Lab 4

Lab Title: Virtualization & Linux Fundamentals

Submitted to: Engr. Muhammad Shoaib

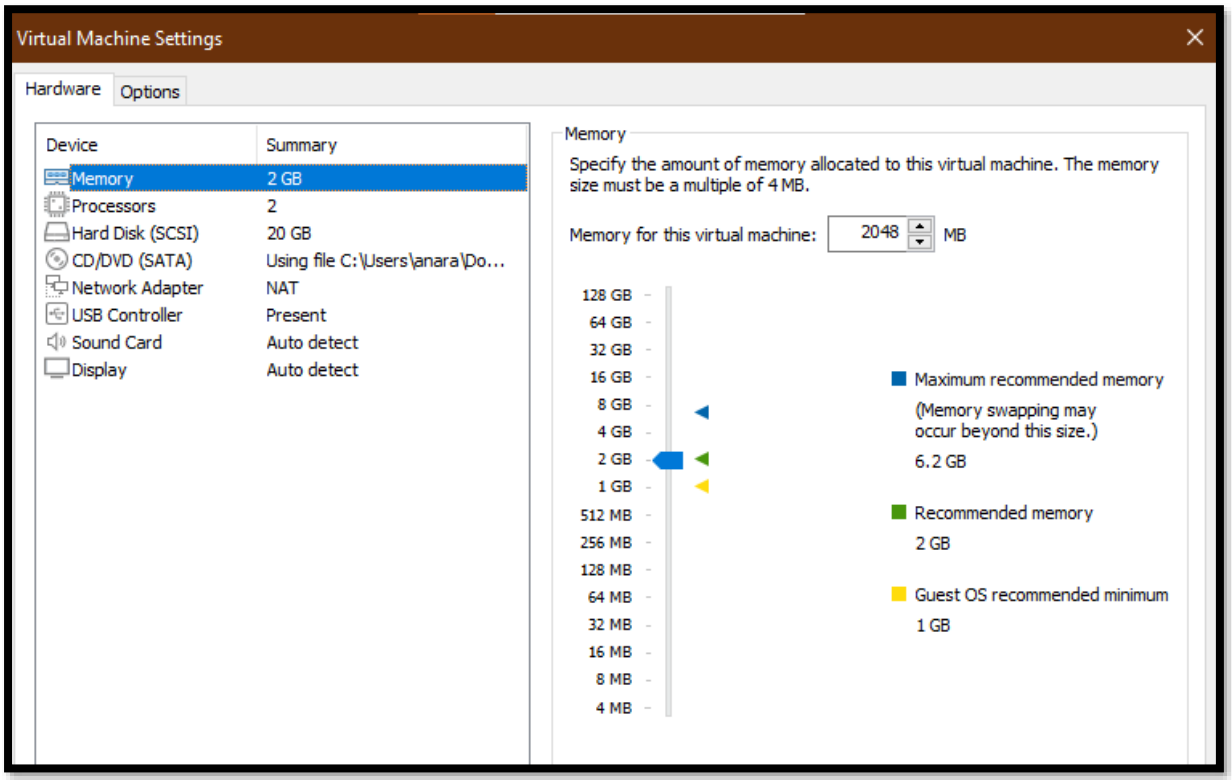
Submitted by: Anara Hayat

Reg#No: 2023-BSE-008

Task 1 .Verify VM resources in VMware

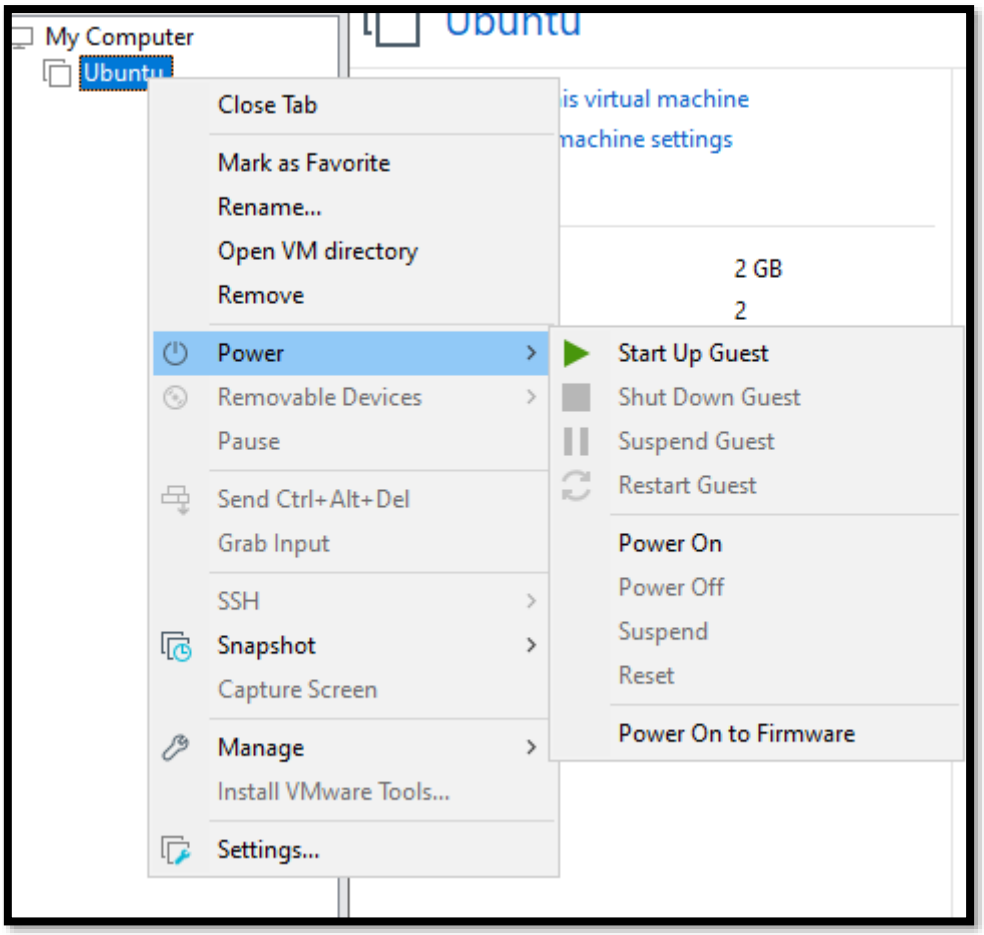
1.Open VMware Workstation and locate the Ubuntu Server VM you used in Lab 1.

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



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

1.Start (or resume) the VM in VMware Workstation on your host.



2.From your host, open your preferred terminal (for example: Windows Command Prompt, PowerShell, macOS Terminal, or Linux Terminal) and connect to the VM using SSH.

```
    inet 192.168.111.129/24 metric 100 brd 192.168.111.255 scope global dynamic ens33
       valid_lft 1467sec preferred_lft 1467sec
    inet6 fe80::20c:29ff:feba:83da/64 scope link
       valid_lft forever preferred_lft forever
anara@ubuntu:~$ ssh anara@192.168.111.129
The authenticity of host '192.168.111.129 (192.168.111.129)' can't be established.
ED25519 key fingerprint is SHA256:qtQKrWqPkeXr3mH/xuBEU5qh73DvzRSPAP4v74hscC0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.111.129' (ED25519) to the list of known hosts.
anara@192.168.111.129's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

 System information as of Fri Oct 17 06:45:35 AM UTC 2025

  System load:  0.0               Processes:              215
  Usage of /:   45.5% of 9.75GB   Users logged in:        1
  Memory usage: 13%               IPv4 address for ens33: 192.168.111.129
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

42 updates can be applied immediately.
42 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: Sat Sep 27 10:06:19 2025 from 192.168.111.1
```

