Cloud Computing Lab

Lab #4

Submitted to:

Engr. Muhammad Shoaib

Submitted by:

Hania Akbar

Reg no:

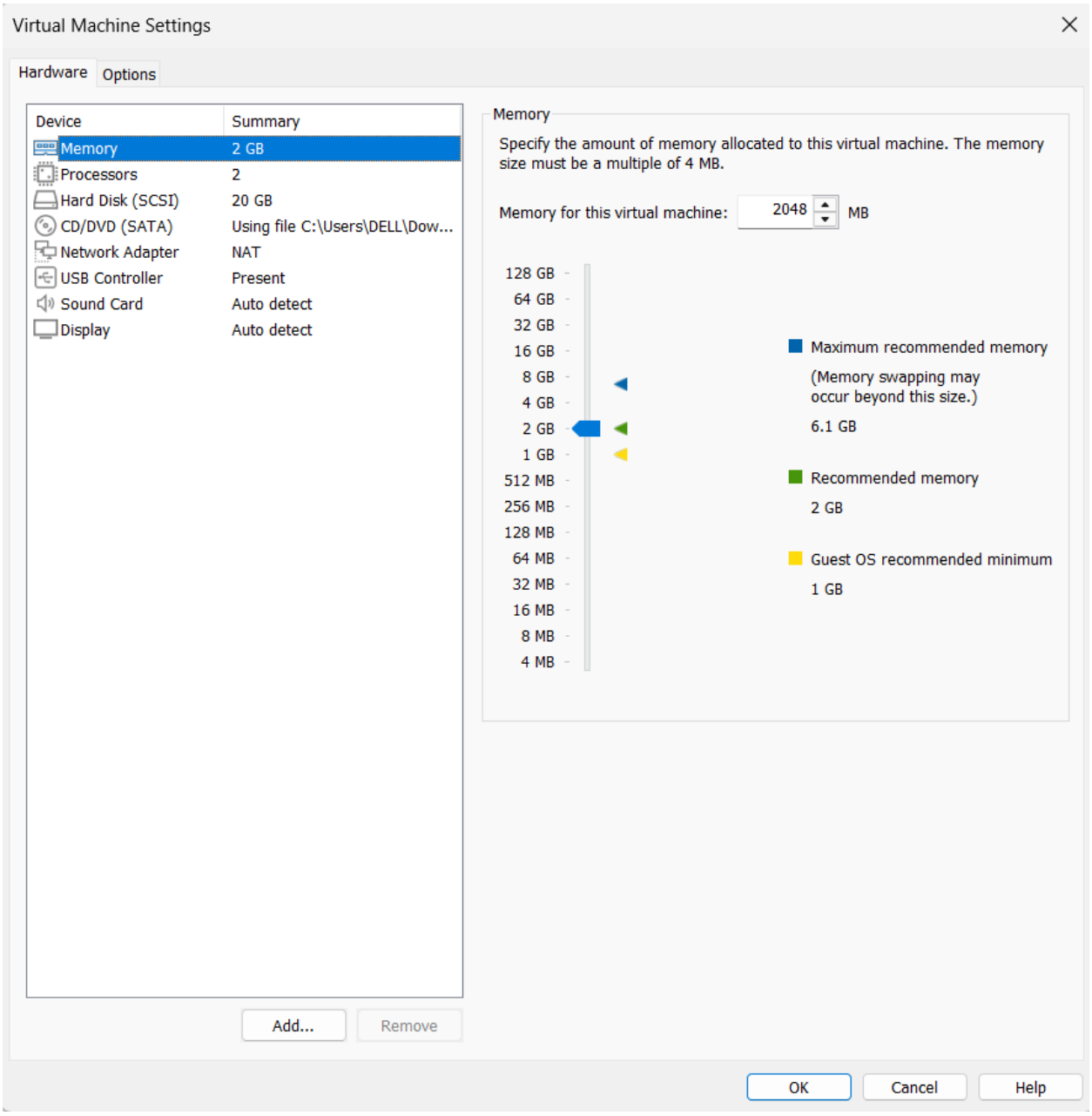
2023-BSE-026

Section:

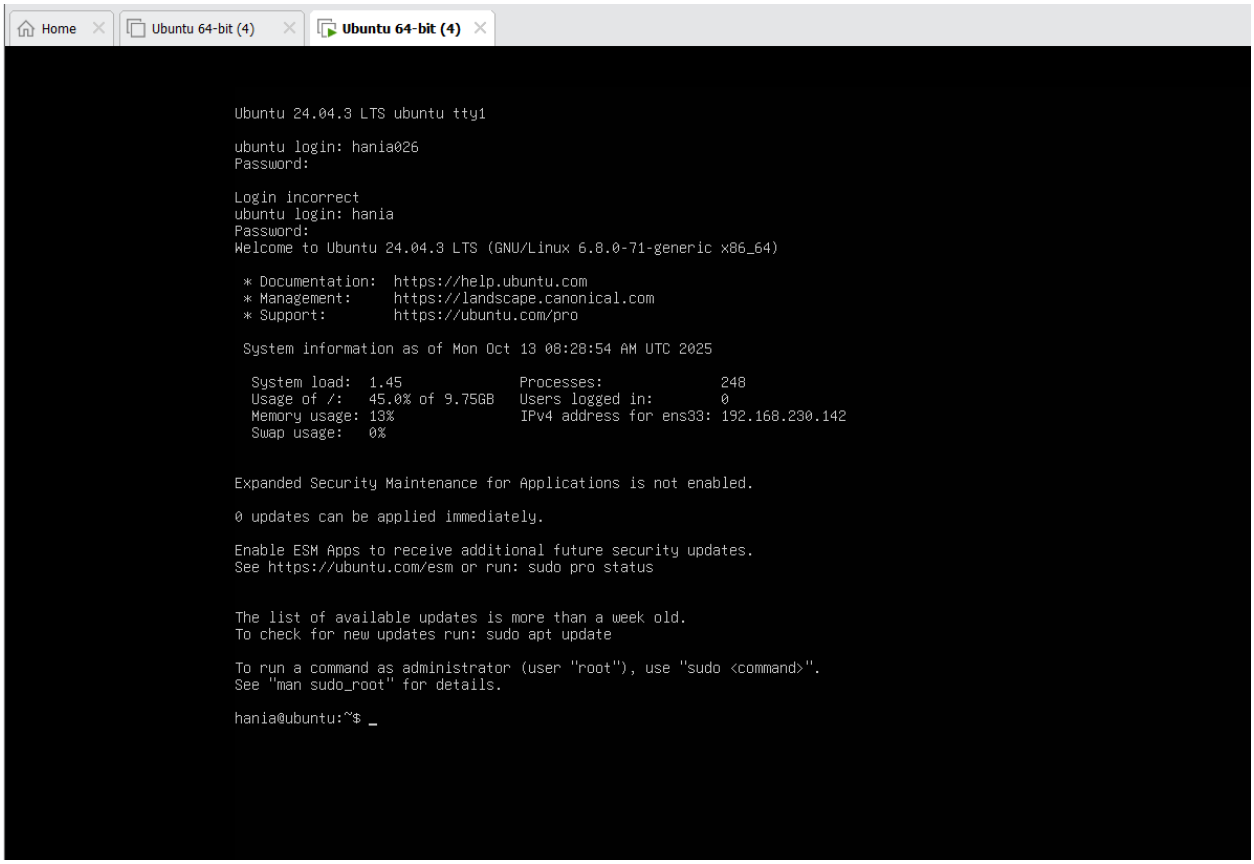
A

Lab 4

Task 1 – Verify VM resources in VMware



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




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

```
hania@ubuntu:~$ 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:29:76:e8:58 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.230.142/24 metric 100 brd 192.168.230.255 scope global dynamic ens33
       valid_lft 1666sec preferred_lft 1666sec
    inet6 fe80::20c:29ff:fe76:e858/64 scope link
       valid_lft forever preferred_lft forever
hania@ubuntu:~$
```

```
PS C:\Users\DELL> ssh hania@192.168.230.142
hania@192.168.230.142'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 24 06:53:46 AM UTC 2025

  System load:  0.0               Processes:             213
  Usage of /:   45.3% of 9.75GB   Users logged in:       1
  Memory usage: 14%               IPv4 address for ens33: 192.168.230.142
  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: Tue Sep 30 09:14:46 2025 from 192.168.230.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hania@ubuntu:~$
```

