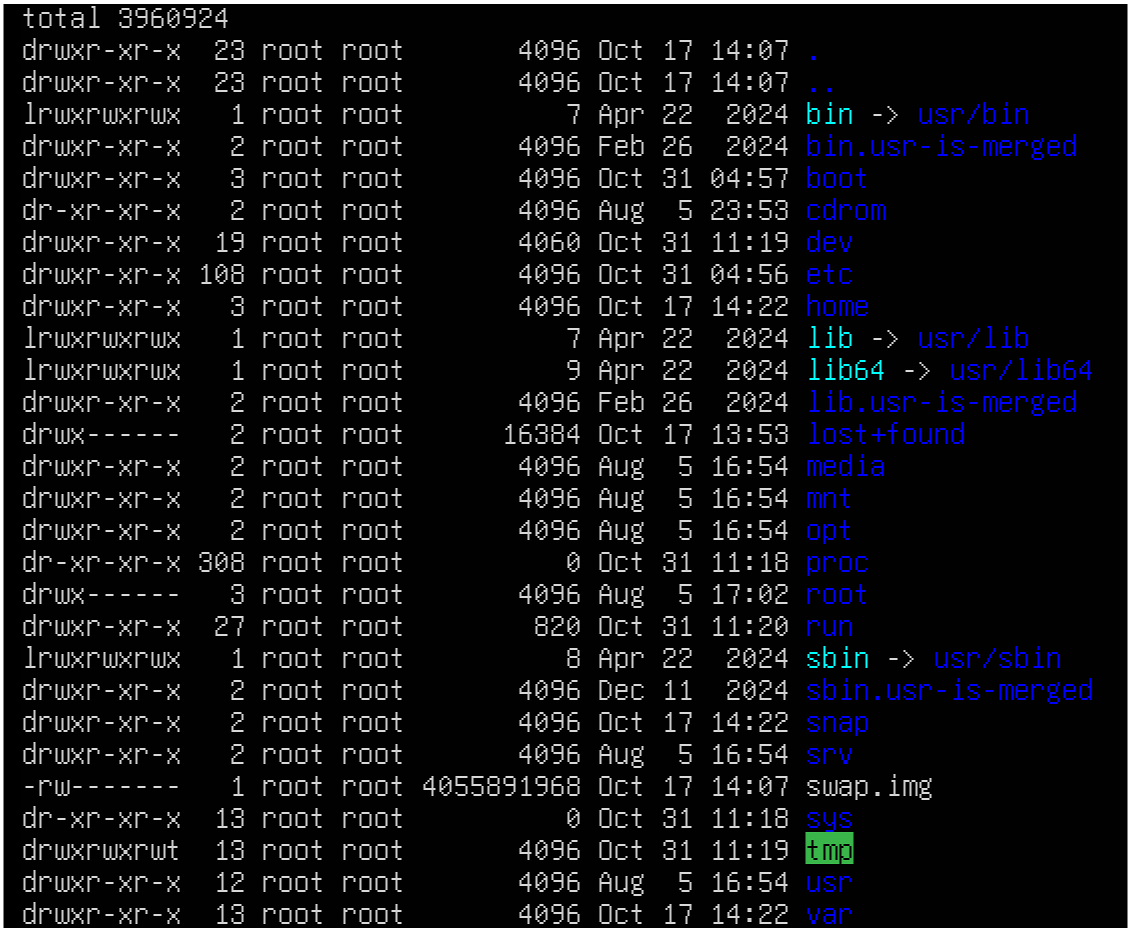


```
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

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

 System information as of Fri Oct 31 11:19:27 AM UTC 2025

  System load:  0.42               Processes:             241
  Usage of /:   35.1% of 19.51GB   Users logged in:       0
  Memory usage: 7%                 IPv4 address for ens33: 192.168.154.141
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


Last login: Fri Oct 17 09:36:47 2025 from 192.168.154.141
```

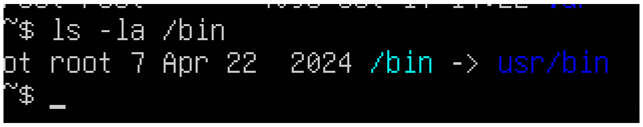


```
:~$ whoami

:~$ pwd

:~$
```

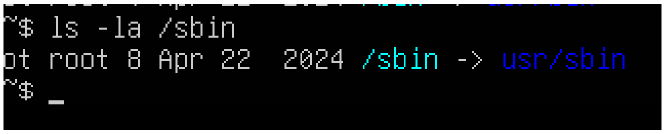
Task 3 – Filesystem exploration — root tree and dotfiles



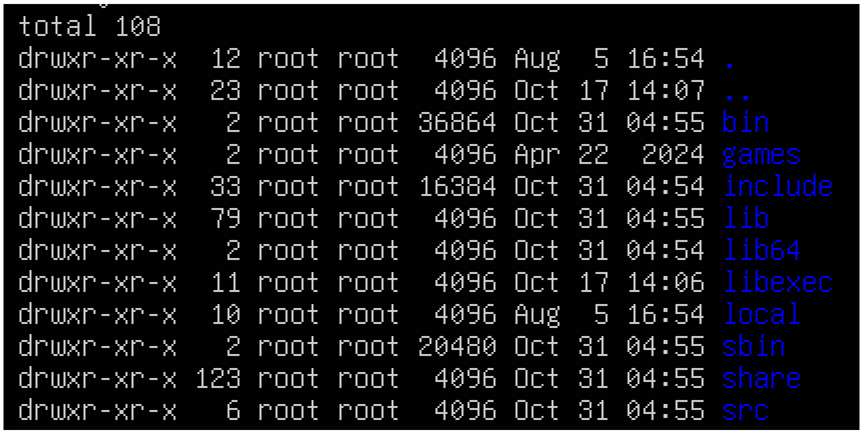
```
total 3960924
drwxr-xr-x  23 root root       4096 Oct 17 14:07 .
drwxr-xr-x  23 root root       4096 Oct 17 14:07 ..
lrwxrwxrwx   1 root root          7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x   2 root root       4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x   3 root root       4096 Oct 31 04:57 boot
dr-xr-xr-x   2 root root       4096 Aug  5 23:53 cdrom
drwxr-xr-x  19 root root       4060 Oct 31 11:19 dev
drwxr-xr-x 108 root root       4096 Oct 31 04:56 etc
drwxr-xr-x   3 root root       4096 Oct 17 14:22 home
lrwxrwxrwx   1 root root          7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx   1 root root          9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x   2 root root       4096 Feb 26  2024 lib.usr-is-merged
drwx------   2 root root      16384 Oct 17 13:53 lost+found
drwxr-xr-x   2 root root       4096 Aug  5 16:54 media
drwxr-xr-x   2 root root       4096 Aug  5 16:54 mnt
drwxr-xr-x   2 root root       4096 Aug  5 16:54 opt
dr-xr-xr-x 308 root root          0 Oct 31 11:18 proc
drwx------   3 root root       4096 Aug  5 17:02 root
drwxr-xr-x  27 root root        820 Oct 31 11:20 run
lrwxrwxrwx   1 root root          8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root       4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x   2 root root       4096 Oct 17 14:22 snap
drwxr-xr-x   2 root root       4096 Aug  5 16:54 srv
-rw-------   1 root root 4055891968 Oct 17 14:07 swap.img
dr-xr-xr-x  13 root root          0 Oct 31 11:18 sys
drwxrwxrwt  13 root root       4096 Oct 31 11:19 tmp
drwxr-xr-x  12 root root       4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root       4096 Oct 17 14:22 var
```



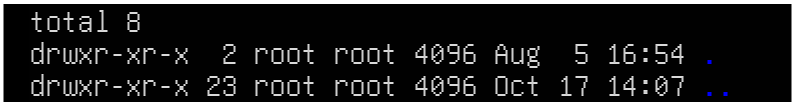
```
~$ ls -la /bin
ot root 7 Apr 22  2024 /bin -> usr/bin
~$ _
```



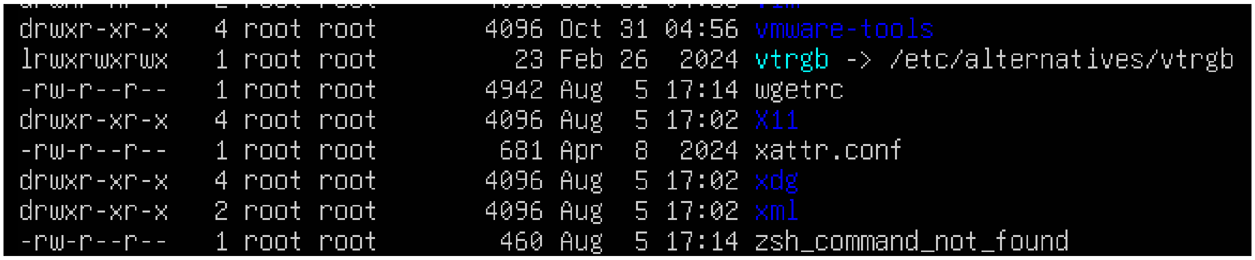
```
~$ ls -la /sbin
ot root 8 Apr 22  2024 /sbin -> usr/sbin
~$ _
```



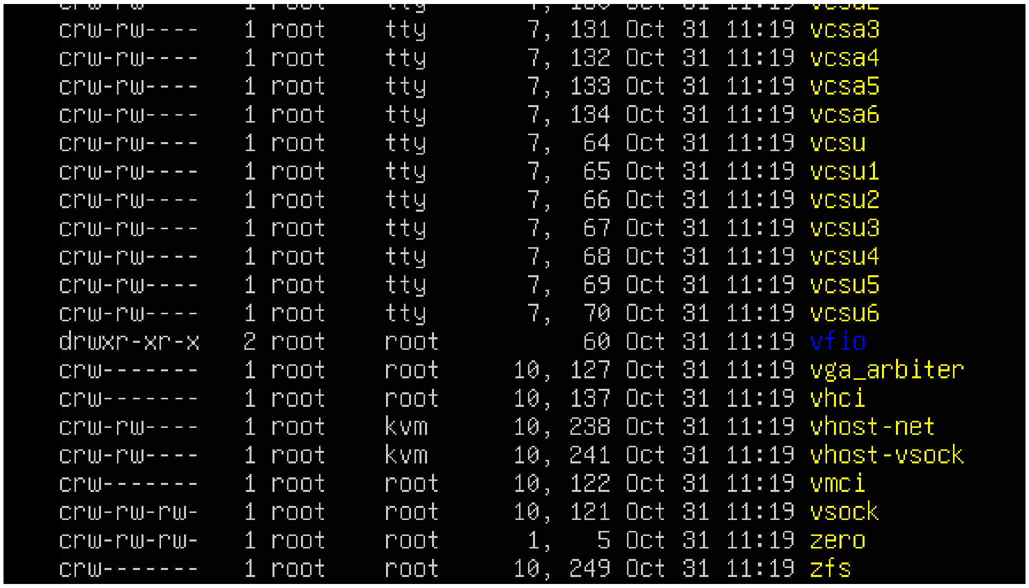
```
total 108
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Oct 17 14:07 ..
drwxr-xr-x   2 root root 36864 Oct 31 04:55 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root 16384 Oct 31 04:54 include
drwxr-xr-x  79 root root  4096 Oct 31 04:55 lib
drwxr-xr-x   2 root root  4096 Oct 31 04:54 lib64
drwxr-xr-x  11 root root  4096 Oct 17 14:06 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Oct 31 04:55 sbin
drwxr-xr-x 123 root root  4096 Oct 31 04:55 share
drwxr-xr-x   6 root root  4096 Oct 31 04:55 src
```



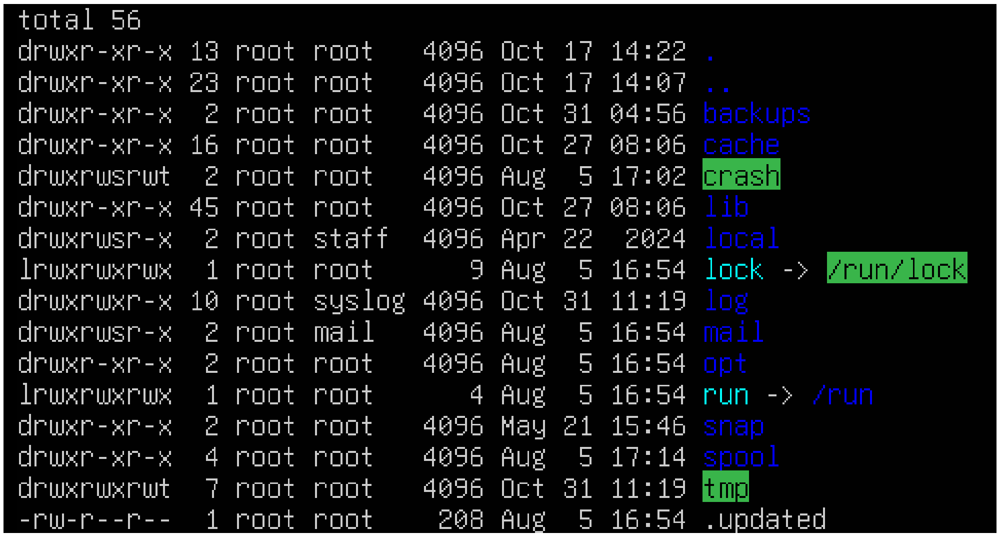
```
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Oct 17 14:07 ..
```



