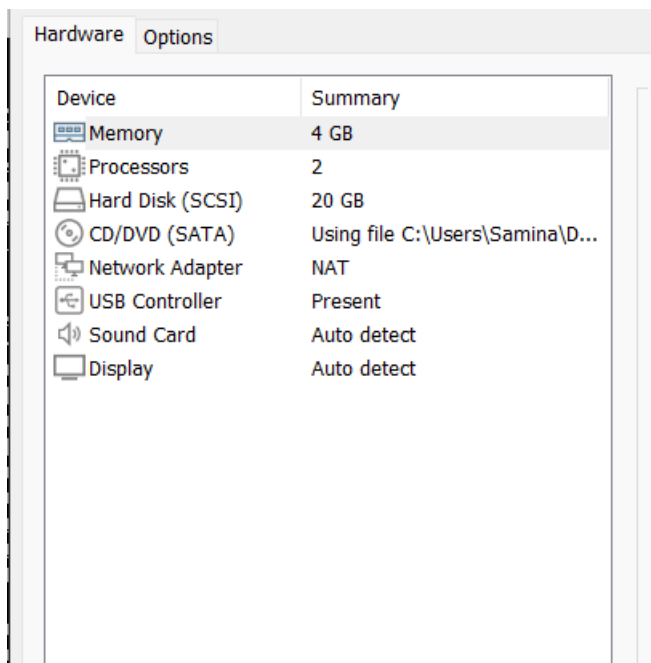


Name : Shumaila Munsib

Roll No: 2023-BSE-062

Submitted to: Sir Shoaib

Task 1:



The screenshot shows the 'Hardware' tab in a virtual machine's settings window. It contains a table with hardware components and their configurations.

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

Task 2:

```
Last login: Mon Sep 29 14:17:33 2025 from 192.168.9.1
shumaila062@shumailaa:~$ whoami
shumaila062
shumaila062@shumailaa:~$ pwd
/home/shumaila062
shumaila062@shumailaa:~$
```

Task 3:

```
shumaila062@shumailaa:~$ ls -la
total 28
drwxr-x--- 4 shumaila062 shumaila062 4096 Oct 20 09:45 .
drwxr-xr-x 3 root      root          4096 Sep 28 14:12 ..
-rw-r--r-- 1 shumaila062 shumaila062 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 shumaila062 shumaila062 3771 Mar 31 2024 .bashrc
drwx----- 2 shumaila062 shumaila062 4096 Sep 28 14:15 .cache
-rw-r--r-- 1 shumaila062 shumaila062 807 Mar 31 2024 .profile
drwx----- 2 shumaila062 shumaila062 4096 Sep 29 14:16 .ssh
-rw-r--r-- 1 shumaila062 shumaila062  0 Oct 20 09:45 .sudo_as_admin_successful
shumaila062@shumailaa:~$ _
```

```
ls -ls --help for more information.
shumaila062@shumailaa:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22 2024 /bin -> usr/bin
shumaila062@shumailaa:~$ _
```

```
shumaila062@shumailaa:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22 2024 /bin -> usr/bin
shumaila062@shumailaa:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22 2024 /sbin -> usr/sbin
shumaila062@shumailaa:~$ _
```

```
total 92
drwxr-xr-x 12 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 28 08:12 ..
drwxr-xr-x  2 root root 32768 Sep 28 08:15 bin
drwxr-xr-x  2 root root 4096 Apr 22 2024 games
drwxr-xr-x 33 root root 4096 Sep 28 08:11 include
drwxr-xr-x 78 root root 4096 Sep 28 08:13 lib
drwxr-xr-x  2 root root 4096 Sep 28 08:11 lib64
drwxr-xr-x 11 root root 4096 Sep 28 08:11 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x  2 root root 20480 Sep 28 08:18 sbin
drwxr-xr-x 124 root root 4096 Sep 28 08:13 share
drwxr-xr-x  4 root root 4096 Sep 28 08:11 src
shumaila062@shumailaa:~$ _
```

```
shumaila062@shumailaa:~$ ls -ls /opt
total 0
shumaila062@shumailaa:~$ _
```

```

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 973 Sep 28 14:12 shadow
-rw-r----- 1 root shadow 973 Sep 28 14:12 shadow-
-rw-r--r-- 1 root root 148 Aug 5 17:14 shells
drwxr-xr-x 2 root root 4096 Aug 5 16:55 skel
drwxr-xr-x 6 root root 4096 Aug 5 17:14 sos
drwxr-xr-x 4 root root 4096 Sep 28 14:12 ssh
drwxr-xr-x 4 root root 4096 Aug 5 17:02 ssl
-rw-r--r-- 1 root root 25 Sep 28 14:12 subgid
-rw-r--r-- 1 root root 0 Aug 5 16:54 subgid-
-rw-r--r-- 1 root root 25 Sep 28 14:12 subuid
-rw-r--r-- 1 root root 0 Aug 5 16:54 subuid-
-rw-r--r-- 1 root root 4343 Jun 25 12:42 sudo.conf
-r--r----- 1 root root 1800 Jan 29 2024 sudoers
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sudoers.d
-rw-r--r-- 1 root root 9804 Jun 25 12:42 sudo_logsrvd.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:14 supercat
-rw-r--r-- 1 root root 2209 Mar 24 2024 sysctl.conf
drwxr-xr-x 2 root root 4096 Aug 5 17:02 sysctl.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 sysstat
drwxr-xr-x 6 root root 4096 Aug 5 16:49 systemd
drwxr-xr-x 2 root root 4096 Aug 5 17:00 terminfo
drwxr-xr-x 2 root root 4096 Sep 28 08:12 thermald
-rw-r--r-- 1 root root 8 Aug 5 17:02 timezone
drwxr-xr-x 2 root root 4096 Aug 5 17:14 tmpfiles.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 ubuntu-advantage
-rw-r--r-- 1 root root 1260 Jan 27 2023 ucf.conf
drwxr-xr-x 4 root root 4096 Aug 5 17:02 udev
drwxr-xr-x 2 root root 4096 Sep 28 08:15 udisks2
drwxr-xr-x 3 root root 4096 Aug 5 17:14 ufw
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated
drwxr-xr-x 3 root root 4096 Aug 5 17:02 update-manager
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-motd.d
drwxr-xr-x 2 root root 4096 Aug 5 17:14 update-notifier
drwxr-xr-x 2 root root 4096 Sep 28 08:12 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 Sep 28 08:15 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
shumaila062@shumailaa:~$