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

Task 3 – Filesystem exploration — root tree and dotfiles

```
hania@ubuntu:~$ ls -la /
total 1994844
drwxr-xr-x  23 root root       4096 Sep 29 05:09 .
drwxr-xr-x  23 root root       4096 Sep 29 05:09 ..
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 29 05:09 boot
dr-xr-xr-x   2 root root       4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root       4120 Oct 24 05:10 dev
drwxr-xr-x 108 root root       4096 Sep 29 05:28 etc
drwxr-xr-x   3 root root       4096 Sep 29 05:28 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 29 05:07 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 278 root root          0 Oct 24 05:10 proc
drwx------   3 root root       4096 Aug  5 17:02 root
drwxr-xr-x  28 root root        840 Oct 24 06:53 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 29 05:28 snap
drwxr-xr-x   2 root root       4096 Aug  5 16:54 srv
-rw-------   1 root root 2042626048 Sep 29 05:09 swap.img
dr-xr-xr-x  13 root root          0 Oct 24 05:10 sys
drwxrwxrwt  13 root root       4096 Oct 24 06:46 tmp
drwxr-xr-x  12 root root       4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root       4096 Sep 29 05:28 var
hania@ubuntu:~$ _
```

```
hania@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
hania@ubuntu:~$ _
```

```
hania@ubuntu:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
hania@ubuntu:~$ ls -ls /sbin
0 lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
hania@ubuntu:~$ ls -ls /usr
total 88
36 drwxr-xr-x   2 root root 36864 Sep 29 05:09 bin
 4 drwxr-xr-x   2 root root  4096 Apr 22  2024 games
 4 drwxr-xr-x  33 root root  4096 Sep 29 05:08 include
 4 drwxr-xr-x  78 root root  4096 Sep 29 05:09 lib
 4 drwxr-xr-x   2 root root  4096 Aug  5 17:01 lib64
 4 drwxr-xr-x  11 root root  4096 Sep 29 05:08 libexec
 4 drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
20 drwxr-xr-x   2 root root 20480 Sep 29 05:09 sbin
 4 drwxr-xr-x 124 root root  4096 Sep 29 05:09 share
 4 drwxr-xr-x   4 root root  4096 Sep 29 05:08 src
hania@ubuntu:~$ _
```

```
hania@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 29 05:09 ..
hania@ubuntu:~$
```

```
hania@ubuntu:~$ 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 29 05:28 shadow
-rw-r-----   1 root shadow      967 Sep 29 05:28 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 29 05:28 ssh
drwxr-xr-x   4 root root      4096 Aug  5 17:02 ssl
-rw-r--r--   1 root root        19 Sep 29 05:28 subgid
-rw-r--r--   1 root root         0 Aug  5 16:54 subgid-
-rw-r--r--   1 root root        19 Sep 29 05:28 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 29 05:09 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 29 05:09 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
hania@ubuntu:~$
```

```
hania@ubuntu:~$ ls -la /dev_
```

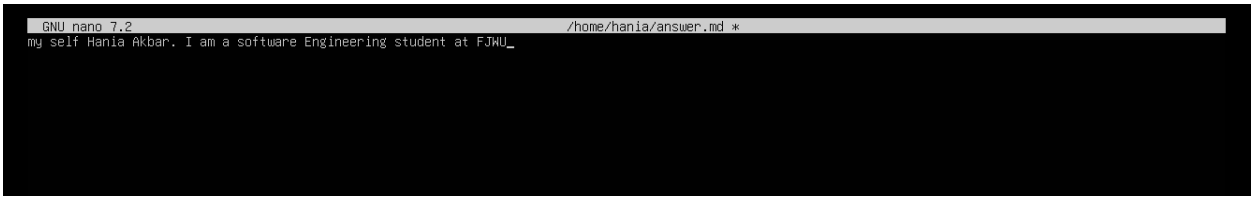
```
crw-rw----   1 root  dialout   4,  91 Oct 24 05:10 ttyS27
crw-rw----   1 root  dialout   4,  92 Oct 24 05:10 ttyS28
crw-rw----   1 root  dialout   4,  93 Oct 24 05:10 ttyS29
crw-rw----   1 root  dialout   4,  67 Oct 24 05:10 ttyS3
crw-rw----   1 root  dialout   4,  94 Oct 24 05:10 ttyS30
crw-rw----   1 root  dialout   4,  95 Oct 24 05:10 ttyS31
crw-rw----   1 root  dialout   4,  68 Oct 24 05:10 ttyS4
crw-rw----   1 root  dialout   4,  69 Oct 24 05:10 ttyS5
crw-rw----   1 root  dialout   4,  70 Oct 24 05:10 ttyS6
crw-rw----   1 root  dialout   4,  71 Oct 24 05:10 ttyS7
crw-rw----   1 root  dialout   4,  72 Oct 24 05:10 ttyS8
crw-rw----   1 root  dialout   4,  73 Oct 24 05:10 ttyS9
drwxr-xr-x   2 root  root          60 Oct 24 05:10 ubuntu-vg
crw-rw----   1 root  kvm      10, 124 Oct 24 05:10 udmabuf
crw-------   1 root  root     10, 239 Oct 24 05:10 uhid
crw-------   1 root  root     10, 223 Oct 24 05:10 uinput
crw-rw-rw-   1 root  root      1,   9 Oct 24 05:10 urandom
crw-------   1 root  root     10, 126 Oct 24 05:10 userfaultfd
crw-------   1 root  root     10, 240 Oct 24 05:10 userio
crw-rw----   1 root  tty       7,   0 Oct 24 05:10 vcs
crw-rw----   1 root  tty       7,   1 Oct 24 05:10 vcs1
crw-rw----   1 root  tty       7,   2 Oct 24 05:10 vcs2
crw-rw----   1 root  tty       7,   3 Oct 24 05:10 vcs3
crw-rw----   1 root  tty       7,   4 Oct 24 05:10 vcs4
crw-rw----   1 root  tty       7,   5 Oct 24 05:10 vcs5
crw-rw----   1 root  tty       7,   6 Oct 24 05:10 vcs6
crw-rw----   1 root  tty       7, 128 Oct 24 05:10 vcsa
crw-rw----   1 root  tty       7, 129 Oct 24 05:10 vcsa1
crw-rw----   1 root  tty       7, 130 Oct 24 05:10 vcsa2
crw-rw----   1 root  tty       7, 131 Oct 24 05:10 vcsa3
crw-rw----   1 root  tty       7, 132 Oct 24 05:10 vcsa4
crw-rw----   1 root  tty       7, 133 Oct 24 05:10 vcsa5
crw-rw----   1 root  tty       7, 134 Oct 24 05:10 vcsa6
crw-rw----   1 root  tty       7,  64 Oct 24 05:10 vcsu
crw-rw----   1 root  tty       7,  65 Oct 24 05:10 vcsu1
crw-rw----   1 root  tty       7,  66 Oct 24 05:10 vcsu2
crw-rw----   1 root  tty       7,  67 Oct 24 05:10 vcsu3
crw-rw----   1 root  tty       7,  68 Oct 24 05:10 vcsu4
crw-rw----   1 root  tty       7,  69 Oct 24 05:10 vcsu5
crw-rw----   1 root  tty       7,  70 Oct 24 05:10 vcsu6
drwxr-xr-x   2 root  root          60 Oct 24 05:10 vfio
crw-------   1 root  root     10, 127 Oct 24 05:10 vga_arbiter
crw-------   1 root  root     10, 137 Oct 24 05:10 vhci
crw-rw----   1 root  kvm      10, 238 Oct 24 05:10 vhost-net
crw-rw----   1 root  kvm      10, 241 Oct 24 05:10 vhost-vsock
crw-------   1 root  root     10, 122 Oct 24 05:10 vmci
crw-rw-rw-   1 root  root     10, 121 Oct 24 05:10 vsock
crw-rw-rw-   1 root  root      1,   5 Oct 24 05:10 zero
crw-------   1 root  root     10, 249 Oct 24 05:10 zfs
hania@ubuntu:~$ _
```