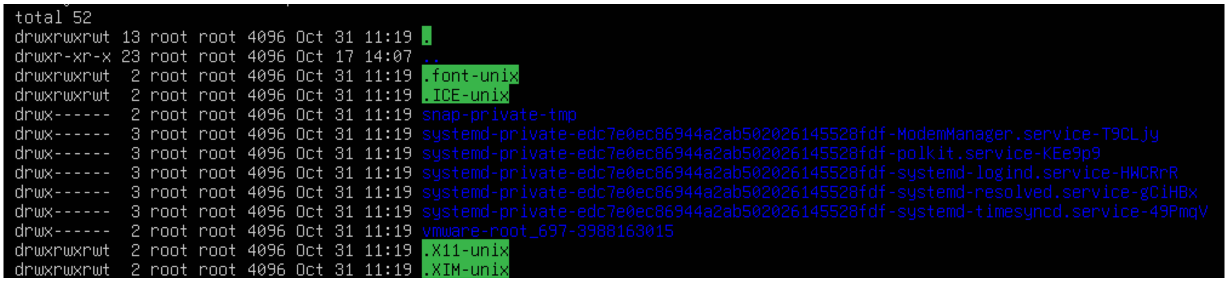
```
drwxr-xr-x   4 root root       4096 Oct 31 04:56 vmware-tools
lrwxrwxrwx   1 root root         23 Feb 26  2024 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r--   1 root root       4942 Aug  5 17:14 wgetrc
drwxr-xr-x   4 root root       4096 Aug  5 17:02 X11
-rw-r--r--   1 root root        681 Apr  8  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
```



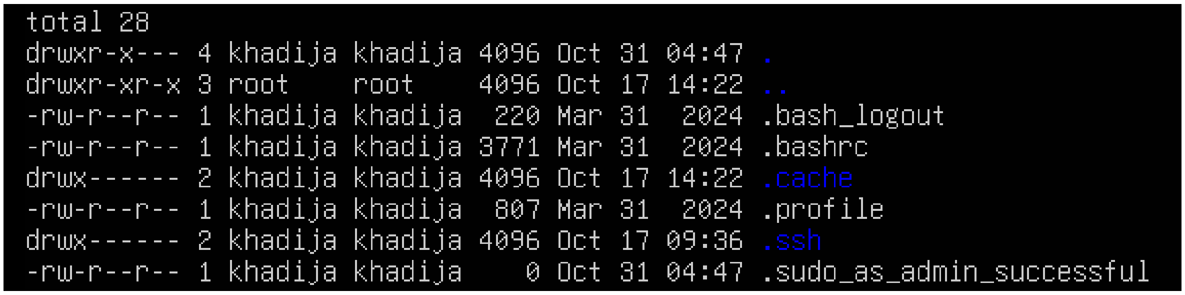
```
crw-rw----   1 root    tty       7, 131 Oct 31 11:19 vcsa3
crw-rw----   1 root    tty       7, 132 Oct 31 11:19 vcsa4
crw-rw----   1 root    tty       7, 133 Oct 31 11:19 vcsa5
crw-rw----   1 root    tty       7, 134 Oct 31 11:19 vcsa6
crw-rw----   1 root    tty       7,  64 Oct 31 11:19 vcsu
crw-rw----   1 root    tty       7,  65 Oct 31 11:19 vcsu1
crw-rw----   1 root    tty       7,  66 Oct 31 11:19 vcsu2
crw-rw----   1 root    tty       7,  67 Oct 31 11:19 vcsu3
crw-rw----   1 root    tty       7,  68 Oct 31 11:19 vcsu4
crw-rw----   1 root    tty       7,  69 Oct 31 11:19 vcsu5
crw-rw----   1 root    tty       7,  70 Oct 31 11:19 vcsu6
drwxr-xr-x   2 root    root          60 Oct 31 11:19 vfio
crw-------   1 root    root     10, 127 Oct 31 11:19 vga_arbiter
crw-------   1 root    root     10, 137 Oct 31 11:19 vhci
crw-rw----   1 root    kvm      10, 238 Oct 31 11:19 vhost-net
crw-rw----   1 root    kvm      10, 241 Oct 31 11:19 vhost-vsock
crw-------   1 root    root     10, 122 Oct 31 11:19 vmci
crw-rw-rw-   1 root    root     10, 121 Oct 31 11:19 vsock
crw-rw-rw-   1 root    root      1,   5 Oct 31 11:19 zero
crw-------   1 root    root     10, 249 Oct 31 11:19 zfs
```



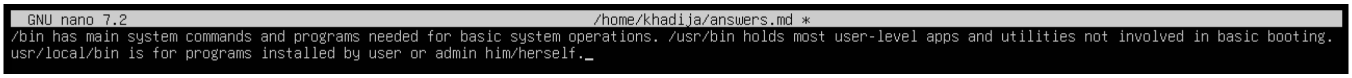
```
total 56
drwxr-xr-x 13 root root   4096 Oct 17 14:22 .
drwxr-xr-x 23 root root   4096 Oct 17 14:07 ..
drwxr-xr-x  2 root root   4096 Oct 31 04:56 backups
drwxr-xr-x 16 root root   4096 Oct 27 08:06 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct 27 08:06 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 31 11:19 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  7 root root   4096 Oct 31 11:19 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
```



```
total 52
drwxrwxrwt 13 root root 4096 Oct 31 11:19 .
drwxr-xr-x 23 root root 4096 Oct 17 14:07 ..
drwxrwxrwt  2 root root 4096 Oct 31 11:19 .font-unix
drwxrwxrwt  2 root root 4096 Oct 31 11:19 .ICE-unix
drwx------  2 root root 4096 Oct 31 11:19 snap-private-tmp
drwx------  3 root root 4096 Oct 31 11:19 systemd-private-edc7e0ec86944a2ab502026145528fdf-ModemManager.service-T9CLjy
drwx------  3 root root 4096 Oct 31 11:19 systemd-private-edc7e0ec86944a2ab502026145528fdf-polkit.service-KEe9p9
drwx------  3 root root 4096 Oct 31 11:19 systemd-private-edc7e0ec86944a2ab502026145528fdf-systemd-logind.service-HWCRrR
drwx------  3 root root 4096 Oct 31 11:19 systemd-private-edc7e0ec86944a2ab502026145528fdf-systemd-resolved.service-gCiHBx
drwx------  3 root root 4096 Oct 31 11:19 systemd-private-edc7e0ec86944a2ab502026145528fdf-systemd-timesyncd.service-49PmqV
drwx------  2 root root 4096 Oct 31 11:19 vmware-root_697-3988163015
drwxrwxrwt  2 root root 4096 Oct 31 11:19 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 31 11:19 .XIM-unix
```

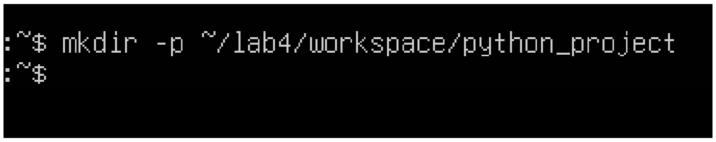


```
total 28
drwxr-x--- 4 khadija khadija 4096 Oct 31 04:47 .
drwxr-xr-x 3 root    root    4096 Oct 17 14:22 ..
-rw-r--r-- 1 khadija khadija  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 khadija khadija 3771 Mar 31  2024 .bashrc
drwx------ 2 khadija khadija 4096 Oct 17 14:22 .cache
-rw-r--r-- 1 khadija khadija  807 Mar 31  2024 .profile
drwx------ 2 khadija khadija 4096 Oct 17 09:36 .ssh
-rw-r--r-- 1 khadija khadija    0 Oct 31 04:47 .sudo_as_admin_successful
```

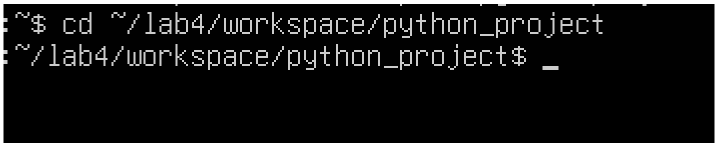


```
  GNU nano 7.2                                          /home/khadija/answers.md *
/bin has main system commands and programs needed for basic system operations. /usr/bin holds most user-level apps and utilities not involved in basic booting.
usr/local/bin is for programs installed by user or admin him/herself._
```

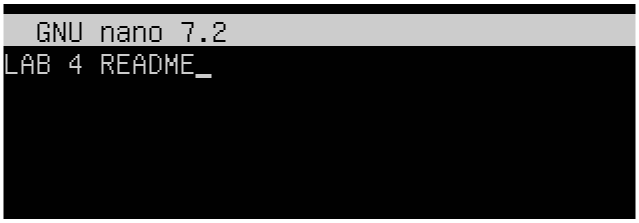
Task 4 – Essential CLI tasks — navigation and file operations



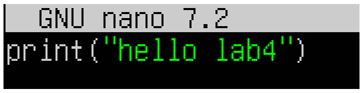
```
:~$ mkdir -p ~/lab4/workspace/python_project
:~$
```



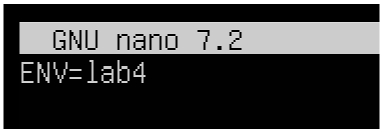
```
:~$ cd ~/lab4/workspace/python_project
:~/lab4/workspace/python_project$ _
```



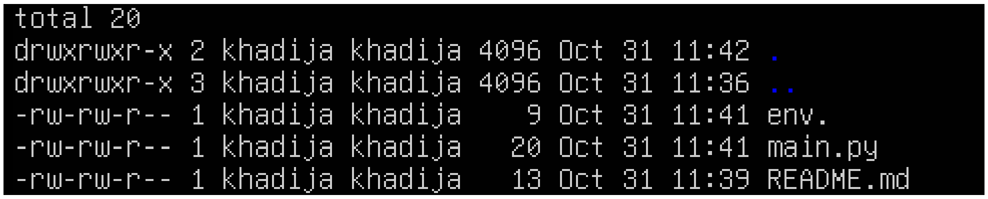
```
  GNU nano 7.2
LAB 4 README_
```



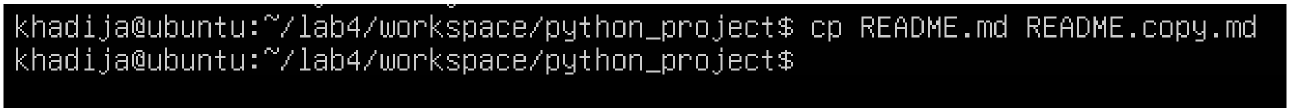
```
  GNU nano 7.2
print("hello lab4")
```



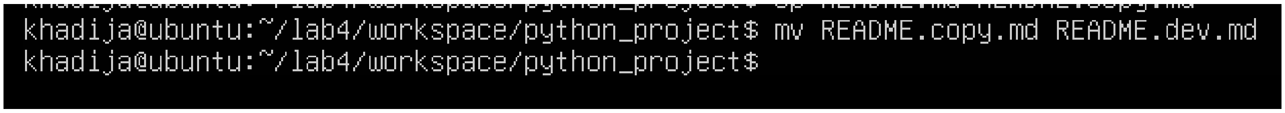
```
  GNU nano 7.2
ENV=lab4
```



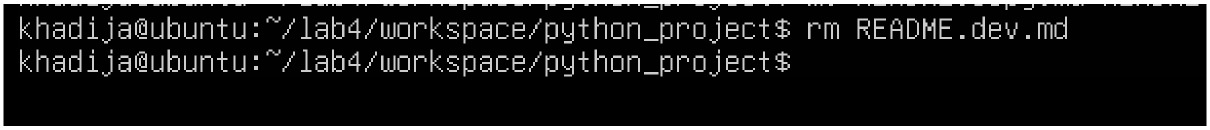
```
total 20
drwxrwxr-x 2 khadija khadija 4096 Oct 31 11:42 .
drwxrwxr-x 3 khadija khadija 4096 Oct 31 11:36 ..
-rw-rw-r-- 1 khadija khadija    9 Oct 31 11:41 env.
-rw-rw-r-- 1 khadija khadija   20 Oct 31 11:41 main.py
-rw-rw-r-- 1 khadija khadija   13 Oct 31 11:39 README.md
```



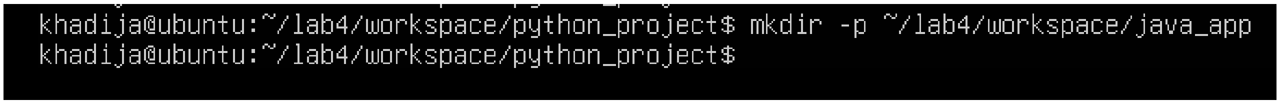
```
khadija@ubuntu:~/lab4/workspace/python_project$ cp README.md README.copy.md
khadija@ubuntu:~/lab4/workspace/python_project$
```



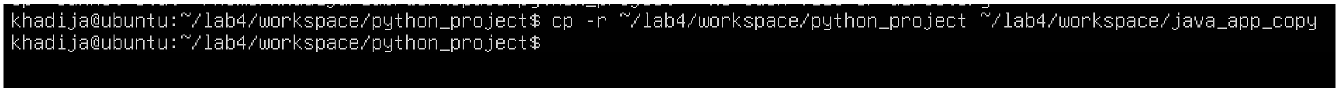
```
khadija@ubuntu:~/lab4/workspace/python_project$ mv README.copy.md README.dev.md
khadija@ubuntu:~/lab4/workspace/python_project$
```



