Submitted to:-

Engr. Muhammad Shoaib

Submitted by:-

Hafsa Khalid

Reg no:-

2023-BSE-021

Section:-

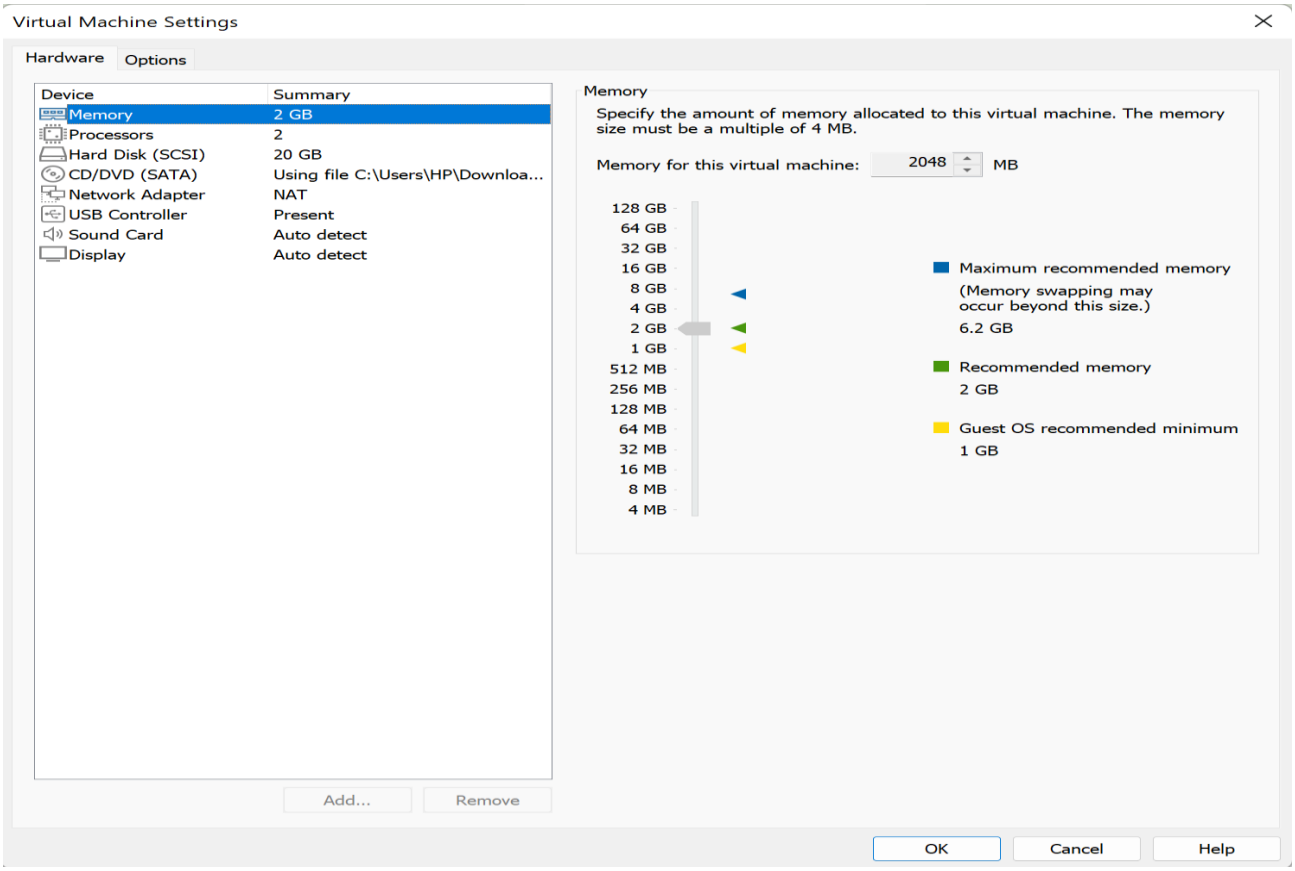
5 A

Cloud Computing

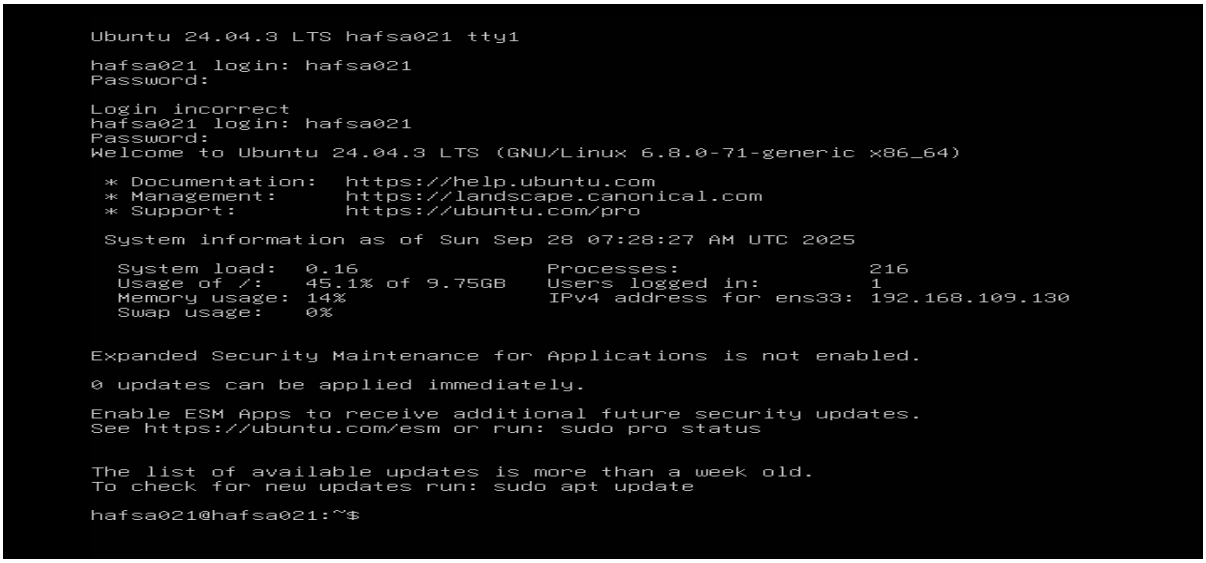
LAB O4

Virtualization & Linux Fundamentals

Task 1 – Verify VM resources in VMware



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



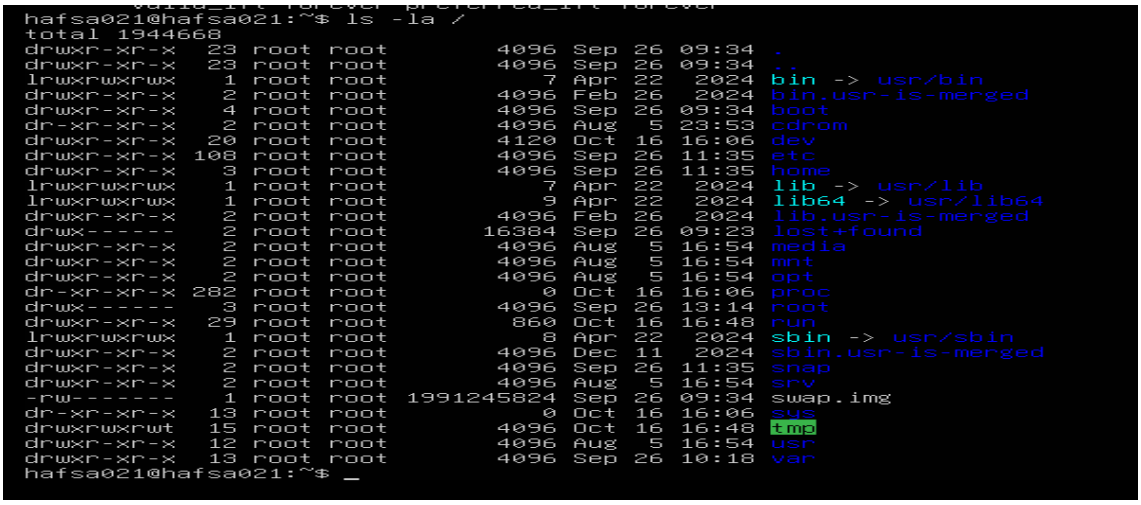
```
hafsa021@hafsa021:~$ pwd
/home/hafsa021
hafsa021@hafsa021:~$
```