```

```

crw-rw---- 1 root dialout 4, 90 Sep 28 14:11 ttyS26
crw-rw---- 1 root dialout 4, 91 Sep 28 14:11 ttyS27
crw-rw---- 1 root dialout 4, 92 Sep 28 14:11 ttyS28
crw-rw---- 1 root dialout 4, 93 Sep 28 14:11 ttyS29
crw-rw---- 1 root dialout 4, 67 Sep 28 14:11 ttyS3
crw-rw---- 1 root dialout 4, 94 Sep 28 14:11 ttyS30
crw-rw---- 1 root dialout 4, 95 Sep 28 14:11 ttyS31
crw-rw---- 1 root dialout 4, 68 Sep 28 14:11 ttyS4
crw-rw---- 1 root dialout 4, 69 Sep 28 14:11 ttyS5
crw-rw---- 1 root dialout 4, 70 Sep 28 14:11 ttyS6
crw-rw---- 1 root dialout 4, 71 Sep 28 14:11 ttyS7
crw-rw---- 1 root dialout 4, 72 Sep 28 14:11 ttyS8
crw-rw---- 1 root dialout 4, 73 Sep 28 14:11 ttyS9
crw-rw---- 1 root kvm 10, 124 Sep 28 14:12 udmabuf
crw----- 1 root root 10, 239 Sep 28 14:11 uhid
crw----- 1 root root 10, 223 Sep 28 14:12 uinput
crw-rw-rw- 1 root root 1, 9 Sep 28 14:12 urandom
crw----- 1 root root 10, 126 Sep 28 14:12 userfaultfd
crw----- 1 root root 10, 240 Sep 28 14:11 userio
crw-rw---- 1 root tty 7, 0 Sep 28 14:12 vcs
crw-rw---- 1 root tty 7, 1 Sep 28 14:12 vcs1
crw-rw---- 1 root tty 7, 2 Sep 28 14:12 vcs2
crw-rw---- 1 root tty 7, 3 Sep 28 14:12 vcs3
crw-rw---- 1 root tty 7, 4 Sep 28 14:12 vcs4
crw-rw---- 1 root tty 7, 5 Sep 28 14:12 vcs5
crw-rw---- 1 root tty 7, 6 Sep 28 14:12 vcs6
crw-rw---- 1 root tty 7, 128 Sep 28 14:12 vcsa
crw-rw---- 1 root tty 7, 129 Sep 28 14:12 vcsa1
crw-rw---- 1 root tty 7, 130 Sep 28 14:12 vcsa2
crw-rw---- 1 root tty 7, 131 Sep 28 14:12 vcsa3
crw-rw---- 1 root tty 7, 132 Sep 28 14:12 vcsa4
crw-rw---- 1 root tty 7, 133 Sep 28 14:12 vcsa5
crw-rw---- 1 root tty 7, 134 Sep 28 14:12 vcsa6
crw-rw---- 1 root tty 7, 64 Sep 28 14:12 vcsu
crw-rw---- 1 root tty 7, 65 Sep 28 14:12 vcsu1
crw-rw---- 1 root tty 7, 66 Sep 28 14:12 vcsu2
crw-rw---- 1 root tty 7, 67 Sep 28 14:12 vcsu3
crw-rw---- 1 root tty 7, 68 Sep 28 14:12 vcsu4
crw-rw---- 1 root tty 7, 69 Sep 28 14:12 vcsu5
crw-rw---- 1 root tty 7, 70 Sep 28 14:12 vcsu6
drwxr-xr-x 2 root root 60 Sep 28 14:11 vfio
crw----- 1 root root 10, 127 Sep 28 14:12 vga_arbiter
crw----- 1 root root 10, 137 Sep 28 14:11 vhci
crw-rw---- 1 root kvm 10, 238 Sep 28 14:11 vhost-net
crw-rw---- 1 root kvm 10, 241 Sep 28 14:11 vhost-vsock
crw----- 1 root root 10, 122 Sep 28 14:12 vmci
crw-rw-rw- 1 root root 10, 121 Sep 28 14:12 vsock
crw-rw-rw- 1 root root 1, 5 Sep 28 14:12 zero
crw----- 1 root root 10, 249 Sep 28 14:11 zfs
shumaila062@shumailaa:~$

```

```

shumaila062@shumailaa:~$ ls -la /var
total 56
drwxr-xr-x 13 root root 4096 Sep 28 14:11 .
drwxr-xr-x 23 root root 4096 Sep 28 08:12 ..
drwxr-xr-x 2 root root 4096 Sep 29 14:15 backups
drwxr-xr-x 16 root root 4096 Sep 28 15:20 cache
drwxrwsrwt 2 root root 4096 Aug 5 17:02 crash
drwxr-xr-x 45 root root 4096 Sep 28 15:20 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 20 09:27 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 20 09:27 tmp
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated
shumaila062@shumailaa:~$

```

```

shumaila062@shumailaa:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 20 09:27 .
drwxr-xr-x 23 root root 4096 Sep 28 08:12 ..
drwxrwxrwt 2 root root 4096 Sep 28 14:11 .font-unix
drwxrwxrwt 2 root root 4096 Sep 28 14:11 .ICE-unix
drwx----- 2 root root 4096 Sep 28 14:11 snap-private-tmp
drwx----- 3 root root 4096 Sep 28 15:20 systemd-private-93f85b5df79c4357b281e071d2f01662-fwupd.service-Qnrfus
drwx----- 3 root root 4096 Sep 28 14:12 systemd-private-93f85b5df79c4357b281e071d2f01662-ModemManager.service-ppWzUP
drwx----- 3 root root 4096 Sep 28 14:12 systemd-private-93f85b5df79c4357b281e071d2f01662-polkit.service-Ln1Knd
drwx----- 3 root root 4096 Sep 28 14:12 systemd-private-93f85b5df79c4357b281e071d2f01662-systemd-logind.service-lwGHpa
drwx----- 3 root root 4096 Sep 28 14:11 systemd-private-93f85b5df79c4357b281e071d2f01662-systemd-resolved.service-S3W7Xl
drwx----- 3 root root 4096 Sep 28 14:11 systemd-private-93f85b5df79c4357b281e071d2f01662-systemd-timesyncd.service-ZateWj
drwx----- 2 root root 4096 Sep 28 15:20 systemd-private-93f85b5df79c4357b281e071d2f01662-upower.service-eYHpxo
drwx----- 2 root root 4096 Sep 28 14:11 vmware-root_729-4257135007
drwxrwxrwt 2 root root 4096 Sep 28 14:11 .X11-unix
drwxrwxrwt 2 root root 4096 Sep 28 14:11 .XIM-unix
shumaila062@shumailaa:~$ _