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

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

Task 3 – Filesystem exploration — root tree and dotfiles

1.List root directory contents:

```
anara@ubuntu:~$ ls -la /
total 1994844
drwxr-xr-x  23 root root       4096 Sep 27 09:55 .
drwxr-xr-x  23 root root       4096 Sep 27 09:55 ..
lrwxrwxrwx   1 root root          7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x   2 root root       4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x   4 root root       4096 Sep 27 09:55 boot
dr-xr-xr-x   2 root root       4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root       4120 Oct 17 06:35 dev
drwxr-xr-x 108 root root       4096 Sep 27 10:00 etc
drwxr-xr-x   3 root root       4096 Sep 27 10:00 home
lrwxrwxrwx   1 root root          7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx   1 root root          9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x   2 root root       4096 Feb 26  2024 lib.usr-is-merged
drwx------   2 root root      16384 Sep 27 09:50 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 280 root root          0 Oct 17 06:35 proc
drwx------   3 root root       4096 Aug  5 17:02 root
drwxr-xr-x  28 root root        840 Oct 17 06:45 run
lrwxrwxrwx   1 root root          8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root       4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x   2 root root       4096 Sep 27 10:00 snap
drwxr-xr-x   2 root root       4096 Aug  5 16:54 srv
-rw-------   1 root root 2042626048 Sep 27 09:55 swap.img
dr-xr-xr-x  13 root root          0 Oct 17 06:35 sys
drwxrwxrwt  13 root root       4096 Oct 17 06:50 tmp
drwxr-xr-x  12 root root       4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root       4096 Sep 27 10:00 var
```

