



CLOUD COMPUTING

LAB:4

Submitted By:

Seerat Fatima

Registration.no:

2023-BSE-060

Submitted To:


Engr. Shoaib

Secton:

5B









Task 1 – Verify VM resources in VMware

Ubuntu 64-bit

 [Power on this virtual machine](#)

 [Edit virtual machine settings](#)

▼ Devices

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

▼ Description

Type here to enter a description of this virtual machine.

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

```

PS C:\Users\Waseem> ssh serat060@192.168.243.128
The authenticity of host '192.168.243.128 (192.168.243.128)' can't be established.
ED25519 key fingerprint is SHA256:tuTtXbv4M223qLA3Ua6ofkfC3kK4KGWls9Zx94jBL/w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (C:\\Users\\Waseem\\.ssh\\known_hosts).
serat060@192.168.243.128's password:
hostfile_replace_entries: mkstemp: Permission denied
update_known_hosts: hostfile_replace_entries failed for C:\\Users\\Waseem\\.ssh\\known_hosts: Permission denied
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

System information as of Fri Oct 17 04:49:01 AM UTC 2025

System load:  0.14           Processes:           213
Usage of /:   25.8% of 9.75GB Users logged in:      1
Memory usage: 7%           IPv4 address for ens33: 192.168.243.128
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: Thu Oct 2 04:17:19 2025 from 192.168.243.1
serat060@ubuntu60: $

```

The screenshot shows a VMware Workstation window titled "Ubuntu 64-bit - VMware Workstation". The main window displays the terminal output from the previous block. The host window shows the VM's file system structure, including the "My Computer" view and the "Ubuntu 64-bit" view. The terminal output shows the system information, security updates, and network configuration. The host window shows the VM's file system structure, including the "My Computer" view and the "Ubuntu 64-bit" view.

```

File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu 64-bit
System load: 0.36 Processes: 243
Usage of /: 25.7% of 9.75GB Users logged in: 0
Memory usage: 7% IPv4 address for ens33: 192.168.243.128
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

serat060@ubuntu60:~$ ip a
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: <BR0ADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:1f:2e:ce brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.243.128/24 metric 100 brd 192.168.243.255 scope global dynamic ens33
        valid_lft 1570sec preferred_lft 1570sec
    inet6 fe80::20c:29ff:fe1f:2ece/64 scope link
        valid_lft forever preferred_lft forever
serat060@ubuntu60:~$ whoami
serat060
serat060@ubuntu60:~$ pwd
/home/serat060
serat060@ubuntu60:~$

```

To direct input to this VM, click inside or press Ctrl-G.

Windows taskbar at the bottom shows the time as 9:51 AM on 10/17/2025.

Task 3 – Filesystem exploration — root tree and dotfiles

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu 64-bit
serat060@ubuntu60:~$ whoami
serat060
serat060@ubuntu60:~$ pwd
/home/serat060
serat060@ubuntu60:~$ ls -la /
ls: invalid option -- '/'
Try 'ls --help' for more information.
serat060@ubuntu60:~$ ls -la /
total 88
drwxr-xr-x 23 root root 4096 Sep 30 16:13 .
drwxr-xr-x 23 root root 4096 Sep 30 16:13 ..
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 30 16:38 boot
dr-xr-xr-x 2 root root 4096 Aug 5 23:53 cdrom
drwxr-xr-x 20 root root 4120 Oct 17 04:42 dev
drwxr-xr-x 108 root root 4096 Sep 30 18:16 etc
drwxr-xr-x 3 root root 4096 Sep 30 18:16 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 16:20 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 opt
dr-xr-xr-x 277 root root 0 Oct 17 04:41 proc
drwx----- 3 root root 4096 Aug 5 17:02 root
drwxr-xr-x 28 root root 860 Oct 17 04:52 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 18:16 snap
drwxr-xr-x 2 root root 4096 Aug 5 16:54 srv
dr-xr-xr-x 13 root root 0 Oct 17 04:41 sys
drwxrwxrwt 13 root root 4096 Oct 17 04:42 tmp
drwxr-xr-x 12 root root 4096 Aug 5 16:54 usr
drwxr-xr-x 13 root root 4096 Sep 30 18:16 var
serat060@ubuntu60:~$
```

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu 64-bit
drwxr-xr-x 2 root root 4096 Sep 30 18:50 snap
dr-xr-xr-x 2 root root 4096 Aug 5 23:53 cdrom
drwxr-xr-x 20 root root 4120 Oct 17 04:42 dev
drwxr-xr-x 108 root root 4096 Sep 30 18:16 etc
drwxr-xr-x 3 root root 4096 Sep 30 18:16 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 16:20 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 opt
dr-xr-xr-x 277 root root 0 Oct 17 04:41 proc
drwx----- 3 root root 4096 Aug 5 17:02 root
drwxr-xr-x 28 root root 860 Oct 17 04:52 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 18:16 snap
drwxr-xr-x 2 root root 4096 Aug 5 16:54 srv
dr-xr-xr-x 13 root root 0 Oct 17 04:41 sys
drwxrwxrwt 13 root root 4096 Oct 17 04:42 tmp
drwxr-xr-x 12 root root 4096 Aug 5 16:54 usr
drwxr-xr-x 13 root root 4096 Sep 30 18:16 var
serat060@ubuntu60:~$ 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
serat060@ubuntu60:~$
```

```
LOGO=ubuntu-logo
serat060@ubuntu60:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22 2024 /bin -> usr/bin
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22 2024 /sbin -> usr/sbin
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ ls -la /usr
total 88
drwxr-xr-x 12 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 30 16:13 ..
drwxr-xr-x  2 root root 28672 Sep 30 16:44 bin
drwxr-xr-x  2 root root 4096 Apr 22  2024 games
drwxr-xr-x 33 root root 4096 Sep 30 16:36 include
drwxr-xr-x 78 root root 4096 Sep 30 16:44 lib
drwxr-xr-x  2 root root 4096 Aug  5 17:01 lib64
drwxr-xr-x 11 root root 4096 Sep 30 16:37 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x  2 root root 20480 Sep 30 16:51 sbin
drwxr-xr-x 124 root root 4096 Sep 30 16:44 share
drwxr-xr-x  4 root root 4096 Sep 30 16:37 src
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ 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 16:13 ..
serat060@ubuntu60:~$
```

```

drwxr-xr-x  2 root root      4096 Aug  5 17:14 sensors.d
-rw-r--r--  1 root root    12813 Mar 27 2021 services
drwxr-xr-x  2 root root      4096 Aug  5 17:02 sgml
-rw-r-----  1 root shadow    970 Sep 30 18:16 shadow
-rw-r-----  1 root shadow    970 Sep 30 18:16 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 30 18:16 ssh
drwxr-xr-x  4 root root      4096 Aug  5 17:02 ssl
-rw-r--r--  1 root root        22 Sep 30 18:16 subgid
-rw-r--r--  1 root root         0 Aug  5 16:54 subgid-
-rw-r--r--  1 root root        22 Sep 30 18:16 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 30 16:37 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 30 16:37 UPower