```

```

shumaila062@shumailaa:~$ ls -la ~
total 28
drwxr-x-- 4 shumaila062 shumaila062 4096 Oct 20 09:45 .
drwxr-xr-x 3 root root 4096 Sep 28 14:12 ..
-rw-r--r-- 1 shumaila062 shumaila062 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 shumaila062 shumaila062 3771 Mar 31 2024 .bashrc
drwx----- 2 shumaila062 shumaila062 4096 Sep 28 14:15 .cache
-rw-r--r-- 1 shumaila062 shumaila062 807 Mar 31 2024 .profile
drwx----- 2 shumaila062 shumaila062 4096 Sep 29 14:16 .ssh
-rw-r--r-- 1 shumaila062 shumaila062 0 Oct 20 09:45 .sudo_as_admin_successful
shumaila062@shumailaa:~$

```

```

shumaila062@shumailaa:~$ cat ~/answers.md
/bin contains essential commands used by all users and needed for system boot or repair./usr /bin holds most user level programs and applications installed by s
ystem.. /usr/local/bin stores softwares installed manually by administrator.
shumaila062@shumailaa:~$ _

```

Task 4:

```

shumaila062@shumailaa:~/lab4/workspace/python_project$ mv README.md README.dev.md
shumaila062@shumailaa:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
shumaila062@shumailaa:~/lab4/workspace/python_project$

```

```
-bash: cd: too many arguments
shumaila062@shumailaa:~$ cd ~/lab4/workspace/python_project
shumaila062@shumailaa:~/lab4/workspace/python_project$ pwd
/home/shumaila062/lab4/workspace/python_project
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

```
GNU nano 7.2
Lab 4 README
```

```
GNU nano 7.2
env= lab4
```

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 shumaila062 shumaila062 4096 Oct 21 09:34 .
drwxrwxr-x 3 shumaila062 shumaila062 4096 Oct 20 11:26 ..
-rw-rw-r-- 1 shumaila062 shumaila062  10 Oct 21 09:34 .env
-rw-rw-r-- 1 shumaila062 shumaila062  12 Oct 21 09:33 main.py
-rw-rw-r-- 1 shumaila062 shumaila062  13 Oct 21 09:32 readme.md
shumaila062@shumailaa:~/lab4/workspace/python_project$
```

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 shumaila062 shumaila062 4096 Oct 21 09:34 .
drwxrwxr-x 3 shumaila062 shumaila062 4096 Oct 20 11:26 ..
-rw-rw-r-- 1 shumaila062 shumaila062  10 Oct 21 09:34 .env
-rw-rw-r-- 1 shumaila062 shumaila062  12 Oct 21 09:33 main.py
-rw-rw-r-- 1 shumaila062 shumaila062  13 Oct 21 09:32 readme.md
shumaila062@shumailaa:~/lab4/workspace/python_project$ cp readme.md readme.copy.md
shumaila062@shumailaa:~/lab4/workspace/python_project$
```

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ mv readme.copy.md readme.dev.md
shumaila062@shumailaa:~/lab4/workspace/python_project$
```

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ mv readme.copy.md readme.dev.md
shumaila062@shumailaa:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
shumaila062@shumailaa:~/lab4/workspace/python_project$
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
shumaila062@shumailaa:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python-project ~/lab4/workspace/java_app_copy
cp: cannot stat '/home/shumaila062/lab4/workspace/python-project': No such file or directory
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ history
 1 hostname
 2 mkdir -p ~/lab4/workspace/python_project
 3 pwd
 4 cd mkdir -p ~/lab4/workspace/python_project
 5 cd ~/lab4/workspace/python_project
 6 pwd
 7 nano readme.md
 8 nano main.py
 9 nano .env
10 ls -la
11 cp readme.md readme.copy.md
12 mv readme.copy.md readme.dev.md
13 mkdir -p ~/lab4/workspace/java_app
14 sudo apt install open-vm-tools open-vm-tools-desktop -y
15 cp -r ~/lab4/workspace/python-project ~/lab4/workspace/java_app_copy
16 ls -la ~/lab4/workspace
17 history
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ cd ~/lab4/workspace/python_project/
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

Task 5:

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ uname -a
Linux shumailaa 6.8.0-84-generic #84-Ubuntu SMP PREEMPT_DYNAMIC Fri Sep  5 22:36:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

```

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_rndand hypervisor lahf_lm abm 3dnowprefetch pt1 ssbd ibrs lbpb 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    : 4600.01
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) i7-10510U CPU @ 1.80GHz
stepping     : 12
microcode    : 0xffffffff
cpu MHz      : 2304.007
cache size   : 8192 KB
physical id   : 2
siblings     : 1
core id      : 0
cpu cores    : 1
apicid       : 2
initial apicid : 2
fpu          : yes
fpu_exception : yes
cpuid level   : 22
wp           : yes
flags        : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 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_rndand hypervisor lahf_lm abm 3dnowprefetch pt1 ssbd ibrs lbpb 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     : 4600.01
clflush size  : 64
cache_alignment : 64
address sizes  : 45 bits physical, 48 bits virtual
power management:

shumaila062@shumailaa:~/lab4/workspace/python_project$ _