2.View OS release information:

```
anara@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-poli
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

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

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

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

```
anara@ubuntu:~$ ls -la /usr
total 96
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Sep 27 09:55 ..
drwxr-xr-x   2 root root 36864 Sep 27 09:56 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root  4096 Sep 27 09:52 include
drwxr-xr-x  78 root root  4096 Sep 27 09:56 lib
drwxr-xr-x   2 root root  4096 Aug  5 17:01 lib64
drwxr-xr-x  11 root root  4096 Sep 27 09:53 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Sep 27 09:56 sbin
drwxr-xr-x 124 root root  4096 Sep 27 09:56 share
drwxr-xr-x   4 root root  4096 Sep 27 09:53 src
```

```
anara@ubuntu:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 27 09:55 ..
```

Ls -la /etc

```
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      967 Sep 27 10:00 shadow
-rw-r-----   1 root shadow      967 Sep 27 10:00 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 27 10:00 ssh
drwxr-xr-x   4 root root       4096 Aug  5 17:02 ssl
-rw-r--r--   1 root root         19 Sep 27 10:00 subgid
-rw-r--r--   1 root root          0 Aug  5 16:54 subgid-
-rw-r--r--   1 root root         19 Sep 27 10:00 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 27 09:54 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 Aug  5 17:14 udisks2
drwxr-xr-x   3 root root       4096 Aug  5 17:14 ufw
-rw-r--r--   1 root root        208 Aug  5 16:54 .updated
drwxr-xr-x   3 root root       4096 Aug  5 17:02 update-manager
drwxr-xr-x   2 root root       4096 Aug  5 17:14 update-motd.d
drwxr-xr-x   2 root root       4096 Aug  5 17:14 update-notifier
```

Ls -la /dev

```
crw-rw----   1 root  dialout   4,  91 Oct 17 06:35 ttyS27
crw-rw----   1 root  dialout   4,  92 Oct 17 06:35 ttyS28
crw-rw----   1 root  dialout   4,  93 Oct 17 06:35 ttyS29
crw-rw----   1 root  dialout   4,  67 Oct 17 06:35 ttyS3
crw-rw----   1 root  dialout   4,  94 Oct 17 06:35 ttyS30
crw-rw----   1 root  dialout   4,  95 Oct 17 06:35 ttyS31
crw-rw----   1 root  dialout   4,  68 Oct 17 06:35 ttyS4
crw-rw----   1 root  dialout   4,  69 Oct 17 06:35 ttyS5
crw-rw----   1 root  dialout   4,  70 Oct 17 06:35 ttyS6
crw-rw----   1 root  dialout   4,  71 Oct 17 06:35 ttyS7
crw-rw----   1 root  dialout   4,  72 Oct 17 06:35 ttyS8
crw-rw----   1 root  dialout   4,  73 Oct 17 06:35 ttyS9
drwxr-xr-x   2 root  root          60 Oct 17 06:35 ubuntu-vg
crw-rw----   1 root  kvm      10, 124 Oct 17 06:35 udmabuf
crw-------   1 root  root     10, 239 Oct 17 06:35 uhid
crw-------   1 root  root     10, 223 Oct 17 06:35 uinput
crw-rw-rw-   1 root  root      1,   9 Oct 17 06:35 urandom
crw-------   1 root  root     10, 126 Oct 17 06:35 userfaultfd
crw-------   1 root  root     10, 240 Oct 17 06:35 userio
crw-rw----   1 root  tty       7,   0 Oct 17 06:35 vcs
crw-rw----   1 root  tty       7,   1 Oct 17 06:35 vcs1
crw-rw----   1 root  tty       7,   2 Oct 17 06:35 vcs2
crw-rw----   1 root  tty       7,   3 Oct 17 06:35 vcs3
crw-rw----   1 root  tty       7,   4 Oct 17 06:35 vcs4
crw-rw----   1 root  tty       7,   5 Oct 17 06:35 vcs5
crw-rw----   1 root  tty       7,   6 Oct 17 06:35 vcs6
crw-rw----   1 root  tty       7, 128 Oct 17 06:35 vcsa
crw-rw----   1 root  tty       7, 129 Oct 17 06:35 vcsa1
crw-rw----   1 root  tty       7, 130 Oct 17 06:35 vcsa2
crw-rw----   1 root  tty       7, 131 Oct 17 06:35 vcsa3
crw-rw----   1 root  tty       7, 132 Oct 17 06:35 vcsa4
crw-rw----   1 root  tty       7, 133 Oct 17 06:35 vcsa5
crw-rw----   1 root  tty       7, 134 Oct 17 06:35 vcsa6
crw-rw----   1 root  tty       7,  64 Oct 17 06:35 vcsu
crw-rw----   1 root  tty       7,  65 Oct 17 06:35 vcsu1
crw-rw----   1 root  tty       7,  66 Oct 17 06:35 vcsu2
crw-rw----   1 root  tty       7,  67 Oct 17 06:35 vcsu3
crw-rw----   1 root  tty       7,  68 Oct 17 06:35 vcsu4
```

