

FATIMA JINNAH WOMEN UNIVERSITY

Department of Software Engineering



LAB #04

SUBJECT: CLOUD COMPUTING

SUBMITTED TO: SIR MUHAMMAD SHOAIB

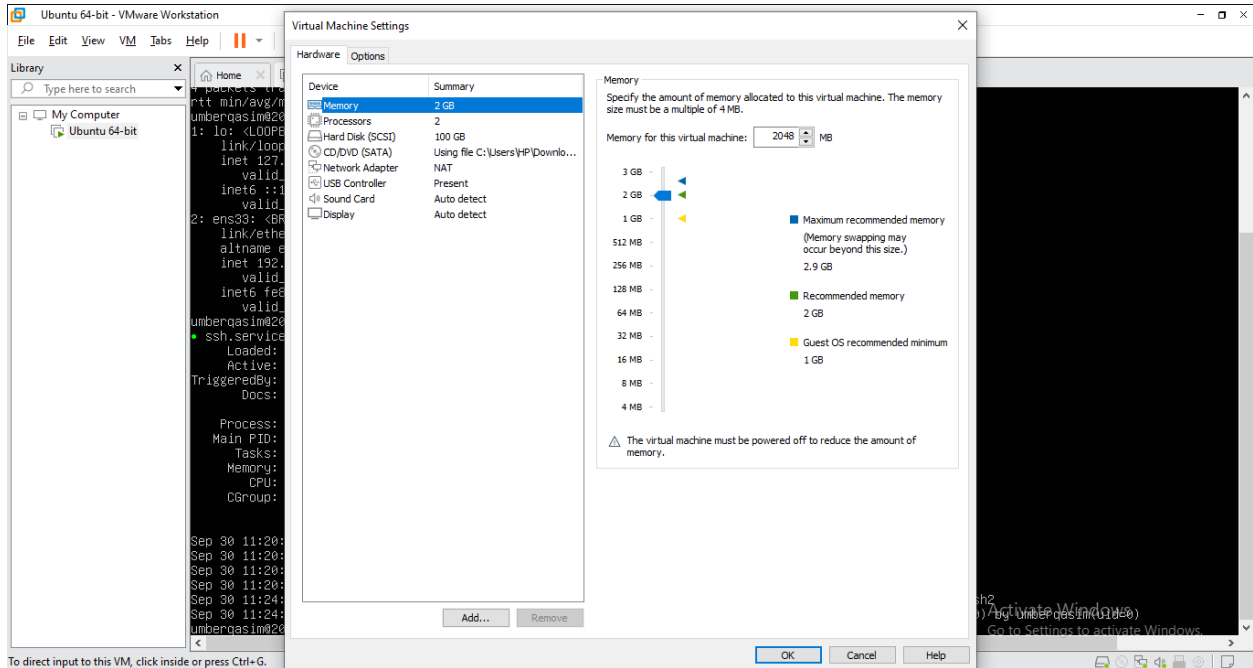
SUBMITTED BY: UMBER QASIM

REGISTRATION NO: 2023-BSE-066

CLASS: BSSE V-B

Virtualization & Linux Fundamentals

Task#01: Verify VM resources in VMware



Task#02: Start VM and log in (use your preferred host terminal method only)

```
umbergasim@2023-bse-066: ~  
Microsoft Windows [Version 10.0.19045.6456]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\HP>ssh umbergasim@192.168.254.129  
umbergasim@192.168.254.129'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 Fri Oct 17 05:14:13 AM UTC 2025  
  
System load:  0.0      Processes:            222  
Usage of /:   10.5% of 47.93GB  Users logged in:     1  
Memory usage: 20%      IPv4 address for ens33: 192.168.254.129  
Swap usage:   0%  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s  
  just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
Expanded Security Maintenance for Applications is not enabled.  
  
17 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: Fri Oct 17 05:07:43 2025 from 192.168.254.1  
umbergasim@2023-bse-066:~$
```

```
umberqasim@2023-bse-066:~$ whoami
umberqasim
umberqasim@2023-bse-066:~$ pwd
/home/umberqasim
umberqasim@2023-bse-066:~$
```

Task#03: Filesystem exploration – root tree and dotfiles

List root directory

```
umberqasim@2023-bse-066:~$ ls -la /
total 2097244
drwxr-xr-x  23 root root    4096 Sep 30 03:05 .
drwxr-xr-x  23 root root    4096 Sep 30 03:05 ..
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 Oct 17 04:18 boot
dr-xr-xr-x   2 root root    4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root   4120 Sep 30 11:20 dev
drwxr-xr-x 108 root root    4096 Oct 17 04:16 etc
drwxr-xr-x   3 root root    4096 Sep 30 03:12 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 30 02:57 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 283 root root      0 Sep 30 11:19 proc
drwx-----  3 root root    4096 Oct 17 04:54 root
drwxr-xr-x  31 root root   1000 Oct 17 05:14 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 30 03:12 snap
drwxr-xr-x   2 root root    4096 Aug  5 16:54 srv
-rw-----  1 root root 2147483648 Sep 30 03:05 swap.img
dr-xr-xr-x  13 root root      0 Sep 30 11:19 sys
drwxrwxrwt  16 root root    4096 Oct 17 04:17 tmp
drwxr-xr-x  12 root root    4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root    4096 Sep 30 03:12 var
```

Explore key directories

```
umberqasim@2023-bse-066:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
```

```
umberqasim@2023-bse-066:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
```

```

umberqasim@2023-bse-066:~$ ls -la /usr
total 108
drwxr-xr-x 12 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..
drwxr-xr-x  2 root root 36864 Oct 17 04:17 bin
drwxr-xr-x  2 root root 4096 Apr 22  2024 games
drwxr-xr-x 33 root root 16384 Sep 30 11:13 include
drwxr-xr-x 79 root root 4096 Oct 17 04:18 lib
drwxr-xr-x  2 root root 4096 Sep 30 11:13 lib64
drwxr-xr-x 11 root root 4096 Sep 30 03:05 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x  2 root root 20480 Oct 17 04:17 sbin
drwxr-xr-x 124 root root 4096 Sep 30 05:21 share
drwxr-xr-x  6 root root 4096 Oct 17 04:18 src

```

```

umberqasim@2023-bse-066:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..