```

```

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_rndand hypervisor lahf_lm abm 3dnowprefetch pt1 ssbd ibrs lbpb 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    : 4600.01
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) i7-10510U CPU @ 1.80GHz
stepping     : 12
microcode    : 0xffffffff
cpu MHz      : 2304.007
cache size   : 8192 KB
physical id   : 2
siblings     : 1
core id      : 0
cpu cores    : 1
apicid       : 2
initial apicid : 2
fpu          : yes
fpu_exception : yes
cpuid level   : 22
wp           : yes
flags        : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 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_rndand hypervisor lahf_lm abm 3dnowprefetch pt1 ssbd ibrs lbpb 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     : 4600.01
clflush size  : 64
cache_alignment : 64
address sizes  : 45 bits physical, 48 bits virtual
power management:

shumaila062@shumailaa:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:            3.86Gi    496Mi      2.76Gi      1.5Mi      918Mi      3.36Gi
Swap:            3.86Gi         0B      3.86Gi
shumaila062@shumailaa:~/lab4/workspace/python_project$

```



```
shumaila062@shumailaa: ~/lab4/workspace/python_project$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            387M  1.5M  386M   1% /run
/dev/sda2        20G   7.0G   12G  38% /
tmpfs            1.9G   0  1.9G   0% /dev/shm
tmpfs            5.0M   0  5.0M   0% /run/lock
tmpfs            387M  12K  387M   1% /run/user/1000
shumaila062@shumailaa:~/lab4/workspace/python_project$
```

```
shumaila062@shumailaa:~/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
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

```
root      483  0.2  0.6 354524 27264 ?    Ssl  09:18  0:08 /sbin/multipathd -d -s
root      499  0.0  0.2  30360  9184 ?    Ss   09:18  0:01 /usr/lib/systemd/systemd-udevd
root      529  0.0  0.0  0 0 ?    Ss   09:18  0:00 [psimom]
systemd+  549  0.0  0.3 21588 12928 ?    Ss   09:18  0:02 /usr/lib/systemd/systemd-resolved
systemd+  544  0.0  0.1 91024 7808 ?    Ssl  09:18  0:00 /usr/lib/systemd/systemd-timesyncd
root      619  0.0  0.0  0 0 ?    I<   09:18  0:00 [kworker/R-cfg80]
root      752  0.0  0.0  0 0 ?    S   09:18  0:00 [irq/57-vmmu_vnci]
root      753  0.0  0.0  0 0 ?    S   09:18  0:00 [irq/58-vmmu_vnci]
root      754  0.0  0.0  0 0 ?    S   09:18  0:00 [irq/59-vmmu_vnci]
message+  764  0.0  0.1 9912 5376 ?    Ss   09:18  0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-o
polkitd   783  0.0  0.1 308164 7808 ?    Ssl  09:18  0:01 /usr/lib/polkit-1/polkitd --no-debug
root      787  0.0  0.0  0 0 ?    S   09:18  0:00 [irq/16-vmmu_vnci]
root      788  0.0  0.0  0 0 ?    I<   09:18  0:00 [kworker/R-ttm]
root      792  0.0  0.2 18140 8704 ?    Ss   09:18  0:00 /usr/lib/systemd/systemd-logind
root      798  0.0  0.3 468956 13568 ?    Ssl  09:18  0:01 /usr/libexec/udisks2/udisksd
root      807  0.0  0.5 109692 22912 ?    Ssl  09:18  0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
syslog    824  0.0  0.1 222508 6016 ?    Ssl  09:18  0:00 /usr/sbin/rsyslogd -n -iNONE
root      839  0.0  0.3 392028 12928 ?    Ssl  09:18  0:00 /usr/sbin/ModemManager
root      851  0.0  0.0 6824 2688 ?    Ss   09:18  0:00 /usr/sbin/cron -f -P
root      876  0.0  0.1 6948 4736 tty1  Ss   09:18  0:00 /bin/login -p --
shumail+ 1341  0.0  0.2 20244 11392 ?    Ss   09:19  0:00 /usr/lib/systemd/systemd --user
shumail+ 1343  0.0  0.0 21152 3472 ?    S   09:19  0:00 (sd-pam)
shumail+ 1354  0.0  0.1 8784 5504 tty1  S   09:19  0:01 -bash
systemd+ 1597  0.0  0.2 18392 9472 ?    Ss   09:30  0:01 /usr/lib/systemd/systemd-networkd
root      1895  0.0  0.0  0 0 ?    I   09:46  0:01 [kworker/u257:0-events_power_efficient]
root      3117  0.1  1.0 551688 41472 ?    Ssl  09:49  0:02 /usr/libexec/fuupd/fuupd
root      3194  0.0  0.2 313996 8960 ?    Ssl  09:49  0:00 /usr/libexec/upoword
root      3264  0.0  0.0  0 0 ?    I   09:49  0:02 [kworker/u258:3-events_power_efficient]
root      3328  0.0  0.3 53464 12160 ?    Ss   09:49  0:00 /usr/bin/VGAuthService
root      3395  2.6  0.2 242136 9212 ?    Ssl  09:49  0:54 /usr/bin/vmtoolsd
root      3508  0.0  0.0  0 0 ?    S   09:50  0:00 [psimom]
root      3518  0.0  0.0 152476 1420 ?    Ssl  09:50  0:00 vmware-vmblock-fuse /run/vmblock-fuse -o rw,subtype=vmware-vmblock,default_permissions,allow_
root      3565  0.0  0.0  0 0 ?    I<   09:50  0:00 [kworker/0:1H-kblockd]
root      3569  0.5  0.0  0 0 ?    I   09:51  0:19 [kworker/0:2-events]
root      3591  0.0  0.0  0 0 ?    I   09:55  0:01 [kworker/u258:2-events_power_efficient]
root      3596  0.7  0.0  0 0 ?    I   09:55  0:13 [kworker/1:0-events]
root      3600  0.0  0.0  0 0 ?    I   09:58  0:01 [kworker/u257:2-events_power_efficient]
root      3615  0.0  0.0  0 0 ?    I<   10:05  0:00 [kworker/1:0H-kblockd]
root      3620  0.0  0.0  0 0 ?    I   10:08  0:00 [kworker/u258:1-events_unbound]
root      3622  0.0  0.0  0 0 ?    I   10:09  0:00 [kworker/u257:1-events_unbound]
root      3625  0.7  0.0  0 0 ?    I   10:10  0:06 [kworker/1:1-events]
root      3626  0.5  0.0  0 0 ?    I   10:11  0:04 [kworker/0:0-rcu_pan_gp]
root      3627  0.0  0.0  0 0 ?    I<   10:11  0:00 [kworker/1:1H]
root      3632  0.0  0.0  0 0 ?    I<   10:15  0:00 [kworker/0:0H-kblockd]
root      3644  1.5  0.0  0 0 ?    I   10:21  0:02 [kworker/0:1-events]
root      3647  0.0  0.0  0 0 ?    I   10:22  0:00 [kworker/u257:3-events_power_efficient]
root      3649  0.9  0.0  0 0 ?    I   10:22  0:00 [kworker/1:2-events]
root      3650  0.0  0.0  0 0 ?    I   10:23  0:00 [kworker/u258:0-events_power_efficient]
shumail+ 3652  266  0.1 10884 4480 tty1  R+   10:24  0:00 ps aux
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