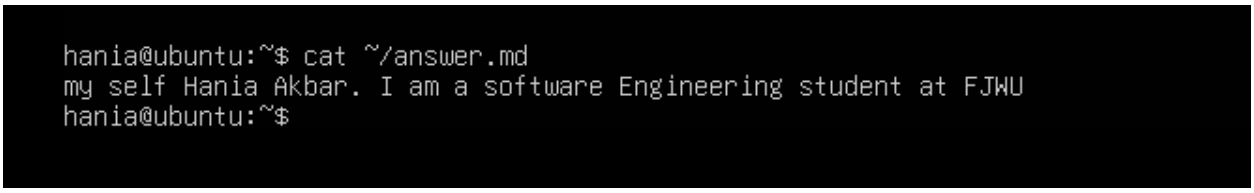
```
hania@ubuntu:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Sep 29 05:28 .
drwxr-xr-x 23 root root   4096 Sep 29 05:09 ..
drwxr-xr-x  2 root root   4096 Oct 24 05:05 backups
drwxr-xr-x 14 root root   4096 Sep 29 05:31 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 44 root root   4096 Sep 29 05:28 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 24 06:40 log
drwxrwsr-x  2 root mail   4096 Aug  5 16:54 mail
drwxr-xr-x  2 root root   4096 Aug  5 16:54 opt
lrwxrwxrwx  1 root root      4 Aug  5 16:54 run -> /run
drwxr-xr-x  2 root root   4096 May 21 15:46 snap
drwxr-xr-x  4 root root   4096 Aug  5 17:14 spool
drwxrwxrwt  7 root root   4096 Oct 24 06:46 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
hania@ubuntu:~$ _
```

```
hania@ubuntu:~$ ls -la /tmp
total 52
drwxrwxrwt 13 root root 4096 Oct 24 06:46 .
drwxr-xr-x 23 root root 4096 Sep 29 05:09 ..
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .font-unix
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .ICE-unix
drwx------  2 root root 4096 Oct 24 05:10 snap-private-tmp
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-ModemManager.service-gNYwO2
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-polkit.service-fxds4S
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-systemd-logind.service-vhvGVq
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-systemd-resolved.service-zsU2V8
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-systemd-timesyncd.service-xQzrYn
drwx------  2 root root 4096 Oct 24 05:10 vmware-root_740-2999460834
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .XIM-unix
hania@ubuntu:~$ _
```

```
hania@ubuntu:~$ ls -la ~
total 40
drwxr-x--- 4 hania hania 4096 Oct 13 08:32 .
drwxr-xr-x 3 root  root  4096 Sep 29 05:28 ..
-rw------- 1 hania hania   23 Oct 13 08:26 .bash_history
-rw-r--r-- 1 hania hania  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hania hania 3771 Mar 31  2024 .bashrc
drwx------ 2 hania hania 4096 Sep 29 05:31 .cache
-rw-r--r-- 1 hania hania  807 Mar 31  2024 .profile
drwx------ 2 hania hania 4096 Sep 29 05:42 .ssh
-rw-rw-r-- 1 hania hania   44 Oct 13 08:33 trmif
-rw------- 1 hania hania  694 Oct 13 08:26 .viminfo
hania@ubuntu:~$ _
```

```
hania@ubuntu:~$ nano ~/answer.md_
```





Task 4 – Essential CLI tasks — navigation and file operations

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

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

```
 GNU nano 7.2                                                    .env *
ENV=Lab 4
```

```
hania@ubuntu:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 hania hania 4096 Oct 24 07:17 .
drwxrwxr-x 3 hania hania 4096 Oct 24 07:12 ..
-rw-rw-r-- 1 hania hania   10 Oct 24 07:17 .env
-rw-rw-r-- 1 hania hania   22 Oct 24 07:16 main.py
-rw-rw-r-- 1 hania hania   13 Oct 24 07:14 README.md
hania@ubuntu:~/lab4/workspace/python_project$ _
```

```
hania@ubuntu:~/lab4/workspace/python_project$ cp README.md README.copy.md
hania@ubuntu:~/lab4/workspace/python_project$ mv README.copy.md README.dev.md
hania@ubuntu:~/lab4/workspace/python_project$ rm README.dev.md
hania@ubuntu:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
hania@ubuntu:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
hania@ubuntu:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 hania hania 4096 Oct 24 07:23 .
drwxrwxr-x 3 hania hania 4096 Oct 24 07:12 ..
drwxrwxr-x 2 hania hania 4096 Oct 24 07:22 java_app
drwxrwxr-x 2 hania hania 4096 Oct 24 07:23 java_app_copy
drwxrwxr-x 2 hania hania 4096 Oct 24 07:21 python_project
hania@ubuntu:~/lab4/workspace/python_project$
```

```
hania@ubuntu:~/lab4/workspace/python_project$ history
    1  ip addr
    2  vi nestedif.sh
    3  pwd
    4  ip addr
    5  hostname -I
    6  ls -la /
    7  cat /etc/os-release
    8  ls -la /bin
    9  ls -ls /sbin
   10  ls -ls /usr
   11  ls -la /opt
   12  ls -la /etc
   13  ls -la /bin
   14  ls -ls /sbin
   15* 
   16  ls -la /opt
   17  ls -la /etc
   18  l
   19  ls -la /dev
   20  ls -la /var
   21  ls -la /tmp
   22  ls -la~
   23  ls -la ~
   24  nano ~/answer.md
   25  cat ~/answer.md
   26  mkdir -p ~/lab4/workspace/python_project
   27  cd ~/lab4/workspace/python_project
   28  pwd
   29  nano README.md
   30  nano main.py
   31  nano.env
   32  ls -la
   33  cp README.md README.copy.md
   34  mv README.copy.md README.dev.md
   35  rm README.dev.md
   36  mkdir -p ~/lab4/workspace/java_app
   37  cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
   38  ls -la ~/lab4/workspace
   39  history
hania@ubuntu:~/lab4/workspace/python_project$ _
```

```
hania@ubuntu:~/lab4/workspace/python_project$ cat README.md
Lab 4 README
hania@ubuntu:~/lab4/workspace/python_project$ _
```