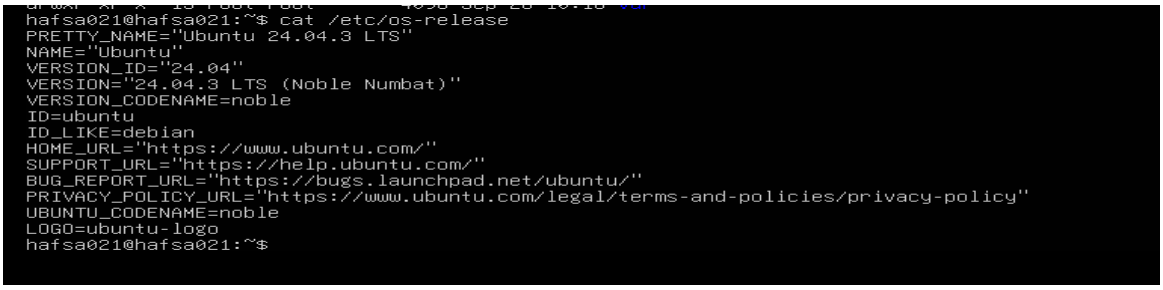
```
hafsa021@hafsa021:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2a:d1:a3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.109.130/24 metric 100 brd 192.168.109.255 scope global dynamic ens33
       valid_lft 1558sec preferred_lft 1558sec
    inet6 fe80::20c:29ff:fe2a:d1a3/64 scope link
       valid_lft forever preferred_lft forever
hafsa021@hafsa021:~$
```

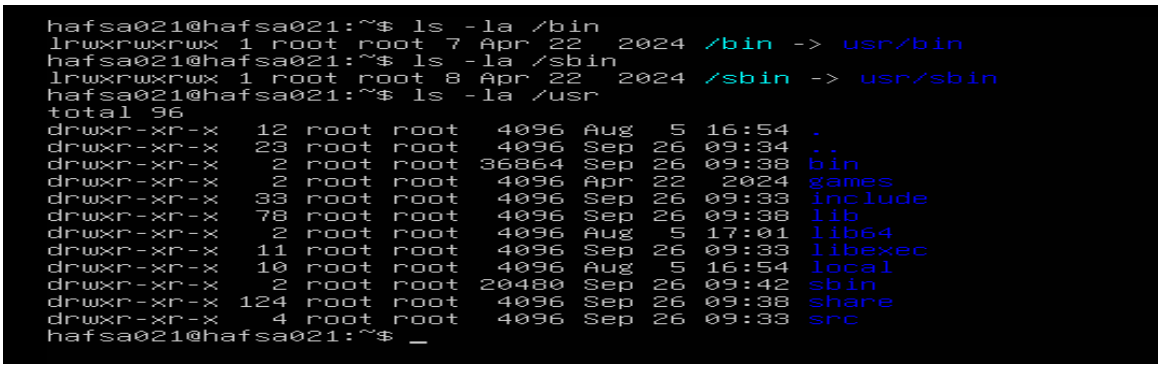
```
C:\Users\HP>ssh hafsa021@192.168.109.130
hafsa021@192.168.109.130's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

 System information as of Thu Oct 16 04:11:57 PM UTC 2025

  System load:  0.08              Processes:               250
  Usage of /:   45.3% of 9.75GB   Users logged in:         1
  Memory usage: 14%               IPv4 address for ens33: 192.168.109.130
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


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

Last login: Sun Sep 28 07:28:28 2025 from 192.168.109.1
hafsa021@hafsa021:~$
```

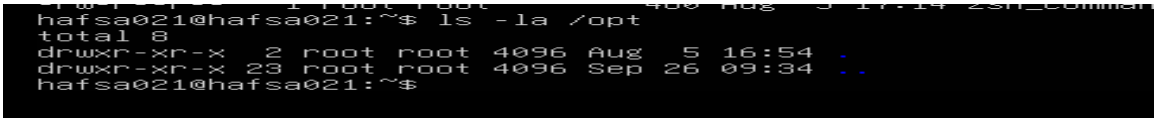
```
hafsa021@hafsa021:~$ whoami
hafsa021
hafsa021@hafsa021:~$ pwd
/home/hafsa021
hafsa021@hafsa021:~$
```