```
anara@ubuntu:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Sep 27 10:00 .
drwxr-xr-x 23 root root   4096 Sep 27 09:55 ..
drwxr-xr-x  2 root root   4096 Oct 16 03:45 backups
drwxr-xr-x 16 root root   4096 Sep 27 14:44 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Sep 27 14:44 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 17 06:35 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 17 06:36 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
```

```
anara@ubuntu:~$ ls -la /tmp
total 52
drwxrwxrwt 13 root root 4096 Oct 17 06:50 .
drwxr-xr-x 23 root root 4096 Sep 27 09:55 ..
drwxrwxrwt  2 root root 4096 Oct 17 06:35 .font-unix
drwxrwxrwt  2 root root 4096 Oct 17 06:35 .ICE-unix
drwx------  2 root root 4096 Oct 17 06:35 snap-private-tmp
drwx------  3 root root 4096 Oct 17 06:35 systemd-private-e8f8de7803514d9584f834125
drwx------  3 root root 4096 Oct 17 06:35 systemd-private-e8f8de7803514d9584f834125
drwx------  3 root root 4096 Oct 17 06:35 systemd-private-e8f8de7803514d9584f834125
drwx------  3 root root 4096 Oct 17 06:35 systemd-private-e8f8de7803514d9584f834125
drwx------  3 root root 4096 Oct 17 06:35 systemd-private-e8f8de7803514d9584f834125
drwx------  2 root root 4096 Oct 17 06:35 vmware-root_742-2991137376
drwxrwxrwt  2 root root 4096 Oct 17 06:35 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 17 06:35 .XIM-unix
```

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

```
anara@ubuntu:~$ ls -la ~
total 28
drwxr-x--- 4 anara anara 4096 Sep 27 10:03 .
drwxr-xr-x 3 root  root  4096 Sep 27 10:00 ..
-rw-r--r-- 1 anara anara  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 anara anara 3771 Mar 31  2024 .bashrc
drwx------ 2 anara anara 4096 Sep 27 10:03 .cache
-rw-r--r-- 1 anara anara  807 Mar 31  2024 .profile
drwx------ 2 anara anara 4096 Oct 17 06:45 .ssh
```

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

```
anara@ubuntu: ~
  GNU nano 7.2                                  /home/anara/answers.md *
The main difference between /bin, /usr/bin, and /usr/local/bin lies in where their programs come from and who maintains them.
The /bin directory contains essential system binaries needed for basic operation,
such as ls, cp, and mv, which are required even
when the system is in single-user or recovery mode.
The /usr/bin directory holds most of the user commands and applicatio
ns installed by the operating system's package manager.
In contrast, /usr/local/bin is reserved for software manually installed
 by the system administrator or user,
ensuring that locally added programs do not interfere with system-managed ones.
```

Task 4 – Essential CLI tasks — navigation and file operations

1.Create a workspace and navigate:

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

```
anara@ubuntu:~$ cd ~/lab4/workspace/python_project
anara@ubuntu:~/lab4/workspace/python_project$
```

```
anara@ubuntu:~/lab4/workspace/python_project$ pwd
/home/anara/lab4/workspace/python_project
anara@ubuntu:~/lab4/workspace/python_project$
```

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

Nano README.md

```
Ubuntu
  GNU nano 7.2
This is lab 4 README
```

Nano main.py

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

Nano .env

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

3.List files and capture

```
anara@ubuntu:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 anara anara 4096 Oct 17 07:27 .
drwxrwxr-x 3 anara anara 4096 Oct 17 07:16 ..
-rw-rw-r-- 1 anara anara    9 Oct 17 07:27 .env
-rw-rw-r-- 1 anara anara   20 Oct 17 07:22 main.py
-rw-rw-r-- 1 anara anara   21 Oct 17 07:21 README.md
```

4.Copy, move and remove:

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

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

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

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

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