```

```

crw-rw---- 1 root dialout 4, 91 Oct 17 04:42 ttyS27
crw-rw---- 1 root dialout 4, 92 Oct 17 04:42 ttyS28
crw-rw---- 1 root dialout 4, 93 Oct 17 04:42 ttyS29
crw-rw---- 1 root dialout 4, 67 Oct 17 04:42 ttyS3
crw-rw---- 1 root dialout 4, 94 Oct 17 04:42 ttyS30
crw-rw---- 1 root dialout 4, 95 Oct 17 04:42 ttyS31
crw-rw---- 1 root dialout 4, 68 Oct 17 04:42 ttyS4
crw-rw---- 1 root dialout 4, 69 Oct 17 04:42 ttyS5
crw-rw---- 1 root dialout 4, 70 Oct 17 04:42 ttyS6
crw-rw---- 1 root dialout 4, 71 Oct 17 04:42 ttyS7
crw-rw---- 1 root dialout 4, 72 Oct 17 04:42 ttyS8
crw-rw---- 1 root dialout 4, 73 Oct 17 04:42 ttyS9
drwxr-xr-x 2 root root 60 Oct 17 04:41 ubuntu-vg
crw-rw---- 1 root kvm 10, 124 Oct 17 04:42 udmabuf
crw----- 1 root root 10, 239 Oct 17 04:42 uhid
crw----- 1 root root 10, 223 Oct 17 04:42 uinput
crw-rw-rw- 1 root root 1, 9 Oct 17 04:42 urandom
crw----- 1 root root 10, 126 Oct 17 04:42 userfaultfd
crw----- 1 root root 10, 240 Oct 17 04:42 userio
crw-rw---- 1 root tty 7, 0 Oct 17 04:42 vcs
crw-rw---- 1 root tty 7, 1 Oct 17 04:42 vcs1
crw-rw---- 1 root tty 7, 2 Oct 17 04:42 vcs2
crw-rw---- 1 root tty 7, 3 Oct 17 04:42 vcs3
crw-rw---- 1 root tty 7, 4 Oct 17 04:42 vcs4
crw-rw---- 1 root tty 7, 5 Oct 17 04:42 vcs5
crw-rw---- 1 root tty 7, 6 Oct 17 04:42 vcs6
crw-rw---- 1 root tty 7, 128 Oct 17 04:42 vcsa
crw-rw---- 1 root tty 7, 129 Oct 17 04:42 vcsa1
crw-rw---- 1 root tty 7, 130 Oct 17 04:42 vcsa2
crw-rw---- 1 root tty 7, 131 Oct 17 04:42 vcsa3
crw-rw---- 1 root tty 7, 132 Oct 17 04:42 vcsa4
crw-rw---- 1 root tty 7, 133 Oct 17 04:42 vcsa5
crw-rw---- 1 root tty 7, 134 Oct 17 04:42 vcsa6
crw-rw---- 1 root tty 7, 64 Oct 17 04:42 vcsu
crw-rw---- 1 root tty 7, 65 Oct 17 04:42 vcsu1
crw-rw---- 1 root tty 7, 66 Oct 17 04:42 vcsu2

```

```

serat060@ubuntu60:~$ ls -la /var
total 56
drwxr-xr-x 13 root root  4096 Sep 30 18:16 .
drwxr-xr-x 23 root root  4096 Sep 30 16:13 ..
drwxr-xr-x  2 root root  4096 Oct  2 04:28 backups
drwxr-xr-x 14 root root  4096 Sep 30 18:19 cache
drwxrwsrwt  2 root root  4096 Aug  5 17:02 crash
drwxr-xr-x 44 root root  4096 Sep 30 18:16 lib
drwxrwsr-x  2 root staff 4096 Apr 22 2024 local
lrwxrwxrwx  1 root root    9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 17 04:42 log
drwxrwsr-x  2 root mail  4096 Aug  5 16:54 mail
drwxr-xr-x  2 root root  4096 Aug  5 16:54 opt
lrwxrwxrwx  1 root root    4 Aug  5 16:54 run -> /run
drwxr-xr-x  2 root root  4096 May 21 15:46 snap
drwxr-xr-x  4 root root  4096 Aug  5 17:14 spool
drwxrwxrwt  7 root root  4096 Oct 17 04:42 tmp
-rw-r--r--  1 root root 208 Aug  5 16:54 .updated
serat060@ubuntu60:~$

```

```

serat060@ubuntu60:~$ ls -la /tmp
total 52
drwxrwxrwt 13 root root 4096 Oct 17 04:42 .
drwxr-xr-x 23 root root 4096 Sep 30 16:13 ..
drwxrwxrwt  2 root root 4096 Oct 17 04:42 .font-unix
drwxrwxrwt  2 root root 4096 Oct 17 04:42 .ICE-unix
drwx----- 2 root root 4096 Oct 17 04:42 snap-private-tmp
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-ModemManager.service-17bSUL
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-polkit.service-V1c0Sh
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-systemd-logind.service-zZ1wC2
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-systemd-resolved.service-Pty7Fg
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-systemd-timesyncd.service-2dq9Cz
drwx----- 2 root root 4096 Oct 17 04:42 vmware-root_746-2965906923
drwxrwxrwt  2 root root 4096 Oct 17 04:42 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 17 04:42 .XIM-unix
serat060@ubuntu60:~$

```

```

serat060@ubuntu60:~$ ls -la ~
total 28
drwxr-x--- 4 serat060 serat060 4096 Sep 30 18:21 .
drwxr-xr-x 3 root      root      4096 Sep 30 18:16 ..
-rw-r--r-- 1 serat060 serat060 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 serat060 serat060 3771 Mar 31 2024 .bashrc
drwx----- 2 serat060 serat060 4096 Sep 30 18:19 .cache
-rw-r--r-- 1 serat060 serat060 807 Mar 31 2024 .profile
drwx----- 2 serat060 serat060 4096 Sep 30 18:17 .ssh
-rw-r--r-- 1 serat060 serat060  0 Sep 30 18:21 .sudo_as_admin_successful
serat060@ubuntu60:~$

```

```

/bin:essential system boundaries used by all users
/usr/bin: standard binaries fr norml users
/usr/local/bin: custom or locally bined binaries