```

Ubuntu 64-bit - VMware Workstation

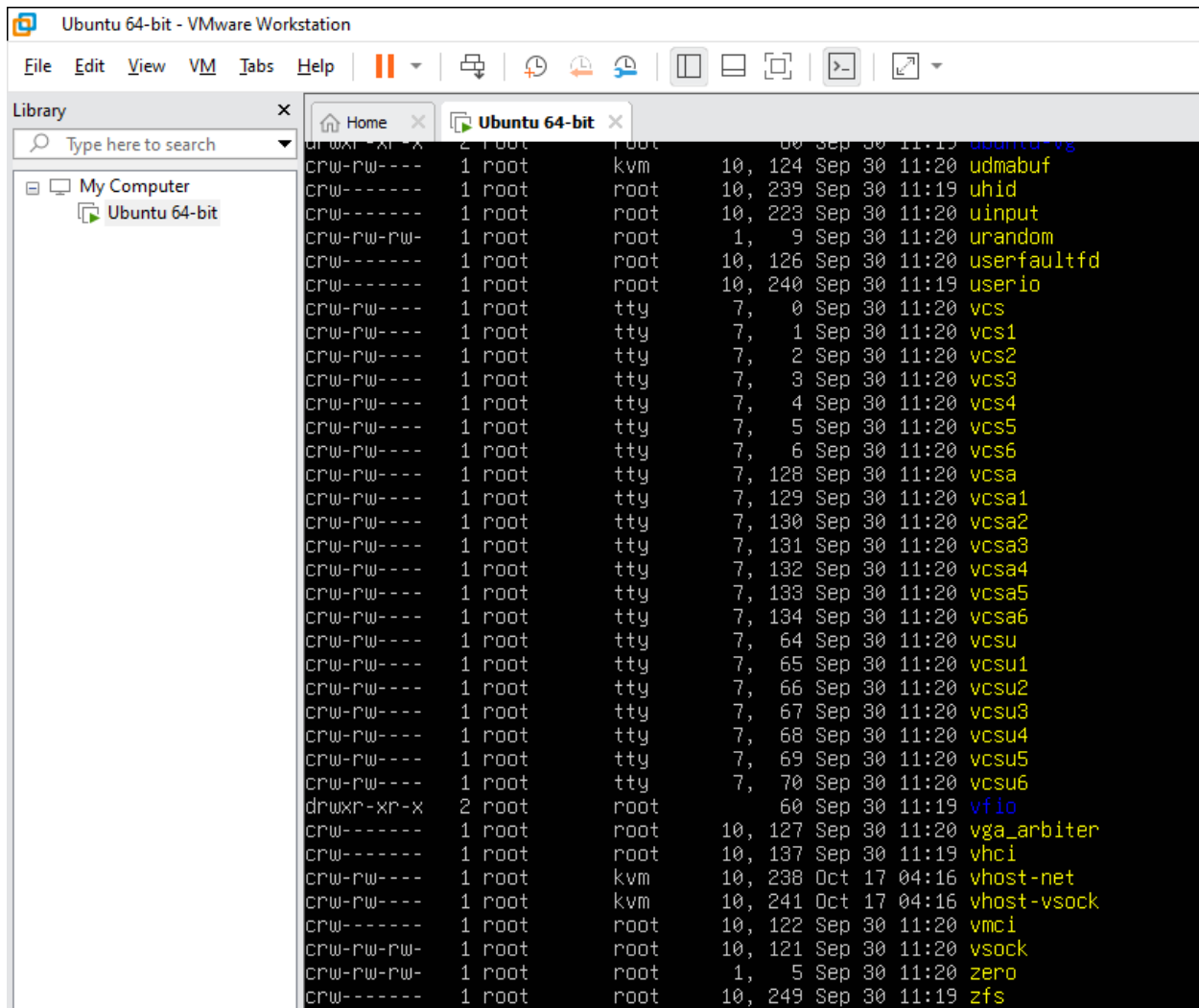
File Edit View VM Tabs Help

Library

My Computer

Ubuntu 64-bit

-rw-r--r--	1	root	root	24	Sep	30	03:12	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--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	30	03:05	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	30	11:15	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	Sep	30	11:15	update-motd.d
drwxr-xr-x	2	root	root	4096	Aug	5	17:14	update-notifier
drwxr-xr-x	2	root	root	4096	Sep	30	03:05	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	30	11:15	vim
drwxr-xr-x	4	root	root	4096	Sep	30	11:15	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



```

umberqasim@2023-bse-066:~$ ls -la /var
total 56
drwxr-xr-x 13 root root 4096 Sep 30 03:12 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..
drwxr-xr-x 2 root root 4096 Oct 19 07:09 backups
drwxr-xr-x 16 root root 4096 Sep 30 05:06 cache
drwxrwsrwt 2 root root 4096 Aug 5 17:02 crash
drwxr-xr-x 45 root root 4096 Sep 30 05:06 lib
drwxrwsr-x 2 root staff 4096 Apr 22 2024 local
lrwxrwxrwx 1 root root 9 Aug 5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 19 07:09 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 19 07:12 tmp
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated

```

```

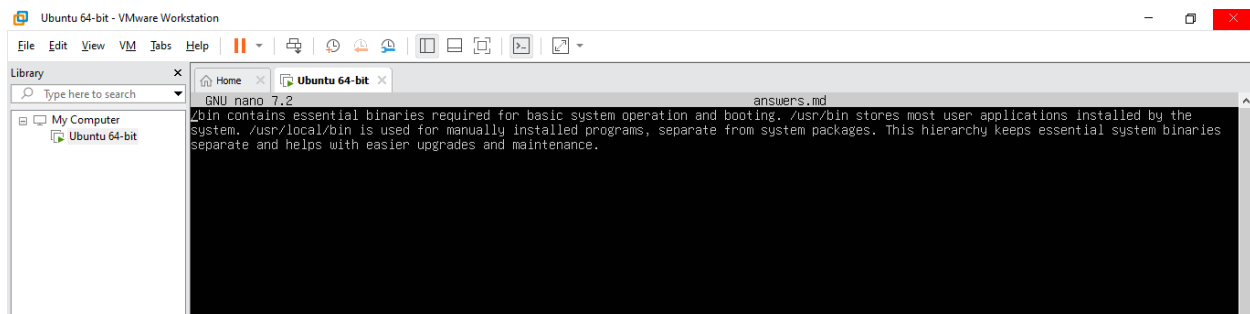
umberqasim@2023-bse-066:~$ ls -la /tmp
total 64
drwxrwxrwt 16 root root 4096 Oct 19 07:12 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .font-unix
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .ICE-unix
drwx----- 2 root root 4096 Sep 30 11:19 snap-private-tmp
drwx----- 3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-fwupd.service-70ZtQF
drwx----- 3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-ModemManager.service-7qmoT9
drwx----- 3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-polkit.service-M5032n
drwx----- 3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-logind.service-YwgFeh
drwx----- 3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-resolved.service-qWrv2f
drwx----- 3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-timesyncd.service-BwRz3V
drwx----- 2 root root 4096 Oct 17 04:16 vmware-root_3320-2999004153
drwx----- 2 root root 4096 Sep 30 11:20 vmware-root_741-4248811580
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .X11-unix
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .XIM-unix

```

```

umberqasim@2023-bse-066:~$ ls -la ~
total 36
drwxr-x--- 4 umberqasim umberqasim 4096 Oct  2 12:23 .
drwxr-xr-x 3 root      root      4096 Sep 30 03:12 ..
-rw----- 1 umberqasim umberqasim  429 Oct 17 05:13 .bash_history
-rw-r--r-- 1 umberqasim umberqasim  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 umberqasim umberqasim 3771 Mar 31  2024 .bashrc
drwx----- 2 umberqasim umberqasim 4096 Sep 30 03:17 .cache
-rw----- 1 umberqasim umberqasim   20 Oct  2 12:23 .lessshst
-rw-r--r-- 1 umberqasim umberqasim  807 Mar 31  2024 .profile
drwx----- 2 umberqasim umberqasim 4096 Sep 30 05:47 .ssh
-rw-r--r-- 1 umberqasim umberqasim    0 Sep 30 05:14 .sudo_as_admin_successful

```



Task#04: Essential CLI tasks – navigation and file operations

Creating Workspace

```

umberqasim@2023-bse-066:~$ mkdir -p ~/lab4/workspace/python_project

```

Navigating

```

umberqasim@2023-bse-066:~$ cd ~/lab4/workspace/python_project
umberqasim@2023-bse-066:~/lab4/workspace/python_project$