```
anara@ubuntu:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 anara anara 4096 Oct 17 07:36 .
drwxrwxr-x 3 anara anara 4096 Oct 17 07:16 ..
drwxrwxr-x 2 anara anara 4096 Oct 17 07:34 java_app
drwxrwxr-x 2 anara anara 4096 Oct 17 07:36 java_app_copy
drwxrwxr-x 2 anara anara 4096 Oct 17 07:31 python_project
```

5.Use command history and tab completion

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

Demonstrate tab completion (type partial name and press Tab) and capture that action

```
anara@ubuntu:~/lab4/workspace/python_project$ cat README.md
This is lab 4 README
```

Task 5 – System info, resources & processes

1.Kernel and OS

```
anara@ubuntu:~$ uname -a
Linux ubuntu 6.8.0-71-generic #71-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 22 16:52:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

cat /proc/cpuinfo

```
core id         : 0
cpu cores       : 1
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge
 arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_f
 aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ss
nopt xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_l1d arch_capabi
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass
bogomips        : 3215.99
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:

processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 142
model name      : Intel(R) Core(TM) m3-7Y30 CPU @ 1.00GHz
stepping        : 9
microcode       : 0xffffffff
cpu MHz         : 1607.998
cache size      : 4096 KB
physical id     : 2
```

3.Memory:

```
anara@ubuntu:~$ free -h
              total        used        free      shared  buff/cache   available
Mem:          1.9Gi       381Mi       1.3Gi       1.2Mi       330Mi       1.5Gi
Swap:         1.9Gi          0B       1.9Gi
```

4.Disk:

```
anara@ubuntu:~$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              192M  1.3M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  9.8G  4.5G  4.8G  49% /
tmpfs                              960M     0  960M   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.8G  100M  1.6G   7% /boot
tmpfs                              192M   12K  192M   1% /run/user/1000
```

5.Os Release:

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

6.Processes (show top lines of ps output)

Ps aux

```
root         578  0.0  0.0      0     0 ?        S    06:35   0:00 [irq/58-vmw_vmci
root         579  0.0  0.0      0     0 ?        S    06:35   0:00 [irq/59-vmw_vmci
root         585  0.0  0.0      0     0 ?        S    06:35   0:00 [irq/16-vmwgfx]
root         586  0.0  0.0      0     0 ?        I<   06:35   0:00 [kworker/R-ttm]
root         594  0.0  0.0      0     0 ?        S    06:35   0:00 [jbd2/sda2-8]
root         595  0.0  0.0      0     0 ?        I<   06:35   0:00 [kworker/R-ext4-
systemd+     630  0.0  0.4  19008  9344 ?        Ss   06:35   0:01 /usr/lib/systemd
systemd+     639  0.0  0.6  21588 12800 ?        Ss   06:35   0:01 /usr/lib/systemd
systemd+     648  0.0  0.3  91024  7808 ?        Ssl  06:35   0:00 /usr/lib/systemd
root         736  0.0  0.0      0     0 ?        I<   06:35   0:00 [kworker/R-cfg80
root         740  0.0  0.5  53464 11776 ?        Ss   06:35   0:00 /usr/bin/VGAuthS
root         742  0.8  0.4 242148  9084 ?        Ssl  06:35   0:49 /usr/bin/vmtools
message+     779  0.0  0.2   9784  5248 ?        Ss   06:35   0:00 @dbus-daemon --s
polkitd      799  0.0  0.4 308164  8064 ?        Ssl  06:35   0:01 /usr/lib/polkit-
root         818  0.0  0.4  18140  8704 ?        Ss   06:35   0:00 /usr/lib/systemd
root         820  0.0  0.6 468988 13696 ?        Ssl  06:35   0:01 /usr/libexec/udi
root         838  0.0  0.0      0     0 ?        I    06:35   0:00 [kworker/u256:2]
syslog       840  0.0  0.2 222508  5760 ?        Ssl  06:35   0:00 /usr/sbin/rsyslo
root         852  0.0  0.1   6824  2688 ?        Ss   06:35   0:00 /usr/sbin/cron -
root         874  0.0  0.6 392092 12544 ?        Ssl  06:35   0:00 /usr/sbin/ModemM
root         880  0.0  1.1 109660 23040 ?        Ssl  06:35   0:00 /usr/bin/python3
root         914  0.0  0.2   6944  4608 tty1     Ss   06:35   0:00 /bin/login -p --
root        1188  0.0  0.0      0     0 ?        S    06:36   0:00 [psimon]
```

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

1.Create a new user named lab4user

```
anara@ubuntu:~$ sudo adduser lab4user
[sudo] password for anara:
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 []: Anara Hayat
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] yes
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
```

2.Verify the user entry

```
anara@ubuntu:~$ getent passwd lab4user
lab4user:x:1001:1001:Anara Hayat,,,:/home/lab4user:/bin/bash
```