Task 3 – Filesystem exploration — root tree and dotfiles









```
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       970 Sep 26 11:35 shadow
-rw-r-----   1 root shadow       970 Sep 26 11:35 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 26 11:35 ssh
drwxr-xr-x   4 root root       4096 Aug  5 17:02 ssl
-rw-r--r--   1 root root         22 Sep 26 11:35 subgid
-rw-r--r--   1 root root          0 Aug  5 16:54 subgid-
-rw-r--r--   1 root root         22 Sep 26 11:35 subuid
-rw-r--r--   1 root root          0 Aug  5 16:54 subuid-
-rw-r--r--   1 root root       4343 Jun 25 12:42 sudo.conf
-r--r-----   1 root root       1800 Jan 29  2024 sudoers
drwxr-xr-x   2 root root       4096 Aug  5 17:02 sudoers.d
-rw-r--r--   1 root root       9804 Jun 25 12:42 sudo_logsrvd.conf
drwxr-xr-x   2 root root       4096 Aug  5 17:14 supercat
-rw-r--r--   1 root root       2209 Mar 24  2024 sysctl.conf
drwxr-xr-x   2 root root       4096 Aug  5 17:02 sysctl.d
drwxr-xr-x   2 root root       4096 Aug  5 17:14 sysstat
drwxr-xr-x   6 root root       4096 Aug  5 16:49 systemd
drwxr-xr-x   2 root root       4096 Aug  5 17:00 terminfo
drwxr-xr-x   2 root root       4096 Sep 26 09:33 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
drwxr-xr-x   2 root root       4096 Sep 26 09:33 UPower
-rw-r--r--   1 root root       1523 Aug  5 17:14 usb_modeswitch.conf
drwxr-xr-x   2 root root       4096 Aug  5 17:14 usb_modeswitch.d
lrwxrwxrwx   1 root root         16 Aug  5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x   2 root root       4096 Aug  5 17:14 vim
drwxr-xr-x   4 root root       4096 Aug  5 17:14 vmware-tools
lrwxrwxrwx   1 root root         23 Feb 26  2024 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
hafsa021@hafsa021:~$
```

```
hafsa021@hafsa021:~$ ls -la /dev
```

```
crw-rw----   1 root     dialout   4,  91 Oct 16 16:06 ttyS27
crw-rw----   1 root     dialout   4,  92 Oct 16 16:06 ttyS28
crw-rw----   1 root     dialout   4,  93 Oct 16 16:06 ttyS29
crw-rw----   1 root     dialout   4,  67 Oct 16 16:06 ttyS3
crw-rw----   1 root     dialout   4,  94 Oct 16 16:06 ttyS30
crw-rw----   1 root     dialout   4,  95 Oct 16 16:06 ttyS31
crw-rw----   1 root     dialout   4,  68 Oct 16 16:06 ttyS4
crw-rw----   1 root     dialout   4,  69 Oct 16 16:06 ttyS5
crw-rw----   1 root     dialout   4,  70 Oct 16 16:06 ttyS6
crw-rw----   1 root     dialout   4,  71 Oct 16 16:06 ttyS7
crw-rw----   1 root     dialout   4,  72 Oct 16 16:06 ttyS8
crw-rw----   1 root     dialout   4,  73 Oct 16 16:06 ttyS9
drwxr-xr-x   2 root     root          60 Oct 16 16:06 ubuntu-vg
crw-rw----   1 root     kvm      10, 124 Oct 16 16:06 udmabuf
crw-------   1 root     root     10, 239 Oct 16 16:06 uhid
crw-------   1 root     root     10, 223 Oct 16 16:06 uinput
crw-rw-rw-   1 root     root      1,   9 Oct 16 16:06 urandom
crw-------   1 root     root     10, 126 Oct 16 16:06 userfaultfd
crw-------   1 root     root     10, 240 Oct 16 16:06 userio
crw-rw----   1 root     tty       7,   0 Oct 16 16:06 vcs
crw-rw----   1 root     tty       7,   1 Oct 16 16:06 vcs1
crw-rw----   1 root     tty       7,   2 Oct 16 16:06 vcs2
crw-rw----   1 root     tty       7,   3 Oct 16 16:06 vcs3
crw-rw----   1 root     tty       7,   4 Oct 16 16:06 vcs4
crw-rw----   1 root     tty       7,   5 Oct 16 16:06 vcs5
crw-rw----   1 root     tty       7,   6 Oct 16 16:06 vcs6
crw-rw----   1 root     tty       7, 128 Oct 16 16:06 vcsa
crw-rw----   1 root     tty       7, 129 Oct 16 16:06 vcsa1
crw-rw----   1 root     tty       7, 130 Oct 16 16:06 vcsa2
crw-rw----   1 root     tty       7, 131 Oct 16 16:06 vcsa3
crw-rw----   1 root     tty       7, 132 Oct 16 16:06 vcsa4
crw-rw----   1 root     tty       7, 133 Oct 16 16:06 vcsa5
crw-rw----   1 root     tty       7, 134 Oct 16 16:06 vcsa6
crw-rw----   1 root     tty       7,  64 Oct 16 16:06 vcsu
crw-rw----   1 root     tty       7,  65 Oct 16 16:06 vcsu1
crw-rw----   1 root     tty       7,  66 Oct 16 16:06 vcsu2
crw-rw----   1 root     tty       7,  67 Oct 16 16:06 vcsu3
crw-rw----   1 root     tty       7,  68 Oct 16 16:06 vcsu4
crw-rw----   1 root     tty       7,  69 Oct 16 16:06 vcsu5
crw-rw----   1 root     tty       7,  70 Oct 16 16:06 vcsu6
drwxr-xr-x   2 root     root          60 Oct 16 16:06 vfio
crw-------   1 root     root     10, 127 Oct 16 16:06 vga_arbiter
crw-------   1 root     root     10, 137 Oct 16 16:06 vhci
crw-rw----   1 root     kvm      10, 238 Oct 16 16:06 vhost-net
crw-rw----   1 root     kvm      10, 241 Oct 16 16:06 vhost-vsock
crw-------   1 root     root     10, 122 Oct 16 16:06 vmci
crw-rw-rw-   1 root     root     10, 121 Oct 16 16:07 vsock
crw-rw-rw-   1 root     root      1,   5 Oct 16 16:06 zero
crw-------   1 root     root     10, 249 Oct 16 16:06 zfs
```

```
hafsa021@hafsa021:~$ ls -la /var
total 56
drwxr-xr-x 13 root root    4096 Sep 26 10:18 .
drwxr-xr-x 23 root root    4096 Sep 26 09:34 ..
drwxr-xr-x  2 root root    4096 Sep 27 06:00 backups
drwxr-xr-x 16 root root    4096 Sep 26 12:39 cache
drwxrwsrwt  2 root root    4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root    4096 Sep 26 12:39 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 16 16:07 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 16 16:48 tmp
-rw-r--r--  1 root root     208 Aug  5 16:54 .updated
hafsa021@hafsa021:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 16 16:48 .
drwxr-xr-x 23 root root 4096 Sep 26 09:34 ..
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .font-unix
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .ICE-unix
drwx------  2 root root 4096 Oct 16 16:06 snap-private-tmp
drwx------  3 root root 4096 Oct 16 16:48 systemd-private-0459fe5a1bac402a96f3642528caf1e5-fwupd.service-xqA4N3
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-ModemManager.service-a2MGeC
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-polkit.service-rQ5hkI
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-systemd-logind.service-AIG9iF
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-systemd-resolved.service-LQBaio
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-systemd-timesyncd.service-cnUcV2
drwx------  3 root root 4096 Oct 16 16:48 systemd-private-0459fe5a1bac402a96f3642528caf1e5-upower.service-c7LeFL
drwx------  2 root root 4096 Oct 16 16:06 vmware-root_742-2991137376
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .XIM-unix
hafsa021@hafsa021:~$ _
```

```
hafsa021@hafsa021:~$ ls -la ¬
ls: cannot access '¬': No such file or directory
hafsa021@hafsa021:~$ ls -la ~
total 32
drwxr-x--- 4 hafsa021 hafsa021 4096 Sep 26 12:08 .
drwxr-xr-x 3 root     root     4096 Sep 26 11:35 ..
-rw------- 1 hafsa021 hafsa021  481 Sep 27 18:45 .bash_history
-rw-r--r-- 1 hafsa021 hafsa021  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hafsa021 hafsa021 3771 Mar 31  2024 .bashrc
drwx------ 2 hafsa021 hafsa021 4096 Sep 26 11:35 .cache
-rw-r--r-- 1 hafsa021 hafsa021  807 Mar 31  2024 .profile
drwx------ 2 hafsa021 hafsa021 4096 Sep 27 06:20 .ssh
-rw-r--r-- 1 hafsa021 hafsa021    0 Sep 26 12:02 .sudo_as_admin_successful
hafsa021@hafsa021:~$ _
```

```
hafsa021@hafsa021:~$ nano ~/answers.md
```

```
 GNU nano 7.2                                  /home/hafsa021/answers.md
Myself Hafsa Khalid. I am a Software Engineering student at FJWU.
```

```
hafsa021@hafsa021:~$ cat ~/answers.md
Myself Hafsa Khalid. I am a Software Engineering student at FJWU.
```

Task 4 – Essential CLI tasks — navigation and file operations

```
hafsa021@hafsa021:~$ mkdir -p ~/lab4/workspace/python_project
hafsa021@hafsa021:~$ cd ~/lab4/workspace/python_project
hafsa021@hafsa021:~/lab4/workspace/python_project$ pwd
/home/hafsa021/lab4/workspace/python_project
hafsa021@hafsa021:~/lab4/workspace/python_project$ nano README.md_
```

```
 GNU nano 7.2                        README.md *                        S
Lab 4 Readme
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ nano main.py
```

```
  GNU nano 7.2                                                  main.py *
print("Hello Lab 4")_
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ nano .env_
```

```
  GNU nano 7.2                                                    .env *
ENV=Lab4
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 17:41 .
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 17:31 ..
-rw-rw-r-- 1 hafsa021 hafsa021    9 Oct 16 17:41 .env
-rw-rw-r-- 1 hafsa021 hafsa021   21 Oct 16 17:39 main.py
-rw-rw-r-- 1 hafsa021 hafsa021   13 Oct 16 17:35 README.md
hafsa021@hafsa021:~/lab4/workspace/python_project$
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 17:41 .
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 17:31 ..
-rw-rw-r-- 1 hafsa021 hafsa021    9 Oct 16 17:41 .env
-rw-rw-r-- 1 hafsa021 hafsa021   21 Oct 16 17:39 main.py
-rw-rw-r-- 1 hafsa021 hafsa021   13 Oct 16 17:35 README.md
hafsa021@hafsa021:~/lab4/workspace/python_project$ cp README.md README.copy.md
hafsa021@hafsa021:~/lab4/workspace/python_project$ mv README.copy.md README.dev.md
hafsa021@hafsa021:~/lab4/workspace/python_project$ rm README.dev.md
hafsa021@hafsa021:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
hafsa021@hafsa021:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
hafsa021@hafsa021:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 hafsa021 hafsa021 4096 Oct 16 17:47 .
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 17:31 ..
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 17:45 java_app
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 17:47 java_app_copy
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 17:44 python_project
hafsa021@hafsa021:~/lab4/workspace/python_project$
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ history_
```

```
15  ip addr show
16  sudo shutdown now
17  ip addr
18  sudo apt install isc-dhcp-client
19  sudo ip link set ens33 up
20  sudo apt install isc-dhcp-client
21  sudo ip link set ens33 up
22  sudo apt install isc-dhcp-client
23  sudo shutdown now
24  pwd
25  ip addr
26  ls -la /
27*
28  ls -la /bin
29  ls -la /sbin
30  ls -la /usr
31  ls -la /opt
32  ls -la /etc
33  ls -la /dev
34  ls -la /var
35  ls -la /tmp
36  clear
37  ls -la /bin
38  ls -la /sbin
39  ls -la /usr
40  ls -la /opt
41  ls -la /etc
42  ls -la /opt
43  ls -la /etc
44  ls -la /dev
45  ls -la /var
46  ls -la ¬
47  ls -la ~
48  nano ~/answers.md
49  cat ~/answers.md
50  mkdir -p ~/lab4/workspace/python_project
51  cd ~/lab4/workspace/python_project
52  pwd
53  nano README.md
54  nano main.py
55  nano .env
56  ls -la
57  cp README.md README.copy.md
58  mv README.copy.md README.dev.md
59  rm README.dev.md
60  mkdir -p ~/lab4/workspace/java_app
61  cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
62  ls -la ~/lab4/workspace
63  history
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ cat README.md
Lab 4 Readme
```