```

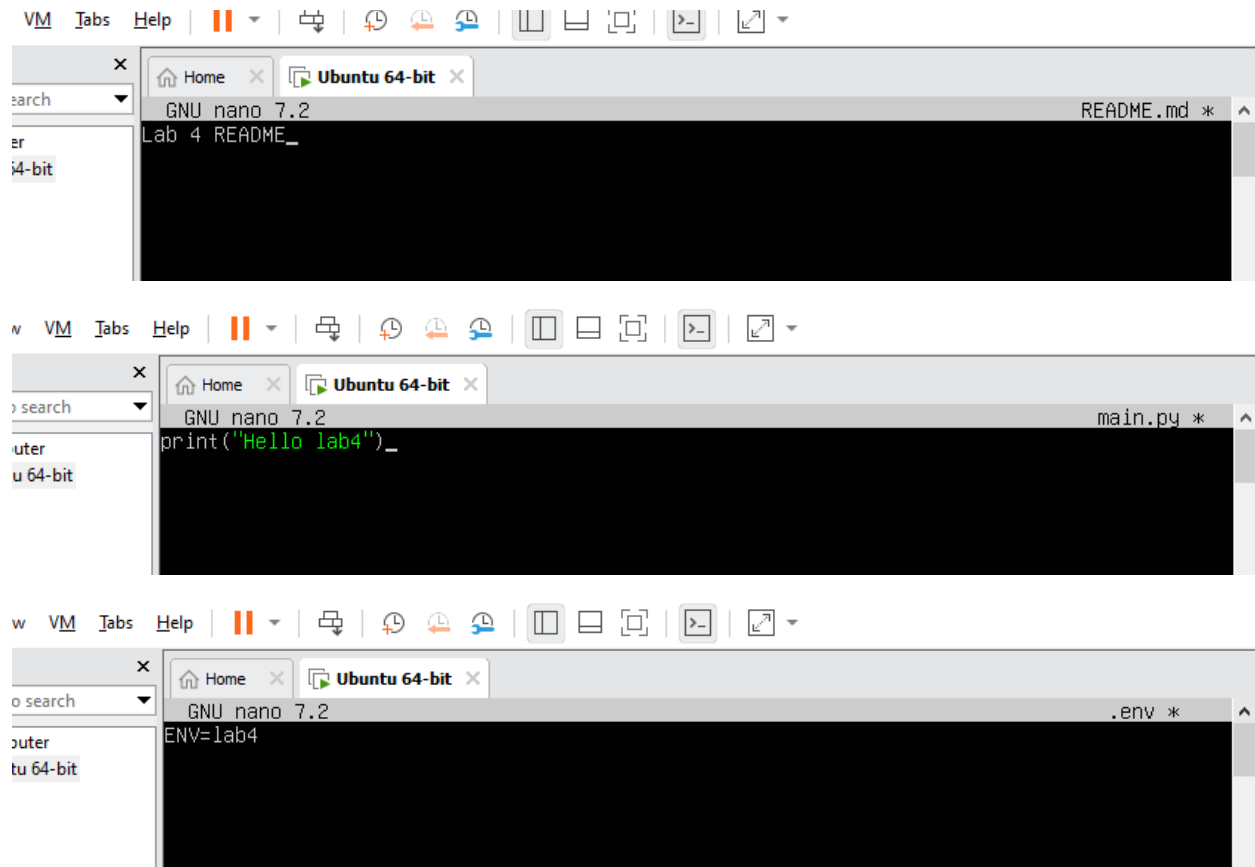
Current directory check

```

umberqasim@2023-bse-066:~/lab4/workspace/python_project$ pwd
/home/umberqasim/lab4/workspace/python_project

```

Creating files



List files

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 umberqasim umberqasim 4096 Oct 23 12:15 .
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 12:05 ..
-rw-rw-r-- 1 umberqasim umberqasim   9 Oct 23 12:15 .env
-rw-rw-r-- 1 umberqasim umberqasim  20 Oct 23 12:14 main.py
-rw-rw-r-- 1 umberqasim umberqasim  13 Oct 23 12:12 README.md
umberqasim@2023-bse-066:~/lab4/workspace/python_project$
```

Copy README.md

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ cp README.md README.copy.md
```

Move (rename) copied file

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ mv README.copy.md README.dev.md
```

Delete that file

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ rm README.dev.md
```

Create another folder (for Java)

```
umbergasim@2023-bse-066:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app_
```

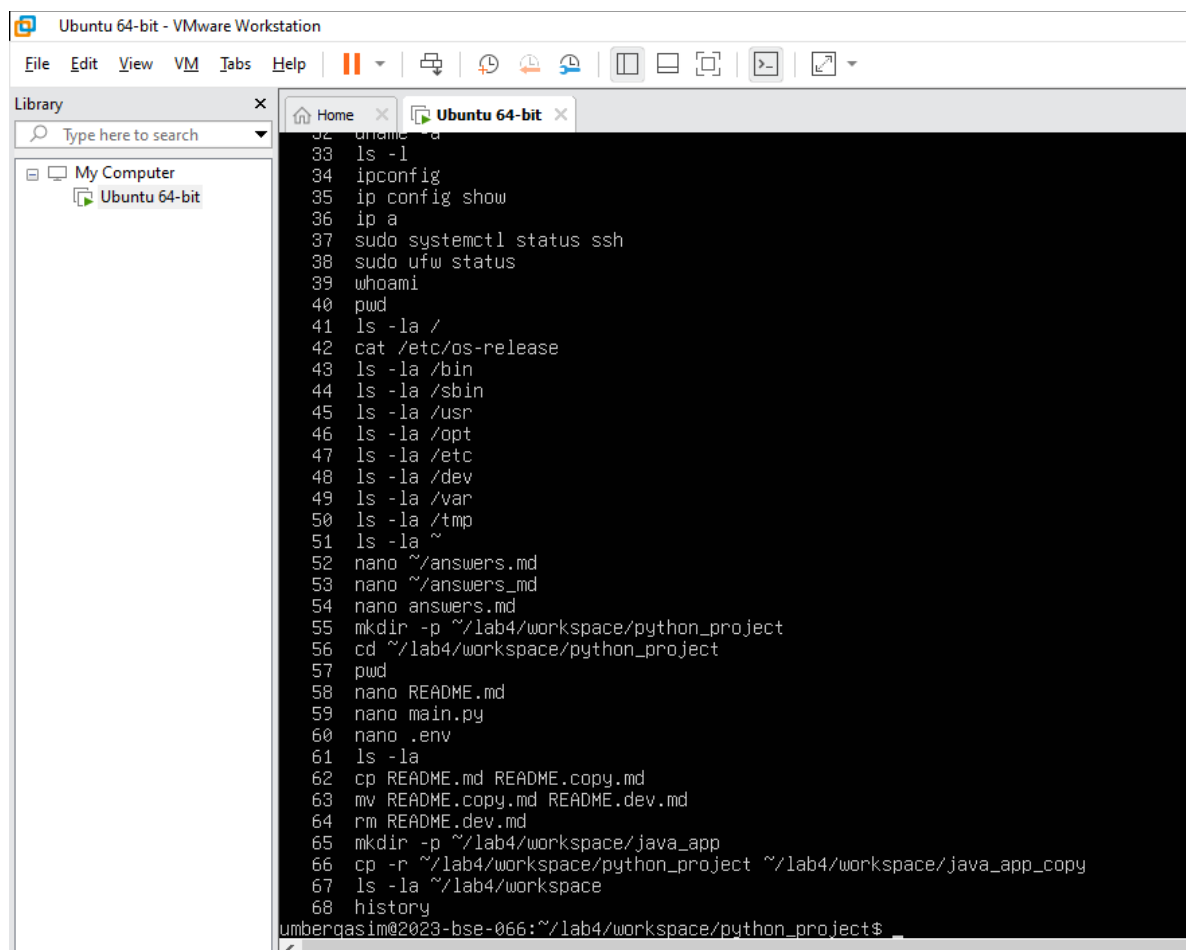
Copy entire python_project folder

```
umbergasim@2023-bse-066:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
```

Verify copy

```
umbergasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace
total 20
drwxrwxr-x 5 umbergasim umbergasim 4096 Oct 23 12:29 .
drwxrwxr-x 3 umbergasim umbergasim 4096 Oct 23 12:05 ..
drwxrwxr-x 2 umbergasim umbergasim 4096 Oct 23 12:25 java_app
drwxrwxr-x 2 umbergasim umbergasim 4096 Oct 23 12:29 java_app_copy
drwxrwxr-x 2 umbergasim umbergasim 4096 Oct 23 12:22 python_project
umbergasim@2023-bse-066:~/lab4/workspace/python_project$
```