Task 5 – System info, resources & processes

```
hania@ubuntu:~/lab4/workspace/python_project$ 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
hania@ubuntu:~/lab4/workspace/python_project$
```

```
hania@ubuntu:~/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 md_clear 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        : 3599.99
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) i5-8250U CPU @ 1.60GHz
stepping        : 10
microcode       : 0xffffffff
cpu MHz         : 1799.997
cache size      : 6144 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 md_clear 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        : 3599.99
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:

hania@ubuntu:~/lab4/workspace/python_project$ _
```

```
hania@ubuntu:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       403Mi       1.3Gi       1.2Mi       337Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
hania@ubuntu:~/lab4/workspace/python_project$
```

```
hania@ubuntu:~/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
hania@ubuntu:~/lab4/workspace/python_project$ _
```

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

```
hania@ubuntu:~/lab4/workspace/python_project$ ps aux
```

```
root         490  0.0  0.0      0     0 ?        I    06:39   0:00 [kworker/u256:1]
root         491  0.0  1.3 354628 27392 ?        SLsl 06:39   0:00 /sbin/multipathd -d -s
root         508  0.0  0.4  30256  8960 ?        Ss   06:39   0:00 /usr/lib/systemd/systemd-udevd
root         516  0.0  0.0      0     0 ?        S    06:39   0:00 [psimon]
root         589  0.0  0.0      0     0 ?        S    06:39   0:00 [jbd2/sda2-8]
root         590  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-ext4-]
systemd+     655  0.0  0.6  21580 12800 ?        Ss   06:39   0:00 /usr/lib/systemd/systemd-resolved
systemd+     660  0.0  0.3  91024  7808 ?        Ssl  06:39   0:00 /usr/lib/systemd/systemd-timesyncd
root         689  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-cfg80]
root         736  0.0  0.6  53464 12032 ?        Ss   06:39   0:00 /usr/bin/VGAuthService
root         737  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/57-vmw_vmci]
root         738  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/58-vmw_vmci]
root         739  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/59-vmw_vmci]
root         740  0.3  0.4 242124  9344 ?        Ssl  06:39   0:10 /usr/bin/vmtoolsd
root         766  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/16-vmwgfx]
root         767  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-ttm]
message+     787  0.0  0.2   9804  5376 ?        Ss   06:39   0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-o
polkitd      807  0.0  0.4 308164  7936 ?        Ssl  06:39   0:00 /usr/lib/polkit-1/polkitd --no-debug
root         815  0.0  0.4  18144  8704 ?        Ss   06:39   0:00 /usr/lib/systemd/systemd-logind
root         816  0.0  0.6 468952 13568 ?        Ssl  06:39   0:00 /usr/libexec/udisks2/udisksd
root         869  0.0  0.1   6824  2688 ?        Ss   06:39   0:00 /usr/sbin/cron -f -P
root         882  0.0  1.1 109660 22912 ?        Ssl  06:39   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
syslog       888  0.0  0.3 222508  6128 ?        Ssl  06:39   0:00 /usr/sbin/rsyslogd -n -iNONE
root         934  0.0  0.6 392028 12800 ?        Ssl  06:39   0:00 /usr/sbin/ModemManager
root         995  0.0  0.2   6948  4608 tty1     Ss   06:39   0:00 /bin/login -p --
systemd+    1491  0.0  0.4  18992  9472 ?        Ss   06:40   0:00 /usr/lib/systemd/systemd-networkd
root        1816  0.0  0.0      0     0 ?        S    06:40   0:00 [psimon]
hania       1818  0.0  0.5  20088 10880 ?        Ss   06:40   0:00 /usr/lib/systemd/systemd --user
hania       1821  0.0  0.1  21152  3520 ?        S    06:40   0:00 (sd-pam)
hania       1841  0.0  0.2   8656  5632 tty1     S    06:40   0:00 -bash
root        1888  0.0  0.0      0     0 ?        I<   06:40   0:00 [kworker/R-tls-s]
root        1899  0.0  0.0      0     0 ?        I    06:46   0:00 [kworker/u258:2-events_power_efficient]
root        1908  0.0  0.4  12020  7936 ?        Ss   06:47   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        1920  0.0  0.5  14956 10368 ?        Ss   06:53   0:00 sshd: hania [priv]
hania       1978  0.0  0.3  15116  6972 ?        S    06:53   0:00 sshd: hania@pts/0
hania       1979  0.0  0.2   8648  5504 pts/0    Ss+  06:53   0:00 -bash
root        2092  0.5  0.0      0     0 ?        I    07:10   0:07 [kworker/0:0-events]
root        2102  0.3  2.2 669304 43368 ?        Ssl  07:14   0:03 /usr/libexec/fwupd/fwupd
root        2109  0.0  0.4 313996  8832 ?        Ssl  07:14   0:00 /usr/libexec/upowerd
root        2134  0.0  0.1  81380  2872 ?        Ss   07:14   0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket --daemon
root        2149  0.3  0.0      0     0 ?        I    07:14   0:03 [kworker/1:0-events]
root        2155  0.0  0.0      0     0 ?        I    07:15   0:00 [kworker/u257:0-events_power_efficient]
root        2157  0.0  0.0      0     0 ?        I    07:16   0:00 [kworker/u258:1-events_unbound]
root        2175  0.0  0.0      0     0 ?        I    07:20   0:00 [kworker/0:3]
root        2179  0.0  0.0      0     0 ?        I    07:21   0:00 [kworker/u258:0-events_power_efficient]
root        2184  0.0  0.0      0     0 ?        I    07:24   0:00 [kworker/u257:1-events_power_efficient]
root        2195  0.0  0.0      0     0 ?        I    07:30   0:00 [kworker/u258:3-events_power_efficient]
root        2198  0.0  0.0      0     0 ?        I    07:30   0:00 [kworker/1:1-cgroup_destroy]
hania       2207  500  0.2  10884  4480 tty1     R+   07:32   0:00 ps aux
hania@ubuntu:~/lab4/workspace/python_project$
```

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

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

```
hania@ubuntu:~/lab4/workspace/python_project$ su - lab4user
Password:
lab4user@ubuntu:~$ _
```

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

```
hania@ubuntu:~/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' ...
hania@ubuntu:~/lab4/workspace/python_project$ _
```

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

```
hania@ubuntu:~/lab4/workspace/python_project$ nano ~/lab4/workspace/run-demo.sh_
```

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

Exam Evaluation Questions

1. Remote Access Verification (Cyber Login Check)

```
hania@ubuntu:~/lab4/workspace/python_project$ 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:29:76:e8:58 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.230.142/24 metric 100 brd 192.168.230.255 scope global dynamic ens33
       valid_lft 1726sec preferred_lft 1726sec
    inet6 fe80::20c:29ff:fe76:e858/64 scope link
       valid_lft forever preferred_lft forever
hania@ubuntu:~/lab4/workspace/python_project$
```

```
PS C:\Users\DELL> ssh hania@192.168.230.142
hania@192.168.230.142'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 24 06:53:46 AM UTC 2025

  System load:  0.0               Processes:             213
  Usage of /:   45.3% of 9.75GB   Users logged in:       1
  Memory usage: 14%               IPv4 address for ens33: 192.168.230.142
  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: Tue Sep 30 09:14:46 2025 from 192.168.230.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hania@ubuntu:~$
```

```
hania@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
hania@ubuntu:~$
```

```
hania@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
hania@ubuntu:~$ hostname
ubuntu
hania@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
```

```
hania@ubuntu:~$ hostnamectl
 Static hostname: ubuntu
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 5ead0d62e68a405d87adafdb12aae965
         Boot ID: 14e9cf42ad6143c6889ccbfc043e9ef3
  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 1w 4d
hania@ubuntu:~$
```