```

Task 4 – Essential CLI tasks — navigation and file operations


```
serat060@ubuntu60:~$ mkdir -p ~/Lab4/workspace/python_project
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ pwd
/home/serat060
serat060@ubuntu60:~$
```

```
GNU nano 7.2
lab4 README
```

```
GNU nano 7.2
print("Hello Lab4")
```

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

```
serat060@ubuntu60:~$ ls -la
total 52
drwxr-x--- 6 serat060 serat060 4096 Oct 17 05:23 .
drwxr-xr-x 3 root      root      4096 Sep 30 18:16 ..
-rw-rw-r-- 1 serat060 serat060  142 Oct 17 05:12 answers.md
-rw-r--r-- 1 serat060 serat060  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 serat060 serat060 3771 Mar 31  2024 .bashrc
drwx----- 2 serat060 serat060 4096 Sep 30 18:19 .cache
-rw-rw-r-- 1 serat060 serat060    9 Oct 17 05:23 .env
drwxrwxr-x 3 serat060 serat060 4096 Oct 17 05:17 Lab4
drwxrwxr-x 3 serat060 serat060 4096 Oct 17 05:07 .local
-rw-rw-r-- 1 serat060 serat060   20 Oct 17 05:22 main.py
-rw-r--r-- 1 serat060 serat060  807 Mar 31  2024 .profile
-rw-rw-r-- 1 serat060 serat060   12 Oct 17 05:19 README.md
drwx----- 2 serat060 serat060 4096 Sep 30 18:17 .ssh
-rw-r--r-- 1 serat060 serat060    0 Sep 30 18:21 .sudo_as_admin_successful
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ cp README.md README.copy.md
```

```
serat060@ubuntu60:~$ mv README.copy.md README.dev.md
serat060@ubuntu60:~$ rm
```

```
serat060@ubuntu60:~$ rm README.dev.md
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ rm README.dev.md
serat060@ubuntu60:~$ mkdir -p ~/Lab4/workspace/java_app
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ mkdir -p ~/Lab4/workspace/java_app
serat060@ubuntu60:~$ cp -r ~/Lab4/workspace/python_project ~/Lab4/workspace/java_app_copy
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ ls -la ~/Lab4/workspace
total 20
drwxrwxr-x 5 serat060 serat060 4096 Oct 17 05:36 .
drwxrwxr-x 3 serat060 serat060 4096 Oct 17 05:17 ..
drwxrwxr-x 2 serat060 serat060 4096 Oct 17 05:35 java_app
drwxrwxr-x 2 serat060 serat060 4096 Oct 17 05:36 java_app_copy
drwxrwxr-x 2 serat060 serat060 4096 Oct 17 05:17 python_project
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ history
1  ip a
2  whoami
3  pwd
4  ls -la/
5  ls -la /
6  cat /etc/os-release
7  ls -la /bin
8  ls -la /sbin
9  ls -la /usr
10 ls -la /opt
11 ls -la /etc
12 ls -la /dev
13 ls -la /var
14 ls -la /tmp
15 ls -la ~
16 nano ~/answers.md
17 mkdir -p ~/Lab4/workspace/python_project
18 pwd
19 nano README.md
20 nano main.py
21 nano .env
22 ls -la
23 cp README.md README.copy.md
24 rm README.dev.md
25 mv README.copy.md README.dev.md
26 rm README.dev.md
27 mkdir -p ~/Lab4/workspace/java_app
28 cp -r ~/Lab4/workspace/python_project ~/Lab4/workspace/java_app_copy
29 ls -la ~/Lab4/workspace
30 history
serat060@ubuntu60:~$
```

Task 5 – System info, resources & processes

```
serat060@ubuntu60:~$ history
30 history
serat060@ubuntu60:~$ uname -a
Linux ubuntu60 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
serat060@ubuntu60:~$
```

```

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 rdtsc
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_c
h_capabilities
bugs        : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_unknown retbleed bhi
bogomips    : 4988.45
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       : 69
model_name  : Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz
stepping    : 1
microcode   : 0x26
cpu_MHz     : 2494.229
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

```

```

serat060@ubuntu60:~$ free -h
              total        used        free      shared  buff/cache   available
Mem:          3.8Gi         492Mi        3.2Gi         1.5Mi         334Mi        3.3Gi
Swap:          0B           0B           0B
serat060@ubuntu60:~$

```

```

serat060@ubuntu60:~$ free -h
              total        used        free      shared  buff/cache   available
Mem:          3.8Gi         492Mi        3.2Gi         1.5Mi         334Mi        3.3Gi
Swap:          0B           0B           0B
serat060@ubuntu60:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            387M  1.5M  386M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 9.8G  2.6G  6.8G  28% /
tmpfs            1.9G   0    1.9G   0% /dev/shm
tmpfs            5.0M   0    5.0M   0% /run/lock
/dev/sda2        1.8G 100M  1.6G   7% /boot
tmpfs            387M  12K  387M   1% /run/user/1000
serat060@ubuntu60:~$

```

```

serat060@ubuntu60:~$ 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
serat060@ubuntu60:~$