3.Switch to the new user to verify login:

```
anara@ubuntu:~$ su - lab4user
Password:
lab4user@ubuntu:~$
```

4.From the new user you may attempt a sudo command to show that sudo is not available for this account (expected failure),

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

5.Return to the original user

```
lab4user@ubuntu:~$ exit
logout
anara@ubuntu:~$
```

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

```
anara@ubuntu:~$ sudo deluser --remove-home lab4user
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

1.Open an editor to create the script

Run-demo.sh

```
Ubuntu
  GNU nano 7.2
#!/bin/bash
echo "Lab 4 demo: current user is $(whoami)"
echo "Current time: $(date)"
uptime
free -h
```

2.Make the script executable:

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

3.Run the script as your regular user

```
anara@ubuntu:~$ ~/lab4/workspace/run-demo.sh
Lab 4 demo: current user is anara
Current time: Fri Oct 17 08:30:36 AM UTC 2025
 08:30:36 up  1:55,  2 users,  load average: 0.01, 0.01, 0.00
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       392Mi       1.3Gi       1.2Mi       344Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
```

Exam Evaluation Questions

Q1. Remote Access Verification (Cyber Login Check)

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

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

```
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

 System information as of Fri Oct 17 08:35:18 AM UTC 2025

  System load:  0.04               Processes:               221
  Usage of /:   45.6% of 9.75GB    Users logged in:         1
  Memory usage: 15%                IPv4 address for ens33: 192.168.111.129
  Swap usage:   0%

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

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

Expanded Security Maintenance for Applications is not enabled.

42 updates can be applied immediately.
42 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 17 06:45:37 2025 from 192.168.111.129
```

2.Verify your current user and home directory path

```
anara@ubuntu:~$ pwd
/home/anara
```

3.Confirm you are connected to the correct host machine

```
anara@ubuntu:~$ uname -a
Linux ubuntu 6.8.0-71-generic #71-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 22 16:52:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

Q2. Filesystem Inspection for Forensic Evidence

Scenario:

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

1.Display the contents of the root directory

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

2.Display the OS version and release information

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

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

```
anara@ubuntu:~$ ls /bin | head -2
[
aa-enabled
anara@ubuntu:~$ ls /sbin | head -2
aa-load
aa-remove-unknown
anara@ubuntu:~$ ls /usr | head -2
bin
games
anara@ubuntu:~$ ls /opt | head -2
anara@ubuntu:~$ ls /etc | head -2
adduser.conf
alternatives
anara@ubuntu:~$
anara@ubuntu:~$ ls /dev | head -2
autofs
block
anara@ubuntu:~$ ls /var | head -2
backups
cache
anara@ubuntu:~$ ls /tmp | head -2
snap-private-tmp
systemd-private-e8f8de7803514d9584f8341297162ea9-fwupd.service-EOwiDm
```

4.Display all hidden files in your home directory

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

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

```
anara@ubuntu: ~
  GNU nano 7.2                                        /home/anara/answers.md *
The main difference between /bin, /usr/bin, and /usr/local/bin lies in where their programs come from and who maintains them.
The /bin directory contains essential system binaries needed for basic operation,
such as ls, cp, and mv, which are required even
when the system is in single-user or recovery mode.
The /usr/bin directory holds most of the user commands and applicatio
ns installed by the operating system's package manager.
In contrast, /usr/local/bin is reserved for software manually installed
 by the system administrator or user,
ensuring that locally added programs do not interfere with system-managed ones.
```

Q3. Evidence Handling & File Operations

Scenario:

You are creating a sandbox environment to safely analyze and handle suspicious files collected from a compromised system**.**

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

```
anara@ubuntu:~$ mkdir -p ~/analysis/{binaries/{bin,usr_bin},configs/etc,logs/{system,apps},reports/{markdown,pdf},evide
ce/{screenshots,scripts}}
anara@ubuntu:~$ ls
analysis  answers.md  lab4
anara@ubuntu:~$ cd ~/analysis
anara@ubuntu:~/analysis$ ls
binaries  configs  evidence  logs  reports
```

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

```
anara@ubuntu:~/analysis$ touch file1.txt file2.txt .hiddenfile.txt
anara@ubuntu:~/analysis$ ls
binaries  configs  evidence  file1.txt  file2.txt  logs  reports
anara@ubuntu:~/analysis$ ls -a
.  ..  binaries  configs  evidence  file1.txt  file2.txt  .hiddenfile.txt  logs  reports
```