Show command history

A screenshot of a VMware Workstation window titled 'Ubuntu 64-bit - VMware Workstation'. The window shows a terminal session with a list of commands and their outputs. The terminal text is as follows:

```
32 nano ~/answers.md
33 ls -l
34 ipconfig
35 ip config show
36 ip a
37 sudo systemctl status ssh
38 sudo ufw status
39 whoami
40 pwd
41 ls -la /
42 cat /etc/os-release
43 ls -la /bin
44 ls -la /sbin
45 ls -la /usr
46 ls -la /opt
47 ls -la /etc
48 ls -la /dev
49 ls -la /var
50 ls -la /tmp
51 ls -la ~
52 nano ~/answers.md
53 nano ~/answers_md
54 nano answers.md
55 mkdir -p ~/lab4/workspace/python_project
56 cd ~/lab4/workspace/python_project
57 pwd
58 nano README.md
59 nano main.py
60 nano .env
61 ls -la
62 cp README.md README.copy.md
63 mv README.copy.md README.dev.md
64 rm README.dev.md
65 mkdir -p ~/lab4/workspace/java_app
66 cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
67 ls -la ~/lab4/workspace
68 history
umbergasim@2023-bse-066:~/lab4/workspace/python_project$
```

Demonstrate tab completion

Before tab:

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ cd ~/lab4/workspace/p_
```

After tab:

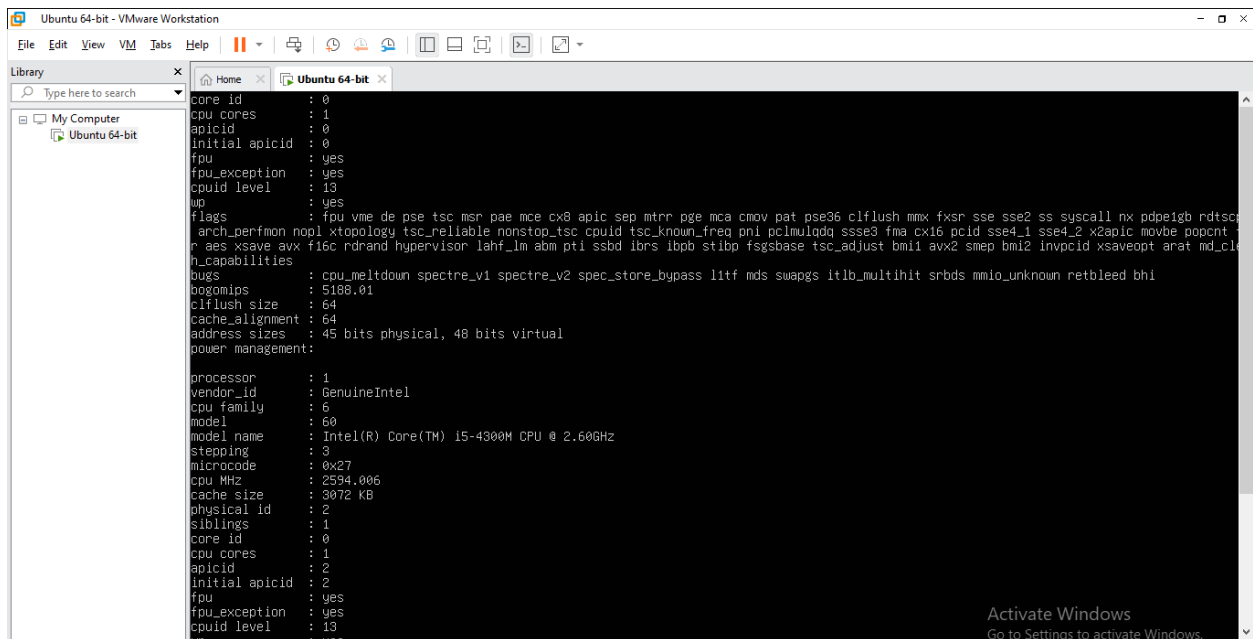
```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ cd ~/lab4/workspace/python_project/_
```

Task#05: System info, resources & processes

Kernel and OS info

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ uname -a
Linux 2023-bse-066 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
```

CPU details



```
core_id      : 0
cpu_cores   : 1
apicid      : 0
initial_apicid : 0
fpu         : yes
fpu_exception : yes
cpuid_level : 13
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
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
r aes xsave avx f16c rdrand hypervisor lahf_lm abm pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid xsaveopt arat md_cl
n_capabilities
bugs        : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swappgs itlb_multihit srbds mmio_unknown retbleed bhi
bogomips    : 5180.01
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       : 60
model name  : Intel(R) Core(TM) i5-4300M CPU @ 2.60GHz
stepping    : 3
microcode   : 0x27
cpu MHz     : 2594.006
cache size  : 3072 KB
physical id : 2
siblings    : 1
core id     : 0
cpu_cores   : 1
apicid      : 2
initial_apicid : 2
fpu         : yes
fpu_exception : yes
cpuid_level : 13
```

Memory information

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ free -h
              total        used        free      shared  buff/cache   available
Mem:          1.9Gi         437Mi        576Mi        920Ki         1.1Gi         1.4Gi
Swap:          2.0Gi         780Ki        2.0Gi
```

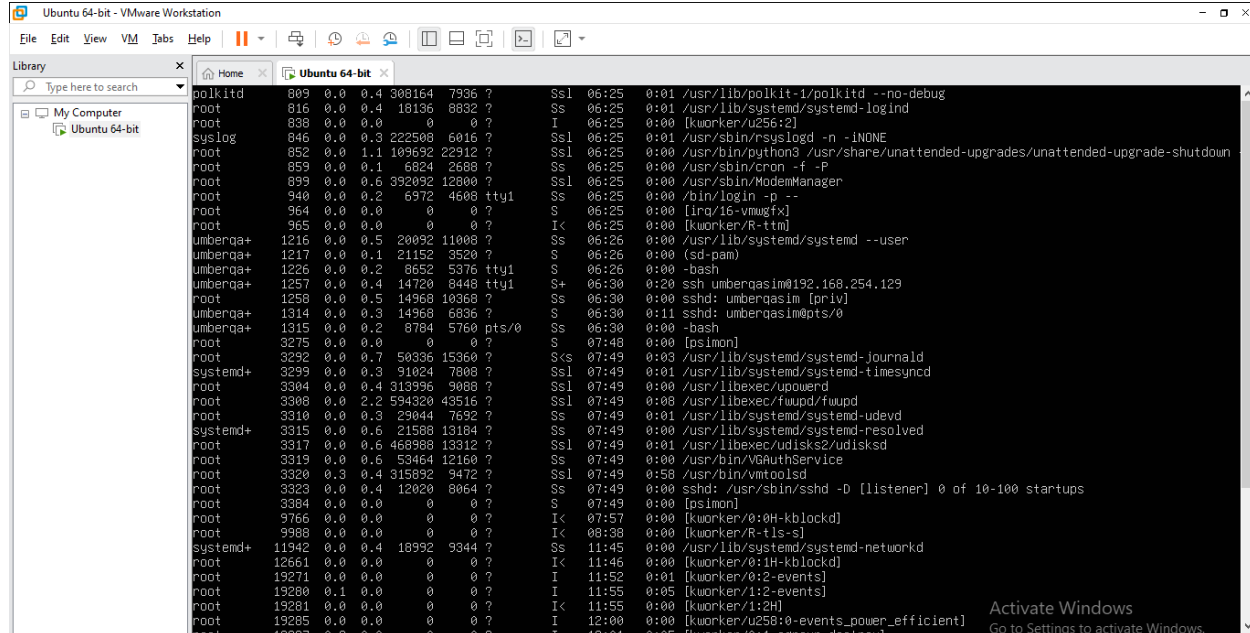
Disk information