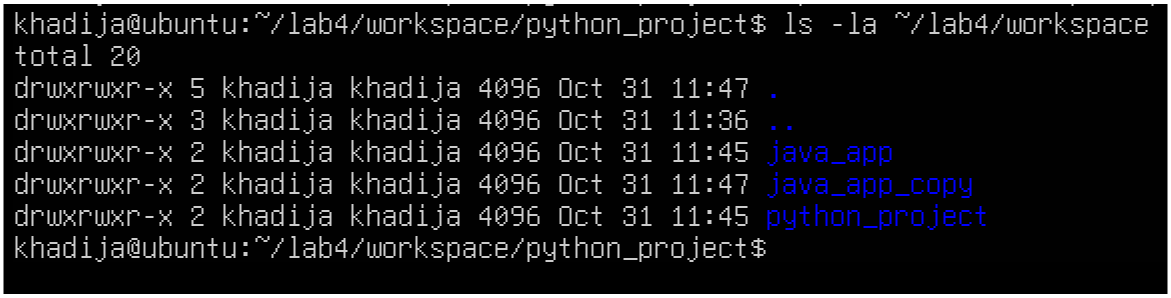
```
khadija@ubuntu:~/lab4/workspace/python_project$ rm README.dev.md
khadija@ubuntu:~/lab4/workspace/python_project$
```



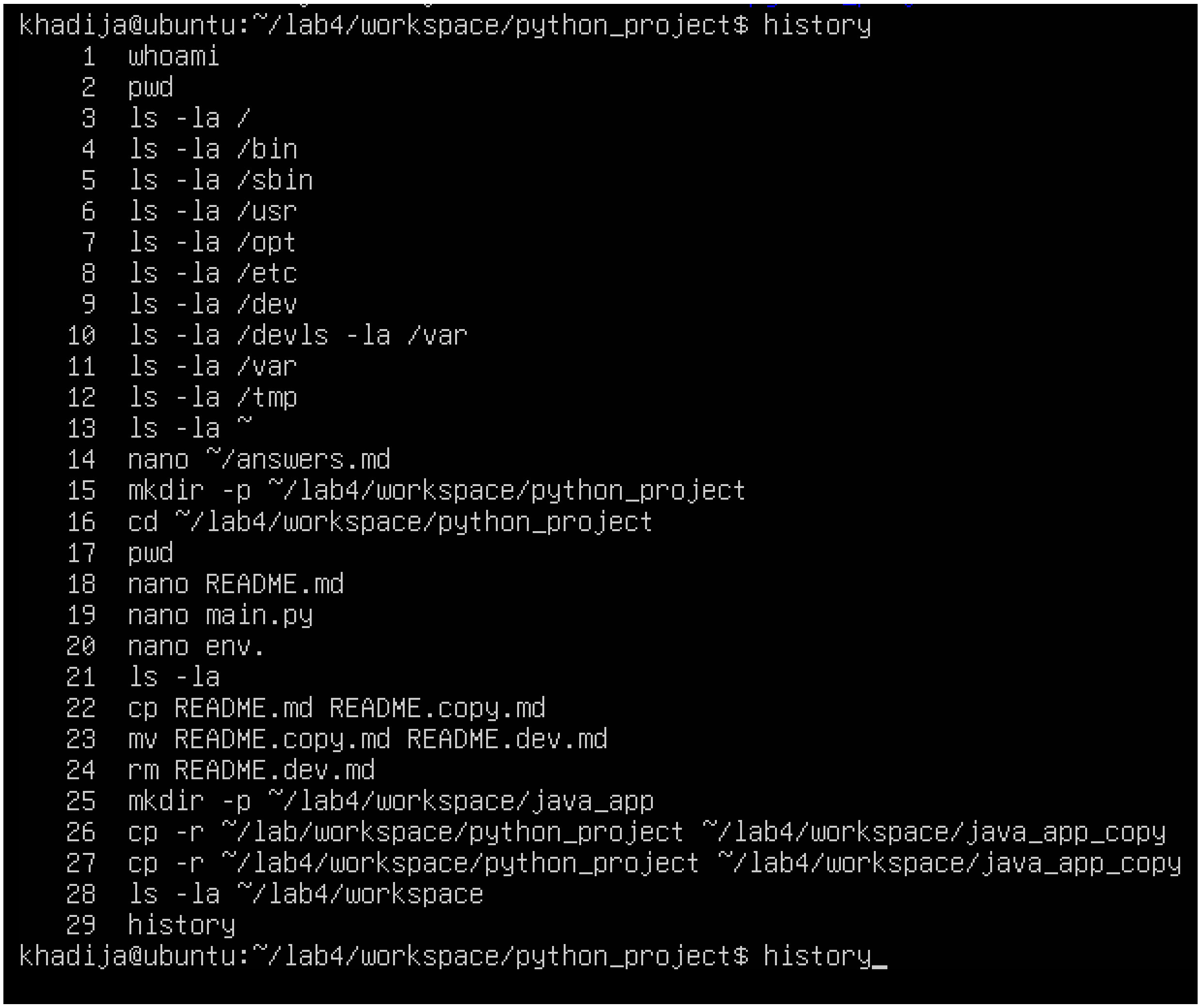
```
khadija@ubuntu:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
khadija@ubuntu:~/lab4/workspace/python_project$
```



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

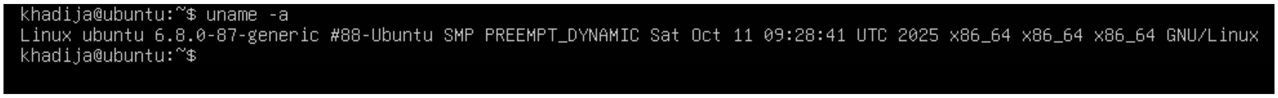


```
khadija@ubuntu:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 khadija khadija 4096 Oct 31 11:47 .
drwxrwxr-x 3 khadija khadija 4096 Oct 31 11:36 ..
drwxrwxr-x 2 khadija khadija 4096 Oct 31 11:45 java_app
drwxrwxr-x 2 khadija khadija 4096 Oct 31 11:47 java_app_copy
drwxrwxr-x 2 khadija khadija 4096 Oct 31 11:45 python_project
khadija@ubuntu:~/lab4/workspace/python_project$
```

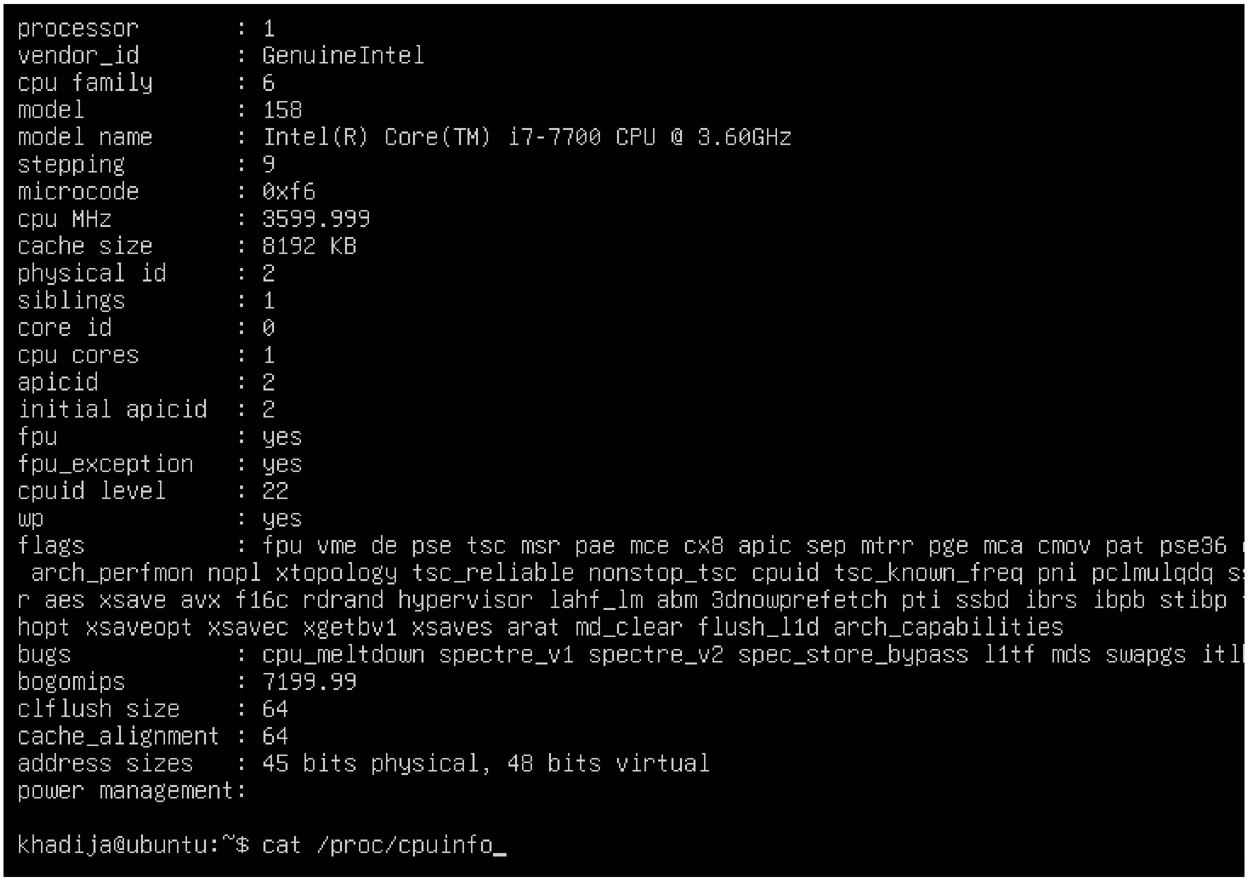


```
khadija@ubuntu:~/lab4/workspace/python_project$ history
    1  whoami
    2  pwd
    3  ls -la /
    4  ls -la /bin
    5  ls -la /sbin
    6  ls -la /usr
    7  ls -la /opt
    8  ls -la /etc
    9  ls -la /dev
   10  ls -la /devls -la /var
   11  ls -la /var
   12  ls -la /tmp
   13  ls -la ~
   14  nano ~/answers.md
   15  mkdir -p ~/lab4/workspace/python_project
   16  cd ~/lab4/workspace/python_project
   17  pwd
   18  nano README.md
   19  nano main.py
   20  nano env.
   21  ls -la
   22  cp README.md README.copy.md
   23  mv README.copy.md README.dev.md
   24  rm README.dev.md
   25  mkdir -p ~/lab4/workspace/java_app
   26  cp -r ~/lab/workspace/python_project ~/lab4/workspace/java_app_copy
   27  cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
   28  ls -la ~/lab4/workspace
   29  history
khadija@ubuntu:~/lab4/workspace/python_project$ history_
```

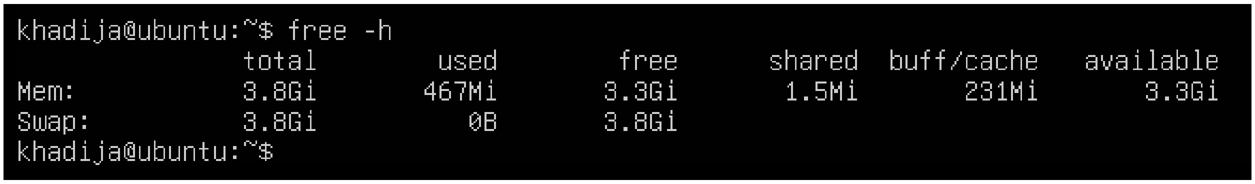
Task 5 – System info, resources & processes



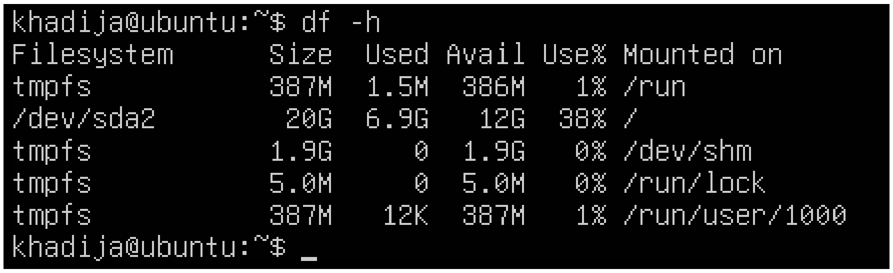
```
khadija@ubuntu:~$ uname -a
Linux ubuntu 6.8.0-87-generic #88-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 09:28:41 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
khadija@ubuntu:~$
```