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

```
anara@ubuntu:~/analysis$ cp file1.txt file1_backup.txt
anara@ubuntu:~/analysis$ mv file1_backup.txt file1_old.txt
anara@ubuntu:~/analysis$ ls
binaries  configs  evidence  file1_old.txt  file1.txt  file2.txt  logs  reports
anara@ubuntu:~/analysis$ rm file1_old.txt
anara@ubuntu:~/analysis$ ls
binaries  configs  evidence  file1.txt  file2.txt  logs  reports
anara@ubuntu:~/analysis$
```

4.Copy the entire workspace as an evidence backup folder

```
anara@ubuntu:~/analysis$ cd ~
anara@ubuntu:~$ cp -r analysis analysis_backup
anara@ubuntu:~$ ls
analysis  analysis_backup  answers.md  lab4
anara@ubuntu:~$
```

5.Display your command history to document all actions performed

```
anara@ubuntu:~$ history
    1  pwd
    2  mkdir "%USERPROFILE%\analysis\binaries\bin" "%USERPROFILE%\analysis\binaries\usr_bin" "%USERPROFILE%\analysis\configs\etc" "%USERPROFILE
%USERPROFILE%\analysis\logs\apps" "%USERPROFILE%\analysis\reports\markdown" "%USERPROFILE%\analysis\reports\pdf" "%USERPROFILE%\analysis\evi
FILE%\analysis\evidence\scripts"
    3  ls
    4  ls %USERPROFILE%
    5  cd /%USERPROFLIE%
    6  rmdir /s /q "%USERPROFILE%\analysis"
    7  rmdir  "%USERPROFILE%\analysis"
    8  rm -rf ~/analysis
    9  ls
   10  rm -rf ~/'%USERPROFILE%\analysis'
   11  ls
   12  rmdir ~/ "%USERPROFILE%\analysis"
   13  rm -rf ~/'%USERPROFILE%\analysis'*
   14  ls
   15  mkdir -p ~/analysis/{binaries/{bin,usr_bin},configs/etc,logs/{system,apps},reports/{markdown,pdf},evidence/{screenshots,scripts}}
   16  ls
   17  cd ~/analysis
   18  ls
   19  touch file1.txt file2.txt .hiddenFile.txt
   20  ls
   21  ls -a
   22  cp file1.txt file1_backup.txt
   23  mv file1_backup.txt file1_old.txt
   24  ls
   25  rm file1_old.txt
   26  ls
   27  cd ~
   28  cp -r analysis analysis_backup
   29  ls
   30  history
```

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

```
anara@ubuntu:~$ cd ~/analysis
anara@ubuntu:~/analysis$
```

Q4. System Profiling and Process Monitoring

Scenario:

You are investigating a potential malware infection that is consuming excessive resources on the Linux VM.

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

```
anara@ubuntu:~/analysis$ 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
anara@ubuntu:~/analysis$ uname -r
6.8.0-71-generic
```

2.Display CPU, memory, and disk usage information

```
anara@ubuntu:~/analysis$ lscpu | head -5
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
anara@ubuntu:~/analysis$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       368Mi       1.4Gi       1.2Mi       229Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
anara@ubuntu:~/analysis$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              193M  1.3M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  9.8G  4.5G  4.8G  49% /
tmpfs                              961M     0  961M   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.8G  100M  1.6G   7% /boot
tmpfs                              192M   12K  192M   1% /run/user/1000
```