2.Filesystem Inspection for Forensic Evidence

```
hania@ubuntu:~$ ls -la
total 52
drwxr-x--- 6 hania hania 4096 Oct 24 07:33 .
drwxr-xr-x 3 root  root  4096 Oct 24 07:37 ..
-rw-rw-r-- 1 hania hania   65 Oct 24 07:10 answer.md
-rw------- 1 hania hania   23 Oct 13 08:26 .bash_history
-rw-r--r-- 1 hania hania  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hania hania 3771 Mar 31  2024 .bashrc
drwx------ 2 hania hania 4096 Sep 29 05:31 .cache
drwxrwxr-x 3 hania hania 4096 Oct 24 07:12 lab4
drwxrwxr-x 3 hania hania 4096 Oct 24 07:09 .local
-rw-r--r-- 1 hania hania  807 Mar 31  2024 .profile
drwx------ 2 hania hania 4096 Sep 29 05:42 .ssh
-rw-r--r-- 1 hania hania    0 Oct 24 07:33 .sudo_as_admin_successful
-rw-rw-r-- 1 hania hania   44 Oct 13 08:33 trmif
-rw------- 1 hania hania  694 Oct 13 08:26 .viminfo
hania@ubuntu:~$
```

```
hania@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
hania@ubuntu:~$ hostnamectl
 Static hostname: ubuntu
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 5ead0d62e68a405d87adafdb12aae965
         Boot ID: 14e9cf42ad6143c6889ccbfc043e9ef3
  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 1w 4d
hania@ubuntu:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
hania@ubuntu:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
```

```
hania@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 29 05:09 ..
drwxr-xr-x   2 root root 36864 Sep 29 05:09 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root  4096 Sep 29 05:08 include
drwxr-xr-x  78 root root  4096 Sep 29 05:09 lib
drwxr-xr-x   2 root root  4096 Aug  5 17:01 lib64
drwxr-xr-x  11 root root  4096 Sep 29 05:08 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Sep 29 05:09 sbin
drwxr-xr-x 124 root root  4096 Sep 29 05:09 share
drwxr-xr-x   4 root root  4096 Sep 29 05:08 src
hania@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 29 05:09 ..
```

```
hania@ubuntu:~$ ls -la /etc
total 936
drwxr-xr-x 108 root root       4096 Oct 24 07:37 .
drwxr-xr-x  23 root root       4096 Sep 29 05:09 ..
-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 29 05:07 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 29 05:28 cloud
drwxr-xr-x   2 root root       4096 Sep 29 05:08 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 29 05:09 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 29 05:09 fonts
-rw-r--r--   1 root root        657 Sep 29 05:09 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      12813 Mar 27  2021 services
drwxr-xr-x   2 root root       4096 Aug  5 17:02 sgml
-rw-r-----   1 root shadow      967 Oct 24 07:37 shadow
-rw-r-----   1 root shadow     1069 Oct 24 07:33 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 29 05:28 ssh
drwxr-xr-x   4 root root       4096 Aug  5 17:02 ssl
-rw-r--r--   1 root root         19 Oct 24 07:37 subgid
-rw-r--r--   1 root root         41 Oct 24 07:33 subgid-
-rw-r--r--   1 root root         19 Oct 24 07:37 subuid
-rw-r--r--   1 root root         41 Oct 24 07:33 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 29 05:09 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 29 05:09 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
```