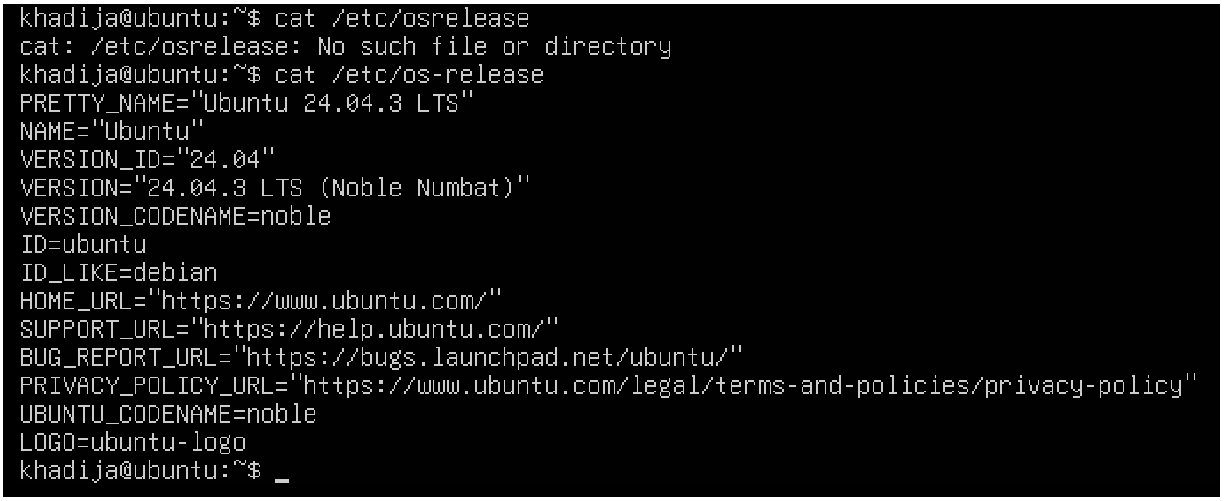
```
processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 158
model name      : Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
stepping        : 9
microcode       : 0xf6
cpu MHz         : 3599.999
cache size      : 8192 KB
physical id     : 2
siblings        : 1
core id         : 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
 arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq s
r aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp
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 itl
bogomips        : 7199.99
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:

khadija@ubuntu:~$ cat /proc/cpuinfo_
```



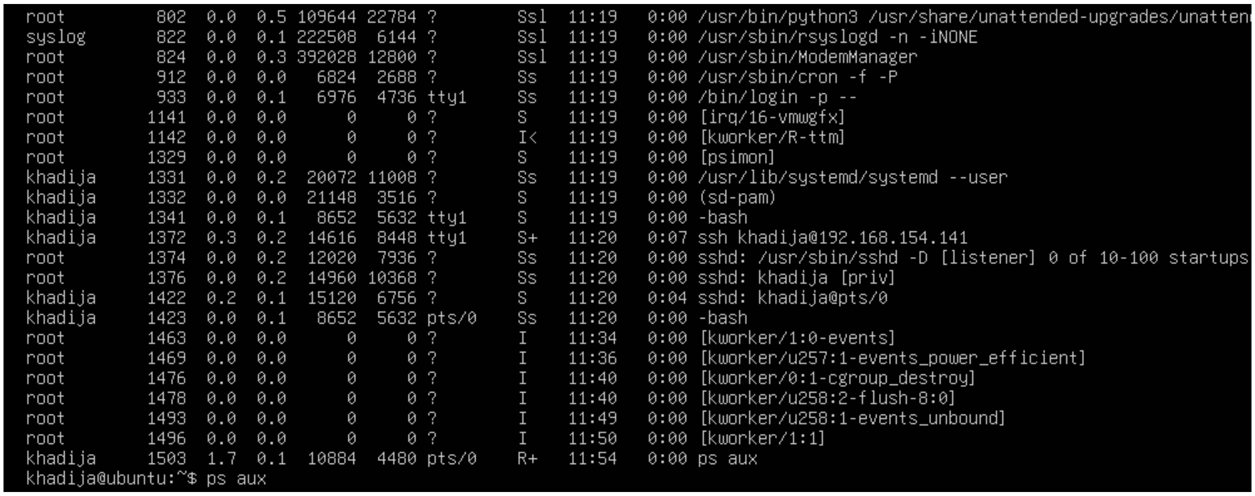
```
khadija@ubuntu:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       467Mi       3.3Gi       1.5Mi       231Mi       3.3Gi
Swap:          3.8Gi          0B       3.8Gi
khadija@ubuntu:~$
```



```
khadija@ubuntu:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           387M  1.5M  386M   1% /run
/dev/sda2        20G  6.9G   12G  38% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           387M   12K  387M   1% /run/user/1000
khadija@ubuntu:~$ _
```

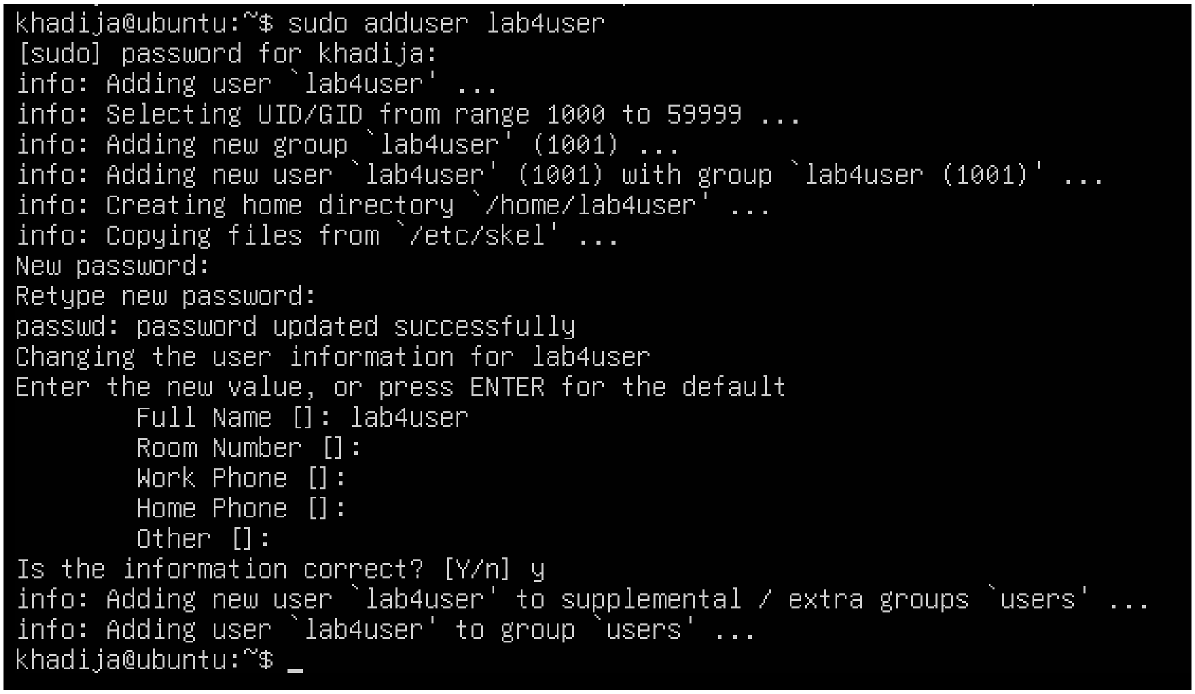


```
khadija@ubuntu:~$ cat /etc/osrelease
cat: /etc/osrelease: No such file or directory
khadija@ubuntu:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
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
khadija@ubuntu:~$ _
```

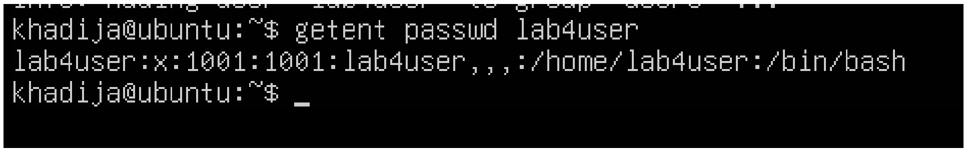


```
root         802  0.0  0.5 109644 22784 ?        Ssl  11:19   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unatten
syslog       822  0.0  0.1 222508  6144 ?        Ssl  11:19   0:00 /usr/sbin/rsyslogd -n -iNONE
root         824  0.0  0.3 392028 12800 ?        Ssl  11:19   0:00 /usr/sbin/ModemManager
root         912  0.0  0.0   6824  2688 ?        Ss   11:19   0:00 /usr/sbin/cron -f -P
root         933  0.0  0.1   6976  4736 tty1     Ss   11:19   0:00 /bin/login -p --
root        1141  0.0  0.0      0     0 ?        S    11:19   0:00 [irq/16-vmwgfx]
root        1142  0.0  0.0      0     0 ?        I<   11:19   0:00 [kworker/R-ttm]
root        1329  0.0  0.0      0     0 ?        S    11:19   0:00 [psimon]
khadija     1331  0.0  0.2  20072 11008 ?        Ss   11:19   0:00 /usr/lib/systemd/systemd --user
khadija     1332  0.0  0.0  21148  3516 ?        S    11:19   0:00 (sd-pam)
khadija     1341  0.0  0.1   8652  5632 tty1     S    11:19   0:00 -bash
khadija     1372  0.3  0.2  14616  8448 tty1     S+   11:20   0:07 ssh khadija@192.168.154.141
root        1374  0.0  0.2  12020  7936 ?        Ss   11:20   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        1376  0.0  0.2  14960 10368 ?        Ss   11:20   0:00 sshd: khadija [priv]
khadija     1422  0.2  0.1  15120  6756 ?        S    11:20   0:04 sshd: khadija@pts/0
khadija     1423  0.0  0.1   8652  5632 pts/0    Ss   11:20   0:00 -bash
root        1463  0.0  0.0      0     0 ?        I    11:34   0:00 [kworker/1:0-events]
root        1469  0.0  0.0      0     0 ?        I    11:36   0:00 [kworker/u257:1-events_power_efficient]
root        1476  0.0  0.0      0     0 ?        I    11:40   0:00 [kworker/0:1-cgroup_destroy]
root        1478  0.0  0.0      0     0 ?        I    11:40   0:00 [kworker/u258:2-flush-8:0]
root        1493  0.0  0.0      0     0 ?        I    11:49   0:00 [kworker/u258:1-events_unbound]
root        1496  0.0  0.0      0     0 ?        I    11:50   0:00 [kworker/1:1]
khadija     1503  1.7  0.1  10884  4480 pts/0    R+   11:54   0:00 ps aux
khadija@ubuntu:~$ ps aux
```

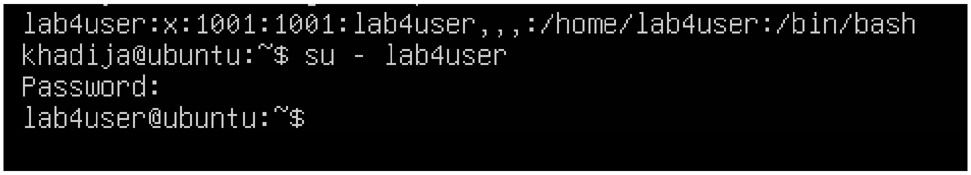
Task 6 – Users and account verification (no sudo group change)



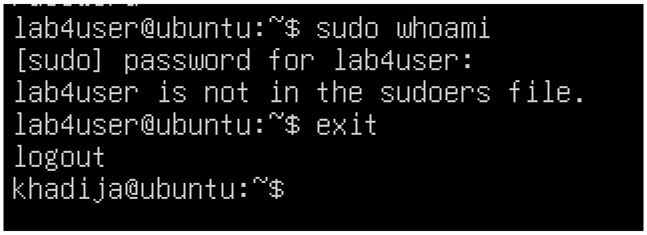
```
khadija@ubuntu:~$ sudo adduser lab4user
[sudo] password for khadija:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
info: Creating home directory `/home/lab4user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lab4user
Enter the new value, or press ENTER for the default
        Full Name []: lab4user
        Room Number []:
        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' ...
khadija@ubuntu:~$ _
```



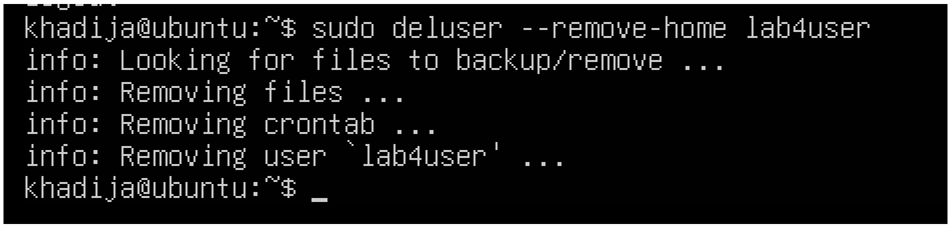
```
khadija@ubuntu:~$ getent passwd lab4user
lab4user:x:1001:1001:lab4user,,,:/home/lab4user:/bin/bash
khadija@ubuntu:~$ _
```



```
lab4user:x:1001:1001:lab4user,,,:/home/lab4user:/bin/bash
khadija@ubuntu:~$ su - lab4user
Password:
lab4user@ubuntu:~$
```