Task 6:

```
shumaila062@shumailaa:~/lab4/workspace/python_project$ sudo adduser lab4user
[sudo] password for shumaila062:
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 []: Shuma
  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' ...
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

```
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
shumaila062@shumailaa:~/lab4/workspace/python_project$ getent passwd lab4user
lab4user:x:1001:1001:Shuma,,,:/home/lab4user:/bin/bash
shumaila062@shumailaa:~/lab4/workspace/python_project$ _
```

```
shumaila062@shumailaa:~$ su - lab4user
Password:
lab4user@shumailaa:~$ _
```

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

```
shumaila062@shumailaa:~$
```

Task 7:

```
GNU nano 7.2 /home/sh
#!/bin/bash
echo "lab 4 demo current user is $(whoami)"
echo "current time: $(date)"
uptime
free -h0
```

```
shumaila062@shumailaa:~$ chmod +x ~/lab4/workspace/run-demo.sh
shumaila062@shumailaa:~$ _
```

```
shumaila062@shumailaa:~$ ~/lab4/workspace/run-demo.sh
lab 4 demo current user is shumaila062
current time: Sat Oct 25 06:01:44 AM UTC 2025
06:01:44 up 1:22, 1 user, load average: 0.00, 0.00, 0.00
free: invalid option -- '0'

Usage:
free [options]

Options:
-b, --bytes          show output in bytes
--kilo              show output in kilobytes
--mega             show output in megabytes
--giga             show output in gigabytes
--tera            show output in terabytes
--peta            show output in petabytes
-k, --kibi          show output in kibibytes
-m, --mebi          show output in mebibytes
-g, --gibi          show output in gibibytes
--tebi            show output in tebibytes
--pebi            show output in pebibytes
-h, --human         show human-readable output
--si              use powers of 1000 not 1024
-l, --lohi          show detailed low and high memory statistics
-L, --line          show output on a single line
-t, --total         show total for RAM + swap
-v, --committed    show committed memory and commit limit
-s N, --seconds N   repeat printing every N seconds
-c N, --count N     repeat printing N times, then exit
-w, --wide          wide output

--help            display this help and exit
-V, --version      output version information and exit

For more details see free(1).
shumaila062@shumailaa:~$ _
```

Exam Evaluation Questions :

1)

```

C:\Users\Samina>ssh shumaila062@192.168.9.131
shumaila062@192.168.9.131's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-84-generic x86_64)

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

System information as of Sat Oct 25 06:33:02 AM UTC 2025

System load:  0.0               Processes:            217
Usage of /:   37.2% of 19.51GB   Users logged in:     1
Memory usage: 10%              IPv4 address for ens33: 192.168.9.131
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

28 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

*** System restart required ***
Last login: Mon Oct 20 09:46:55 2025 from 192.168.9.1
shumaila062@shumailaa:~$ |

```

```

shumaila062@shumailaa:~$ whoami
pwd
shumaila062
/home/shumaila062
shumaila062@shumailaa:~$

```

```

shumaila062@shumailaa:~$ hostname && hostname -I
shumailaa
192.168.9.131
shumaila062@shumailaa:~$ |

```

2)

```

shumaila062
shumaila062@shumailaa:~$ ls /
bin          boot      dev      home    lib64          lost+found  mnt  proc  run  sbin usr-is-merged  srv  sys  usr
bin usr-is-merged  cdrom    etc     lib  lib usr-is-merged  media  opt  root  sbin  snap  swap.img  tmp  var
shumaila062@shumailaa:~$ _

```

```
shumaila062@shumailaa:~$ 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
shumaila062@shumailaa:~$
```