Task 5 – System info, resources & processes

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ uname -a
Linux hafsa021 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
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ 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 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 aes xsave avx f16
c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt xsaveopt xsave
c xgetbv1 xsaves arat flush_l1d arch_capabilities
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs srbds mmio_stale_data retbleed gds bhi
bogomips        : 5424.00
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) i5-7200U CPU @ 2.50GHz
stepping        : 9
microcode       : 0xffffffff
cpu MHz         : 2712.000
cache size      : 3072 KB
physical id     : 2
siblings        : 1
core id         : 0
cpu cores       : 1
apicid          : 2
initial apicid  : 2
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc
 arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx f16
c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt xsaveopt xsave
c xgetbv1 xsaves arat flush_l1d arch_capabilities
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs srbds mmio_stale_data retbleed gds bhi
bogomips        : 5424.00
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:

hafsa021@hafsa021:~/lab4/workspace/python_project$
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       367Mi       1.3Gi       1.2Mi       328Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
hafsa021@hafsa021:~/lab4/workspace/python_project$
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              192M  1.3M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  9.8G  4.5G  4.9G  48% /
tmpfs                              960M     0  960M   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.8G  100M  1.6G   7% /boot
tmpfs                              192M   12K  192M   1% /run/user/1000
hafsa021@hafsa021:~/lab4/workspace/python_project$ _
```

```
hafsa021@hafsa021:~/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
hafsa021@hafsa021:~/lab4/workspace/python_project$
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ ps aux
```

```
systemd+     635  0.0  0.6  21588 12672 ?        Ss   16:33   0:00 /usr/lib/systemd/systemd-resolved
systemd+     642  0.0  0.3  91024  7808 ?        Ssl  16:33   0:00 /usr/lib/systemd/systemd-timesyncd
root         701  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-cfg80]
root         705  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/57-vmw_vmci]
root         706  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/58-vmw_vmci]
root         708  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/59-vmw_vmci]
root         717  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/16-vmwgfx]
root         718  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-ttm]
root         741  0.0  0.6  53480 12032 ?        Ss   16:33   0:00 /usr/bin/VGAuthService
root         742  0.7  0.4 315856  9472 ?        Ssl  16:33   0:50 /usr/bin/vmtoolsd
message+     767  0.0  0.2   9792  5376 ?        Ss   16:33   0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-o
polkitd      792  0.0  0.4 308164  8064 ?        Ssl  16:33   0:00 /usr/lib/polkit-1/polkitd --no-debug
root         820  0.0  0.4  18128  8832 ?        Ss   16:33   0:00 /usr/lib/systemd/systemd-logind
root         824  0.0  0.6 468952 13568 ?        Ssl  16:33   0:00 /usr/libexec/udisks2/udisksd
syslog       850  0.0  0.2 222508  5888 ?        Ssl  16:33   0:00 /usr/sbin/rsyslogd -n -iNONE
root         873  0.0  0.1   6824  2688 ?        Ss   16:33   0:00 /usr/sbin/cron -f -P
root         907  0.0  1.1 109660 23040 ?        Ssl  16:33   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root         951  0.0  0.6 392028 12800 ?        Ssl  16:33   0:00 /usr/sbin/ModemManager
root         968  0.0  0.4  12020  8064 ?        Ss   16:33   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        1072  0.0  0.2   6948  4736 tty1     Ss   16:33   0:00 /bin/login -p --
root        1408  0.0  0.0      0     0 ?        S    16:34   0:00 [psimon]
hafsa021    1411  0.0  0.5  20272 11264 ?        Ss   16:34   0:00 /usr/lib/systemd/systemd --user
hafsa021    1413  0.0  0.1  21148  3516 ?        S    16:34   0:00 (sd-pam)
hafsa021    1424  0.0  0.2   8652  5632 tty1     S    16:34   0:00 -bash
root        1465  0.0  0.0      0     0 ?        I<   16:34   0:00 [kworker/R-tls-s]
root        1470  0.0  0.5  14964 10496 ?        Ss   16:38   0:00 sshd: hafsa021 [priv]
hafsa021    1532  0.0  0.3  15096  6852 ?        S    16:38   0:00 sshd: hafsa021@pts/0
hafsa021    1533  0.0  0.2   8648  5632 pts/0    Ss+  16:38   0:00 -bash
root        1571  0.0  2.2 594240 43460 ?        Ssl  16:48   0:04 /usr/libexec/fwupd/fwupd
root        1579  0.0  0.4 313996  8832 ?        Ssl  16:48   0:00 /usr/libexec/upowerd
root        1588  0.0  0.0      0     0 ?        I<   16:48   0:00 [kworker/1:0H-kblockd]
root        1604  0.0  0.1  81380  3000 ?        Ss   16:49   0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket --daemon
root        1655  0.0  0.0      0     0 ?        I    17:01   0:02 [kworker/0:1-events]
root        1779  0.0  0.0      0     0 ?        I    17:03   0:00 [kworker/u257:2-events_unbound]
root        1791  0.0  0.0      0     0 ?        I    17:08   0:01 [kworker/u258:0-events_unbound]
root        1824  0.0  0.0      0     0 ?        I<   17:17   0:00 [kworker/0:0H-kblockd]
root        1827  0.0  0.0      0     0 ?        I    17:19   0:00 [kworker/u257:1-events_power_efficient]
root        1843  0.0  0.0      0     0 ?        I    17:32   0:00 [kworker/u258:1-events_power_efficient]
root        1907  0.0  0.0      0     0 ?        I<   17:50   0:00 [kworker/0:2H]
root        1916  0.0  0.0      0     0 ?        I    18:00   0:00 [kworker/1:1]
root        1917  0.2  0.0      0     0 ?        I    18:00   0:02 [kworker/1:3-events]
root        1918  0.0  0.0      0     0 ?        I    18:00   0:00 [kworker/u258:3-events_power_efficient]
root        1923  0.3  0.0      0     0 ?        I    18:04   0:03 [kworker/0:0-events]
root        1928  0.0  0.0      0     0 ?        I    18:07   0:00 [kworker/u257:3-events_power_efficient]
root        1932  0.0  0.0      0     0 ?        I    18:13   0:00 [kworker/u257:0-events_power_efficient]
root        1940  0.0  0.0      0     0 ?        I<   18:15   0:00 [kworker/0:1H]
root        1943  0.0  0.0      0     0 ?        I    18:17   0:00 [kworker/u258:2-events_unbound]
root        1947  0.0  0.0      0     0 ?        I    18:17   0:00 [kworker/1:0-events]
hafsa021    1949  150  0.2  10884  4480 tty1     R+   18:17   0:00 ps aux
hafsa021@hafsa021:~/lab4/workspace/python_project$
```

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

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ sudo adduser lab4user
[sudo] password for hafsa021:
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' ...
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ su - lab4user
Password:
su: Authentication failure
hafsa021@hafsa021:~/lab4/workspace/python_project$ su - lab4user
Password:
lab4user@hafsa021:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@hafsa021:~$ exit
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
hafsa021@hafsa021:~/lab4/workspace/python_project$ _
```