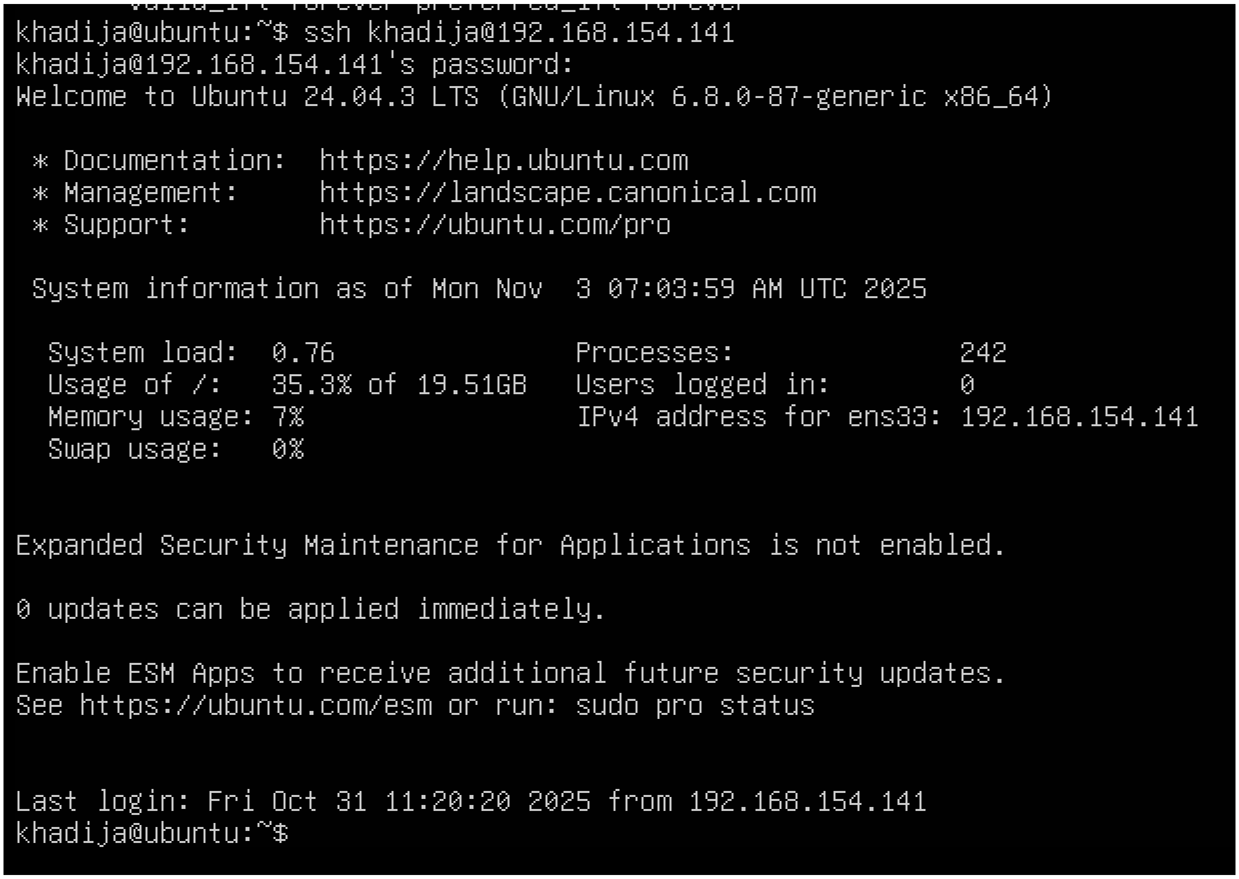
```
lab4user@ubuntu:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu:~$ exit
logout
khadija@ubuntu:~$
```



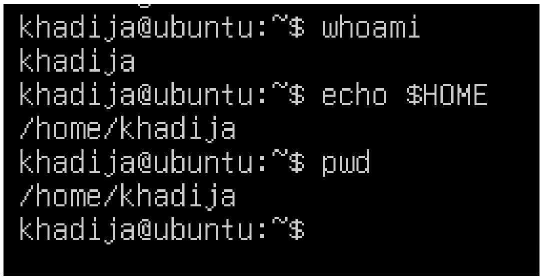
```
khadija@ubuntu:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
khadija@ubuntu:~$ _
```

Exam Evaluation Questions

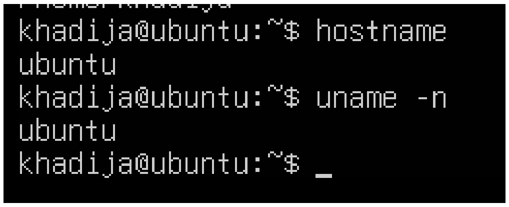
1. Remote Access Verification (Cyber Login Check)



```
       valid_lft forever preferred_lft forever
khadija@ubuntu:~$ ssh khadija@192.168.154.141
khadija@192.168.154.141'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 Mon Nov  3 07:03:59 AM UTC 2025

  System load:  0.76               Processes:              242
  Usage of /:   35.3% of 19.51GB   Users logged in:        0
  Memory usage: 7%                 IPv4 address for ens33: 192.168.154.141
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


Last login: Fri Oct 31 11:20:20 2025 from 192.168.154.141
khadija@ubuntu:~$
```

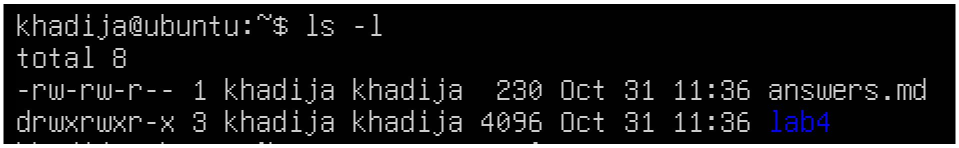


```
khadija@ubuntu:~$ whoami
khadija
khadija@ubuntu:~$ echo $HOME
/home/khadija
khadija@ubuntu:~$ pwd
/home/khadija
khadija@ubuntu:~$
```

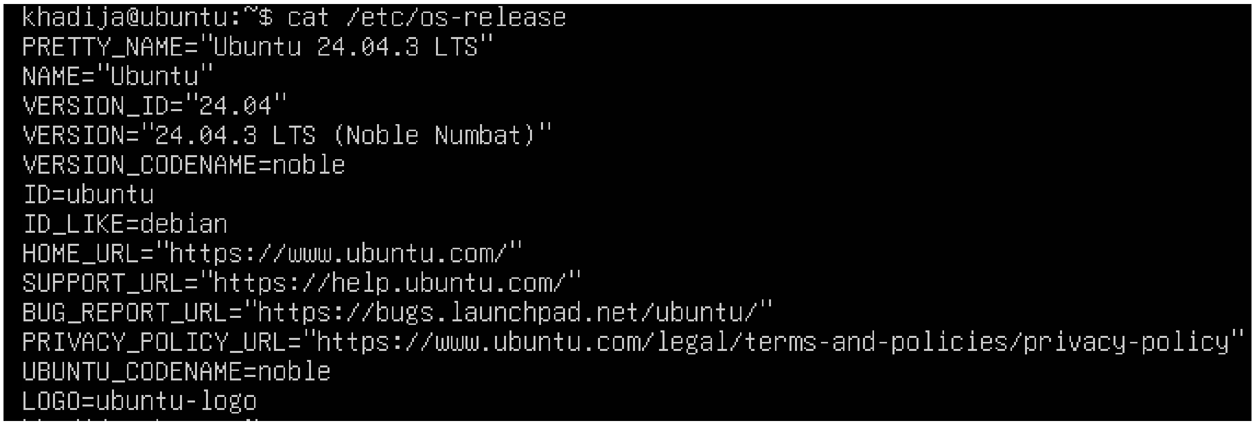


```
/home/khadija
khadija@ubuntu:~$ hostname
ubuntu
khadija@ubuntu:~$ uname -n
ubuntu
khadija@ubuntu:~$ _
```

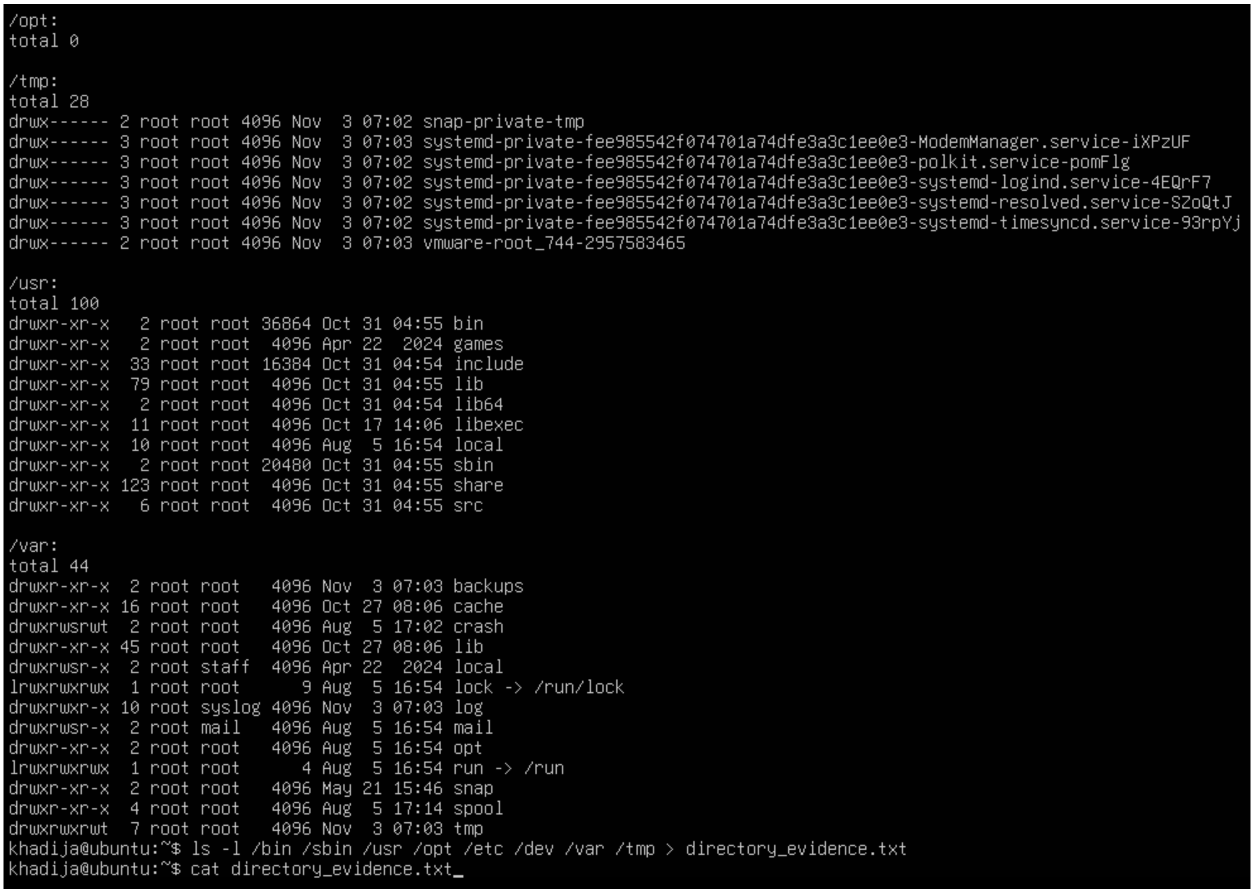
2. Filesystem Inspection for Forensic Evidence



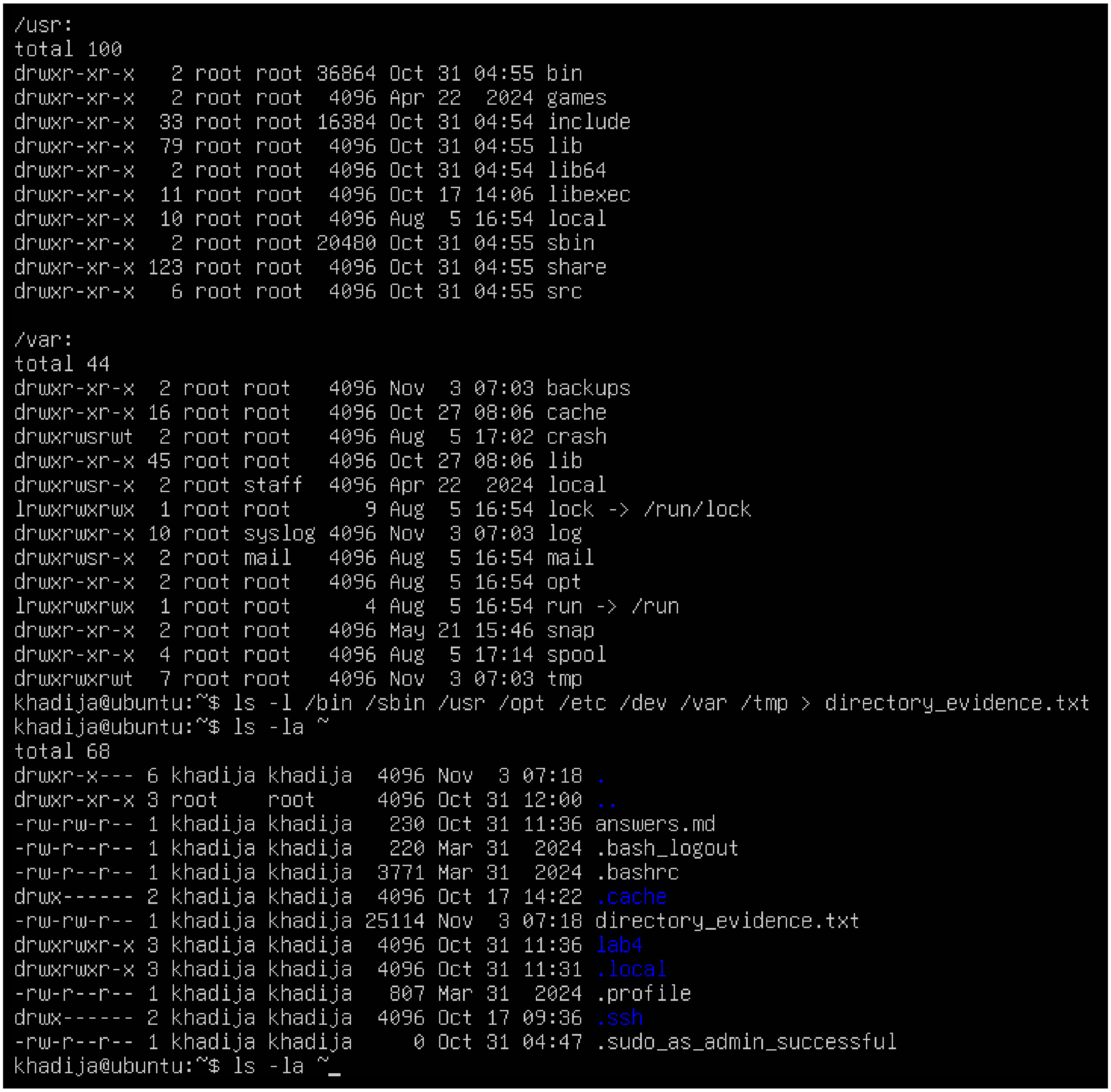
```
khadija@ubuntu:~$ ls -l
total 8
-rw-rw-r-- 1 khadija khadija  230 Oct 31 11:36 answers.md
drwxrwxr-x 3 khadija khadija 4096 Oct 31 11:36 lab4
```