```
umberqasim@2023-bse-066:~/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 48G       5.1G    41G   12% /
tmpfs                     960M        0    960M    0% /dev/shm
tmpfs                     5.0M        0    5.0M    0% /run/lock
/dev/sda2                 2.0G       192M    1.6G   11% /boot
tmpfs                     192M        12K    192M    1% /run/user/1000
```

OS release version

```
umberqasim@2023-bse-066:~/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
```

Running processes



PID	PPID	CPU	MEM	VSZ	RSS	TTY	COMMAND
polkitd	809	0.0	0.4	308164	7936	?	Ssl 06:25 0:01 /usr/lib/polkit-1/polkitd --no-debug
root	816	0.0	0.4	18136	8832	?	Ss 06:25 0:01 /usr/lib/systemd/systemd-logind
root	838	0.0	0.0	0	0	?	I 06:25 0:00 [kworker/u256:2]
syslog	846	0.0	0.3	222508	6016	?	Ssl 06:25 0:01 /usr/sbin/rsyslogd -n -iNONE
root	852	0.0	1.1	109692	22912	?	Ssl 06:25 0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown
root	859	0.0	0.1	6824	2688	?	Ss 06:25 0:00 /usr/sbin/cron -f -P
root	899	0.0	0.6	392092	12800	?	Ssl 06:25 0:00 /usr/sbin/ModemManager
root	940	0.0	0.2	6972	4608	ttty1	Ss 06:25 0:00 /bin/login -p --
root	964	0.0	0.0	0	0	?	S 06:25 0:00 [irq/16-vmwgfx]
root	965	0.0	0.0	0	0	?	I< 06:25 0:00 [kworker/R-ttm]
umberqasim	1216	0.0	0.5	20092	11008	?	Ss 06:25 0:00 /usr/lib/systemd/systemd --user
umberqasim	1217	0.0	0.1	21152	9520	?	S 06:26 0:00 (sd-pam)
umberqasim	1226	0.0	0.2	8652	5376	ttty1	S 06:26 0:00 -bash
umberqasim	1257	0.0	0.4	14720	8448	ttty1	S+ 06:30 0:20 ssh umberqasim@192.168.254.129
root	1258	0.0	0.5	14968	10368	?	Ss 06:30 0:00 sshd: umberqasim [priv]
umberqasim	1314	0.0	0.3	14968	6836	?	S 06:30 0:11 sshd: umberqasim@pts/0
umberqasim	1315	0.0	0.2	8784	5760	pts/0	Ss 06:30 0:00 -bash
root	3275	0.0	0.0	0	0	?	S 07:48 0:00 [psimon]
root	3292	0.0	0.7	50336	15360	?	S<S 07:49 0:03 /usr/lib/systemd/systemd-journald
systemd+	3299	0.0	0.3	91024	7808	?	Ssl 07:49 0:01 /usr/lib/systemd/systemd-timesyncd
root	3384	0.0	0.4	313956	9088	?	Ssl 07:49 0:00 /usr/libexec/upowerd
root	3308	0.0	2.2	594320	49516	?	Ssl 07:49 0:00 /usr/libexec/fwupd/fwupd
root	3310	0.0	0.3	29044	7692	?	Ss 07:49 0:01 /usr/lib/systemd/systemd-udevd
systemd+	3315	0.0	0.6	21588	13184	?	Ss 07:49 0:00 /usr/lib/systemd/systemd-resolved
root	3317	0.0	0.6	468988	13312	?	Ssl 07:49 0:01 /usr/libexec/udisks2/udisksd
root	3319	0.0	0.6	53464	12160	?	Ss 07:49 0:00 /usr/bin/VGAAuthService
root	3320	0.3	0.4	315892	9472	?	Ssl 07:49 0:58 /usr/bin/vmtotlsd
root	3323	0.0	0.4	12020	8064	?	Ss 07:49 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root	3384	0.0	0.0	0	0	?	S 07:49 0:00 [psimon]
root	9766	0.0	0.0	0	0	?	I< 07:57 0:00 [kworker/0:0H-kblockd]
root	9988	0.0	0.0	0	0	?	I< 08:38 0:00 [kworker/R-tls-s]
systemd+	11942	0.0	0.4	18992	9344	?	Ss 11:45 0:00 /usr/lib/systemd/systemd-networkd
root	12661	0.0	0.0	0	0	?	I< 11:46 0:00 [kworker/0:1H-kblockd]
root	19271	0.0	0.0	0	0	?	I 11:52 0:01 [kworker/0:2-events]
root	19280	0.1	0.0	0	0	?	I 11:55 0:05 [kworker/1:2-events]
root	19281	0.0	0.0	0	0	?	I< 11:55 0:00 [kworker/1:2H]
root	19285	0.0	0.0	0	0	?	I 12:00 0:00 [kworker/u256:0-events_power_efficient]

Task#06: Users and account verification (no sudo group change)

Create new user

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ sudo adduser lab4user
[sudo] password for umberqasim:
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' ...
```

Verify user entry

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ getent passwd lab4user
lab4user:x:1001:1001:::/home/lab4user:/bin/bash
```

Switch to new user

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ su - lab4user
Password:
lab4user@2023-bse-066:~$
```

Verify that sudo is not allowed

```
lab4user@2023-bse-066:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
```

Return to original user

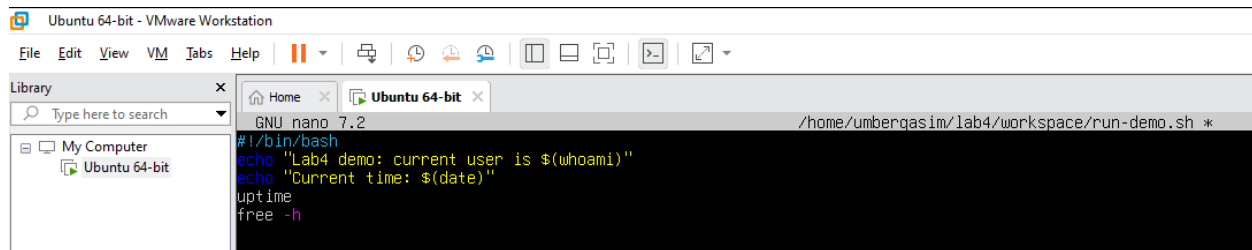
```
lab4user@2023-bse-066:~$ exit
logout
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/python_project
```

Remove test user (cleanup)

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
[sudo] password for umberqasim:
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
umberqasim@2023-bse-066:~/lab4/workspace/python_project$
```

Bonus Task#07: Create a small demo script using an editor and run it

Creating script using nano



```
#!/bin/bash
echo "Lab4 demo: current user is $(whoami)"
echo "Current time: $(date)"
uptime
free -h
```

Make script executable

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ chmod +x ~/lab4/workspace/run-demo.sh
```

Run script like a normal user

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ~/lab4/workspace/run-demo.sh
Lab4 demo: current user is umberqasim
Current time: Thu Oct 23 02:18:09 PM UTC 2025
 14:18:09 up 7:51, 2 users, load average: 0.06, 0.05, 0.00
Mem:      total    used    free   shared  buff/cache   available
Swap:      2.0Gi    780Ki    2.0Gi          1.1Gi      1.5Gi
```

Run with sudo

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ sudo ~/lab4/workspace/run-demo.sh
[sudo] password for umberqasim:
Lab4 demo: current user is root
Current time: Thu Oct 23 02:19:34 PM UTC 2025
 14:19:34 up 7:53, 2 users, load average: 0.01, 0.03, 0.00
Mem:      total    used    free   shared  buff/cache   available
Swap:      2.0Gi    780Ki    2.0Gi          1.1Gi      1.4Gi
```

