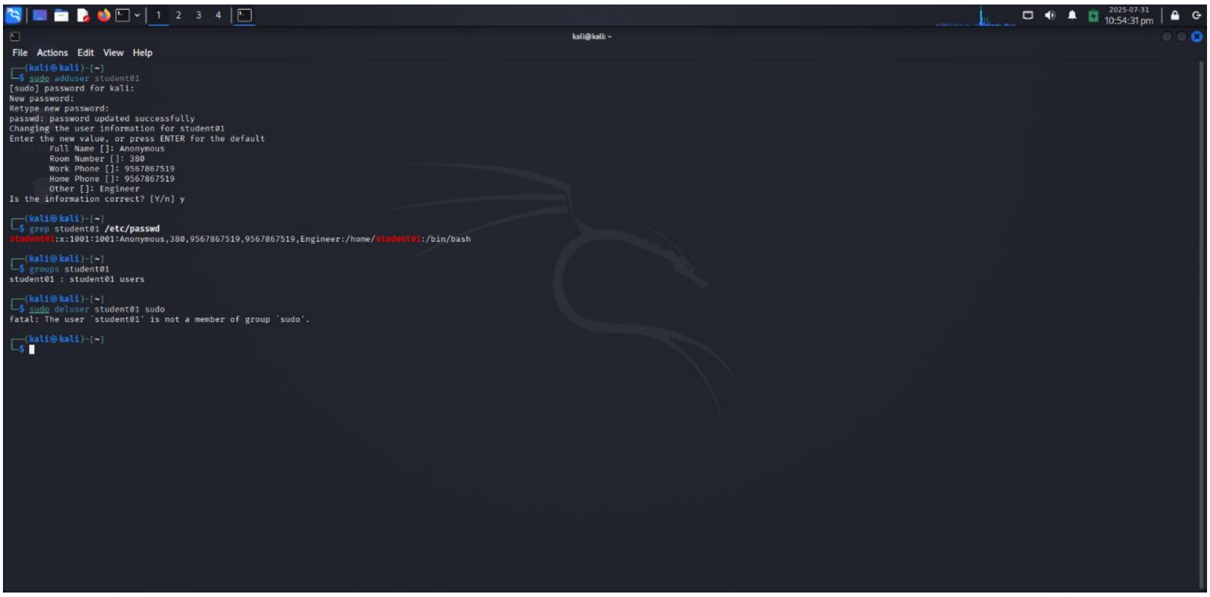
Create Low-Privilege User

Methodology

To set up a secure system, I created a new user account student01 with limited privileges. The task was carried out entirely via terminal using Linux user management commands:

- adduser to create the account.
- usermod to ensure the user had **no sudo/admin rights**.
- groups and /etc/passwd to verify the user's access level.

Screenshot



```
┌──(kali㉿kali)-[~]
└─$ sudo adduser student01
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for student01
Enter the new value, or press ENTER for the default
        Full Name []: Anonymous
        Room Number []: 380
        Work Phone []: 9567867519
        Home Phone []: 9567867519
        Other []: Engineer
Is the information correct? [Y/n] y

┌──(kali㉿kali)-[~]
└─$ grep student01 /etc/passwd
student01:x:1001:1001:Anonymous,380,9567867519,9567867519,Engineer:/home/student01:/bin/bash

┌──(kali㉿kali)-[~]
└─$ groups student01
student01 : student01 users

┌──(kali㉿kali)-[~]
└─$ sudo deluser student01 sudo
fatal: The user `student01' is not a member of group `sudo'.

┌──(kali㉿kali)-[~]
└─$ 
```

Findings

⍰ The user student01 was successfully created.

⍰ Verified that student01 was not in the sudo group.

⍰ The /etc/passwd file showed the default shell and home directory were correctly set.

student01:x:1001:1001::/home/student01:/bin/bash

⍰ Permissions were restricted — student01 couldn't run commands with sudo**.**

Conclusions

Creating users without admin rights enforces the Principle of Least Privilege, which:

- Reduces attack surface.
- Prevents accidental system misconfigurations.
- Enhances overall system security by compartmentalizing permissions.

This is especially critical in penetration testing labs and shared environments like Kali VM.

Name: JOHN JOBY C
Register No. :2460380
Course: Cyber Security