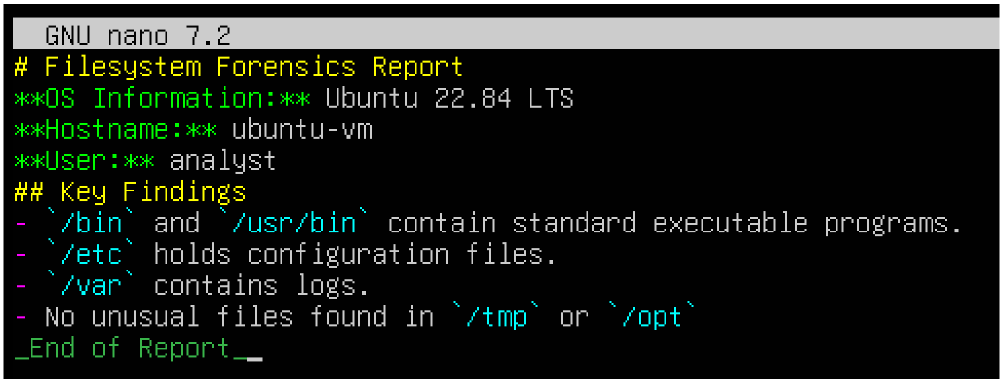
```
khadija@ubuntu:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"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



```
/opt:
total 0

/tmp:
total 28
drwx------ 2 root root 4096 Nov  3 07:02 snap-private-tmp
drwx------ 3 root root 4096 Nov  3 07:03 systemd-private-fee985542f074701a74dfe3a3c1ee0e3-ModemManager.service-iXPzUF
drwx------ 3 root root 4096 Nov  3 07:02 systemd-private-fee985542f074701a74dfe3a3c1ee0e3-polkit.service-pomFlg
drwx------ 3 root root 4096 Nov  3 07:02 systemd-private-fee985542f074701a74dfe3a3c1ee0e3-systemd-logind.service-4EQrF7
drwx------ 3 root root 4096 Nov  3 07:02 systemd-private-fee985542f074701a74dfe3a3c1ee0e3-systemd-resolved.service-SZoQtJ
drwx------ 3 root root 4096 Nov  3 07:02 systemd-private-fee985542f074701a74dfe3a3c1ee0e3-systemd-timesyncd.service-93rpYj
drwx------ 2 root root 4096 Nov  3 07:03 vmware-root_744-2957583465

/usr:
total 100
drwxr-xr-x   2 root root 36864 Oct 31 04:55 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root 16384 Oct 31 04:54 include
drwxr-xr-x  79 root root  4096 Oct 31 04:55 lib
drwxr-xr-x   2 root root  4096 Oct 31 04:54 lib64
drwxr-xr-x  11 root root  4096 Oct 17 14:06 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Oct 31 04:55 sbin
drwxr-xr-x 123 root root  4096 Oct 31 04:55 share
drwxr-xr-x   6 root root  4096 Oct 31 04:55 src

/var:
total 44
drwxr-xr-x  2 root root   4096 Nov  3 07:03 backups
drwxr-xr-x 16 root root   4096 Oct 27 08:06 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct 27 08:06 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Nov  3 07:03 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  7 root root   4096 Nov  3 07:03 tmp
khadija@ubuntu:~$ ls -l /bin /sbin /usr /opt /etc /dev /var /tmp > directory_evidence.txt
khadija@ubuntu:~$ cat directory_evidence.txt_
```

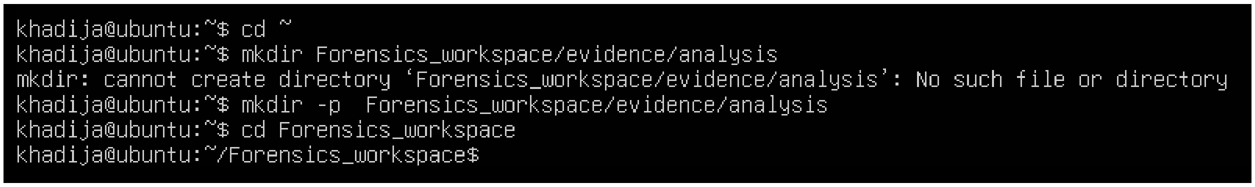


```
/usr:
total 100
drwxr-xr-x   2 root root 36864 Oct 31 04:55 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root 16384 Oct 31 04:54 include
drwxr-xr-x  79 root root  4096 Oct 31 04:55 lib
drwxr-xr-x   2 root root  4096 Oct 31 04:54 lib64
drwxr-xr-x  11 root root  4096 Oct 17 14:06 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Oct 31 04:55 sbin
drwxr-xr-x 123 root root  4096 Oct 31 04:55 share
drwxr-xr-x   6 root root  4096 Oct 31 04:55 src

/var:
total 44
drwxr-xr-x  2 root root   4096 Nov  3 07:03 backups
drwxr-xr-x 16 root root   4096 Oct 27 08:06 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct 27 08:06 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Nov  3 07:03 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  7 root root   4096 Nov  3 07:03 tmp
khadija@ubuntu:~$ ls -l /bin /sbin /usr /opt /etc /dev /var /tmp > directory_evidence.txt
khadija@ubuntu:~$ ls -la ~
total 68
drwxr-x--- 6 khadija khadija  4096 Nov  3 07:18 .
drwxr-xr-x 3 root    root     4096 Oct 31 12:00 ..
-rw-rw-r-- 1 khadija khadija   230 Oct 31 11:36 answers.md
-rw-r--r-- 1 khadija khadija   220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 khadija khadija  3771 Mar 31  2024 .bashrc
drwx------ 2 khadija khadija  4096 Oct 17 14:22 .cache
-rw-rw-r-- 1 khadija khadija 25114 Nov  3 07:18 directory_evidence.txt
drwxrwxr-x 3 khadija khadija  4096 Oct 31 11:36 lab4
drwxrwxr-x 3 khadija khadija  4096 Oct 31 11:31 .local
-rw-r--r-- 1 khadija khadija   807 Mar 31  2024 .profile
drwx------ 2 khadija khadija  4096 Oct 17 09:36 .ssh
-rw-r--r-- 1 khadija khadija     0 Oct 31 04:47 .sudo_as_admin_successful
khadija@ubuntu:~$ ls -la ~_
```

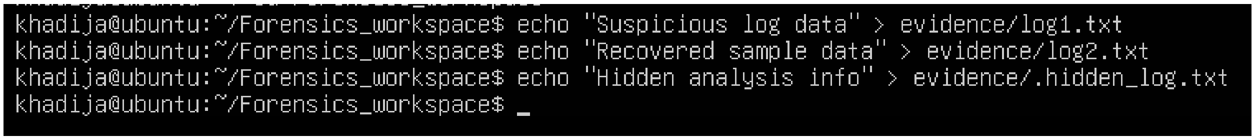


```
  GNU nano 7.2
# Filesystem Forensics Report
**OS Information:** Ubuntu 22.04 LTS
**Hostname:** ubuntu-vm
**User:** analyst
## Key Findings
- `/bin` and `/usr/bin` contain standard executable programs.
- `/etc` holds configuration files.
- `/var` contains logs.
- No unusual files found in `/tmp` or `/opt`
_End of Report__
```

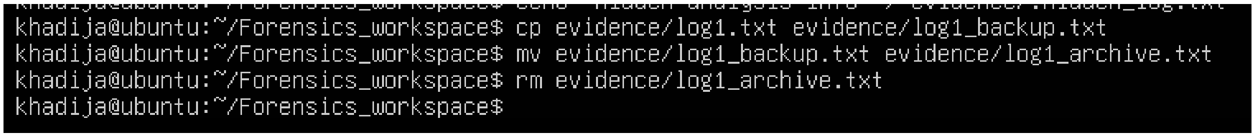
3. Evidence Handling & File Operations



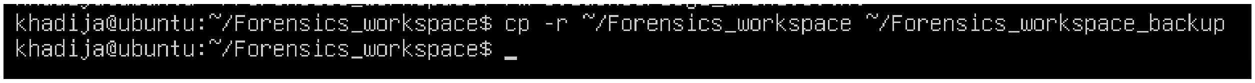
```
khadija@ubuntu:~$ cd ~
khadija@ubuntu:~$ mkdir Forensics_workspace/evidence/analysis
mkdir: cannot create directory ‘Forensics_workspace/evidence/analysis’: No such file or directory
khadija@ubuntu:~$ mkdir -p  Forensics_workspace/evidence/analysis
khadija@ubuntu:~$ cd Forensics_workspace
khadija@ubuntu:~/Forensics_workspace$
```



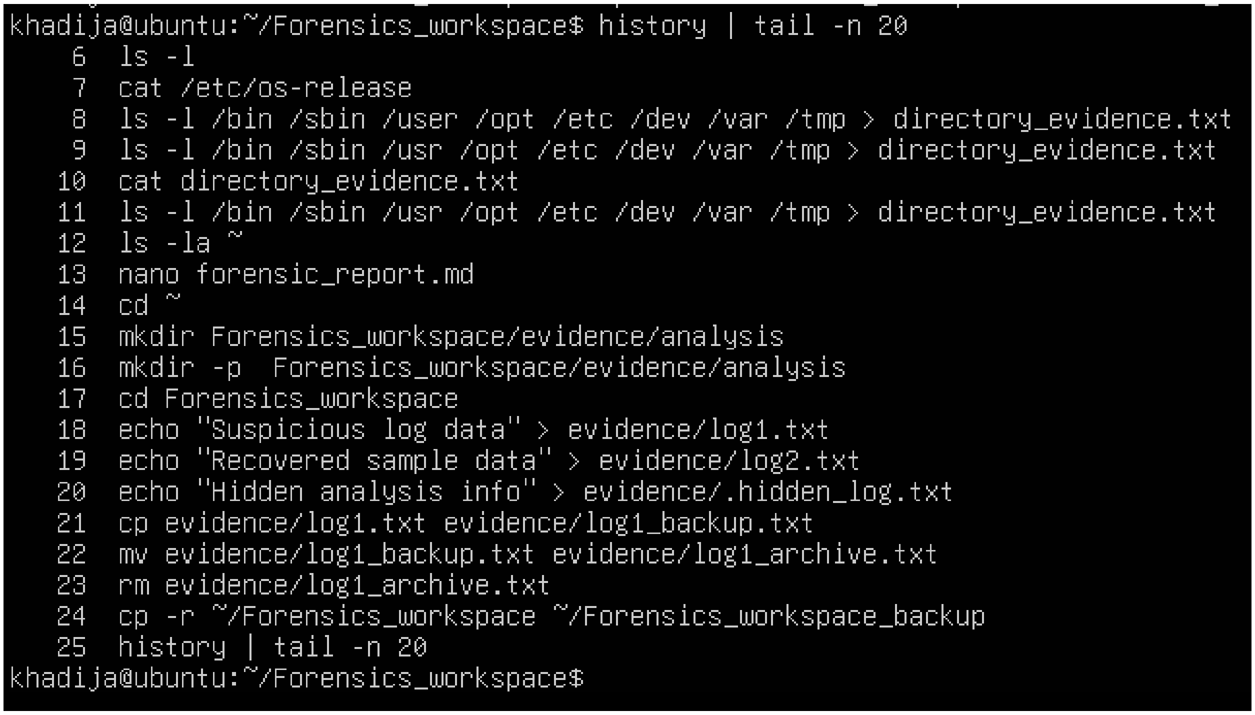
```
khadija@ubuntu:~/Forensics_workspace$ echo "Suspicious log data" > evidence/log1.txt
khadija@ubuntu:~/Forensics_workspace$ echo "Recovered sample data" > evidence/log2.txt
khadija@ubuntu:~/Forensics_workspace$ echo "Hidden analysis info" > evidence/.hidden_log.txt
khadija@ubuntu:~/Forensics_workspace$ _
```



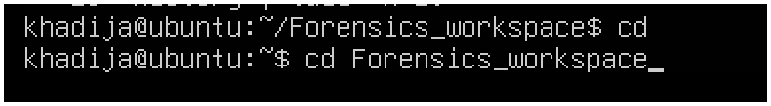
```
khadija@ubuntu:~/Forensics_workspace$ cp evidence/log1.txt evidence/log1_backup.txt
khadija@ubuntu:~/Forensics_workspace$ mv evidence/log1_backup.txt evidence/log1_archive.txt
khadija@ubuntu:~/Forensics_workspace$ rm evidence/log1_archive.txt
khadija@ubuntu:~/Forensics_workspace$
```