Exam Evaluation Questions

I. Remote Access Verification (Cyber Login Check)

Connect remotely from your host (Windows CMD)

```
CA: umberqasim@2023-bse-066: ~
```

```
Microsoft Windows [Version 10.0.19045.6456]  
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\HP>ssh umberqasim@192.168.254.129
```

```
umberqasim@192.168.254.129'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 Thu Oct 23 02:31:42 PM UTC 2025
```

```
System load:  0.22                Processes:            221  
Usage of /:   10.5% of 47.93GB    Users logged in:     1  
Memory usage: 22%                IPv4 address for ens33: 192.168.254.129  
Swap usage:   0%
```

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

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

```
Expanded Security Maintenance for Applications is not enabled.
```

```
19 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: Fri Oct 17 05:14:13 2025 from 192.168.254.1
```

```
umberqasim@2023-bse-066:~$
```

Verify current user and home directory

```
umberqasim@2023-bse-066:~$ whoami  
umberqasim  
umberqasim@2023-bse-066:~$ pwd  
/home/umberqasim  
umberqasim@2023-bse-066:~$
```

Confirm correct host machine

```
umberqasim@2023-bse-066:~$ hostname  
2023-bse-066  
umberqasim@2023-bse-066:~$
```

II. Filesystem Inspection for Forensic Evidence

Root directory contents

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la /
total 2097244
drwxr-xr-x 23 root root      4096 Sep 30 03:05 .
drwxr-xr-x 23 root root      4096 Sep 30 03:05 ..
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 Oct 23 11:49 boot
dr-xr-xr-x  2 root root      4096 Aug  5 23:53 cdrom
drwxr-xr-x 20 root root      4120 Sep 30 11:20 dev
drwxr-xr-x 108 root root      4096 Oct 23 13:25 etc
drwxr-xr-x  3 root root      4096 Oct 23 13:25 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 30 02:57 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 281 root root         0 Sep 30 11:19 proc
drwx----- 3 root root      4096 Oct 17 04:54 root
drwxr-xr-x 31 root root     10200 Oct 23 14:31 run
lrwxrwxrwx  1 root root         8 Apr 22  2024/sbin -> usr/sbin
drwxr-xr-x  2 root root      4096 Dec 11  2024/sbin.usr-is-merged
drwxr-xr-x  2 root root      4096 Sep 30 03:12 snap
drwxr-xr-x  2 root root      4096 Aug  5 16:54 srv
-rw-----  1 root root 2147483648 Sep 30 03:05 swap.img
dr-xr-xr-x 13 root root         0 Oct 17 05:18 sys
drwxrwxrwt 16 root root      4096 Oct 23 14:00 tmp
drwxr-xr-x 12 root root      4096 Aug  5 16:54 usr
drwxr-xr-x 13 root root      4096 Sep 30 03:12 var
umberqasim@2023-bse-066:~/lab4/workspace/python_project$
```

OS version and release info

```
umberqasim@2023-bse-066:~/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
```

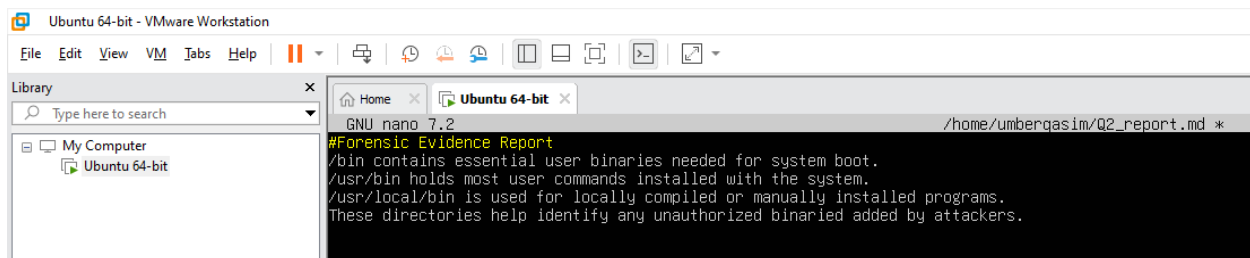
Explore important system directories

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home x Ubuntu 64-bit x
crw-rw---- 1 root tty 7, 67 Sep 30 11:20 vcsu3
crw-rw---- 1 root tty 7, 68 Sep 30 11:20 vcsu4
crw-rw---- 1 root tty 7, 69 Sep 30 11:20 vcsu5
crw-rw---- 1 root tty 7, 70 Sep 30 11:20 vcsu6
drwxr-xr-x 2 root root 10, 127 Sep 30 11:20 vga_arbiter
crw-rw---- 1 root root 10, 137 Sep 30 11:19 vhci
crw-rw---- 1 root kvm 10, 238 Oct 17 04:16 vhost-net
crw-rw---- 1 root kvm 10, 241 Oct 17 04:16 vhost-vsock
crw-rw---- 1 root root 10, 122 Sep 30 11:20 vmci
crw-rw-rw- 1 root root 10, 121 Sep 30 11:20 vsock
crw-rw-rw- 1 root root 1, 5 Sep 30 11:20 zero
crw-rw-rw- 1 root root 10, 249 Sep 30 11:19 zfs
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la /var
total 56
drwxr-xr-x 13 root root 4096 Sep 30 03:12 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..
drwxr-xr-x 2 root root 4096 Oct 19 07:09 backups
drwxr-xr-x 16 root root 4096 Sep 30 05:06 cache
drwxrwxrwt 2 root root 4096 Aug 5 17:02 crash
drwxr-xr-x 45 root root 4096 Sep 30 05:06 lib
drwxrwsr-x 2 root staff 4096 Apr 22 2024 local
lrwxrwxrwx 1 root root 9 Aug 5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 23 11:45 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 23 11:48 tmp
-rw-r--r-- 1 root root 208 Aug 5 16:54 updated
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la /tmp
total 64
drwxrwxrwt 16 root root 4096 Oct 23 14:00 .
drwxr-xr-x 23 root root 4096 Sep 30 03:05 ..
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .font-unix
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .ICE-unix
drwx----- 2 root root 4096 Sep 30 11:19 snap-private-tmp
drwx----- 3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-fwupd.service-7021QF
drwx----- 3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-ModemManager.service-7qmoT9
drwx----- 3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-polkit.service-M5032n
drwx----- 3 root root 4096 Sep 30 11:19 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-logind.service-YwgFeh
drwx----- 3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-resolved.service-qWrvZf
drwx----- 3 root root 4096 Oct 17 04:16 systemd-private-9616dc64969e4511aa4eb488044a1e34-systemd-timesyncd.service-BwRzdv
drwx----- 2 root root 4096 Oct 17 04:16 vmware-root_3320-2999004153
drwx----- 2 root root 4096 Sep 30 11:20 vmware-root_741-4248811580
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .X11-unix
drwxrwxrwt 2 root root 4096 Sep 30 11:19 .XIM-unix
umberqasim@2023-bse-066:~/lab4/workspace/python_project$
To return to your computer, press Ctrl+Alt
```