```

```

root      599  0.0  0.0      0      0 ?      I<   04:42  0:00 [kworker/R-ext4-]
systemd+  626  0.0  0.2  19008  9472 ?      Ss   04:42  0:01 /usr/lib/systemd/systemd-networkd
systemd+  632  0.0  0.3  21508  12928 ?     Ss   04:42  0:01 /usr/lib/systemd/systemd-resolved
systemd+  633  0.0  0.1  91024  7680 ?      Ssl  04:42  0:00 /usr/lib/systemd/systemd-timesyncd
root      690  0.0  0.0      0      0 ?      I<   04:42  0:00 [kworker/R-cfg80]
root      745  0.0  0.3  53464  12032 ?     Ss   04:42  0:00 /usr/bin/VGAuthService
root      746  0.3  0.2  315880  9472 ?     Ssl  04:42  0:15 /usr/bin/vmtoolsd
root      747  0.0  0.0      0      0 ?      S    04:42  0:00 [irq/57-vmw_vmc]
root      748  0.0  0.0      0      0 ?      S    04:42  0:00 [irq/58-vmw_vmc]
root      749  0.0  0.0      0      0 ?      S    04:42  0:00 [irq/59-vmw_vmc]
root      762  0.0  0.0      0      0 ?      S    04:42  0:00 [irq/16-vmwgfx]
root      763  0.0  0.0      0      0 ?      I<   04:42  0:00 [kworker/R-ttm]
message+  816  0.0  0.1   9796  5504 ?      Ss   04:42  0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-
polkitd   824  0.0  0.1  308164  7808 ?     Ssl  04:42  0:00 /usr/lib/polkit-1/polkitd --no-debug
root      832  0.0  0.2  18144  8704 ?      Ss   04:42  0:00 /usr/lib/systemd/systemd-logind
root      833  0.0  0.3  468952  13440 ?     Ssl  04:42  0:00 /usr/libexec/udisks2/udisksd
root      858  0.0  0.0   6824  2688 ?      Ss   04:42  0:00 /usr/sbin/cron -f -P
root      871  0.0  0.5  109660  22912 ?     Ssl  04:42  0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutd
root     1083  0.0  0.3  318360  12800 ?     Ssl  04:42  0:00 /usr/sbin/ModemManager
syslog    1180  0.0  0.1  222508  5760 ?      Ssl  04:42  0:00 /usr/sbin/rsyslogd -n -iNONE
root     1286  0.0  0.0      0      0 ?      I<   04:42  0:00 [kworker/0:2H]
root     1316  0.0  0.1   6948  4608 tty1    Ss   04:43  0:00 /bin/login -p --
root     1421  0.0  0.0      0      0 ?      S    04:45  0:00 [psimon]
serat060  1423  0.0  0.2  20264  11264 ?     Ss   04:45  0:00 /usr/lib/systemd/systemd --user
serat060  1425  0.0  0.0  21148  3516 ?      S    04:45  0:00 (sd-pam)
serat060  1434  0.0  0.1   8652  5504 tty1    S    04:45  0:00 -bash
root     1480  0.0  0.0      0      0 ?      I<   04:45  0:00 [kworker/R-tls-s]
root     1490  0.0  0.2  12020  7936 ?      Ss   04:48  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root     1491  0.0  0.2  14964  10624 ?     Ss   04:48  0:00 sshd: serat060 [priv]
serat060  1549  0.0  0.1  14964  6848 ?      S    04:49  0:00 sshd: serat060@pts/0
serat060  1550  0.0  0.1   8648  5376 pts/0    Ss+  04:49  0:00 -bash
root     1743  0.3  1.0  594284  43372 ?     Ssl  05:18  0:06 /usr/libexec/fwupd/fwupd
root     1750  0.0  0.2  314000  8832 ?      Ssl  05:18  0:00 /usr/libexec/upowerd
root     1773  0.0  0.0   81380  2872 ?      Ss   05:18  0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket --daemon
root     1792  1.5  0.0      0      0 ?      I    05:20  0:31 [kworker/1:0-events]
root     1804  0.0  0.0      0      0 ?      I    05:26  0:00 [kworker/u257:3-events_power_efficient]
root     1806  1.4  0.0      0      0 ?      I    05:26  0:24 [kworker/0:3-events]

```

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

```
serat060@ubuntu60:~$ sudo adduser lab4user
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
info: Creating home directory `/home/lab4user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lab4user
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
info: Adding new user `lab4user' to supplemental / extra groups `users'
info: Adding user `lab4user' to group `users' ...
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ getent passwd lab4user
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
serat060@ubuntu60:~$
```

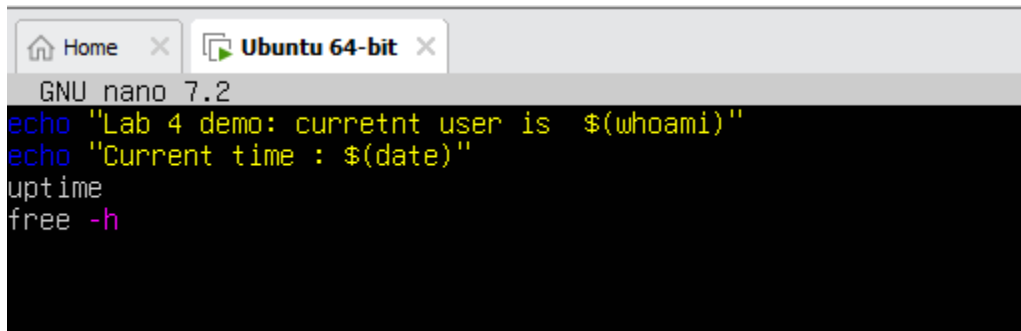
```
serat060@ubuntu60:~$ su - lab4user
Password:
lab4user@ubuntu60:~$
```

```
lab4user@ubuntu60:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu60:~$
```

```
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
serat060@ubuntu60:~$ _
```

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



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

```
serat060@ubuntu60:~$ chmod +x ~/lab4/workspace/run-demo.sh
```

```
serat060@ubuntu60:~$ ~/lab4/workspace/run-demo.sh
Lab4 demo: Current user is serat060
Current time : Thu Oct 23 06:14:14 PM UTC 2025
18:14:14 up 2:06, 2 users, load average: 0.09, 0.08, 0.03
Mem:          total        used        free      shared  buff/cache   available
Swap:          0B           0B           0B
serat060@ubuntu60:~$
```

```
serat060@ubuntu60:~$ sudo ~/lab4/workspace/run-demo.sh
[sudo] password for serat060:
Lab4 demo: Current user is root
Current time : Thu Oct 23 06:16:05 PM UTC 2025
18:16:05 up 2:08, 2 users, load average: 0.08, 0.06, 0.02
Mem:          total        used        free      shared  buff/cache   available
Swap:          0B           0B           0B
serat060@ubuntu60:~$
```

EXAM EVALUATION QUESTIONS:

1. Remote Access Verification (Cyber Login Check)

```

PS C:\Users\Waseem> ssh serat060@192.168.243.128
The authenticity of host '192.168.243.128 (192.168.243.128)' can't be established.
ED25519 key fingerprint is SHA256:tuTtXbv4M223qLA3Ua6ofkfC3kK4KGWls9Zx94j8L/w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (C:\\Users\\Waseem/.ssh/known_hosts).
serat060@192.168.243.128's password:
hostfile_replace_entries: mkstemp: Permission denied
update_known_hosts: hostfile_replace_entries failed for C:\\Users\\Waseem/.ssh/known_hosts: Permission denied
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

System information as of Thu Oct 23 06:20:52 PM UTC 2025

System load:  0.12           Processes:            223
Usage of /:   26.0% of 9.75GB Users logged in:        1
Memory usage: 8%           IPv4 address for ens33: 192.168.243.128
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: Fri Oct 17 04:49:02 2025 from 192.168.243.1
serat060@ubuntu60: $

```

```

serat060@ubuntu60:~$ whoami
serat060
serat060@ubuntu60:~$ pwd
/home/serat060
serat060@ubuntu60:~$