3.Display all active running processes to identify suspicious activity

```
anara@ubuntu:~$ ps aux | tail -25
anara      1381  0.0  0.2   8652  5376 tty1     S    14:56   0:00 -bash
anara      1408  0.0  0.4  14616  8448 tty1     S+   14:57   0:00 ssh anara@192.168.111.129
root       1410  0.0  0.4  12020  7936 ?        Ss   14:57   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root       1412  0.0  0.5  14960 10240 ?        Ss   14:57   0:00 sshd: anara [priv]
anara      1467  0.0  0.3  15120  6832 ?        S    14:57   0:00 sshd: anara@pts/0
anara      1468  0.0  0.2   8652  5376 pts/0    Ss+  14:57   0:00 -bash
root       1477  0.0  0.5  14960 10240 ?        Ss   14:58   0:00 sshd: anara [priv]
anara      1523  1.4  0.3  15120  6976 ?        S    14:58   0:33 sshd: anara@pts/1
anara      1524  0.0  0.2   8700  5504 pts/1    Ss   14:58   0:01 -bash
root       1553  0.0  0.0      0     0 ?        I    15:06   0:14 [kworker/1:2-events]
root       1568  0.0  0.0      0     0 ?        I<   15:10   0:00 [kworker/0:0H-kblockd]
root       1571  0.0  0.0      0     0 ?        I    15:10   0:01 [kworker/u258:1-events_power_efficient]
root       1576  0.0  0.0      0     0 ?        I    15:14   0:00 [kworker/u257:1-events_power_efficient]
root       1589  1.5  0.0      0     0 ?        I    15:17   0:17 [kworker/0:1-events]
root       1622  0.0  0.0      0     0 ?        I    15:24   0:00 [kworker/u258:2-events_power_efficient]
root       1642  1.6  0.0      0     0 ?        I    15:25   0:10 [kworker/1:0-events]
root       1650  0.0  0.0      0     0 ?        I    15:30   0:00 [kworker/0:0-cgroup_destroy]
root       1655  0.0  0.0      0     0 ?        I    15:31   0:00 [kworker/1:1-rcu_par_gp]
root       1657  0.0  0.0      0     0 ?        I    15:33   0:00 [kworker/u257:3-events_unbound]
root       1658  0.0  0.0      0     0 ?        I    15:33   0:00 [kworker/u258:0-events_unbound]
root       1673  2.2  2.1 477880 41340 ?        Ssl  15:35   0:00 /usr/libexec/fwupd/fwupd
root       1680  0.7  0.4 313956  8960 ?        Ssl  15:35   0:00 /usr/libexec/upowerd
root       1689  0.0  0.0      0     0 ?        I    15:35   0:00 [kworker/u257:4]
anara      1692  200  0.2  10684  4480 pts/1    R+   15:36   0:00 ps aux
anara      1693  0.0  0.0   5716  1920 pts/1    S+   15:36   0:00 tail -25
```

5. User Account Audit & Privilege Escalation Simulation

Scenario:

You are performing a user activity audit on a compromised Linux server. The SOC suspects a newly created account (lab4user) may have been used for unauthorized access.

Your task is to simulate the account creation, perform privilege tests, and analyze authentication logs for forensic evidence

1.Create a new test user named lab4user

```
anara@ubuntu:~$ sudo adduser lab4user
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 []: LAB 4 User
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] yes
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
```

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

```
anara@ubuntu:~$ cat /etc/passwd | grep lab4user
lab4user:x:1001:1001:LAB 4 User,,,:/home/lab4user:/bin/bash
```

3.Log in as lab4user and confirm successful login

```
anara@ubuntu:~$ su - lab4user
Password:
lab4user@ubuntu:~$
```

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

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

5.Switch back to your main analyst account.

```
lab4user@ubuntu:~$ exit
logout
anara@ubuntu:~$
```

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

```
anara@ubuntu:~$ sudo cat /var/log/auth.log | grep lab4user
[sudo] password for anara:
2025-10-17T08:12:32.323908+00:00 ubuntu sudo:    anara : TTY=pts/0 ; PWD=/home/anara ; USER=root ; COMMAND=/usr/sbin/
user lab4user
2025-10-17T08:12:32.627806+00:00 ubuntu groupadd[1579]: group added to /etc/group: name=lab4user, GID=1001
2025-10-17T08:12:32.632136+00:00 ubuntu groupadd[1579]: group added to /etc/gshadow: name=lab4user
2025-10-17T08:12:32.636100+00:00 ubuntu groupadd[1579]: new group: name=lab4user, GID=1001
2025-10-17T08:12:32.694845+00:00 ubuntu useradd[1586]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4us
 shell=/bin/bash, from=/dev/pts/1
2025-10-17T08:12:43.470521+00:00 ubuntu passwd[1599]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-17T08:14:41.578595+00:00 ubuntu chfn[1600]: changed user 'lab4user' information
2025-10-17T08:14:45.531730+00:00 ubuntu gpasswd[1608]: members of group users set by root to lab4user
2025-10-17T08:18:05.297862+00:00 ubuntu su[1626]: (to lab4user) anara on pts/0
2025-10-17T08:18:05.303218+00:00 ubuntu su[1626]: pam_unix(su-l:session): session opened for user lab4user(uid=1001)
anara(uid=1000)
2025-10-17T08:19:38.802542+00:00 ubuntu sudo: lab4user : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/lab4user ; USER=
t ; COMMAND=/usr/bin/whoami
2025-10-17T08:21:14.010833+00:00 ubuntu su[1626]: pam_unix(su-l:session): session closed for user lab4user
2025-10-17T08:22:39.139719+00:00 ubuntu sudo:    anara : TTY=pts/0 ; PWD=/home/anara ; USER=root ; COMMAND=/usr/sbin/
user --remove-home lab4user
```

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

```
anara@ubuntu:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
anara@ubuntu:~$ cat /etc/passwd | grep lab4user
anara@ubuntu:~$
```