Hidden files in your home directory

```
umberqasim@2023-bse-066:~/lab4/workspace/python_project$ ls -la ~
total 48
drwxr-xr-x 6 umberqasim umberqasim 4096 Oct 23 12:05 .
drwxr-xr-x 3 root root 4096 Oct 23 13:25 ..
-rw-rw-r-- 1 umberqasim umberqasim 338 Oct 23 11:52 answers.md
-rw----- 1 umberqasim umberqasim 440 Oct 19 07:44 .bash_history
-rw-r--r-- 1 umberqasim umberqasim 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 umberqasim umberqasim 3771 Mar 31 2024 .bashrc
drwx----- 2 umberqasim umberqasim 4096 Sep 30 03:17 .cache
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 12:05 lab4
-rw----- 1 umberqasim umberqasim 20 Oct 2 12:23 .lessht
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 19 07:22 .local
-rw-r--r-- 1 umberqasim umberqasim 807 Mar 31 2024 .profile
drwx----- 2 umberqasim umberqasim 4096 Sep 30 05:47 .ssh
-rw-r--r-- 1 umberqasim umberqasim 0 Sep 30 05:14 .sudo_as_admin_successful
```

Create a file summarizing /bin, /usr/bin, and /usr/local/bin differences:



III. Evidence Handling & File Operations

Create a structured workspace

```
umberqasim@2023-bse-066:~$ mkdir -p ~/analysis/evidence/suspicious_files
```

Create text files (including one hidden)

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ ls -la
total 20
drwxrwxr-x 2 umberqasim umberqasim 4096 Oct 23 16:39 .
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 16:35 ..
-rw-rw-r-- 1 umberqasim umberqasim  22 Oct 23 16:39 .hidden_note.txt
-rw-rw-r-- 1 umberqasim umberqasim  34 Oct 23 16:38 log.txt
-rw-rw-r-- 1 umberqasim umberqasim  37 Oct 23 16:37 report.txt
```

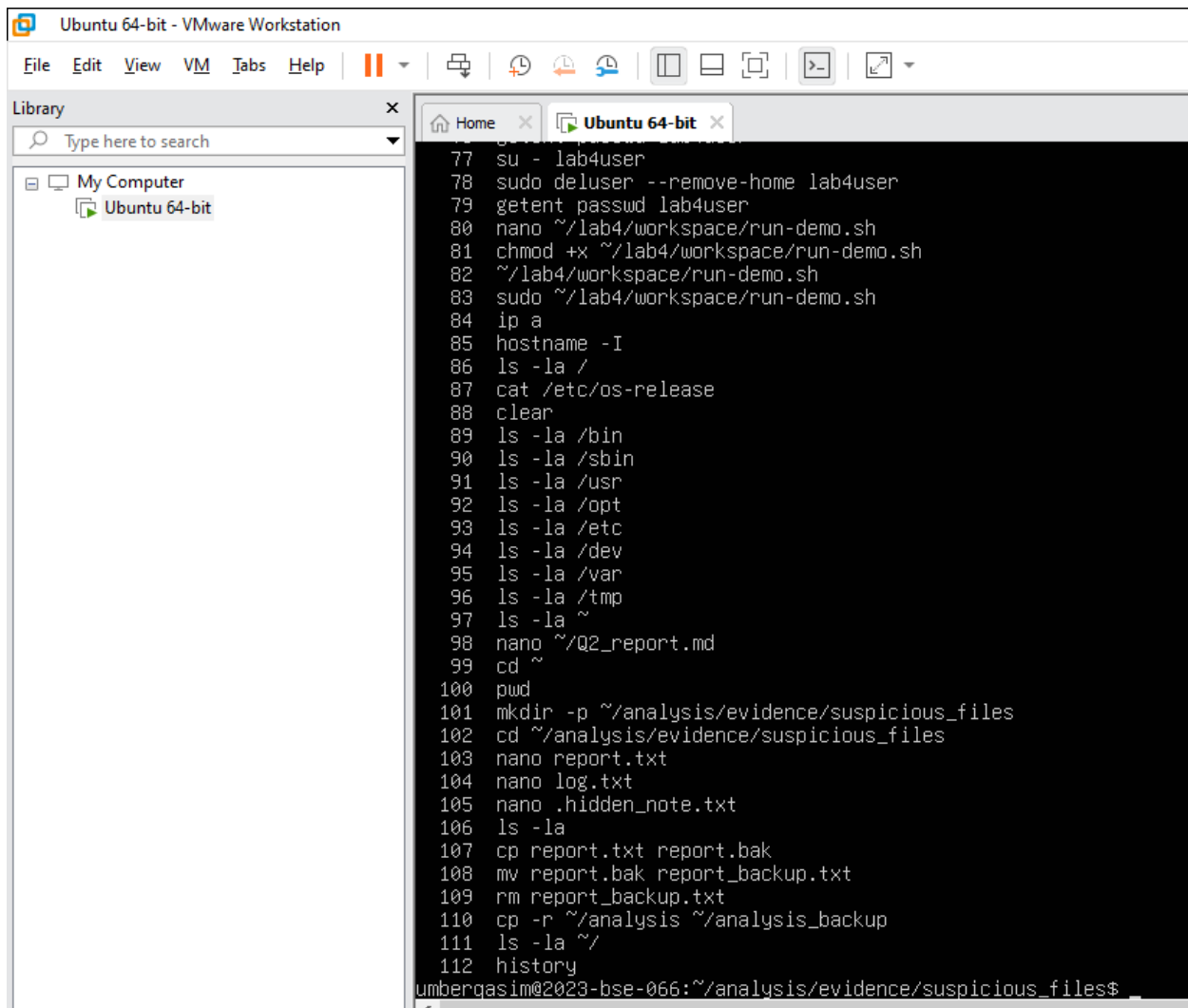
Backup, rename, delete

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ cp report.txt report.bak
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ mv report.bak report_backup.txt
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ rm report_backup.txt
```

Copy entire workspace as a backup

```
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ ls -la ~/
total 60
drwxr-x--- 8 umberqasim umberqasim 4096 Oct 23 16:43 .
drwxr-xr-x 3 root      root      4096 Oct 23 13:25 ..
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 16:35 analysis
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 16:43 analysis_backup
-rw-rw-r-- 1 umberqasim umberqasim  338 Oct 23 11:52 answers.md
-rw----- 1 umberqasim umberqasim  440 Oct 19 07:44 .bash_history
-rw-r--r-- 1 umberqasim umberqasim  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 umberqasim umberqasim 3771 Mar 31  2024 .bashrc
drwx----- 2 umberqasim umberqasim 4096 Sep 30 03:17 .cache
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 23 12:05 lab4
-rw----- 1 umberqasim umberqasim   20 Oct  2 12:23 .lessht
drwxrwxr-x 3 umberqasim umberqasim 4096 Oct 19 07:22 .local
-rw-r--r-- 1 umberqasim umberqasim  807 Mar 31  2024 .profile
-rw-rw-r-- 1 umberqasim umberqasim  303 Oct 23 16:28 Q2_report.md
drwx----- 2 umberqasim umberqasim 4096 Sep 30 05:47 .ssh
-rw-r--r-- 1 umberqasim umberqasim    0 Sep 30 05:14 .sudo_as_admin_successful
```

Show command history



```
77 su - lab4user
78 sudo deluser --remove-home lab4user
79 getent passwd lab4user
80 nano ~/lab4/workspace/run-demo.sh
81 chmod +x ~/lab4/workspace/run-demo.sh
82 ~/lab4/workspace/run-demo.sh
83 sudo ~/lab4/workspace/run-demo.sh
84 ip a
85 hostname -I
86 ls -la /
87 cat /etc/os-release
88 clear
89 ls -la /bin
90 ls -la /sbin
91 ls -la /usr
92 ls -la /opt
93 ls -la /etc
94 ls -la /dev
95 ls -la /var
96 ls -la /tmp
97 ls -la ~
98 nano ~/Q2_report.md
99 cd ~
100 pwd
101 mkdir -p ~/analysis/evidence/suspicious_files
102 cd ~/analysis/evidence/suspicious_files
103 nano report.txt
104 nano log.txt
105 nano .hidden_note.txt
106 ls -la
107 cp report.txt report.bak
108 mv report.bak report_backup.txt
109 rm report_backup.txt
110 cp -r ~/analysis ~/analysis_backup
111 ls -la ~/
112 history
umbergasim@2023-bse-066:~/analysis/evidence/suspicious_files$
```