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

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ nano ~/lab4/workspace/run-demo.sh
```

```
  GNU nano 7.2                                  /home/hafsa021/lab4/workspace/run-demo.sh *
#!/bin/bash
echo "Lab 4 demo: current user is $(whoaaami)"
echo "Current time: $(date)"
uptime
free -h
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ chmod +x ~/lab4/workspace/run-demo.sh
hafsa021@hafsa021:~/lab4/workspace/python_project$ ~/lab4/workspace/run-demo.sh
/home/hafsa021/lab4/workspace/run-demo.sh: line 2: whoaaami: command not found
Lab 4 demo: current user is
Current time: Thu Oct 16 06:54:33 PM UTC 2025
 18:54:33 up  2:21,  2 users,  load average: 0.00, 0.00, 0.00
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       393Mi       1.3Gi       1.2Mi       342Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
hafsa021@hafsa021:~/lab4/workspace/python_project$ _
```

```
hafsa021@hafsa021:~/lab4/workspace/python_project$ sudo ~/lab4/workspace/run-demo.sh
[sudo] password for hafsa021:
/home/hafsa021/lab4/workspace/run-demo.sh: line 2: whoaaami: command not found
Lab 4 demo: current user is
Current time: Thu Oct 16 06:55:38 PM UTC 2025
 18:55:38 up  2:22,  2 users,  load average: 0.00, 0.00, 0.00
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       391Mi       1.3Gi       1.2Mi       342Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
hafsa021@hafsa021:~/lab4/workspace/python_project$ _
```

Exam Evaluation Questions

1. Remote Access Verification (Cyber Login Check)

```
hafsa021@hafsa021:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2a:d1:a3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.109.130/24 metric 100 brd 192.168.109.255 scope global dynamic ens33
       valid_lft 1558sec preferred_lft 1558sec
    inet6 fe80::20c:29ff:fe2a:d1a3/64 scope link
       valid_lft forever preferred_lft forever
hafsa021@hafsa021:~$
```

```
C:\Users\HP>ssh hafsa021@192.168.109.130
hafsa021@192.168.109.130'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 Thu Oct 16 04:11:57 PM UTC 2025

  System load:  0.08              Processes:             250
  Usage of /:   45.3% of 9.75GB   Users logged in:       1
  Memory usage: 14%               IPv4 address for ens33: 192.168.109.130
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


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

Last login: Sun Sep 28 07:28:28 2025 from 192.168.109.1
hafsa021@hafsa021:~$
```

```
hafsa021@hafsa021:~$ uname -a
Linux hafsa021 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
hafsa021@hafsa021:~$ hostname
hafsa021
hafsa021@hafsa021:~$ 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
hafsa021@hafsa021:~$
```

```
hafsa021@hafsa021:~$ hostnamectl
 Static hostname: hafsa021
       Icon name: computer-vm
         Chassis: vm 
      Machine ID: cc52a4448ba24936a1d7ebab0f730799
         Boot ID: 0459fe5a1bac402a96f3642528caf1e5
  Virtualization: vmware
Operating System: Ubuntu 24.04.3 LTS
          Kernel: Linux 6.8.0-71-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 3d
hafsa021@hafsa021:~$
```

2. Filesystem Inspection for Forensic Evidence

```
hafsa021@hafsa021:~$ ls -la /
total 1944668
drwxr-xr-x  23 root root       4096 Sep 26 09:34 .
drwxr-xr-x  23 root root       4096 Sep 26 09:34 ..
lrwxrwxrwx   1 root root          7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x   2 root root       4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x   4 root root       4096 Sep 26 09:34 boot
dr-xr-xr-x   2 root root       4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root       4120 Oct 16 16:06 dev
drwxr-xr-x 108 root root       4096 Oct 16 18:38 etc
drwxr-xr-x   3 root root       4096 Oct 16 18:38 home
lrwxrwxrwx   1 root root          7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx   1 root root          9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x   2 root root       4096 Feb 26  2024 lib.usr-is-merged
drwx------   2 root root      16384 Sep 26 09:23 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 16 16:06 proc
hafsa021@hafsa021:~$
drwxr-xr-x  29 root root        900 Oct 16 18:31 run
lrwxrwxrwx   1 root root          8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root       4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x   2 root root       4096 Sep 26 11:35 snap
drwxr-xr-x   2 root root       4096 Aug  5 16:54 srv
-rw-------   1 root root 1991245824 Sep 26 09:34 swap.img
dr-xr-xr-x  13 root root          0 Oct 16 16:53 sys
drwxrwxrwt  15 root root       4096 Oct 16 19:05 tmp
drwxr-xr-x  12 root root       4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root       4096 Sep 26 10:18 var
```

```
hafsa021@hafsa021:~$ 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
hafsa021@hafsa021:~$ hostnamectl
 Static hostname: hafsa021
       Icon name: computer-vm
         Chassis: vm
      Machine ID: cc52a4448ba24936a1d7ebab0f730799
         Boot ID: 0459fe5a1bac402a96f3642528caf1e5
  Virtualization: vmware
Operating System: Ubuntu 24.04.3 LTS
          Kernel: Linux 6.8.0-71-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 3d
hafsa021@hafsa021:~$
```

```
hafsa021@hafsa021:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
hafsa021@hafsa021:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
hafsa021@hafsa021:~$ ls -la /usr
total 96
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Sep 26 09:34 ..
drwxr-xr-x   2 root root 36864 Sep 26 09:38 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root  4096 Sep 26 09:33 include
drwxr-xr-x  78 root root  4096 Sep 26 09:38 lib
drwxr-xr-x   2 root root  4096 Aug  5 17:01 lib64
drwxr-xr-x  11 root root  4096 Sep 26 09:33 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Sep 26 09:42 sbin
drwxr-xr-x 124 root root  4096 Sep 26 09:38 share
drwxr-xr-x   4 root root  4096 Sep 26 09:33 src
hafsa021@hafsa021:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 26 09:34 ..
hafsa021@hafsa021:~$
```

