DEPARTMENT OF

COMPUTER SCIENCE AND ENGENEERING

(CSHO331CSP)

ETHICAL HACKING

Assignment Report

Name: Kavin M

Register Number: 2460391

B. Tech – Computer Science and Engineering

School of Engineering and Technology,

CHRIST (Deemed to be University),

Kumbalagodu, Bengaluru-560 074

Create Low-Privilege User

Objective:

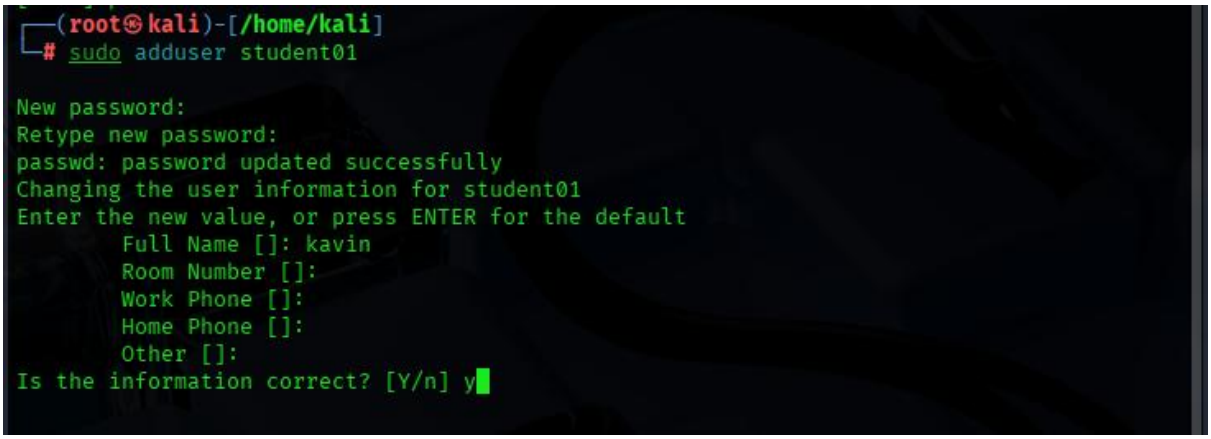
Create a non-admin user (student01) in Kali Linux without sudo privileges for a more secure system configuration.

Step-by-Step Commands:

Step 1 : Create a New User student01.

- Enter into the root terminal.
- Type "**sudo adduser student01**" to create user.
- You'll be prompted to set a password and enter user details.

You can press Enter to skip optional fields.

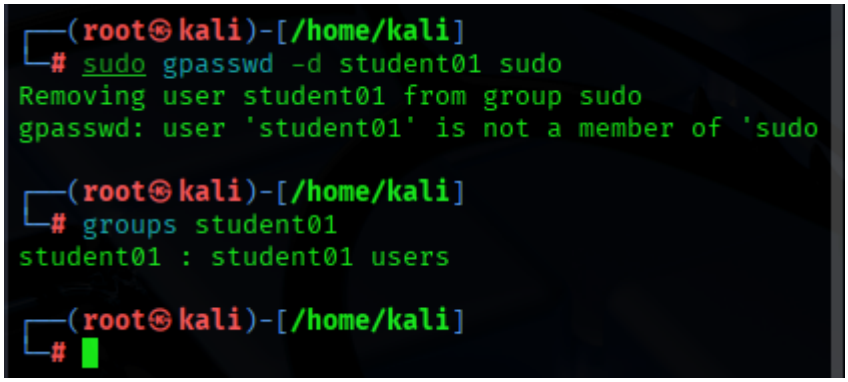


Step 2 : Remove student01 from the sudo Group Using usermod.

- By typing the command "**sudo gpasswd -d student01 sudo**"

  this removes student01 from the sudo group if they were

  automatically added.



Step 3 : Confirm That student01 Has No Sudo Access.

- You should see output like,

  "student01 : student01 users"

- If sudo is missing from the list, the user has no sudo privileges.

Step 4 : Confirm Sudo Access is Denied.

- Switch to student01 by the below command

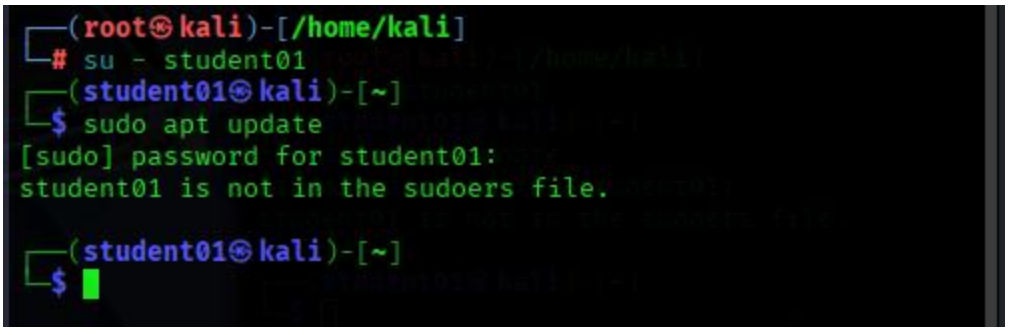
  "**su - student01**".

- Now try,

  "**sudo apt update**".

- Expected:

  "student01 is not in the sudoers file".



Why Limited User Permissions Are Important(Principle of Least Privilege):

1.Improved Security:

Limiting user permissions prevents unauthorized system changes, reducing the risk of malware installation or configuration tampering.

2.Minimized Damage if Compromised:

If a low-privilege user account is hacked, the attacker can't perform critical actions like installing software or modifying system files.

3.Prevents Accidental Mistakes:

Regular users can't accidentally run harmful commands (e.g., rm -rf /) or break the system through misconfiguration.

4.Reduces Attack Surface:

Fewer privileges mean fewer exploitable pathways for attackers, making the system harder to breach.

5.Supports Compliance and Auditing:

Following this principle aligns with industry-standard security practices (like ISO, NIST) and helps in audit trails and compliance checks.

Conclusion:

Giving users only the permissions they need helps keep the system safe. It reduces the risk of mistakes, limits damage if accounts are hacked, and follows good security practices. Keeping users like student01 without admin rights is a simple but effective way to protect the system.