```
alternatives      crypttab          grub.d            libaudit.conf    mtab              polkit-1          services          tmpfiles.d
apparmor          dbus-1            gshadow           libblockdev       multipath          pollinate         sgml              ubuntu-advantage
apparmor.d        dconf             gshadow-          libibverbs.d     multipath.conf    profile          shadow            ucf.conf
apport            debconf.conf     sss               libnl-3           nanorc             gnupgfile.d      shadow-           udev
apt              debian_version   gtk-3.0           locale.alias      needrestart        protocols         shells            udisks2
bash.bashrc       default          hdpamr.conf       locale.conf       netconfig          python3           skel              ufw
bash_completion   deluser.conf     hostname          locale.gen        netplan            python3.12       sos              update-manager
bash_completion.d depmod.d         hosts             localtime         network            rc0.d            ssh              update-notifier
bindresolv.blacklist dhcp             hosts.allow       logcheck          networkd-dispatcher rc1.d            ssl              UPower
binfmt.d          dhcpcd.conf      hosts.deny        login.defs        networks           rc2.d            subgid           usb-modeswitch.conf
bgobu            dokg             e2scrub.conf     logrotate.conf   nftables.conf     rc3.d            subuid           usb-modeswitch.d
ca-certificates  e2scrub.conf    environment       ls-release        nsswitch.conf     rc4.d            sudo.conf        vconsole.conf
ca-certificates.conf cloud            environment.d     lv                os-release         rc5.d            sudoers          vlm
console-setup     credstore        fonts            iscsi            magic              rc6.d            sudoers.d        vmware-tools
credstore         credstore.encrypted fstab             issue            magic.mime        resolv.conf      vmtoolsd         vtrgb
cron.d            cron.daily        fuse.conf         kernel            manpath.config   rpm              sudo_logsrvd.conf vulkan
cron.hourly       cron.monthly      gal.conf         ldapp             mime.types       rmt              sysctl.conf      wgetrc
cron.monthly      cron.monthly      glvnd            ld.so.cache       mk2fs.conf       rpc              sysctl.d         x11
crontab           cron.weekly       gnupg            ld.so.conf        modprobe.d        rsyslog.conf     sysstat          xattr.conf
cron.yearly       dmidekg          group            ld.so.conf.d     modules           rsyslog.d        systemd          xdg
autofs            dmidekg          log              mdadm             mtab              rpm              systemd          xml
block            dri              loop0            null              machine-id       rshlog.conf     terminfo         zsh_command_not_found
btrfs            ecryptfs         loop1            nvram             issue            rpm              systemd          zsh
btrfs-control    fb0              loop2            port              issue            rpm              systemd          zsh
bus              fd               loop3            ppp               issue            rpm              systemd          zsh
cdrom            full            loop4            psaux             issue            rpm              systemd          zsh
char             fuse            loop5            psm              issue            rpm              systemd          zsh
console          hidraw0         loop6            pts               issue            rpm              systemd          zsh
core             hpet            loop7            random            issue            rpm              systemd          zsh
cpu              hugepages       loop-control     rfc722            issue            rpm              systemd          zsh
cpu_dma_latency  hwrng          mapper          rfkill            issue            rpm              systemd          zsh
cuse             initctl         mcelog          rtc               issue            rpm              systemd          zsh
disk             input          mem             rtc               issue            rpm              systemd          zsh
dma_heap         kmsg           midi            sda               issue            rpm              systemd          zsh
backups          crash          lib              lock              issue            rpm              systemd          zsh
snap-private-tno snap-private-tno snap-private-tno snap-private-tno snap-private-tno snap-private-tno snap-private-tno snap-private-tno
systemd-private-103425b7fa3f4ad1a138c398c298eb53-ModemManager.service-pkn2E3
systemd-private-103425b7fa3f4ad1a138c398c298eb53-polkit.service-vtz1PK
systemd-private-103425b7fa3f4ad1a138c398c298eb53-systemd-logind.service-DHtG84
systemd-private-103425b7fa3f4ad1a138c398c298eb53-systemd-resolved.service-Jqx0DQ
systemd-private-103425b7fa3f4ad1a138c398c298eb53-systemd-timesyncd.service-JoVQ13
systemd-private-103425b7fa3f4ad1a138c398c298eb53-upower.service-FNpyHN
VMwareDnD
vmware-root_1918-566269629
vmware-root_764-2999067644
shumaila062@shumailaa:~$
```

```
vmware-root_764-2999067644
shumaila062@shumailaa:~$ ls -la ~
... answers.md .bash_history .bash_logout .bashrc .cache lab4 .local .profile .ssh .sudo_as_admin_successful
shumaila062@shumailaa:~$
```

```
GNU nano 7.2 /home/shumaila062/lab4
# filesystem inspection report
## /bin and /sbin
contain essential binaries and system tools
## /usr
contain user installed applications and tools
# /etc
contains syetm wide configuration files
```

3)

```
shumaila062@shumailaa:~$ mkdir -p ~/lab4/workspace/evidence/{suspicious, logs, backup}
shumaila062@shumailaa:~$ _
```

```
shumaila062@shumailaa:~$ touch file1.txt file2.txt .hiddenfiles.txt
shumaila062@shumailaa:~$ ls -la
.  answers.md  .bash_history  .bashrc  file1.txt  .hiddenfiles.txt  .local  .profile  .sudo_as_admin_successful
.. backup}    .bash_logout  .cache  file2.txt  lab4      logs,  .ssh
shumaila062@shumailaa:~$
```

```
shumaila062@shumailaa:~/lab4$ cp -r workspace workspace_backup
shumaila062@shumailaa:~/lab4$ ls
workspace  workspace_backup
shumaila062@shumailaa:~/lab4$ _
```

```
shumaila062@shumailaa:~/lab4$ history
 1 hostname
 2 su - lab4user
 3 nano ~/lab4/workspace/run-demo.sh
 4 chmod +x ~/lab4/workspace/run-demo.sh
 5 ip
 6 ip add
 7 ip addr show
 8 sudo systemctl status ssh
 9 whoami
10 ls /
11 cat /etc/os-release
12 ls /bin; ls /sbin; ls /usr; ls /opt; ls /etc; ls /dev; ls /var; ls /tmp
13 ls -a ~
14 nano ~/lab4/workspace/Q2_report.md
15 mkdir -p ~/lab4/workspace/evidence/{suspicious, logs, backup}
16 touch file1.txt file2.txt .hiddenfiles.txt
17 ls -a
18 cd ~/lab4
19 cp -r workspace workspace_backup
20 ls
21 history
shumaila062@shumailaa:~/lab4$
```

```
21 history
shumaila062@shumailaa:~/lab4$ cd ~/lab4/workspace/evidence/_
```

4)

```
shumaila062@shumailaa:~/lab4/workspace/evidence$ uname -a
Linux shumailaa 6.8.0-84-generic #84-Ubuntu SMP PREEMPT_DYNAMIC Fri Sep  5 22:36:38 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
shumaila062@shumailaa:~/lab4/workspace/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
shumaila062@shumailaa:~/lab4/workspace/evidence$
```

```

On-line CPU(s) list: 0,1
Vendor ID: GenuineIntel
Model name: Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz
CPU family: 6
Model: 142
Thread(s) per core: 1
Core(s) per socket: 1
Socket(s): 2
Stepping: 12
BogoMIPS: 4608.01
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 pt1 sssd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt xsaveopt 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: 16 MiB (2 instances)
NUMA:
NUMA node(s): 1
NUMA node0 CPU(s): 0,1
Vulnerabilities:
Gather data sampling: Unknown: Dependent on hypervisor status
Itlb multihit: 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; PFRSB-eIBRS Not affected; BHI SW loop, KVM SW loop
Srbds: Unknown: Dependent on hypervisor status
Tsx async abort: Not affected

Mem: total used free shared buff/cache available
      3.8Gi 538Mi 2.5Gi 1.5Mi 1.0Gi 3.3Gi
Swap: 3.8Gi 0B 3.8Gi
Filesystem      Size Used Avail Use% Mounted on
tmpfs            387M 1.5M 386M 1% /run
/dev/sda2        20G  7.3G  12G 40% /
tmpfs            1.9G  0  1.9G 0% /dev/shm
tmpfs            5.0M  0  5.0M 0% /run/lock
tmpfs            387M 20K 387M 1% /run/user/1000
shumaila062@shumailaa:~/lab4/workspace/evidences$

```