```
hafsa021@hafsa021:~$ ls -la /etc
total 936
drwxr-xr-x 108 root root       4096 Oct 16 18:38 .
drwxr-xr-x  23 root root       4096 Sep 26 09:34 ..
-rw-r--r--   1 root root       3444 Jul  5  2023 adduser.conf
drwxr-xr-x   2 root root       4096 Aug  5 17:14 alternatives
drwxr-xr-x   2 root root       4096 Aug  5 17:02 apparmor
drwxr-xr-x   9 root root       4096 Aug  5 17:14 apparmor.d
drwxr-xr-x   3 root root       4096 Aug  5 17:02 apport
drwxr-xr-x   9 root root       4096 Sep 26 09:19 apt
-rw-r--r--   1 root root       2319 Mar 31  2024 bash.bashrc
-rw-r--r--   1 root root         45 Aug  5 17:14 bash_completion
drwxr-xr-x   2 root root       4096 Aug  5 17:14 bash_completion.d
-rw-r--r--   1 root root        367 Aug  2  2022 bindresvport.blacklist
drwxr-xr-x   2 root root       4096 Jul  2 14:04 binfmt.d
drwxr-xr-x   2 root root       4096 Aug  5 17:14 byobu
drwxr-xr-x   3 root root       4096 Aug  5 17:02 ca-certificates
-rw-r--r--   1 root root       6288 Aug  5 17:02 ca-certificates.conf
drwxr-xr-x   5 root root       4096 Sep 26 11:35 cloud
drwxr-xr-x   2 root root       4096 Sep 26 09:24 console-setup
drwx------   2 root root       4096 Jul  2 14:04 credstore
drwx------   2 root root       4096 Jul  2 14:04 credstore.encrypted
drwxr-xr-x   2 root root       4096 Aug  5 17:14 cron.d
drwxr-xr-x   2 root root       4096 Aug  5 17:14 cron.daily
drwxr-xr-x   2 root root       4096 Aug  5 17:14 cron.hourly
drwxr-xr-x   2 root root       4096 Aug  5 17:14 cron.monthly
-rw-r--r--   1 root root       1136 Aug  5 17:14 crontab
drwxr-xr-x   2 root root       4096 Aug  5 17:14 cron.weekly
drwxr-xr-x   2 root root       4096 Aug  5 17:14 cron.yearly
drwxr-xr-x   2 root root       4096 Aug  5 17:02 cryptsetup-initramfs
-rw-r--r--   1 root root         54 Aug  5 17:02 crypttab
drwxr-xr-x   4 root root       4096 Aug  5 17:02 dbus-1
-rw-r--r--   1 root root       2967 Apr 12  2024 debconf.conf
-rw-r--r--   1 root root         11 Apr 22  2024 debian_version
drwxr-xr-x   3 root root       4096 Sep 26 09:38 default
-rw-r--r--   1 root root       1706 Jul  5  2023 deluser.conf
drwxr-xr-x   2 root root       4096 Aug  5 17:02 depmod.d
drwxr-xr-x   3 root root       4096 Aug  5 17:02 dhcp
-rw-r--r--   1 root root       1429 May  7  2024 dhcpcd.conf
drwxr-xr-x   4 root root       4096 Aug  5 17:01 dpkg
-rw-r--r--   1 root root        685 Apr  8  2024 e2scrub.conf
-rw-r--r--   1 root root        106 Aug  5 16:54 environment
-rw-r--r--   1 root root       1853 Oct 17  2022 ethertypes
drwxr-xr-x   4 root root       4096 Sep 26 09:33 fonts
-rw-r--r--   1 root root        657 Sep 26 09:34 fstab
-rw-r--r--   1 root root        694 Apr  8  2024 fuse.conf
drwxr-xr-x   4 root root       4096 Aug  5 17:14 fwupd
-rw-r--r--   1 root root       2584 Jan 31  2024 gai.conf
drwxr-xr-x   2 root root       4096 Aug  5 17:01 gnutls
drwxr-xr-x   2 root root       4096 Aug  5 17:02 groff
-rw-r--r--   1 root root        822 Oct 16 18:38 group
-rw-r--r--   1 root root        847 Oct 16 18:32 group-
drwxr-xr-x   2 root root       4096 Sep 26 09:28 grub.d
-rw-r-----   1 root shadow      699 Oct 16 18:38 gshadow
-rw-r-----   1 root shadow      720 Oct 16 18:32 gshadow-
drwxr-xr-x   3 root root       4096 Aug  5 17:02 gss
-rw-r--r--   1 root root       4436 Aug  5 17:14 hdparm.conf
-rw-r--r--   1 root root         92 Apr 22  2024 host.conf
-rw-r--r--   1 root root          9 Sep 26 09:38 hostname
-rw-r--r--   1 root root        223 Sep 26 09:38 hosts
```

```
hafsa021@hafsa021:~$ ls -la /dev
total 4
drwxr-xr-x  20 root     root        4120 Oct 16 16:06 .
drwxr-xr-x  23 root     root        4096 Sep 26 09:34 ..
crw-r--r--   1 root     root     10, 235 Oct 16 16:06 autofs
drwxr-xr-x   2 root     root         320 Oct 16 16:07 block
drwxr-xr-x   2 root     root          80 Oct 16 16:06 bsg
crw-rw----   1 root     disk     10, 234 Oct 16 16:06 btrfs-control
drwxr-xr-x   3 root     root          60 Oct 16 16:06 bus
lrwxrwxrwx   1 root     root           3 Oct 16 16:06 cdrom -> sr0
drwxr-xr-x   2 root     root        3700 Oct 16 17:11 char
crw--w----   1 root     tty       5,   1 Oct 16 16:06 console
lrwxrwxrwx   1 root     root          11 Oct 16 16:06 core -> /proc/kcore
drwxr-xr-x   4 root     root          80 Oct 16 16:06 cpu
crw-------   1 root     root     10, 123 Oct 16 16:06 cpu_dma_latency
crw-------   1 root     root     10, 203 Oct 16 16:06 cuse
drwxr-xr-x   8 root     root         160 Oct 16 16:06 disk
brw-rw----   1 root     disk    252,   0 Oct 16 16:06 dm-0
drwxr-xr-x   2 root     root          60 Oct 16 16:06 dma_heap
crw-rw----+  1 root     audio    14,   9 Oct 16 16:07 dmmidi
drwxr-xr-x   3 root     root         100 Oct 16 16:07 dri
crw-------   1 root     root     10, 125 Oct 16 16:06 ecryptfs
crw-rw----   1 root     video    29,   0 Oct 16 16:07 fb0
lrwxrwxrwx   1 root     root          13 Oct 16 16:06 fd -> /proc/self/fd
crw-rw-rw-   1 root     root      1,   7 Oct 16 16:06 full
crw-rw-rw-   1 root     root     10, 229 Oct 16 16:06 fuse
crw-------   1 root     root    241,   0 Oct 16 16:06 hidraw0
crw-------   1 root     root     10, 228 Oct 16 16:06 hpet
drwxr-xr-x   2 root     root           0 Oct 16 16:06 hugepages
crw-------   1 root     root     10, 183 Oct 16 16:06 hwrng
lrwxrwxrwx   1 root     root          12 Oct 16 16:06 initctl -> /run/initctl
drwxr-xr-x   4 root     root         260 Oct 16 16:06 input
crw-r--r--   1 root     root      1,  11 Oct 16 16:06 kmsg
lrwxrwxrwx   1 root     root          28 Oct 16 16:06 log -> /run/systemd/journal/dev-log
brw-rw----   1 root     disk      7,   0 Oct 16 16:07 loop0
brw-rw----   1 root     disk      7,   1 Oct 16 16:06 loop1
brw-rw----   1 root     disk      7,   2 Oct 16 16:06 loop2
brw-rw----   1 root     disk      7,   3 Oct 16 16:06 loop3
brw-rw----   1 root     disk      7,   4 Oct 16 16:06 loop4
brw-rw----   1 root     disk      7,   5 Oct 16 16:06 loop5
brw-rw----   1 root     disk      7,   6 Oct 16 16:06 loop6
brw-rw----   1 root     disk      7,   7 Oct 16 16:06 loop7
crw-rw----   1 root     disk     10, 237 Oct 16 16:06 loop-control
drwxr-xr-x   2 root     root          80 Oct 16 16:06 mapper
crw-------   1 root     root     10, 227 Oct 16 16:06 mcelog
crw-r-----   1 root     kmem      1,   1 Oct 16 16:06 mem
crw-rw----+  1 root     audio    14,   2 Oct 16 16:07 midi
drwxrwxrwt   2 root     root          40 Oct 16 16:06 mqueue
drwxr-xr-x   2 root     root          60 Oct 16 16:06 net
crw-rw-rw-   1 root     root      1,   3 Oct 16 16:06 null
crw-------   1 root     root     10, 144 Oct 16 16:06 nvram
crw-r-----   1 root     kmem      1,   4 Oct 16 16:06 port
crw-------   1 root     root    108,   0 Oct 16 16:06 ppp
crw-------   1 root     root     10,   1 Oct 16 16:06 psaux
crw-rw-rw-   1 root     tty       5,   2 Oct 16 19:15 ptmx
drwxr-xr-x   2 root     root           0 Oct 16 16:06 pts
crw-rw-rw-   1 root     root      1,   8 Oct 16 16:06 random
crw-rw-r--+  1 root     root     10, 242 Oct 16 16:06 rfkill
lrwxrwxrwx   1 root     root           4 Oct 16 16:06 rtc -> rtc0
crw-------   1 root     root    248,   0 Oct 16 16:06 rtc0
```