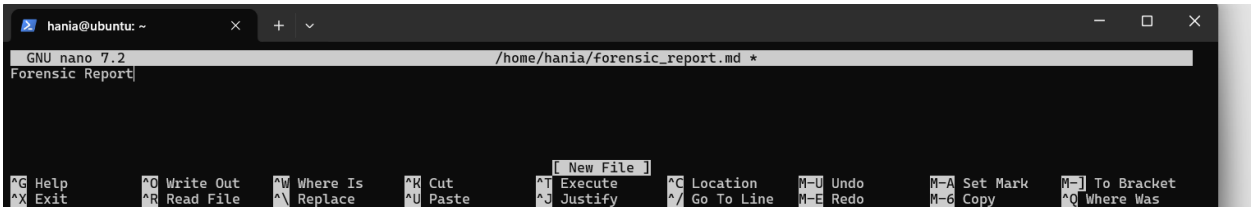
```
hania@ubuntu:~$ ls -la /dev
total 4
drwxr-xr-x  20 root  root        4120 Oct 24 05:10 .
drwxr-xr-x  23 root  root        4096 Sep 29 05:09 ..
crw-r--r--   1 root  root     10, 235 Oct 24 05:10 autofs
drwxr-xr-x   2 root  root         320 Oct 24 05:10 block
drwxr-xr-x   2 root  root          80 Oct 24 05:10 bsg
crw-rw----   1 root  disk     10, 234 Oct 24 05:10 btrfs-control
drwxr-xr-x   3 root  root          60 Oct 24 05:10 bus
lrwxrwxrwx   1 root  root           3 Oct 24 05:10 cdrom -> sr0
drwxr-xr-x   2 root  root        3700 Oct 24 07:49 char
crw--w----   1 root  tty       5,   1 Oct 24 05:10 console
lrwxrwxrwx   1 root  root          11 Oct 24 05:10 core -> /proc/kcore
drwxr-xr-x   4 root  root          80 Oct 24 05:10 cpu
crw-------   1 root  root     10, 123 Oct 24 05:10 cpu_dma_latency
crw-------   1 root  root     10, 203 Oct 24 05:10 cuse
drwxr-xr-x   8 root  root         160 Oct 24 05:10 disk
brw-rw----   1 root  disk    252,   0 Oct 24 05:10 dm-0
drwxr-xr-x   2 root  root          60 Oct 24 05:10 dma_heap
crw-rw----+  1 root  audio    14,   9 Oct 24 05:10 dmmidi
drwxr-xr-x   3 root  root         100 Oct 24 05:10 dri
crw-------   1 root  root     10, 125 Oct 24 05:10 ecryptfs
crw-rw----   1 root  video    29,   0 Oct 24 05:10 fb0
lrwxrwxrwx   1 root  root          13 Oct 24 05:10 fd -> /proc/self/fd
crw-rw-rw-   1 root  root       1,   7 Oct 24 05:10 full
crw-rw-rw-   1 root  root     10, 229 Oct 24 05:10 fuse
crw-------   1 root  root    241,   0 Oct 24 05:10 hidraw0
crw-------   1 root  root     10, 228 Oct 24 05:10 hpet
drwxr-xr-x   2 root  root           0 Oct 24 05:10 hugepages
crw-------   1 root  root     10, 183 Oct 24 05:10 hwrng
lrwxrwxrwx   1 root  root          12 Oct 24 05:10 initctl -> /run/initctl
drwxr-xr-x   4 root  root         260 Oct 24 05:10 input
crw-r--r--   1 root  root       1,  11 Oct 24 05:10 kmsg
lrwxrwxrwx   1 root  root          28 Oct 24 05:10 log -> /run/systemd/journal/dev-log
brw-rw----   1 root  disk      7,   0 Oct 24 05:10 loop0
brw-rw----   1 root  disk      7,   1 Oct 24 05:10 loop1
brw-rw----   1 root  disk      7,   2 Oct 24 05:10 loop2
brw-rw----   1 root  disk      7,   3 Oct 24 05:10 loop3
brw-rw----   1 root  disk      7,   4 Oct 24 05:10 loop4
brw-rw----   1 root  disk      7,   5 Oct 24 05:10 loop5
brw-rw----   1 root  disk      7,   6 Oct 24 05:10 loop6
brw-rw----   1 root  disk      7,   7 Oct 24 05:10 loop7
crw-rw----   1 root  disk     10, 237 Oct 24 05:10 loop-control
drwxr-xr-x   2 root  root          80 Oct 24 05:10 mapper
crw-------   1 root  root     10, 227 Oct 24 05:10 mcelog
crw-r-----   1 root  kmem      1,   1 Oct 24 05:10 mem
crw-rw----+  1 root  audio    14,   2 Oct 24 05:10 midi
drwxrwxrwt   2 root  root          40 Oct 24 05:10 mqueue
drwxr-xr-x   2 root  root          60 Oct 24 05:10 net
```

```
crw-rw----   1 root  dialout   4,  90 Oct 24 05:10 ttyS26
crw-rw----   1 root  dialout   4,  91 Oct 24 05:10 ttyS27
crw-rw----   1 root  dialout   4,  92 Oct 24 05:10 ttyS28
crw-rw----   1 root  dialout   4,  93 Oct 24 05:10 ttyS29
crw-rw----   1 root  dialout   4,  67 Oct 24 05:10 ttyS3
crw-rw----   1 root  dialout   4,  94 Oct 24 05:10 ttyS30
crw-rw----   1 root  dialout   4,  95 Oct 24 05:10 ttyS31
crw-rw----   1 root  dialout   4,  68 Oct 24 05:10 ttyS4
crw-rw----   1 root  dialout   4,  69 Oct 24 05:10 ttyS5
crw-rw----   1 root  dialout   4,  70 Oct 24 05:10 ttyS6
crw-rw----   1 root  dialout   4,  71 Oct 24 05:10 ttyS7
crw-rw----   1 root  dialout   4,  72 Oct 24 05:10 ttyS8
crw-rw----   1 root  dialout   4,  73 Oct 24 05:10 ttyS9
drwxr-xr-x   2 root  root          60 Oct 24 05:10 ubuntu-vg
crw-rw----   1 root  kvm      10, 124 Oct 24 05:10 udmabuf
crw-------   1 root  root     10, 239 Oct 24 05:10 uhid
crw-------   1 root  root     10, 223 Oct 24 05:10 uinput
crw-rw-rw-   1 root  root      1,   9 Oct 24 05:10 urandom
crw-------   1 root  root     10, 126 Oct 24 05:10 userfaultfd
crw-------   1 root  root     10, 240 Oct 24 05:10 userio
crw-rw----   1 root  tty       7,   0 Oct 24 05:10 vcs
crw-rw----   1 root  tty       7,   1 Oct 24 05:10 vcs1
crw-rw----   1 root  tty       7,   2 Oct 24 05:10 vcs2
crw-rw----   1 root  tty       7,   3 Oct 24 05:10 vcs3
crw-rw----   1 root  tty       7,   4 Oct 24 05:10 vcs4
crw-rw----   1 root  tty       7,   5 Oct 24 05:10 vcs5
crw-rw----   1 root  tty       7,   6 Oct 24 05:10 vcs6
crw-rw----   1 root  tty       7, 128 Oct 24 05:10 vcsa
crw-rw----   1 root  tty       7, 129 Oct 24 05:10 vcsa1
crw-rw----   1 root  tty       7, 130 Oct 24 05:10 vcsa2
crw-rw----   1 root  tty       7, 131 Oct 24 05:10 vcsa3
crw-rw----   1 root  tty       7, 132 Oct 24 05:10 vcsa4
crw-rw----   1 root  tty       7, 133 Oct 24 05:10 vcsa5
crw-rw----   1 root  tty       7, 134 Oct 24 05:10 vcsa6
crw-rw----   1 root  tty       7,  64 Oct 24 05:10 vcsu
crw-rw----   1 root  tty       7,  65 Oct 24 05:10 vcsu1
crw-rw----   1 root  tty       7,  66 Oct 24 05:10 vcsu2
crw-rw----   1 root  tty       7,  67 Oct 24 05:10 vcsu3
crw-rw----   1 root  tty       7,  68 Oct 24 05:10 vcsu4
crw-rw----   1 root  tty       7,  69 Oct 24 05:10 vcsu5
crw-rw----   1 root  tty       7,  70 Oct 24 05:10 vcsu6
drwxr-xr-x   2 root  root          60 Oct 24 05:10 vfio
crw-------   1 root  root     10, 127 Oct 24 05:10 vga_arbiter
crw-------   1 root  root     10, 137 Oct 24 05:10 vhci
crw-rw----   1 root  kvm      10, 238 Oct 24 05:10 vhost-net
crw-rw----   1 root  kvm      10, 241 Oct 24 05:10 vhost-vsock
crw-------   1 root  root     10, 122 Oct 24 05:10 vmci
crw-rw-rw-   1 root  root     10, 121 Oct 24 05:10 vsock
crw-rw-rw-   1 root  root      1,   5 Oct 24 05:10 zero
crw-------   1 root  root     10, 249 Oct 24 05:10 zfs
```

```
hania@ubuntu:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Sep 29 05:28 .
drwxr-xr-x 23 root root   4096 Sep 29 05:09 ..
drwxr-xr-x  2 root root   4096 Oct 24 05:05 backups
drwxr-xr-x 16 root root   4096 Oct 24 07:14 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct 24 07:14 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 24 06:40 log
drwxrwsr-x  2 root mail   4096 Aug  5 16:54 mail
drwxr-xr-x  2 root root   4096 Aug  5 16:54 opt
lrwxrwxrwx  1 root root      4 Aug  5 16:54 run -> /run
drwxr-xr-x  2 root root   4096 May 21 15:46 snap
drwxr-xr-x  4 root root   4096 Aug  5 17:14 spool
drwxrwxrwt  9 root root   4096 Oct 24 07:58 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
hania@ubuntu:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 24 07:58 .
drwxr-xr-x 23 root root 4096 Sep 29 05:09 ..
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .font-unix
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .ICE-unix
drwx------  2 root root 4096 Oct 24 05:10 snap-private-tmp
drwx------  3 root root 4096 Oct 24 07:14 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-fwupd.service-tHwRTt
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-ModemManager.service-gNYwO2
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-polkit.service-fxds4S
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-systemd-logind.service-vhvGVq
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-systemd-resolved.service-zsU2V8
drwx------  3 root root 4096 Oct 24 05:10 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-systemd-timesyncd.service-xQzrYn
drwx------  3 root root 4096 Oct 24 07:14 systemd-private-14e9cf42ad6143c6889ccbfc043e9ef3-upower.service-jFan3Y
drwx------  2 root root 4096 Oct 24 05:10 vmware-root_740-2999460834
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 24 05:10 .XIM-unix
```

```
hania@ubuntu:~$ ls -la ~
total 52
drwxr-x--- 6 hania hania 4096 Oct 24 07:33 .
drwxr-xr-x 3 root  root  4096 Oct 24 07:37 ..
-rw-rw-r-- 1 hania hania   65 Oct 24 07:10 answer.md
-rw------- 1 hania hania   23 Oct 13 08:26 .bash_history
-rw-r--r-- 1 hania hania  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hania hania 3771 Mar 31  2024 .bashrc
drwx------ 2 hania hania 4096 Sep 29 05:31 .cache
drwxrwxr-x 3 hania hania 4096 Oct 24 07:12 lab4
drwxrwxr-x 3 hania hania 4096 Oct 24 07:09 .local
-rw-r--r-- 1 hania hania  807 Mar 31  2024 .profile
drwx------ 2 hania hania 4096 Sep 29 05:42 .ssh
-rw-r--r-- 1 hania hania    0 Oct 24 07:33 .sudo_as_admin_successful
-rw-rw-r-- 1 hania hania   44 Oct 13 08:33 trmif
-rw------- 1 hania hania  694 Oct 13 08:26 .viminfo
hania@ubuntu:~$
```

```
hania@ubuntu:~$ nano ~/forensic_report.md
```



```
hania@ubuntu:~$ cat ~/forensic_report.md
Forensic Report
hania@ubuntu:~$
```