```

```

/home/serat060
serat060@ubuntu60:~$ hostname
ubuntu60
serat060@ubuntu60:~$ uname -a
Linux ubuntu60 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
serat060@ubuntu60:~$

```

2. Filesystem Inspection for Forensic Evidence

```
serat060@ubuntu60:~$ ls -la /
total 88
drwxr-xr-x 23 root root 4096 Sep 30 16:13 .
drwxr-xr-x 23 root root 4096 Sep 30 16:13 ..
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 30 16:38 boot
dr-xr-xr-x 2 root root 4096 Aug 5 23:53 cdrom
drwxr-xr-x 20 root root 4120 Oct 17 04:42 dev
drwxr-xr-x 108 root root 4096 Oct 17 06:15 etc
drwxr-xr-x 3 root root 4096 Oct 17 06:15 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 16:20 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 285 root root 0 Oct 17 04:41 proc
drwx----- 3 root root 4096 Aug 5 17:02 root
drwxr-xr-x 29 root root 900 Oct 23 18:20 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 18:16 snap
drwxr-xr-x 2 root root 4096 Aug 5 16:54 srv
dr-xr-xr-x 13 root root 0 Oct 17 04:54 sys
drwxrwxrwt 15 root root 4096 Oct 23 18:04 tmp
drwxr-xr-x 12 root root 4096 Aug 5 16:54 usr
drwxr-xr-x 13 root root 4096 Sep 30 18:16 var
```

```
serat060@ubuntu60:~$ 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
```



```
serat060@ubuntu60:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> usr/bin
serat060@ubuntu60:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
serat060@ubuntu60:~$ ls -la /usr
total 88
drwxr-xr-x 12 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Sep 30 16:13 ..
drwxr-xr-x  2 root root 28672 Sep 30 16:44 bin
drwxr-xr-x  2 root root 4096 Apr 22  2024 games
drwxr-xr-x 33 root root 4096 Sep 30 16:36 include
drwxr-xr-x 78 root root 4096 Sep 30 16:44 lib
drwxr-xr-x  2 root root 4096 Aug  5 17:01 lib64
drwxr-xr-x 11 root root 4096 Sep 30 16:37 libexec
drwxr-xr-x 10 root root 4096 Aug  5 16:54 local
drwxr-xr-x  2 root root 20480 Sep 30 16:51 sbin
drwxr-xr-x 124 root root 4096 Sep 30 16:44 share
drwxr-xr-x  4 root root 4096 Sep 30 16:37 src
serat060@ubuntu60:~$ 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 16:13 ..
```

```

-rw-r--r-- 1 root root      44 Oct 17 06:00 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 30 16:37 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 30 16:37 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
serat060@ubuntu60:~$

```

```

crw-rw----  1 root    kvm      10, 124 Oct 17 04:42 udmabuf
crw-----  1 root    root      10, 239 Oct 17 04:42 uhid
crw-----  1 root    root      10, 223 Oct 17 04:42 uinput
crw-rw-rw-  1 root    root        1,   9 Oct 17 04:42 urandom
crw-----  1 root    root      10, 126 Oct 17 04:42 userfaultfd
crw-----  1 root    root      10, 240 Oct 17 04:42 userio
crw-rw----  1 root    tty       7,   0 Oct 17 04:42 vcs
crw-rw----  1 root    tty       7,   1 Oct 17 04:42 vcs1
crw-rw----  1 root    tty       7,   2 Oct 17 04:42 vcs2
crw-rw----  1 root    tty       7,   3 Oct 17 04:42 vcs3
crw-rw----  1 root    tty       7,   4 Oct 17 04:42 vcs4
crw-rw----  1 root    tty       7,   5 Oct 17 04:42 vcs5
crw-rw----  1 root    tty       7,   6 Oct 17 04:42 vcs6
crw-rw----  1 root    tty       7, 128 Oct 17 04:42 vcsa
crw-rw----  1 root    tty       7, 129 Oct 17 04:42 vcsa1
crw-rw----  1 root    tty       7, 130 Oct 17 04:42 vcsa2
crw-rw----  1 root    tty       7, 131 Oct 17 04:42 vcsa3
crw-rw----  1 root    tty       7, 132 Oct 17 04:42 vcsa4
crw-rw----  1 root    tty       7, 133 Oct 17 04:42 vcsa5
crw-rw----  1 root    tty       7, 134 Oct 17 04:42 vcsa6
crw-rw----  1 root    tty       7,  64 Oct 17 04:42 vcsu
crw-rw----  1 root    tty       7,  65 Oct 17 04:42 vcsu1
crw-rw----  1 root    tty       7,  66 Oct 17 04:42 vcsu2
crw-rw----  1 root    tty       7,  67 Oct 17 04:42 vcsu3
crw-rw----  1 root    tty       7,  68 Oct 17 04:42 vcsu4
crw-rw----  1 root    tty       7,  69 Oct 17 04:42 vcsu5
crw-rw----  1 root    tty       7,  70 Oct 17 04:42 vcsu6
drwxr-xr-x  2 root    root        60 Oct 17 04:42 vfio
crw-----  1 root    root      10, 127 Oct 17 04:42 vga_arbiter
crw-----  1 root    root      10, 137 Oct 17 04:42 vhci
crw-rw----  1 root    kvm      10, 238 Oct 17 04:42 vhost-net
crw-rw----  1 root    kvm      10, 241 Oct 17 04:42 vhost-vsock
crw-----  1 root    root      10, 122 Oct 17 04:42 vmci
crw-rw-rw-  1 root    root      10, 121 Oct 17 04:42 vsock
crw-rw-rw-  1 root    root        1,   5 Oct 17 04:42 zero
crw-----  1 root    root      10, 249 Oct 17 04:42 zfs
serat060@ubuntu60:~$