```
khadija@ubuntu:~/Forensics_workspace$ cp -r ~/Forensics_workspace ~/Forensics_workspace_backup
khadija@ubuntu:~/Forensics_workspace$ _
```

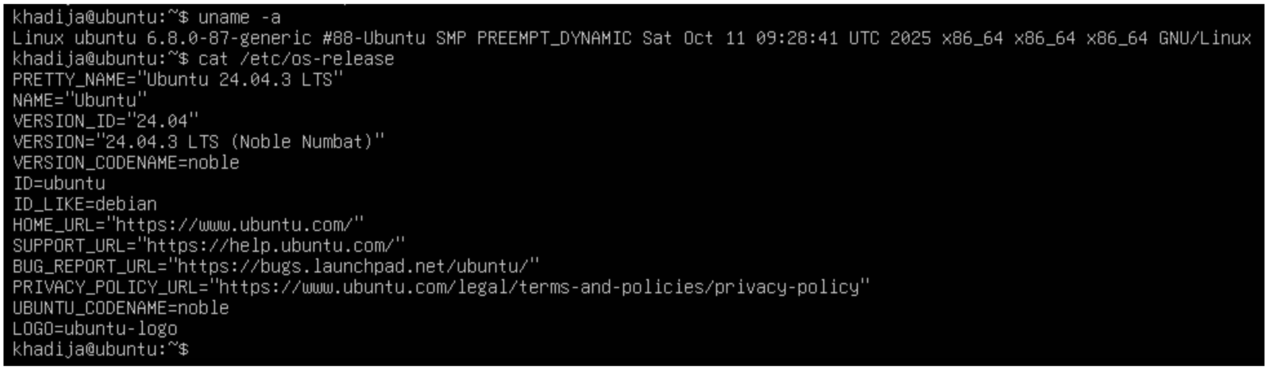


```
khadija@ubuntu:~/Forensics_workspace$ history | tail -n 20
    6  ls -l
    7  cat /etc/os-release
    8  ls -l /bin /sbin /user /opt /etc /dev /var /tmp > directory_evidence.txt
    9  ls -l /bin /sbin /usr /opt /etc /dev /var /tmp > directory_evidence.txt
   10  cat directory_evidence.txt
   11  ls -l /bin /sbin /usr /opt /etc /dev /var /tmp > directory_evidence.txt
   12  ls -la ~
   13  nano forensic_report.md
   14  cd ~
   15  mkdir Forensics_workspace/evidence/analysis
   16  mkdir -p  Forensics_workspace/evidence/analysis
   17  cd Forensics_workspace
   18  echo "Suspicious log data" > evidence/log1.txt
   19  echo "Recovered sample data" > evidence/log2.txt
   20  echo "Hidden analysis info" > evidence/.hidden_log.txt
   21  cp evidence/log1.txt evidence/log1_backup.txt
   22  mv evidence/log1_backup.txt evidence/log1_archive.txt
   23  rm evidence/log1_archive.txt
   24  cp -r ~/Forensics_workspace ~/Forensics_workspace_backup
   25  history | tail -n 20
khadija@ubuntu:~/Forensics_workspace$
```

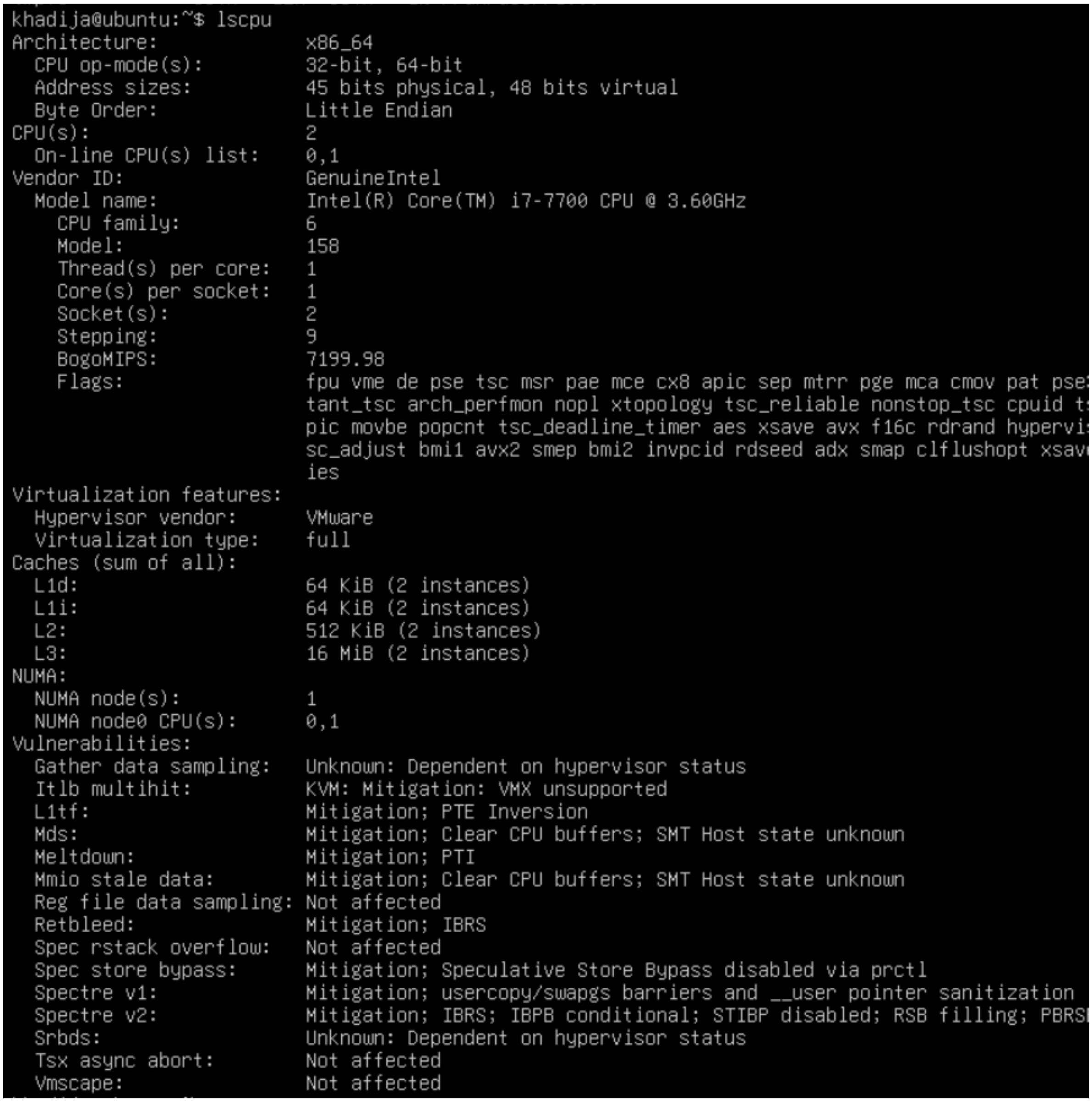


```
khadija@ubuntu:~/Forensics_workspace$ cd
khadija@ubuntu:~$ cd Forensics_workspace_
```

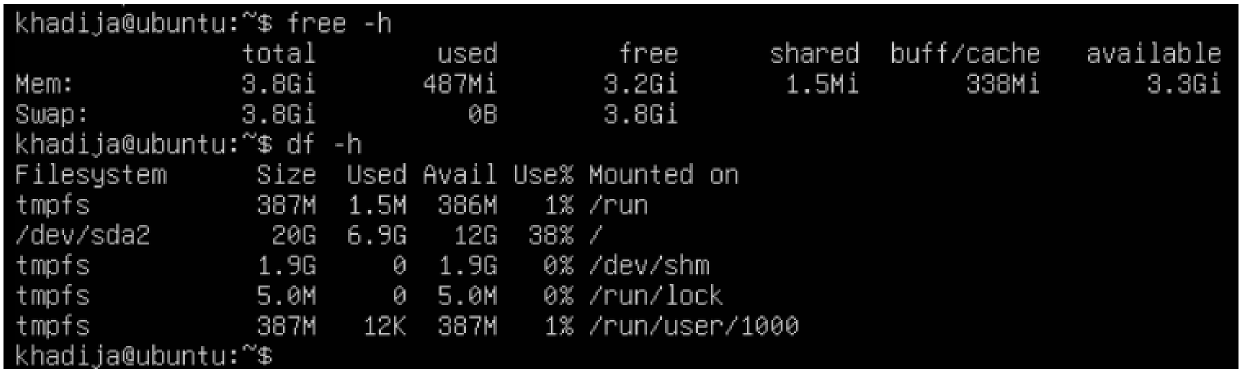
4. **System Profiling and Process Monitoring**



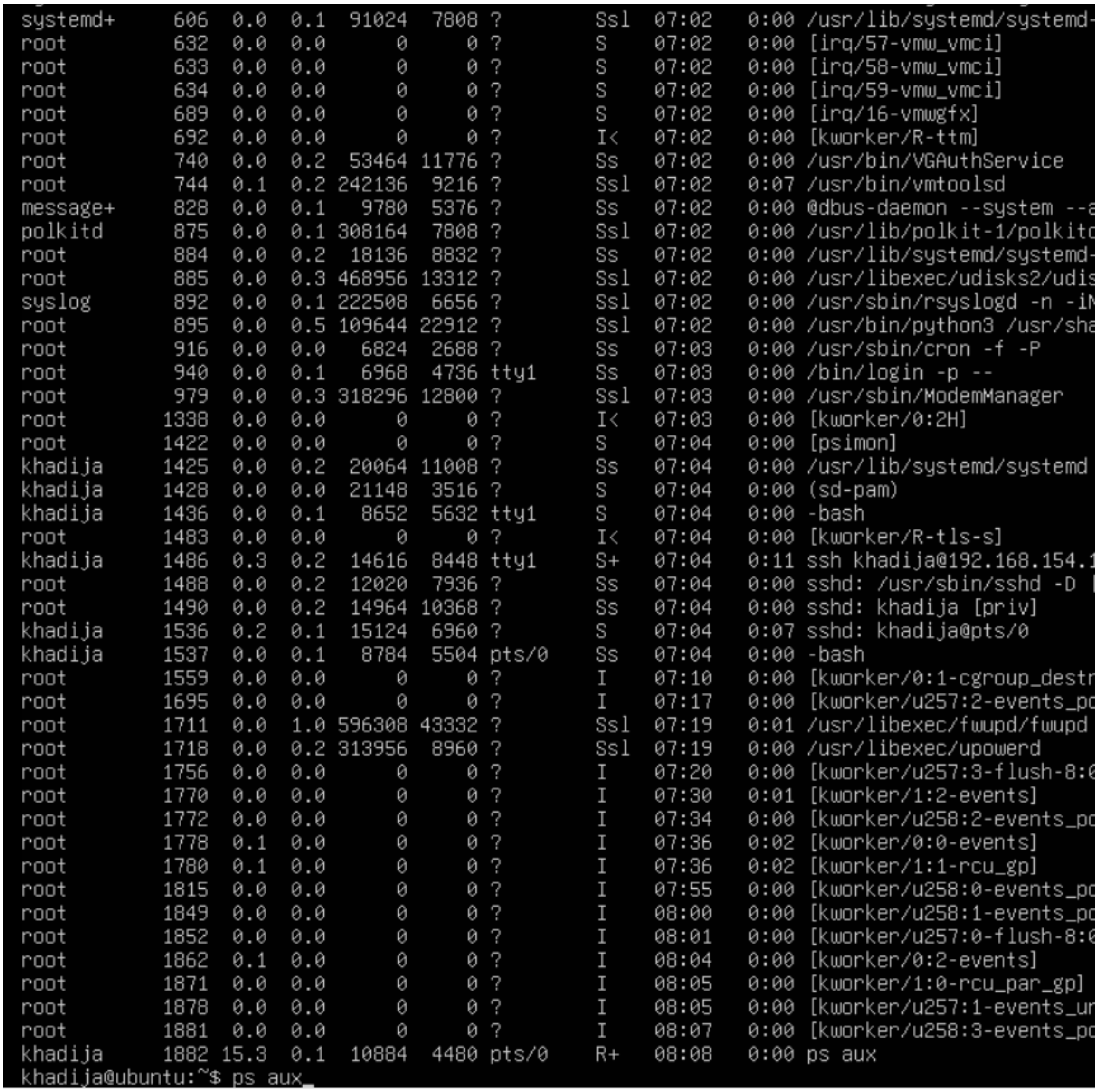
```
khadija@ubuntu:~$ uname -a
Linux ubuntu 6.8.0-87-generic #88-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 09:28:41 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
khadija@ubuntu:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
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
khadija@ubuntu:~$
```