3.Evidence Handling & File Operations

```
hania@ubuntu:~$ mkdir -p ~/lab4/evidence/analysis
hania@ubuntu:~$ ls -la ~/lab4/evidence
total 12
drwxrwxr-x 3 hania hania 4096 Oct 24 08:05 .
drwxrwxr-x 4 hania hania 4096 Oct 24 08:05 ..
drwxrwxr-x 2 hania hania 4096 Oct 24 08:05 analysis
hania@ubuntu:~$
```

```
hania@ubuntu:~$ nano file1.txt
```


```
hania@ubuntu:~$ nano file2.txt
```

```
hania@ubuntu:~$ nano .secret.txt
```


```
hania@ubuntu:~$ ls -la
total 68
drwxr-x--- 6 hania hania 4096 Oct 24 08:08 .
drwxr-xr-x 3 root  root  4096 Oct 24 07:37 ..
-rw-rw-r-- 1 hania hania   65 Oct 24 07:10 answer.md
-rw------- 1 hania hania   23 Oct 13 08:26 .bash_history
-rw-r--r-- 1 hania hania  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hania hania 3771 Mar 31  2024 .bashrc
drwx------ 2 hania hania 4096 Sep 29 05:31 .cache
-rw-rw-r-- 1 hania hania   19 Oct 24 08:06 file1.txt
-rw-rw-r-- 1 hania hania   19 Oct 24 08:07 file2.txt
-rw-rw-r-- 1 hania hania   16 Oct 24 08:04 forensic_report.md
drwxrwxr-x 4 hania hania 4096 Oct 24 08:05 lab4
drwxrwxr-x 3 hania hania 4096 Oct 24 07:09 .local
-rw-r--r-- 1 hania hania  807 Mar 31  2024 .profile
-rw-rw-r-- 1 hania hania   23 Oct 24 08:08 .secret.txt
drwx------ 2 hania hania 4096 Sep 29 05:42 .ssh
-rw-r--r-- 1 hania hania    0 Oct 24 07:33 .sudo_as_admin_successful
-rw-rw-r-- 1 hania hania   44 Oct 13 08:33 trmif
-rw------- 1 hania hania  694 Oct 13 08:26 .viminfo
hania@ubuntu:~$
```

```
hania@ubuntu:~$ cp file1.txt file1.bak.txt
hania@ubuntu:~$ ls -la file1.txt file1.bak.txt
-rw-rw-r-- 1 hania hania 19 Oct 24 08:10 file1.bak.txt
-rw-rw-r-- 1 hania hania 19 Oct 24 08:06 file1.txt
hania@ubuntu:~$ mv file1.bak.txt file1.verified.txt
hania@ubuntu:~$ ls -la file1.verified.txt
-rw-rw-r-- 1 hania hania 19 Oct 24 08:10 file1.verified.txt
hania@ubuntu:~$ rm file1.verified.txt
hania@ubuntu:~$ ls -la
total 68
drwxr-x--- 6 hania hania 4096 Oct 24 08:12 .
drwxr-xr-x 3 root  root  4096 Oct 24 07:37 ..
-rw-rw-r-- 1 hania hania   65 Oct 24 07:10 answer.md
-rw------- 1 hania hania   23 Oct 13 08:26 .bash_history
-rw-r--r-- 1 hania hania  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hania hania 3771 Mar 31  2024 .bashrc
drwx------ 2 hania hania 4096 Sep 29 05:31 .cache
-rw-rw-r-- 1 hania hania   19 Oct 24 08:06 file1.txt
-rw-rw-r-- 1 hania hania   19 Oct 24 08:07 file2.txt
-rw-rw-r-- 1 hania hania   16 Oct 24 08:04 forensic_report.md
drwxrwxr-x 4 hania hania 4096 Oct 24 08:05 lab4
drwxrwxr-x 3 hania hania 4096 Oct 24 07:09 .local
-rw-r--r-- 1 hania hania  807 Mar 31  2024 .profile
-rw-rw-r-- 1 hania hania   23 Oct 24 08:08 .secret.txt
drwx------ 2 hania hania 4096 Sep 29 05:42 .ssh
-rw-r--r-- 1 hania hania    0 Oct 24 07:33 .sudo_as_admin_successful
-rw-rw-r-- 1 hania hania   44 Oct 13 08:33 trmif
-rw------- 1 hania hania  694 Oct 13 08:26 .viminfo
hania@ubuntu:~$
```

```
hania@ubuntu:~$ cd ~/lab4/evidence
hania@ubuntu:~/lab4/evidence$ cp -r ~/lab4/evidence ~/lab4/evidence_backup
hania@ubuntu:~/lab4/evidence$ ls -la ~/lab4 | grep evidence
drwxrwxr-x 3 hania hania 4096 Oct 24 08:05 evidence
drwxrwxr-x 3 hania hania 4096 Oct 24 08:13 evidence_backup
hania@ubuntu:~/lab4/evidence$ ls -la ~/lab4/evidence_backup
total 12
drwxrwxr-x 3 hania hania 4096 Oct 24 08:13 .
drwxrwxr-x 5 hania hania 4096 Oct 24 08:13 ..
drwxrwxr-x 2 hania hania 4096 Oct 24 08:13 analysis
hania@ubuntu:~/lab4/evidence$
```