```

```

serat060@ubuntu60:~$ ls -la /var
total 56
drwxr-xr-x 13 root root 4096 Sep 30 18:16 .
drwxr-xr-x 23 root root 4096 Sep 30 16:13 ..
drwxr-xr-x 2 root root 4096 Oct 2 04:28 backups
drwxr-xr-x 16 root root 4096 Oct 17 05:18 cache
drwxrwsrwt 2 root root 4096 Aug 5 17:02 crash
drwxr-xr-x 45 root root 4096 Oct 17 05:18 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 17:45 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
drwxrwsrwt 9 root root 4096 Oct 23 17:45 tmp
-rw-r--r-- 1 root root 208 Aug 5 16:54 .updated
serat060@ubuntu60:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 23 18:04 .
drwxr-xr-x 23 root root 4096 Sep 30 16:13 ..
drwxrwxrwt 2 root root 4096 Oct 17 04:42 .font-unix
drwxrwxrwt 2 root root 4096 Oct 17 04:42 .ICE-unix
drwx----- 2 root root 4096 Oct 17 04:42 snap-private-tmp
drwx----- 3 root root 4096 Oct 17 05:18 systemd-private-42ab35ab8dd34958b0401685228e71a0-fwupd.service-SBr8bq
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-ModemManager.service-17bSUL
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-polkit.service-Vic0Sh
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-systemd-logind.service-z21wC2
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-systemd-resolved.service-Pty7Fg
drwx----- 3 root root 4096 Oct 17 04:42 systemd-private-42ab35ab8dd34958b0401685228e71a0-systemd-timesyncd.service-2dqSCz
drwx----- 3 root root 4096 Oct 17 05:18 systemd-private-42ab35ab8dd34958b0401685228e71a0-upower.service-tCMAdN
drwx----- 2 root root 4096 Oct 17 04:42 vmware-root_746-2965906923
drwxrwxrwt 2 root root 4096 Oct 17 04:42 .X11-unix
drwxrwxrwt 2 root root 4096 Oct 17 04:42 .XIM-unix

```

```

serat060@ubuntu60:~$ ls -la ~
total 56
drwxr-x--- 7 serat060 serat060 4096 Oct 23 18:01 .
drwxr-xr-x 3 root      root      4096 Oct 17 06:15 ..
-rw-rw-r-- 1 serat060 serat060 142 Oct 17 05:12 answers.md
-rw-r--r-- 1 serat060 serat060 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 serat060 serat060 3771 Mar 31 2024 .bashrc
drwx----- 2 serat060 serat060 4096 Sep 30 18:19 .cache
-rw-rw-r-- 1 serat060 serat060 9 Oct 17 05:23 .env
drwxrwxr-x 3 serat060 serat060 4096 Oct 23 18:01 lab4
drwxrwxr-x 3 serat060 serat060 4096 Oct 17 05:17 Lab4
drwxrwxr-x 3 serat060 serat060 4096 Oct 17 05:07 .local
-rw-rw-r-- 1 serat060 serat060 20 Oct 17 05:22 main.py
-rw-r--r-- 1 serat060 serat060 807 Mar 31 2024 .profile
-rw-rw-r-- 1 serat060 serat060 12 Oct 17 05:19 README.md
drwx----- 2 serat060 serat060 4096 Sep 30 18:17 .ssh
-rw-r--r-- 1 serat060 serat060 0 Sep 30 18:21 .sudo_as_admin_successful

```

```

serat060@ubuntu60:~$ cat ~/Q2
cat: /home/serat060/Q2: No such file or directory
serat060@ubuntu60:~$ cat ~/Q2_report.md
/bin contains essential command binaries for all users.
/usr/bin includes non-essential commands and user applications.
/usr/local/bin stores custom software installed by the local administrator.
/sbin holds system binaries for administrative tasks.

```

3. Evidence Handling & File Operations

```
serat060@ubuntu60:~$ mkdir -p ~/sandbox/evidence/suspicious
serat060@ubuntu60:~$ mkdir ~/sandbox/evidence/suspicious
mkdir: cannot create directory '/home/serat060/sandbox/evidence/suspicious': File exists
```

```
serat060@ubuntu60:~$ cd ~/sandbox/evidence/suspicious
serat060@ubuntu60:~/sandbox/evidence/suspicious$ echo "This is file A" > fileA.txt
serat060@ubuntu60:~/sandbox/evidence/suspicious$ echo "This is file B" > fileB.txt
serat060@ubuntu60:~/sandbox/evidence/suspicious$ echo " This is hidden evidence" > hiddenfile.txt
serat060@ubuntu60:~/sandbox/evidence/suspicious$ ls -la
total 20
drwxrwxr-x 2 serat060 serat060 4096 Oct 23 18:42 .
drwxrwxr-x 3 serat060 serat060 4096 Oct 23 18:38 ..
-rw-rw-r-- 1 serat060 serat060  15 Oct 23 18:41 fileA.txt
-rw-rw-r-- 1 serat060 serat060  15 Oct 23 18:41 fileB.txt
-rw-rw-r-- 1 serat060 serat060  25 Oct 23 18:42 hiddenfile.txt
```

```
serat060@ubuntu60:~/sandbox/evidence/suspicious$ ls -la
total 20
drwxrwxr-x 2 serat060 serat060 4096 Oct 23 18:42 .
drwxrwxr-x 3 serat060 serat060 4096 Oct 23 18:38 ..
-rw-rw-r-- 1 serat060 serat060  15 Oct 23 18:41 fileA.txt
-rw-rw-r-- 1 serat060 serat060  15 Oct 23 18:41 fileB.txt
-rw-rw-r-- 1 serat060 serat060  25 Oct 23 18:42 hiddenfile.txt
serat060@ubuntu60:~/sandbox/evidence/suspicious$ cp fileA.txt fileA_backup.txt
serat060@ubuntu60:~/sandbox/evidence/suspicious$ mv fielA_backup.txt fileA_review.txt
mv: cannot stat 'fielA_backup.txt': No such file or directory
serat060@ubuntu60:~/sandbox/evidence/suspicious$ mv fileA_backup.txt fileA_review.txt
serat060@ubuntu60:~/sandbox/evidence/suspicious$ ls -la
total 24
drwxrwxr-x 2 serat060 serat060 4096 Oct 23 18:46 .
drwxrwxr-x 3 serat060 serat060 4096 Oct 23 18:38 ..
-rw-rw-r-- 1 serat060 serat060  15 Oct 23 18:44 fileA_review.txt
-rw-rw-r-- 1 serat060 serat060  15 Oct 23 18:41 fileA.txt
-rw-rw-r-- 1 serat060 serat060  15 Oct 23 18:41 fileB.txt
-rw-rw-r-- 1 serat060 serat060  25 Oct 23 18:42 hiddenfile.txt
serat060@ubuntu60:~/sandbox/evidence/suspicious$ rm fileA_review.txt
```

```

serat060@ubuntu60:~$ cp -r sandbox sandbox_backup
serat060@ubuntu60:~$ ls -la
total 68
drwxr-x---  9 serat060 serat060 4096 Oct 23 18:48 .
drwxr-xr-x  3 root      root      4096 Oct 17 06:15 ..
-rw-rw-r--  1 serat060 serat060  142 Oct 17 05:12 answers.md
-rw-r--r--  1 serat060 serat060  220 Mar 31  2024 .bash_logout
-rw-r--r--  1 serat060 serat060 3771 Mar 31  2024 .bashrc
drwx-----  2 serat060 serat060 4096 Sep 30 18:19 .cache
-rw-rw-r--  1 serat060 serat060    9 Oct 17 05:23 .env
drwxrwxr-x  3 serat060 serat060 4096 Oct 23 18:01 lab4
drwxrwxr-x  3 serat060 serat060 4096 Oct 17 05:17 Lab4
drwxrwxr-x  3 serat060 serat060 4096 Oct 17 05:07 .local
-rw-rw-r--  1 serat060 serat060   20 Oct 17 05:22 main.py
-rw-r--r--  1 serat060 serat060  807 Mar 31  2024 .profile
-rw-rw-r--  1 serat060 serat060  247 Oct 23 18:34 Q2_report.md
-rw-rw-r--  1 serat060 serat060   12 Oct 17 05:19 README.md
drwxrwxr-x  3 serat060 serat060 4096 Oct 23 18:38 sandbox
drwxrwxr-x  3 serat060 serat060 4096 Oct 23 18:48 sandbox_backup
drwx-----  2 serat060 serat060 4096 Sep 30 18:17 .ssh
-rw-r--r--  1 serat060 serat060    0 Sep 30 18:21 .sudo_as_admin_successful
serat060@ubuntu60:~$