```
hafsa021@hafsa021:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Sep 26 10:18 .
drwxr-xr-x 23 root root   4096 Sep 26 09:34 ..
drwxr-xr-x  2 root root   4096 Sep 27 06:00 backups
drwxr-xr-x 16 root root   4096 Sep 26 12:39 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Sep 26 12:39 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 16 16:07 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 16 19:12 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
hafsa021@hafsa021:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 16 19:12 .
drwxr-xr-x 23 root root 4096 Sep 26 09:34 ..
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .font-unix
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .ICE-unix
drwx------  2 root root 4096 Oct 16 16:06 snap-private-tmp
drwx------  3 root root 4096 Oct 16 16:48 systemd-private-0459fe5a1bac402a96f3642528caf1e5-fwupd.service-xqA4N3
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-ModemManager.service-a2MGeC
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-polkit.service-rQ5hKI
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-systemd-logind.service-AIG9iF
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-systemd-resolved.service-LQBaio
drwx------  3 root root 4096 Oct 16 16:06 systemd-private-0459fe5a1bac402a96f3642528caf1e5-systemd-timesyncd.service-cnUcVZ
drwx------  3 root root 4096 Oct 16 16:48 systemd-private-0459fe5a1bac402a96f3642528caf1e5-upower.service-c7LeFL
drwx------  2 root root 4096 Oct 16 16:06 vmware-root_742-2991137376
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 16 16:06 .XIM-unix
hafsa021@hafsa021:~$
```

```
hafsa021@hafsa021:~$ ls -la ~
total 44
drwxr-x--- 6 hafsa021 hafsa021 4096 Oct 16 17:31 .
drwxr-xr-x 3 root     root     4096 Oct 16 18:38 ..
-rw-rw-r-- 1 hafsa021 hafsa021   66 Oct 16 17:20 answers.md
-rw------- 1 hafsa021 hafsa021  481 Sep 27 18:45 .bash_history
-rw-r--r-- 1 hafsa021 hafsa021  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hafsa021 hafsa021 3771 Mar 31  2024 .bashrc
drwx------ 2 hafsa021 hafsa021 4096 Sep 26 11:35 .cache
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 17:31 lab4
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 17:16 .local
-rw-r--r-- 1 hafsa021 hafsa021  807 Mar 31  2024 .profile
drwx------ 2 hafsa021 hafsa021 4096 Sep 27 06:20 .ssh
-rw-r--r-- 1 hafsa021 hafsa021    0 Sep 26 12:02 .sudo_as_admin_successful
hafsa021@hafsa021:~$
```

```
hafsa021@hafsa021:~$ nano ~/forensic_report.md
```

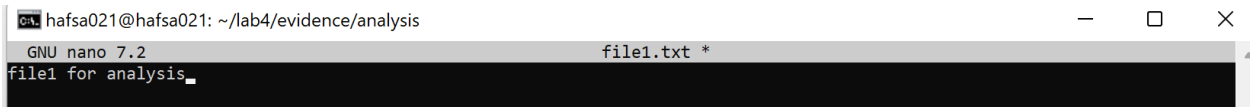
```
 GNU nano 7.2                        /home/hafsa021/forensic_report.md *
forensic report0
```

```
hafsa021@hafsa021:~$ hafsa021@hafsa021:~$ cat ~/forensic_report.md
forensic report0
```

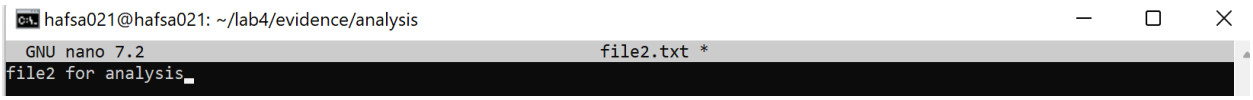
3. Evidence Handling & File Operations

```
hafsa021@hafsa021:~$ mkdir -p ~/lab4/evidence/analysis
hafsa021@hafsa021:~$ ls -la ~/lab4/evidence
total 12
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 19:31 .
drwxrwxr-x 4 hafsa021 hafsa021 4096 Oct 16 19:31 ..
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 19:31 analysis
hafsa021@hafsa021:~$
```

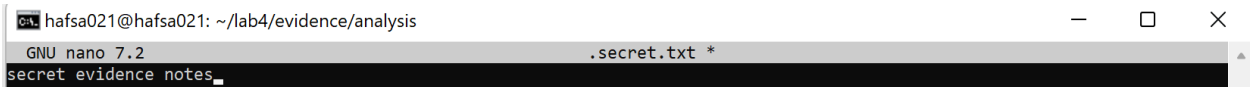
```
hafsa021@hafsa021:~/lab4/evidence/analysis$ nano file1.txt
```




```
hafsa021@hafsa021:~/lab4/evidence/analysis$ nano file2.txt
```




```
hafsa021@hafsa021:~/lab4/evidence/analysis$ nano .secret.txt
```




```
hafsa021@hafsa021:~/lab4/evidence/analysis$ ls -la
total 20
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 19:38 .
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 19:31 ..
-rw-rw-r-- 1 hafsa021 hafsa021   19 Oct 16 19:34 file1.txt
-rw-rw-r-- 1 hafsa021 hafsa021   19 Oct 16 19:35 file2.txt
-rw-rw-r-- 1 hafsa021 hafsa021   22 Oct 16 19:38 .secret.txt
hafsa021@hafsa021:~/lab4/evidence/analysis$
```

```
hafsa021@hafsa021:~/lab4/evidence/analysis$ cp file1.txt file1.bak.txt
hafsa021@hafsa021:~/lab4/evidence/analysis$ ls -la file1.txt file1.bak.txt
-rw-rw-r-- 1 hafsa021 hafsa021 19 Oct 16 19:39 file1.bak.txt
-rw-rw-r-- 1 hafsa021 hafsa021 19 Oct 16 19:34 file1.txt
hafsa021@hafsa021:~/lab4/evidence/analysis$ mv file1.bak.txt file1.verified.txt
hafsa021@hafsa021:~/lab4/evidence/analysis$ ls -la file1.verufied.txt
ls: cannot access 'file1.verufied.txt': No such file or directory
hafsa021@hafsa021:~/lab4/evidence/analysis$ ls -la file1.verified.txt
-rw-rw-r-- 1 hafsa021 hafsa021 19 Oct 16 19:39 file1.verified.txt
hafsa021@hafsa021:~/lab4/evidence/analysis$ rm file1.verified.txt
hafsa021@hafsa021:~/lab4/evidence/analysis$ ls =la
ls: cannot access '=la': No such file or directory
hafsa021@hafsa021:~/lab4/evidence/analysis$ ls -la
total 20
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 19:40 .
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 19:31 ..
-rw-rw-r-- 1 hafsa021 hafsa021   19 Oct 16 19:34 file1.txt
-rw-rw-r-- 1 hafsa021 hafsa021   19 Oct 16 19:35 file2.txt
-rw-rw-r-- 1 hafsa021 hafsa021   22 Oct 16 19:38 .secret.txt
hafsa021@hafsa021:~/lab4/evidence/analysis$
```

```
hafsa021@hafsa021:~/lab4/evidence/analysis$ cd ~/lab4/evidence
hafsa021@hafsa021:~/lab4/evidence$ cp -r ~/lab4/evidence ~/lab4/evidence_backup
hafsa021@hafsa021:~/lab4/evidence$ ls -la ~/lab4 | grep evidence
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 19:31 evidence
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 19:42 evidence_backup
hafsa021@hafsa021:~/lab4/evidence$ ls -la ~ls -la ~/lab4/evidence_backup
ls: cannot access '~ls': No such file or directory
/home/hafsa021/lab4/evidence_backup:
total 12
drwxrwxr-x 3 hafsa021 hafsa021 4096 Oct 16 19:42 .
drwxrwxr-x 5 hafsa021 hafsa021 4096 Oct 16 19:42 ..
drwxrwxr-x 2 hafsa021 hafsa021 4096 Oct 16 19:42 analysis
hafsa021@hafsa021:~/lab4/evidence$
```