4.System Profiling and Process Monitoring

```
hania@ubuntu:~/lab4/evidence$ 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
hania@ubuntu:~/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
hania@ubuntu:~/lab4/evidence$
```

```
hania@ubuntu:~/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) i5-8250U CPU @ 1.60GHz
    CPU family:           6
    Model:                142
    Thread(s) per core:   1
    Core(s) per socket:   1
    Socket(s):            2
    Stepping:             10
    BogoMIPS:             3599.99
    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 pdpe1g
                          b 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 ss
                          bd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt xsaveopt xsavec xgetbv1
                          xsaves arat md_clear flush_l1d arch_capabilities
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:                     12 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:                    Mitigation; Clear CPU buffers; SMT Host state unknown
  Meltdown:               Mitigation; PTI
  Mmio stale data:        Mitigation; Clear CPU buffers; SMT Host state unknown
  Reg file data sampling: Not affected
  Retbleed:               Mitigation; IBRS
  Spec rstack overflow:   Not affected
  Spec store bypass:      Mitigation; Speculative Store Bypass disabled via prctl
  Spectre v1:             Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:             Mitigation; IBRS; IBPB conditional; STIBP disabled; RSB filling; PBRSB-eIBRS Not affected; BHI SW loop, KVM SW loop
  Srbds:                  Unknown: Dependent on hypervisor status
  Tsx async abort:        Not affected
hania@ubuntu:~/lab4/evidence$
```

```
hania@ubuntu:~/lab4/evidence$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       382Mi       1.3Gi       1.2Mi       353Mi       1.5Gi
Swap:          1.9Gi          0B       1.9Gi
hania@ubuntu:~/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
hania@ubuntu:~/lab4/evidence$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.6  22016 12992 ?        Ss   06:39   0:06 /sbin/init
root           2  0.0  0.0      0     0 ?        S    06:39   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    06:39   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-netns]
root           9  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/0:0H-events_highpri]
root          11  0.0  0.0      0     0 ?        I    06:39   0:00 [kworker/u256:0-ext4-rsv-conversion]
root          12  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-mm_pe]
root          13  0.0  0.0      0     0 ?        I    06:39   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    06:39   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    06:39   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    06:39   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    06:39   0:00 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    06:39   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    06:39   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    06:39   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    06:39   0:00 [cpuhp/1]
root          22  0.0  0.0      0     0 ?        S    06:39   0:00 [idle_inject/1]
root          23  0.0  0.0      0     0 ?        S    06:39   0:00 [migration/1]
root          24  0.0  0.0      0     0 ?        S    06:39   0:00 [ksoftirqd/1]
root          26  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/1:0H-kblockd]
root          29  0.0  0.0      0     0 ?        S    06:39   0:00 [kdevtmpfs]
root          30  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-inet_]
root          32  0.0  0.0      0     0 ?        S    06:39   0:00 [kauditd]
root          34  0.0  0.0      0     0 ?        S    06:39   0:00 [khungtaskd]
root          36  0.0  0.0      0     0 ?        S    06:39   0:00 [oom_reaper]
```

```
root         736  0.0  0.6  53464 12032 ?        Ss   06:39   0:00 /usr/bin/VGAuthService
root         737  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/57-vmw_vmci]
root         738  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/58-vmw_vmci]
root         739  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/59-vmw_vmci]
root         740  0.3  0.4 242124  9344 ?        Ssl  06:39   0:20 /usr/bin/vmtoolsd
root         766  0.0  0.0      0     0 ?        S    06:39   0:00 [irq/16-vmwgfx]
root         767  0.0  0.0      0     0 ?        I<   06:39   0:00 [kworker/R-ttm]
message+     787  0.0  0.2   9804  5376 ?        Ss   06:39   0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activ
polkitd      807  0.0  0.4 308164  7936 ?        Ssl  06:39   0:00 /usr/lib/polkit-1/polkitd --no-debug
root         815  0.0  0.4  18144  8704 ?        Ss   06:39   0:00 /usr/lib/systemd/systemd-logind
root         816  0.0  0.6 468952 13568 ?        Ssl  06:39   0:00 /usr/libexec/udisks2/udisksd
root         869  0.0  0.1   6824  2688 ?        Ss   06:39   0:00 /usr/sbin/cron -f -P
root         882  0.0  1.1 109660 22912 ?        Ssl  06:39   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown -
syslog       888  0.0  0.3 222508  6128 ?        Ssl  06:39   0:00 /usr/sbin/rsyslogd -n -iNONE
root         934  0.0  0.6 392028 12800 ?        Ssl  06:39   0:00 /usr/sbin/ModemManager
root         995  0.0  0.2   6948  4608 tty1     Ss   06:39   0:00 /bin/login -p --
systemd+    1491  0.0  0.4  18992  9472 ?        Ss   06:40   0:00 /usr/lib/systemd/systemd-networkd
root        1816  0.0  0.0      0     0 ?        S    06:40   0:00 [psimon]
hania       1818  0.0  0.5  20088 10880 ?        Ss   06:40   0:00 /usr/lib/systemd/systemd --user
hania       1821  0.0  0.1  21152  3520 ?        S    06:40   0:00 (sd-pam)
hania       1841  0.0  0.2   8656  5632 tty1     S+   06:40   0:00 -bash
root        1888  0.0  0.0      0     0 ?        I<   06:40   0:00 [kworker/R-tls-s]
root        1908  0.0  0.4  12020  7936 ?        Ss   06:47   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        1920  0.0  0.5  14956 10368 ?        Ss   06:53   0:00 sshd: hania [priv]
hania       1978  0.1  0.3  15116  6972 ?        S    06:53   0:08 sshd: hania@pts/0
hania       1979  0.0  0.2   8648  5504 pts/0    Ss   06:53   0:00 -bash
root        2102  0.1  2.2 669304 43368 ?        Ssl  07:14   0:04 /usr/libexec/fwupd/fwupd
root        2109  0.0  0.4 313996  8832 ?        Ssl  07:14   0:00 /usr/libexec/upowerd
root        2134  0.0  0.1  81380  2872 ?        Ss   07:14   0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket --daemon
root        2157  0.0  0.0      0     0 ?        I    07:16   0:00 [kworker/u258:1-events_power_efficient]
root        2184  0.0  0.0      0     0 ?        I    07:24   0:00 [kworker/u257:1-events_unbound]
root        2195  0.0  0.0      0     0 ?        I    07:30   0:00 [kworker/u258:3-events_power_efficient]
root        2198  0.1  0.0      0     0 ?        I    07:30   0:03 [kworker/1:1-events]
root        2269  0.0  0.0   6104  1920 tty6     Ss+  07:36   0:00 /sbin/agetty -o -p -- \u --noclear - linux
root        2271  0.2  0.0      0     0 ?        I    07:36   0:06 [kworker/0:1-rcu_par_gp]
root        2339  0.2  0.0      0     0 ?        I    07:55   0:02 [kworker/1:0-events]
root        2373  0.0  0.0      0     0 ?        I    08:00   0:00 [kworker/u257:0-events_power_efficient]
root        2381  0.7  0.0      0     0 ?        I    08:05   0:06 [kworker/0:2-events]
root        2400  0.0  0.0      0     0 ?        I    08:10   0:00 [kworker/u258:0-events_power_efficient]
root        2407  0.0  0.0      0     0 ?        I    08:13   0:00 [kworker/u257:2-events_unbound]
hania       2423  200  0.2  10884  4480 pts/0    R+   08:18   0:00 ps aux
hania@ubuntu:~/lab4/evidence$
```

5. User Account Audit & Privilege Escalation Simulation

```
hania@ubuntu:~/lab4/evidence$ sudo adduser lab4user
[sudo] password for hania:
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:
No password has been supplied.
New password:
Retype new password:
No password has been supplied.
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
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' ...
```

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

^[[A^[[Asu: Authentication failure
hania@ubuntu:~/lab4/evidence$
hania@ubuntu:~/lab4/evidence$ su - lab4user
Password:
lab4user@ubuntu:~$ whoami
lab4user
lab4user@ubuntu:~$ pwd
/home/lab4user
lab4user@ubuntu:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu:~$ exit
logout
hania@ubuntu:~/lab4/evidence$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
hania@ubuntu:~/lab4/evidence$
```