```

```

serat060@ubuntu60:~$ history | tail -n 20
 65  nano ~/Q2_report.md
 66  cat ~/Q2
 67  cat ~/Q2_report.md
 68  mkdir ~/sandbox/evidence/suspicious
 69  mkdir -p ~/sandbox/evidence/suspicious
 70  mkdir ~/sandbox/evidence/suspicious
 71  cd ~/sandbox/evidence/suspicious
 72  echo "This is file A" > fileA.txt
 73  echo "This is file B" > fileB.txt
 74  echo " This is hidden evidence" > hiddenfile.txt
 75  ls -la
 76  cp fileA.txt fileA_backup.txt
 77  mv fielA_backup.txt fileA_review.txt
 78  mv fileA_backup.txt fileA_review.txt
 79  ls -la
 80  rm fileA_review.txt
 81  cd ~
 82  cp -r sandbox sandbox_backup
 83  ls -la
 84  history | tail -n 20

```

```

serat060@ubuntu60:~$ cat fi
fielA_backup.txt fileA_backup.txt fileA_review.txt fileA.txt      fileB.txt

```

4. System Profiling and Process Monitoring

```

serat060@ubuntu60:~$ uname -a
Linux ubuntu60 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

```

```

top - 18:53:33 up 2:45, 2 users, load average: 0.07, 0.08, 0.05
Tasks: 217 total, 1 running, 216 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 1.6 sy, 0.0 ni, 98.2 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3868.1 total, 3236.5 free, 503.5 used, 355.3 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 3364.7 avail Mem

```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2892	serat060	20	0	11944	5760	3584	R	1.9	0.1	0:00.41	top
2890	root	20	0	0	0	0	I	1.3	0.0	0:00.29	kworker/1:0-events
746	root	20	0	315880	9472	7936	S	0.6	0.2	0:34.50	vmtoolsd
2362	root	20	0	0	0	0	I	0.3	0.0	0:00.33	kworker/u258:1-events_unbound
2677	root	20	0	0	0	0	I	0.3	0.0	0:06.97	kworker/0:1-events
1	root	20	0	22120	13156	9444	S	0.0	0.3	0:07.79	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.08	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	0:00.00	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
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	kworker/u256:0-ext4-rsv-conve
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	0:00.10	ksoftirqd/0
17	root	20	0	0	0	0	I	0.0	0.0	0:01.81	rcu_preempt
18	root	rt	0	0	0	0	S	0.0	0.0	0:00.17	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	0:02.02	migration/1
24	root	20	0	0	0	0	S	0.0	0.0	0:00.14	ksoftirqd/1
26	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/1:0H-kblockd
29	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kdevtmpfs
30	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-inet_
32	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kauditd

```

poikitu 824 0.0 0.1 300104 7000 ? Ssl 16:00 0:00 /usr/lib/poikitu-1/poikitu --no-debug
root 832 0.0 0.2 18144 8704 ? Ss 16:08 0:00 /usr/lib/systemd/systemd-logind
root 833 0.0 0.3 468952 13440 ? Ssl 16:08 0:00 /usr/libexec/udisks2/udisksd
root 858 0.0 0.0 6824 2688 ? Ss 16:08 0:00 /usr/sbin/cron -f -P
root 871 0.0 0.5 109660 22912 ? Ssl 16:08 0:00 /usr/bin/python3 /usr/share/unattended-upgr
root 1083 0.0 0.3 318360 12800 ? Ssl 16:08 0:00 /usr/sbin/ModemManager
syslog 1180 0.0 0.1 222508 5760 ? Ssl 16:08 0:00 /usr/sbin/rsyslogd -n -iNONE
root 1316 0.0 0.1 6948 4608 tty1 Ss 16:10 0:00 /bin/login -p --
root 1421 0.0 0.0 0 0 ? S 16:11 0:00 [psimon]
serat060 1423 0.0 0.2 20264 11264 ? Ss 16:11 0:00 /usr/lib/systemd/systemd --user
serat060 1425 0.0 0.0 21148 3516 ? S 16:11 0:00 (sd-pam)
serat060 1434 0.0 0.1 8756 5632 tty1 S 16:11 0:02 -bash
root 1480 0.0 0.0 0 0 ? I< 16:11 0:00 [kworker/R-tls-s]
root 1490 0.0 0.2 12020 7936 ? Ss 16:14 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10
root 1743 0.1 1.0 602880 43312 ? Ssl 16:44 0:10 /usr/libexec/fwupd/fwupd
root 1750 0.0 0.2 314000 8832 ? Ssl 16:44 0:00 /usr/libexec/upowerd
root 1773 0.0 0.0 81380 2872 ? Ss 16:44 0:00 gpg-agent --homedir /var/lib/fwupd/gnupg -
root 1950 0.0 0.0 6104 1920 tty6 Ss+ 17:38 0:00 /sbin/agetty -o -p -- \u --noclear - linux
root 2349 0.0 0.0 0 0 ? I 17:45 0:00 [kworker/u257:4-events_power_efficient]
root 2362 0.0 0.0 0 0 ? I 17:50 0:00 [kworker/u258:1-events_power_efficient]
root 2381 0.0 0.0 0 0 ? I 18:00 0:00 [kworker/u258:2-flush-252:0]
root 2464 0.0 0.2 14964 10496 ? Ss 18:20 0:00 sshd: serat060 [priv]
serat060 2566 0.0 0.1 14964 6852 ? S 18:20 0:00 sshd: serat060@pts/1
serat060 2567 0.0 0.1 8648 5504 pts/1 Ss+ 18:20 0:00 -bash
root 2609 0.0 0.0 0 0 ? I< 18:21 0:00 [kworker/0:0H]
root 2618 0.0 0.0 0 0 ? I 18:24 0:00 [kworker/u257:0-flush-252:0]
root 2641 3.1 0.0 0 0 ? I 18:31 0:42 [kworker/0:0-events]
root 2643 0.0 0.0 0 0 ? I 18:34 0:00 [kworker/u257:2-events_unbound]
root 2646 1.8 0.0 0 0 ? I 18:34 0:21 [kworker/1:1-events]
root 2651 0.0 0.0 0 0 ? I< 18:36 0:00 [kworker/0:2H-kblockd]
root 2672 0.3 0.0 0 0 ? I 18:46 0:01 [kworker/1:2-events]
root 2675 0.0 0.0 0 0 ? I 18:47 0:00 [kworker/u258:0-events_unbound]
root 2677 2.1 0.0 0 0 ? I 18:48 0:07 [kworker/0:1-events]
root 2685 0.0 0.0 0 0 ? I 18:50 0:00 [kworker/u257:1-events_power_efficient]
root 2890 0.7 0.0 0 0 ? I 18:52 0:00 [kworker/1:0-events]
root 2893 4.9 0.0 0 0 ? I 18:53 0:00 [kworker/0:2-mm_percpu_wq]
serat060 2894 300 0.1 10884 4480 tty1 R+ 18:54 0:00 ps aux