```

root      785  0.0  0.0    0    0 ?      S   04:41  0:00 [irq/59-vmx]
message+  804  0.0  0.1   9916 5504 ?    Ss  04:41  0:00 qdbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog
polkitd   828  0.0  0.2 308164 8064 ?    Ssl 04:41  0:00 /usr/lib/polkit-1/polkitd --no-debug
root      864  0.0  0.2  18140 8832 ?    Ss  04:41  0:00 /usr/lib/systemd/systemd-logind
root      915  0.0  0.5 109692 22912 ?   Ssl 04:41  0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-sign
syslog    921  0.0  0.1 222508 5888 ?    Ssl 04:41  0:00 /usr/sbin/rsyslogd -n -iNONE
root      981  0.0  0.3 392092 12800 ?   Ssl 04:41  0:00 /usr/sbin/ModemManager
root     1042  0.0  0.0   6824 2688 ?    Ss  04:41  0:00 /usr/sbin/cron -f -P
root     1151  0.0  0.1   6944 4480 tty1   Ss  04:41  0:00 /bin/login -p --
shumail+ 1501  0.0  0.2 20064 11136 ?   Ss  04:45  0:00 /usr/lib/systemd/systemd --user
shumail+ 1503  0.0  0.0 21152 3520 ?    S   04:45  0:00 (sd-pam)
shumail+ 1514  0.0  0.1   8788 5504 tty1   S   04:45  0:00 -bash
root     1555  0.0  0.0    0    0 ?      I<   04:45  0:00 [kworker/R-tls-s]
root     1587  0.0  0.0   6104 1920 tty6   Ss+  04:54  0:00 /sbin/agetty -o -p -- \u --noclear - linux
root     1865  0.0  0.0    0    0 ?      S   05:12  0:00 [psimon]
root     1898  0.0  0.3 50320 13824 ?   S<   05:12  0:00 /usr/lib/systemd/systemd-journald
systemd+ 1900  0.0  0.3 21580 12928 ?   Ss   05:12  0:00 /usr/lib/systemd/systemd-resolved
systemd+ 1901  0.0  0.1  91024 7808 ?    Ssl 05:12  0:00 /usr/lib/systemd/systemd-timesyncd
root     1902  0.0  0.3 468976 13440 ?   Ssl 05:12  0:00 /usr/libexec/udisks2/udisksd
root     1903  0.0  0.2 313960 9088 ?    Ssl 05:12  0:00 /usr/libexec/upowerd
root     1906  0.0  0.1 28916 7784 ?    Ss   05:12  0:00 /usr/lib/systemd/systemd-udev
root     1909  0.0  0.3 53464 12160 ?   Ss   05:12  0:00 /usr/bin/VGAuthService
root     1918  0.4  0.2 315868 9340 ?   Ssl 05:12  0:39 /usr/bin/vmtoolsd
root     1967  0.0  0.0    0    0 ?      S   05:12  0:00 [psimon]
root     8054  0.0  0.2 12020 8064 ?    Ss   06:06  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root     8085  0.1  0.0    0    0 ?      I   06:21  0:05 [kworker/1:3-events]
root     8137  0.0  0.2 14964 10496 ?   Ss   06:34  0:00 sshd: shumaila062 [priv]
shumail+ 8217  0.0  0.1 14964 6976 ?    S   06:34  0:00 sshd: shumaila062@pts/0
shumail+ 8248  0.0  0.1   8648 5376 pts/0   Ss+  06:34  0:00 -bash
root     8241  0.1  0.0    0    0 ?      I   06:35  0:03 [kworker/0:1-events]
root     8362  0.0  0.0    0    0 ?      I   06:36  0:00 [kworker/u258:1-events_unbound]
root     8373  0.0  0.0    0    0 ?      I   06:42  0:00 [kworker/u257:1-events_unbound]
root     8386  0.0  0.0    0    0 ?      I   06:54  0:02 [kworker/1:0-events]
systemd+ 8600  0.0  0.2 18992 9344 ?    Ss   06:56  0:00 /usr/lib/systemd/systemd-networkd
root     8868  0.0  0.0    0    0 ?      I   07:02  0:00 [kworker/u258:2-events_power_efficient]
root     8877  0.0  0.0    0    0 ?      I<   07:05  0:00 [kworker/0:0H]
root     8884  0.0  0.0    0    0 ?      I   07:12  0:00 [kworker/1:1]
root     8889  0.0  0.0    0    0 ?      I<   07:15  0:00 [kworker/0:1H-kblockd]
root     8896  0.0  0.2 14960 10496 ?   Ss   07:19  0:00 sshd: shumaila062 [priv]
shumail+ 8953  0.0  0.1 15092 6976 ?    S   07:19  0:00 sshd: shumaila062@pts/1
shumail+ 8954  0.0  0.1   8648 5504 pts/1   Ss+  07:19  0:00 -bash
root     8973  0.0  0.0    0    0 ?      I   07:20  0:00 [kworker/u257:3-events_power_efficient]
root     8984  0.0  0.0    0    0 ?      I   07:28  0:00 [kworker/u257:0-events_power_efficient]
root     8985  0.0  0.0    0    0 ?      I   07:29  0:00 [kworker/u258:0-flush-8:0]
root     8988  0.0  0.0    0    0 ?      I   07:30  0:00 [kworker/0:0-cgroup_destroy]
root     8995  0.0  0.0    0    0 ?      I   07:33  0:00 [kworker/u257:2-events_power_efficient]
root     9000  0.0  0.0    0    0 ?      I<   07:35  0:00 [kworker/0:2H-kblockd]
root     9001  0.0  0.0    0    0 ?      I   07:35  0:00 [kworker/u258:3-events_unbound]
shumail+ 9002  200 0.1 10884 4480 tty1   R+   07:36  0:00 ps aux
shumaila062@shumailaa:~/lab4/workspace/evidences$

```



```
shumaila062@shumailaa:~/lab4/workspace/evidence$ getent passwd lab4user
lab4user:x:1001:1001:Shuma,,,:/home/lab4user:/bin/bash
shumaila062@shumailaa:~/lab4/workspace/evidence$
```

