1. Firewall Proof (Network Hardening)

When you run sudo ufw status verbose, your terminal should display that the firewall is active and blocking incoming traffic by default.

Simulated Terminal Output:

user@ubuntu:~$ sudo ufw status verbose

Status: active

Logging: on (low)

Default: deny (incoming), allow (outgoing), disabled (routed)

New profiles: skip

To Action From

-- ------ ----

22/tcp ALLOW IN Anywhere

22/tcp (v6) ALLOW IN Anywhere (v6)

---

2. Permission Proof (File Hardening)

When you run ls -l ~/sensitive_data.txt, you are looking for the -rw------- string, which proves only the owner has access.

Simulated Terminal Output:

Plaintext

user@ubuntu:~$ ls -l ~/sensitive_data.txt

-rw------- 1 student student 16 JAN 26 19:55 /home/student/sensitive_data.txt

Note: The -rw------- means:

- **First -**: It is a regular file.
- **rw-**: The owner (student) can Read and Write.
- **---**: The group has NO permissions.
- **---**: Others have NO permissions.

---

3. Service Hardening Proof

This proves you have successfully reduced the attack surface by disabling unused services like the print scheduler (CUPS).

Simulated Terminal Output:

user@ubuntu:~$ systemctl is-active cups

inactive

user@ubuntu:~$ systemctl is-enabled cups

disabled

---

4. Final Deliverable: OS Security Checklist (Updated)

Task ID	Security Requirement	Implementation Method	Status
01	System Patching	apt upgrade & unattended-upgrades	**COMPLETED**
02	Default Firewall Policy	ufw default deny incoming	**COMPLETED**
03	Least Privilege (Files)	chmod 600 on sensitive data	**COMPLETED**
04	Attack Surface Reduction	systemctl disable cups	**COMPLETED**
05	Secure Shared Memory	Modified /etc/fstab to read-only	**COMPLETED**