```

5. User Account Audit & Privilege Escalation Simulation

```

serat060@ubuntu60:~$ sudo adduser lab4user
[sudo] password for serat060:
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' ...

```



```
serat060@ubuntu60:~$ getent passwd lab4user
lab4user:x:1001:1001:,,,:/home/lab4user:/bin/bash
```

```
serat060@ubuntu60:~$ su - lab4user
Password:
lab4user@ubuntu60:~$
```

```
lab4user@ubuntu60:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu60:~$
```

```
serat060@ubuntu60:~$ sudo cat /var/log/auth.log | grep lab4user
2025-10-17T06:00:47.148392+00:00 ubuntu60 sudo: serat060 : TTY=tty1 ; PWD=/home/serat060 ; USER=root ; COMMAND=/usr/sbin/adduser lab4user
2025-10-17T06:00:47.410459+00:00 ubuntu60 groupadd[1875]: group added to /etc/group: name=lab4user, GID=1001
2025-10-17T06:00:47.418491+00:00 ubuntu60 groupadd[1875]: group added to /etc/gshadow: name=lab4user
2025-10-17T06:00:47.434105+00:00 ubuntu60 groupadd[1875]: new group: name=lab4user, GID=1001
2025-10-17T06:00:47.675388+00:00 ubuntu60 useradd[1882]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/bin/bash, from
2025-10-17T06:01:21.300394+00:00 ubuntu60 passwd[1895]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-17T06:04:21.317126+00:00 ubuntu60 chfn[1898]: changed user 'lab4user' information
2025-10-17T06:04:28.786305+00:00 ubuntu60 gpasswd[1908]: members of group users set by root to lab4user
2025-10-17T06:09:32.449288+00:00 ubuntu60 su: pam_unix(su-l:auth): authentication failure; logname=serat060 uid=1000 euid=0 tty=/dev/tty1 ruser=
user=lab4user
2025-10-17T06:09:34.107985+00:00 ubuntu60 su[1928]: FAILED SU (to lab4user) serat060 on tty1
2025-10-17T06:10:54.422409+00:00 ubuntu60 su[1933]: (to lab4user) serat060 on tty1
2025-10-17T06:10:54.424256+00:00 ubuntu60 su[1933]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by serat060(uid=1000)
2025-10-17T06:11:57.765458+00:00 ubuntu60 sudo: lab4user : user NOT in sudoers ; TTY=tty1 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/w
2025-10-17T06:12:43.606618+00:00 ubuntu60 su[1933]: pam_unix(su-l:session): session closed for user lab4user
2025-10-17T06:15:32.152752+00:00 ubuntu60 sudo: serat060 : TTY=tty1 ; PWD=/home/serat060 ; USER=root ; COMMAND=/usr/sbin/deluser --remove-home
2025-10-17T06:15:32.176872+00:00 ubuntu60 userdel[1963]: delete user 'lab4user'
2025-10-17T06:15:32.178232+00:00 ubuntu60 userdel[1963]: delete 'lab4user' from group 'users'
2025-10-17T06:15:32.179076+00:00 ubuntu60 userdel[1963]: removed group 'lab4user' owned by 'lab4user'
2025-10-17T06:15:32.179500+00:00 ubuntu60 userdel[1963]: removed shadow group 'lab4user' owned by 'lab4user'
2025-10-17T06:15:32.179500+00:00 ubuntu60 userdel[1963]: delete 'lab4user' from shadow group 'users'
2025-10-23T18:56:59.160773+00:00 ubuntu60 sudo: serat060 : TTY=tty1 ; PWD=/home/serat060 ; USER=root ; COMMAND=/usr/sbin/adduser lab4user
2025-10-23T18:56:59.321486+00:00 ubuntu60 groupadd[2906]: group added to /etc/group: name=lab4user, GID=1001
2025-10-23T18:56:59.325941+00:00 ubuntu60 groupadd[2906]: group added to /etc/gshadow: name=lab4user
2025-10-23T18:56:59.330897+00:00 ubuntu60 groupadd[2906]: new group: name=lab4user, GID=1001
2025-10-23T18:56:59.369709+00:00 ubuntu60 useradd[2913]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/bin/bash, from
2025-10-23T18:57:33.913401+00:00 ubuntu60 passwd[2926]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-23T18:58:04.126730+00:00 ubuntu60 chfn[2928]: changed user 'lab4user' information
2025-10-23T18:58:08.724952+00:00 ubuntu60 gpasswd[2936]: members of group users set by root to lab4user
2025-10-23T18:59:45.409838+00:00 ubuntu60 su[2945]: (to lab4user) serat060 on tty1
2025-10-23T18:59:45.412425+00:00 ubuntu60 su[2945]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by serat060(uid=1000)
2025-10-23T19:00:40.983099+00:00 ubuntu60 sudo: lab4user : user NOT in sudoers ; TTY=tty1 ; PWD=/home/lab4user ; USER=root ; COMMAND=/usr/bin/w
2025-10-23T19:01:12.236797+00:00 ubuntu60 su[2945]: pam_unix(su-l:session): session closed for user lab4user
serat060@ubuntu60:~$
```