```
shumaila062@shumailaa:~/lab4/workspace/evidence$ su - lab4user
Password:
lab4user@shumailaa:~$
```

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

```
shumaila062@shumailaa:~/lab4/workspace/evidence$
```

```
2025-10-25T06:25:01.173432+00:00 shumailaa CRON[8108]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T06:25:01.188359+00:00 shumailaa CRON[8108]: pam_unix(cron:session): session closed for user root
2025-10-25T06:25:01.193821+00:00 shumailaa CRON[8107]: pam_unix(cron:session): session closed for user root
2025-10-25T06:32:09.595547+00:00 shumailaa sudo: shumaila062 : TTY=ttty1 : PWD=/home/shumaila062 : USER=root : COMMAND=/usr/bin/systemctl status ssh
2025-10-25T06:32:09.591526+00:00 shumailaa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by shumaila062(uid=1000)
2025-10-25T06:32:09.648296+00:00 shumailaa sudo: pam_unix(sudo:session): session closed for user root
2025-10-25T06:33:02.197836+00:00 shumailaa sshd[8137]: Accepted password for shumaila062 from 192.168.9.1 port 62067 ssh2
2025-10-25T06:33:02.202328+00:00 shumailaa sshd[8137]: pam_unix(sshd:session): session opened for user shumaila062(uid=1000) by shumaila062(uid=0)
2025-10-25T06:33:02.233077+00:00 shumailaa systemd-logind[864]: New session 17 of user shumaila062.
2025-10-25T06:35:01.201297+00:00 shumailaa CRON[8363]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T06:35:01.221399+00:00 shumailaa CRON[8363]: pam_unix(cron:session): session closed for user root
2025-10-25T06:45:01.250845+00:00 shumailaa CRON[8376]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T06:45:01.275443+00:00 shumailaa CRON[8376]: pam_unix(cron:session): session closed for user root
2025-10-25T06:55:01.670946+00:00 shumailaa CRON[8387]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T06:55:01.680116+00:00 shumailaa CRON[8387]: pam_unix(cron:session): session closed for user root
2025-10-25T07:05:02.042646+00:00 shumailaa CRON[8874]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T07:05:02.058778+00:00 shumailaa CRON[8874]: pam_unix(cron:session): session closed for user root
2025-10-25T07:15:01.088598+00:00 shumailaa CRON[8886]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T07:15:01.113328+00:00 shumailaa CRON[8886]: pam_unix(cron:session): session closed for user root
2025-10-25T07:17:01.135978+00:00 shumailaa CRON[8891]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T07:17:01.161765+00:00 shumailaa CRON[8891]: pam_unix(cron:session): session closed for user root
2025-10-25T07:19:43.169993+00:00 shumailaa sshd[8896]: Accepted password for shumaila062 from 192.168.9.1 port 55600 ssh2
2025-10-25T07:19:43.173307+00:00 shumailaa sshd[8896]: pam_unix(sshd:session): session opened for user shumaila062(uid=1000) by shumaila062(uid=0)
2025-10-25T07:19:43.200620+00:00 shumailaa systemd-logind[864]: New session 24 of user shumaila062.
2025-10-25T07:25:01.192873+00:00 shumailaa CRON[8978]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T07:25:01.220543+00:00 shumailaa CRON[8978]: pam_unix(cron:session): session closed for user root
2025-10-25T07:35:01.261419+00:00 shumailaa CRON[8996]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T07:35:01.286880+00:00 shumailaa CRON[8996]: pam_unix(cron:session): session closed for user root
2025-10-25T07:40:16.935603+00:00 shumailaa sudo: shumaila062 : TTY=ttty1 : PWD=/home/shumaila062/lab4/workspace/evidence : USER=root : COMMAND=/usr/sbin/adduser lab4user
2025-10-25T07:40:16.940047+00:00 shumailaa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by shumaila062(uid=1000)
2025-10-25T07:40:17.105821+00:00 shumailaa sudo: pam_unix(sudo:session): session closed for user root
2025-10-25T07:41:05.130534+00:00 shumailaa sudo: shumaila062 : TTY=ttty1 : PWD=/home/shumaila062/lab4/workspace/evidence : USER=root : COMMAND=/usr/sbin/adduser lab4user
2025-10-25T07:41:05.132292+00:00 shumailaa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by shumaila062(uid=1000)
2025-10-25T07:41:05.187672+00:00 shumailaa sudo: pam_unix(sudo:session): session closed for user root
2025-10-25T07:45:01.300970+00:00 shumailaa CRON[9020]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-10-25T07:45:01.397408+00:00 shumailaa CRON[9020]: pam_unix(cron:session): session closed for user root
2025-10-25T07:45:35.747857+00:00 shumailaa su: pam_unix(su-l:auth): authentication failure; logname=shumaila062 uid=1000 euid=0 tty=/dev/tty1 ruser=shumaila062 rhost= user=lab4user
2025-10-25T07:45:38.051242+00:00 shumailaa su[9025]: FAILED SU (to lab4user) shumaila062 on ttty1
2025-10-25T07:45:45.803578+00:00 shumailaa su[9026]: (to lab4user) shumaila062 on ttty1
2025-10-25T07:45:45.804755+00:00 shumailaa su[9026]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by shumaila062(uid=1000)
2025-10-25T07:46:50.599344+00:00 shumailaa sudo: lab4user : user NOT in sudoers ; TTY=ttty1 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/whoami
2025-10-25T07:48:04.410281+00:00 shumailaa su[9026]: pam_unix(su-l:session): session closed for user lab4user
2025-10-25T07:53:30.850618+00:00 shumailaa sudo: shumaila062 : TTY=ttty1 : PWD=/home/shumaila062/lab4/workspace/evidence : USER=root : COMMAND=/usr/bin/cat /var/log/auth.log
2025-10-25T07:53:30.853358+00:00 shumailaa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by shumaila062(uid=1000)
shumaila062@shumailaa:~/lab4/workspace/evidence$
shumaila062@shumailaa:~/lab4/workspace/evidence$ _
```

```
shumaila062@shumailaa:~/lab4/workspace/evidence$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user 'lab4user' ...
shumaila062@shumailaa:~/lab4/workspace/evidence$ _
```