```
    6  sudo apt install openssh-server -y
    7  sudo systemctl status ssh
    8  sudo systemctl start ssh
    9  sudo shutdown now
   10  ip addr
   11  sudo systemctl enable ssh
   12  ip addr
   13  sudo systemctl start ssh
   14  sudo systemctl status ssh
   15  ip addr show
   16  sudo shutdown now
   17  ip addr
   18  sudo apt install isc-dhcp-client
   19  sudo ip link set ens33 up
   20  sudo apt install isc-dhcp-client
   21  sudo ip link set ens33 up
   22  sudo apt install isc-dhcp-client
   23  sudo shutdown now
   24  whoami
   25  pwd
   26  cat REA
   27  uname -a
   28  hostname
   29  cat /etc/os-release
   30  hostnamectl
   31  ls -la /
   32  cat /etc/os-release
   33  hostnamectl
   34  ls -la /bin
   35  ls -la /sbin
   36  ls -la /usr
   37*
   38  ls -la /etc
   39  ls -la /dev
   40  ls -la /var
   41  ls -la /tmp
   42  ls -la ~
   43  nano ~/forensic_report.md
   44  cat ~/forensic_report.md
   45  mkdir -p ~/lab4/evidence/analysis
   46  ls -la ~/lab4/evidence
   47  cd ~/lab4/evidence/analysis
   48  nano file1.txt
   49  nano file2.txt
   50  nano .secret.txt
   51  ls -la
   52  cp file1.txt file1.bak.txt
   53  ls -la file1.txt file1.bak.txt
   54  mv file1.bak.txt file1.verified.txt
   55  ls -la file1.verufied.txt
   56  ls -la file1.verified.txt
   57  rm file1.verified.txt
   58  ls =la
   59  ls -la
   60  cd ~/lab4/evidence
   61  cp -r ~/lab4/evidence ~/lab4/evidence_backup
   62  ls -la ~/lab4 | grep evidence
   63  ls -la ~ls -la ~/lab4/evidence_backup
   64  history
hafsa021@hafsa021:~/lab4/evidence$
```

4. System Profiling and Process Monitoring

```
hafsa021@hafsa021:~/lab4/evidence$ uname -a
Linux hafsa021 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
hafsa021@hafsa021:~/lab4/evidence$ 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
hafsa021@hafsa021:~/lab4/evidence$
```

```
hafsa021@hafsa021:~/lab4/evidence$ 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) i5-7200U CPU @ 2.50GHz
    CPU family:           6
    Model:                142
    Thread(s) per core:   1
    Core(s) per socket:   1
    Socket(s):            2
    Stepping:             9
    BogoMIPS:             5424.00
    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 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 clflushopt xsaveopt xsavec xgetbv1 xsaves arat flush_                      l1d arch_capabil
ities
Virtualization features:
  Hypervisor vendor:      VMware
  Virtualization type:    full
Caches (sum of all):
  L1d:                    64 KiB (2 instances)
  L1i:                    64 KiB (2 instances)
  L2:                     512 KiB (2 instances)
  L3:                     6 MiB (2 instances)
NUMA:
  NUMA node(s):           1
  NUMA node0 CPU(s):      0,1
Vulnerabilities:
  Gather data sampling:   Unknown: Dependent on hypervisor status
  Itlb multihit:          Not affected
  L1tf:                   Mitigation; PTE Inversion
  Mds:                    Vulnerable: Clear CPU buffers attempted, no microcode; SMT Host state unknown
  Meltdown:               Mitigation; PTI
  Mmio stale data:        Vulnerable: Clear CPU buffers attempted, no microcode; SMT Host state unknown
  Reg file data sampling: Not affected
  Retbleed:               Mitigation; IBRS
  Spec rstack overflow:   Not affected
  Spec store bypass:      Mitigation; Speculative Store Bypass disabled via prctl
  Spectre v1:             Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:             Mitigation; IBRS; IBPB conditional; STIBP disabled; RSB filling; PBRSB-eIBRS Not affected; BHI SW
                          loop, KVM SW loop
  Srbds:                  Unknown: Dependent on hypervisor status
  Tsx async abort:        Not affected
hafsa021@hafsa021:~/lab4/evidence$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       409Mi       1.0Gi       1.3Mi       626Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
hafsa021@hafsa021:~/lab4/evidence$ 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
```

```
hafsa021@hafsa021:~/lab4/evidence$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.6  22028 13160 ?        Ss   16:33   0:06 /sbin/init
root           2  0.0  0.0      0     0 ?        S    16:33   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    16:33   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-netns]
root          11  0.0  0.0      0     0 ?        I    16:33   0:00 [kworker/u256:0-ext4-rsv-conversion]
root          12  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-mm_pe]
root          13  0.0  0.0      0     0 ?        I    16:33   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    16:33   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    16:33   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    16:33   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    16:33   0:01 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    16:33   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    16:33   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    16:33   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    16:33   0:00 [cpuhp/1]
root          22  0.0  0.0      0     0 ?        S    16:33   0:00 [idle_inject/1]
root          23  0.0  0.0      0     0 ?        S    16:33   0:00 [migration/1]
root          24  0.0  0.0      0     0 ?        S    16:33   0:00 [ksoftirqd/1]
root          29  0.0  0.0      0     0 ?        S    16:33   0:00 [kdevtmpfs]
root          30  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-inet_]
root          32  0.0  0.0      0     0 ?        S    16:33   0:00 [kauditd]
root          34  0.0  0.0      0     0 ?        S    16:33   0:00 [khungtaskd]
root          35  0.0  0.0      0     0 ?        S    16:33   0:00 [oom_reaper]
root          37  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-write]
root          38  0.0  0.0      0     0 ?        S    16:33   0:01 [kcompactd0]
root          39  0.0  0.0      0     0 ?        SN   16:33   0:00 [ksmd]
root          42  0.0  0.0      0     0 ?        SN   16:33   0:00 [khugepaged]
root          43  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-kinte]
root          44  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-kbloc]
root          45  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-blkcg]
root          46  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/9-acpi]
root          47  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-tpm_d]
root          48  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-ata_s]
root          49  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-md]
root          50  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-md_bi]
root          51  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-edac-]
root          52  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-devfr]
root          53  0.0  0.0      0     0 ?        S    16:33   0:00 [watchdogd]
root          55  0.0  0.0      0     0 ?        S    16:33   0:00 [kswapd0]
root          56  0.0  0.0      0     0 ?        S    16:33   0:00 [ecryptfs-kthread]
root          57  0.0  0.0      0     0 ?        I<   16:33   0:00 [kworker/R-kthro]
root          58  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/24-pciehp]
root          59  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/25-pciehp]
root          60  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/26-pciehp]
root          61  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/27-pciehp]
root          62  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/28-pciehp]
root          63  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/29-pciehp]
root          64  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/30-pciehp]
root          65  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/31-pciehp]
root          66  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/32-pciehp]
root          67  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/33-pciehp]
root          68  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/34-pciehp]
root          69  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/35-pciehp]
root          70  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/36-pciehp]
root          71  0.0  0.0      0     0 ?        S    16:33   0:00 [irq/37-pciehp]
```

5. User Account Audit & Privilege Escalation Simulation

```
hafsa021@hafsa021:~/lab4/evidence$ 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 []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
hafsa021@hafsa021:~/lab4/evidence$
```

```
hafsa021@hafsa021:~/lab4/evidence$ getent passwd lab4user
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
hafsa021@hafsa021:~/lab4/evidence$ su - lab4user
Password:
lab4user@hafsa021:~$
```

```
lab4user@hafsa021:~$ whoami
lab4user
lab4user@hafsa021:~$ pwd
/home/lab4user
lab4user@hafsa021:~$
```

```
lab4user@hafsa021:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@hafsa021:~$
```

```
lab4user@hafsa021:~$ exit
logout
hafsa021@hafsa021:~/lab4/evidence$
```

```
hafsa021@hafsa021:~/lab4/evidence$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
hafsa021@hafsa021:~/lab4/evidence$
```