```
khadija@ubuntu:~$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         45 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  2
  On-line CPU(s) list:   0,1
Vendor ID:               GenuineIntel
  Model name:            Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
    CPU family:          6
    Model:               158
    Thread(s) per core:  1
    Core(s) per socket:  1
    Socket(s):           2
    Stepping:            9
    BogoMIPS:            7199.98
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse
                         tant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid t
                         pic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervi
                         sc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt xsav
                         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:                    16 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; PBRS
  Srbds:                 Unknown: Dependent on hypervisor status
  Tsx async abort:       Not affected
  Vmscape:               Not affected
```

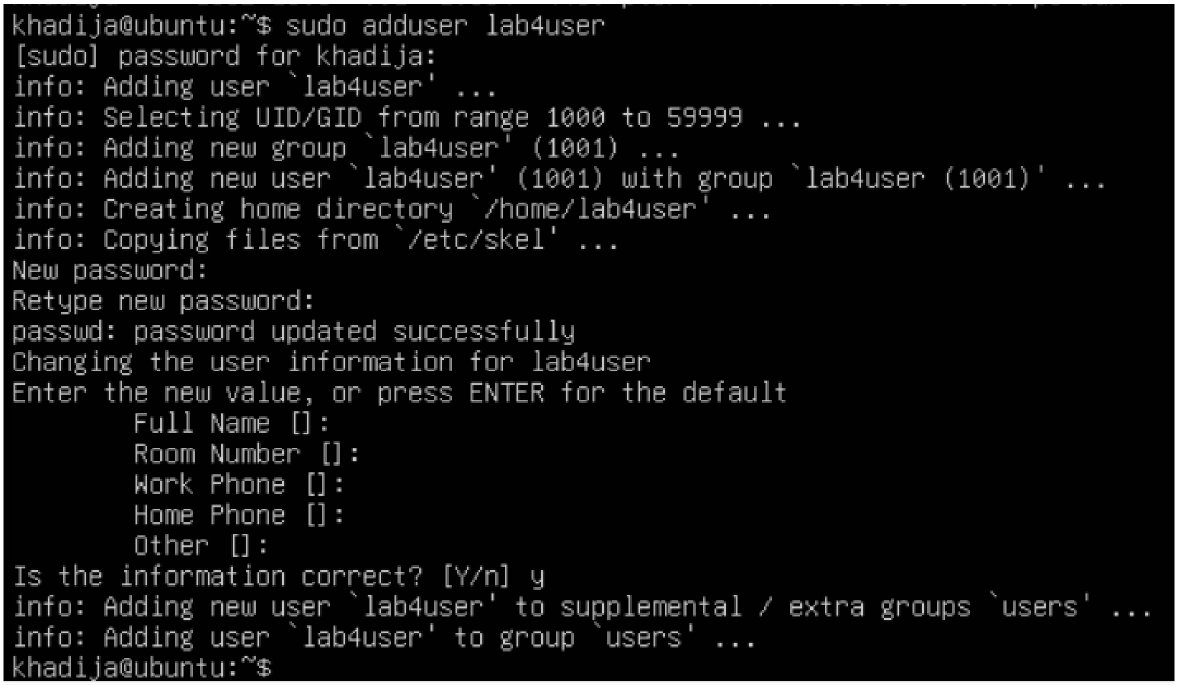


```
khadija@ubuntu:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       487Mi       3.2Gi       1.5Mi       338Mi       3.3Gi
Swap:          3.8Gi          0B       3.8Gi
khadija@ubuntu:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           387M  1.5M  386M   1% /run
/dev/sda2        20G  6.9G   12G  38% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           387M   12K  387M   1% /run/user/1000
khadija@ubuntu:~$
```

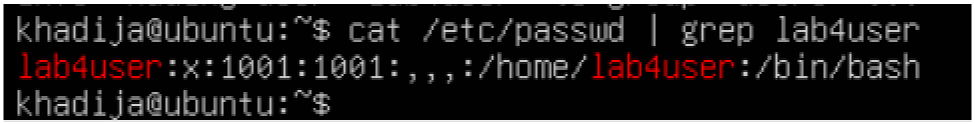


```
systemd+     606  0.0  0.1  91024  7808 ?        Ssl  07:02   0:00 /usr/lib/systemd/systemd-
root         632  0.0  0.0      0     0 ?        S    07:02   0:00 [irq/57-vmw_vmci]
root         633  0.0  0.0      0     0 ?        S    07:02   0:00 [irq/58-vmw_vmci]
root         634  0.0  0.0      0     0 ?        S    07:02   0:00 [irq/59-vmw_vmci]
root         689  0.0  0.0      0     0 ?        S    07:02   0:00 [irq/16-vmwgfx]
root         692  0.0  0.0      0     0 ?        I<   07:02   0:00 [kworker/R-ttm]
root         740  0.0  0.2  53464 11776 ?        Ss   07:02   0:00 /usr/bin/VGAuthService
root         744  0.1  0.2 242136  9216 ?        Ssl  07:02   0:07 /usr/bin/vmtoolsd
message+     828  0.0  0.1   9780  5376 ?        Ss   07:02   0:00 @dbus-daemon --system --a
polkitd      875  0.0  0.1 308164  7808 ?        Ssl  07:02   0:00 /usr/lib/polkit-1/polkitd
root         884  0.0  0.2  18136  8832 ?        Ss   07:02   0:00 /usr/lib/systemd/systemd-
root         885  0.0  0.3 468956 13312 ?        Ssl  07:02   0:00 /usr/libexec/udisks2/udis
syslog       892  0.0  0.1 222508  6656 ?        Ssl  07:02   0:00 /usr/sbin/rsyslogd -n -iN
root         895  0.0  0.5 109644 22912 ?        Ssl  07:02   0:00 /usr/bin/python3 /usr/sha
root         916  0.0  0.0   6824  2688 ?        Ss   07:03   0:00 /usr/sbin/cron -f -P
root         940  0.0  0.1   6968  4736 tty1     Ss   07:03   0:00 /bin/login -p --
root         979  0.0  0.3 318296 12800 ?        Ssl  07:03   0:00 /usr/sbin/ModemManager
root        1338  0.0  0.0      0     0 ?        I<   07:03   0:00 [kworker/0:2H]
root        1422  0.0  0.0      0     0 ?        S    07:04   0:00 [psimon]
khadija     1425  0.0  0.2  20064 11008 ?        Ss   07:04   0:00 /usr/lib/systemd/systemd
khadija     1428  0.0  0.0  21148  3516 ?        S    07:04   0:00 (sd-pam)
khadija     1436  0.0  0.1   8652  5632 tty1     S    07:04   0:00 -bash
root        1483  0.0  0.0      0     0 ?        I<   07:04   0:00 [kworker/R-tls-s]
khadija     1486  0.3  0.2  14616  8448 tty1     S+   07:04   0:11 ssh khadija@192.168.154.1
root        1488  0.0  0.2  12020  7936 ?        Ss   07:04   0:00 sshd: /usr/sbin/sshd -D [
root        1490  0.0  0.2  14964 10368 ?        Ss   07:04   0:00 sshd: khadija [priv]
khadija     1536  0.2  0.1  15124  6960 ?        S    07:04   0:07 sshd: khadija@pts/0
khadija     1537  0.0  0.1   8784  5504 pts/0    Ss   07:04   0:00 -bash
root        1559  0.0  0.0      0     0 ?        I    07:10   0:00 [kworker/0:1-cgroup_destr
root        1695  0.0  0.0      0     0 ?        I    07:17   0:00 [kworker/u257:2-events_po
root        1711  0.0  1.0 596308 43332 ?        Ssl  07:19   0:01 /usr/libexec/fwupd/fwupd
root        1718  0.0  0.2 313956  8960 ?        Ssl  07:19   0:00 /usr/libexec/upowerd
root        1756  0.0  0.0      0     0 ?        I    07:20   0:00 [kworker/u257:3-flush-8:0
root        1770  0.0  0.0      0     0 ?        I    07:30   0:01 [kworker/1:2-events]
root        1772  0.0  0.0      0     0 ?        I    07:34   0:00 [kworker/u258:2-events_po
root        1778  0.1  0.0      0     0 ?        I    07:36   0:02 [kworker/0:0-events]
root        1780  0.1  0.0      0     0 ?        I    07:36   0:02 [kworker/1:1-rcu_gp]
root        1815  0.0  0.0      0     0 ?        I    07:55   0:00 [kworker/u258:0-events_po
root        1849  0.0  0.0      0     0 ?        I    08:00   0:00 [kworker/u258:1-events_po
root        1852  0.0  0.0      0     0 ?        I    08:01   0:00 [kworker/u257:0-flush-8:0
root        1862  0.1  0.0      0     0 ?        I    08:04   0:00 [kworker/0:2-events]
root        1871  0.0  0.0      0     0 ?        I    08:05   0:00 [kworker/1:0-rcu_par_gp]
root        1878  0.0  0.0      0     0 ?        I    08:05   0:00 [kworker/u257:1-events_un
root        1881  0.0  0.0      0     0 ?        I    08:07   0:00 [kworker/u258:3-events_po
khadija     1882 15.3  0.1  10884  4480 pts/0    R+   08:08   0:00 ps aux
khadija@ubuntu:~$ ps aux
```

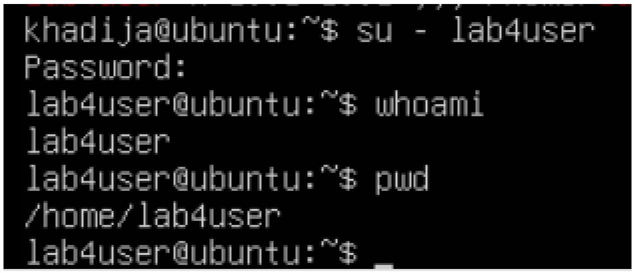
5. User Account Audit & Privilege Escalation Simulation



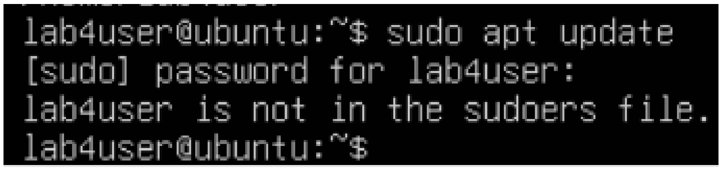
```
khadija@ubuntu:~$ sudo adduser lab4user
[sudo] password for khadija:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
info: Creating home directory `/home/lab4user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lab4user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
khadija@ubuntu:~$
```



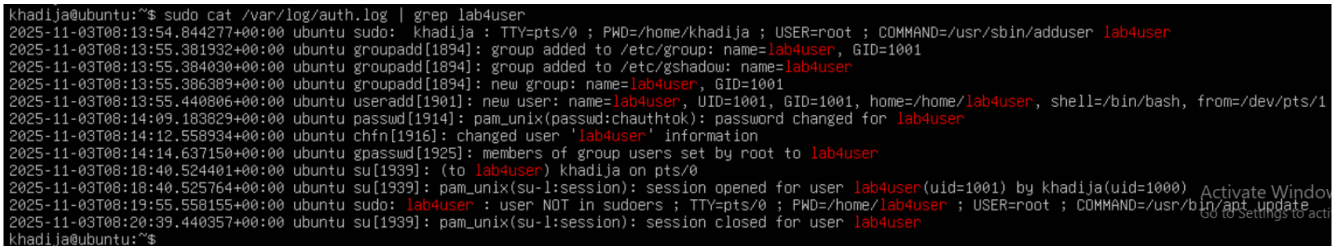
```
khadija@ubuntu:~$ cat /etc/passwd | grep lab4user
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
khadija@ubuntu:~$
```



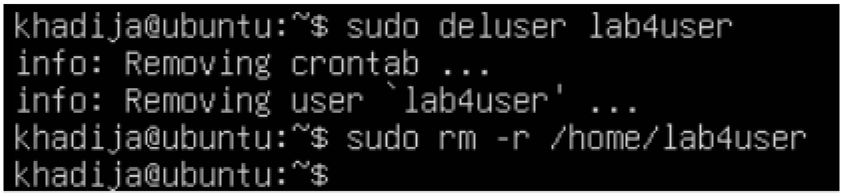
```
khadija@ubuntu:~$ su - lab4user
Password:
lab4user@ubuntu:~$ whoami
lab4user
lab4user@ubuntu:~$ pwd
/home/lab4user
lab4user@ubuntu:~$ _
```



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



```
khadija@ubuntu:~$ sudo cat /var/log/auth.log | grep lab4user
2025-11-03T08:13:54.844277+00:00 ubuntu sudo:  khadija : TTY=pts/0 ; PWD=/home/khadija ; USER=root ; COMMAND=/usr/sbin/adduser lab4user
2025-11-03T08:13:55.381932+00:00 ubuntu groupadd[1894]: group added to /etc/group: name=lab4user, GID=1001
2025-11-03T08:13:55.384030+00:00 ubuntu groupadd[1894]: group added to /etc/gshadow: name=lab4user
2025-11-03T08:13:55.386389+00:00 ubuntu groupadd[1894]: new group: name=lab4user, GID=1001
2025-11-03T08:13:55.440806+00:00 ubuntu useradd[1901]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/bin/bash, from=/dev/pts/1
2025-11-03T08:14:09.183829+00:00 ubuntu passwd[1914]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-11-03T08:14:12.558934+00:00 ubuntu chfn[1916]: changed user 'lab4user' information
2025-11-03T08:14:14.637150+00:00 ubuntu gpasswd[1925]: members of group users set by root to lab4user
2025-11-03T08:18:40.524401+00:00 ubuntu su[1939]: (to lab4user) khadija on pts/0
2025-11-03T08:18:40.525764+00:00 ubuntu su[1939]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by khadija(uid=1000)
2025-11-03T08:19:55.558155+00:00 ubuntu sudo: lab4user : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/apt update
2025-11-03T08:20:39.440357+00:00 ubuntu su[1939]: pam_unix(su-l:session): session closed for user lab4user
khadija@ubuntu:~$
```



```
khadija@ubuntu:~$ sudo deluser lab4user
info: Removing crontab ...
info: Removing user `lab4user' ...
khadija@ubuntu:~$ sudo rm -r /home/lab4user
khadija@ubuntu:~$
```

END