Demonstrate auto-completion

Before tab:

```
umbergasim@2023-bse-066:~/analysis/evidence/suspicious_files$ cd ~/anal_
```

After tab:

```
umbergasim@2023-bse-066:~/analysis/evidence/suspicious_files$ cd ~/analysis
```

IV. System Profiling and Process Monitoring

Display OS and kernel version

```

umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ uname -a
Linux 2023-bse-066 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
umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ 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

```

Activate Windows

Display CPU, memory, and disk usage

```

Home x Ubuntu 64-bit x
microcode      : 0x27
cpu MHz        : 2594.006
cache size     : 3072 KB
physical id    : 2
siblings       : 1
core id        : 0
cpu cores      : 1
apicid         : 2
initial apicid : 2
fpu            : yes
fpu_exception  : yes
cpuid level    : 13
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 pdcm
arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic mov
r aes xsave avx f16c rdrand hypervisor lahf_lm abm pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid xsaveopt
h_capabilities
bugs           : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_unknow retbleed bhi
bogomips       : 5188.01
clflush size   : 64
cache_alignmen : 64
address sizes  : 45 bits physical, 48 bits virtual
power managemen:

umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ free -h
              total        used        free      shared  buff/cache   available
Mem:           1.9Gi       445Mi       531Mi        932Ki        1.1Gi        1.4Gi
Swap:          2.0Gi        780Ki        2.0Gi

umberqasim@2023-bse-066:~/analysis/evidence/suspicious_files$ df -h
Filesystem                Size      Used Avail Use% Mounted on
tmpfs                     192M        1.3M  191M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 48G       5.1G   41G  12% /
tmpfs                     960M         0  960M   0% /dev/shm
tmpfs                     5.0M         0   5.0M   0% /run/lock
/dev/sda2                  2.0G      192M   1.6G  11% /boot
tmpfs                     192M        12K  192M   1% /run/user/1000

```

Activate Windows

Display all active processes

```
Home x Ubuntu 64-bit x
1 root      20  0  22204 13440 9600 S  0.0  0.7  0:15.38 systemd
2 root      20  0  0 0 0 S  0.0  0.0  0:00.45 kthreadd
3 root      20  0  0 0 0 S  0.0  0.0  0:00.00 pool_workqueue_release
4 root      0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-rcu_g
5 root      0 -20 0 0 0 I  0.0  0.0  0:00.01 kworker/R-rcu_p
6 root      0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-slub_
7 root      0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-netns
12 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-mm_pe
13 root     20  0  0 0 0 I  0.0  0.0  0:00.00 rcu_tasks_kthread
14 root     20  0  0 0 0 I  0.0  0.0  0:00.00 rcu_tasks_rude_kthread
15 root     20  0  0 0 0 I  0.0  0.0  0:00.00 rcu_tasks_trace_kthread
16 root     20  0  0 0 0 S  0.0  0.0  0:01.25 ksoftirqd/0
17 root     20  0  0 0 0 I  0.0  0.0  0:11.28 rcu_preempt
18 root     rt  0  0 0 0 S  0.0  0.0  0:00.48 migration/0
19 root     -51 0  0 0 0 S  0.0  0.0  0:00.00 idle_inject/0
20 root     20  0  0 0 0 S  0.0  0.0  0:00.00 cpuhp/0
21 root     20  0  0 0 0 S  0.0  0.0  0:00.00 cpuhp/1
22 root     -51 0  0 0 0 S  0.0  0.0  0:00.00 idle_inject/1
23 root     rt  0  0 0 0 S  0.0  0.0  0:00.99 migration/1
24 root     20  0  0 0 0 S  0.0  0.0  0:01.38 ksoftirqd/1
29 root     20  0  0 0 0 S  0.0  0.0  0:00.00 kdevtmpfs
30 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-inet_
31 root     20  0  0 0 0 S  0.0  0.0  0:00.04 kauditd
33 root     20  0  0 0 0 S  0.0  0.0  0:00.16 khungtaskd
34 root     20  0  0 0 0 S  0.0  0.0  0:00.00 oom_reaper
36 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-write
38 root     20  0  0 0 0 S  0.0  0.0  0:08.92 kcompactd0
39 root     25  5  0 0 0 S  0.0  0.0  0:00.00 ksmd
42 root     39 19 0 0 0 S  0.0  0.0  0:00.00 khugepaged
43 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-kinte
44 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-kbloc
45 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-blkcg
46 root     -51 0  0 0 0 S  0.0  0.0  0:00.00 irq/9-acpi
47 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-tpm_d
48 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-ata_s
49 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-md
50 root     0 -20 0 0 0 I  0.0  0.0  0:00.00 kworker/R-md_bi

Activate Windows
Go to Settings to activate Windows
```

V. User Account Audit & Privilege Escalation Simulation

Create a new test user

```
umberqasim@2023-bse-066:~$ sudo adduser lab4user
[sudo] password for umberqasim:
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' ...
```

Verify user record in system database

```
umberqasim@2023-bse-066:~$ grep 'lab4user' /etc/passwd
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
```

Log in as lab4user

```
umberqasim@2023-bse-066:~$ su - lab4user
Password:
lab4user@2023-bse-066:~$
```

Try an administrative command

```
lab4user@2023-bse-066:~$ sudo apt update
[sudo] password for lab4user:
lab4user is not in the sudoers file.
```

Switch back to your main analyst account

```
lab4user@2023-bse-066:~$ exit
logout
umberqasim@2023-bse-066:~$
```

Inspect authentication logs

```
umberqasim@2023-bse-066:~$ sudo grep lab4user /var/log/auth.log
2025-10-26T11:06:17.364898+00:00 2023-bse-066 sudo: umberqasim : TTY=pts/0 ; PWD=/home/umberqasim ; USER=root ; COMMAND=/usr/sbin/add
2025-10-26T11:06:17.742893+00:00 2023-bse-066 groupadd[21389]: group added to /etc/group: name=lab4user, GID=1001
2025-10-26T11:06:17.746351+00:00 2023-bse-066 groupadd[21389]: group added to /etc/gshadow: name=lab4user
2025-10-26T11:06:17.749525+00:00 2023-bse-066 groupadd[21389]: new group: name=lab4user, GID=1001
2025-10-26T11:06:17.798384+00:00 2023-bse-066 useradd[21396]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell
2025-10-26T11:07:07.062546+00:00 2023-bse-066 passwd[21409]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-26T11:07:10.060256+00:00 2023-bse-066 chfn[21412]: changed user 'lab4user' information
2025-10-26T11:07:12.219421+00:00 2023-bse-066 gpasswd[21420]: members of group users set by root to lab4user
2025-10-26T11:11:38.430645+00:00 2023-bse-066 su[21436]: (to lab4user) umberqasim on pts/0
2025-10-26T11:11:38.432731+00:00 2023-bse-066 su[21436]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by umberq
2025-10-26T11:13:16.668859+00:00 2023-bse-066 sudo: lab4user : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/lab4user ; USER=root ; COM
2025-10-26T11:14:07.893328+00:00 2023-bse-066 su[21436]: pam_unix(su-l:session): session closed for user lab4user
2025-10-26T11:16:35.144431+00:00 2023-bse-066 sudo: umberqasim : TTY=pts/0 ; PWD=/home/umberqasim ; USER=root ; COMMAND=/usr/bin/grep
```

Remove the test user

```
umberqasim@2023-bse-066:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user 'lab4user' ...
umberqasim@2023-bse-066:~$ grep 'lab4user' /etc/passwd
```