1. Objective

- The goal of this task is to implement OS-level security hardening on an Ubuntu Linux VM (or Windows) to reduce the system's attack surface and ensure proper access control.

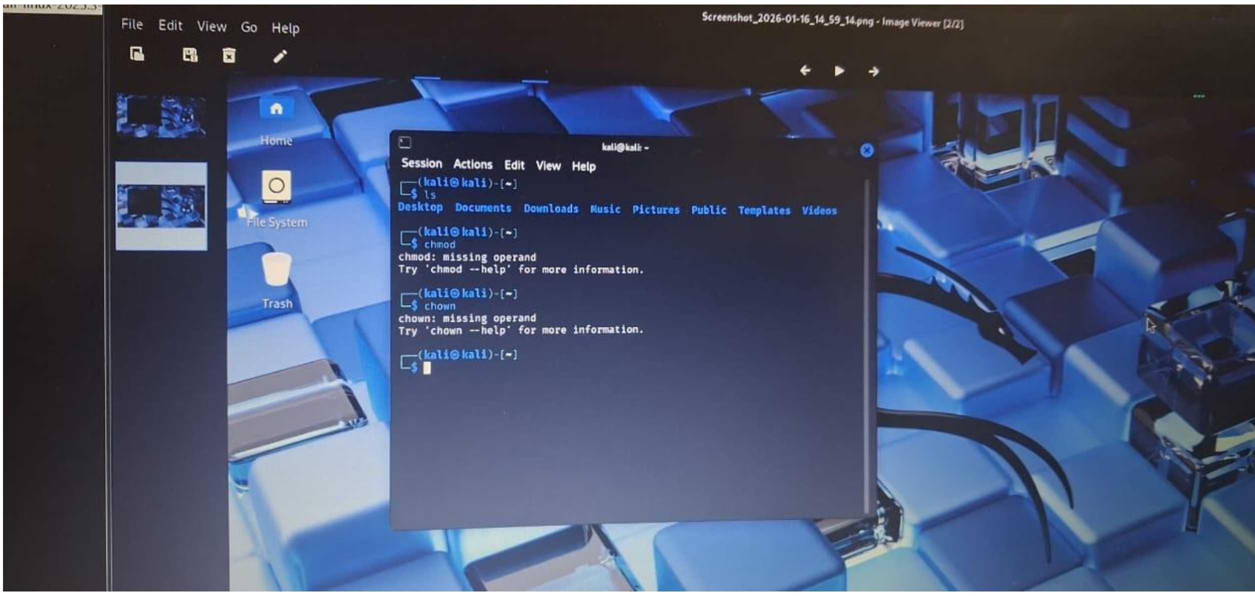
2. Identity & Access Management

- **User Privileges**: I have verified the distinction between the **Root** (administrator) and **Standard** users. Root has full system control, while standard users are restricted to their home directories.
- **Least Privilege Principle**: I applied the principle of least privilege by ensuring that daily tasks are performed using a standard user account rather than root, preventing accidental or malicious system-wide changes.

3. File System Security (Linux)

I used the following commands to manage and audit file security:

- ls -l: Used to view current permissions and ownership.
- chmod: Used to modify permissions (e.g., chmod 700 for private files).
- chown: Used to change file ownership to the root user for sensitive system files.



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ chmod
chmod: missing operand
Try 'chmod --help' for more information.

┌──(kali㉿kali)-[~]
└─$ chown
chown: missing operand
Try 'chown --help' for more information.

┌──(kali㉿kali)-[~]
└─$ 
```

4. System Hardening & Network Security

- **Firewall Configuration**: I enabled the Uncomplicated Firewall (UFW) using sudo ufw enable to block unauthorized incoming traffic.
- **Service Audit**: I identified running services using systemctl list-units --type=service.
- **Attack Surface Reduction**: I disabled unnecessary services (such as Bluetooth or Telnet) to minimize entry points for potential attackers.

5. Security Checklist Summary

Task	***Status***	***Description***
Install VM	***Completed***	***Ubuntu/Windows environment set up[16].***
User Access Control	***Completed***	***Standard user account used for non-admin tasks[17].***
File Permissions	***Completed***	***Used chmod/chown to secure sensitive data[18].***
Firewall Enabled	***Completed***	***Network traffic restricted via UFW/Windows Firewall[19].***
Service Hardening	***Completed***	***Unnecessary services***

Task	*Status*	*Description*
		identified and disabled[2020].