# POC TASK 1

To address Task 1: User & Permission Misconfigurations, we'll go through the setup, exploitation, and mitigation phases on a Linux system. This demonstration will highlight how improper permissions can lead to security vulnerabilities and how to rectify them.

**Setup:**

**Create Multiple Users:**

- **To add new users, we will execute the command Sudo:**

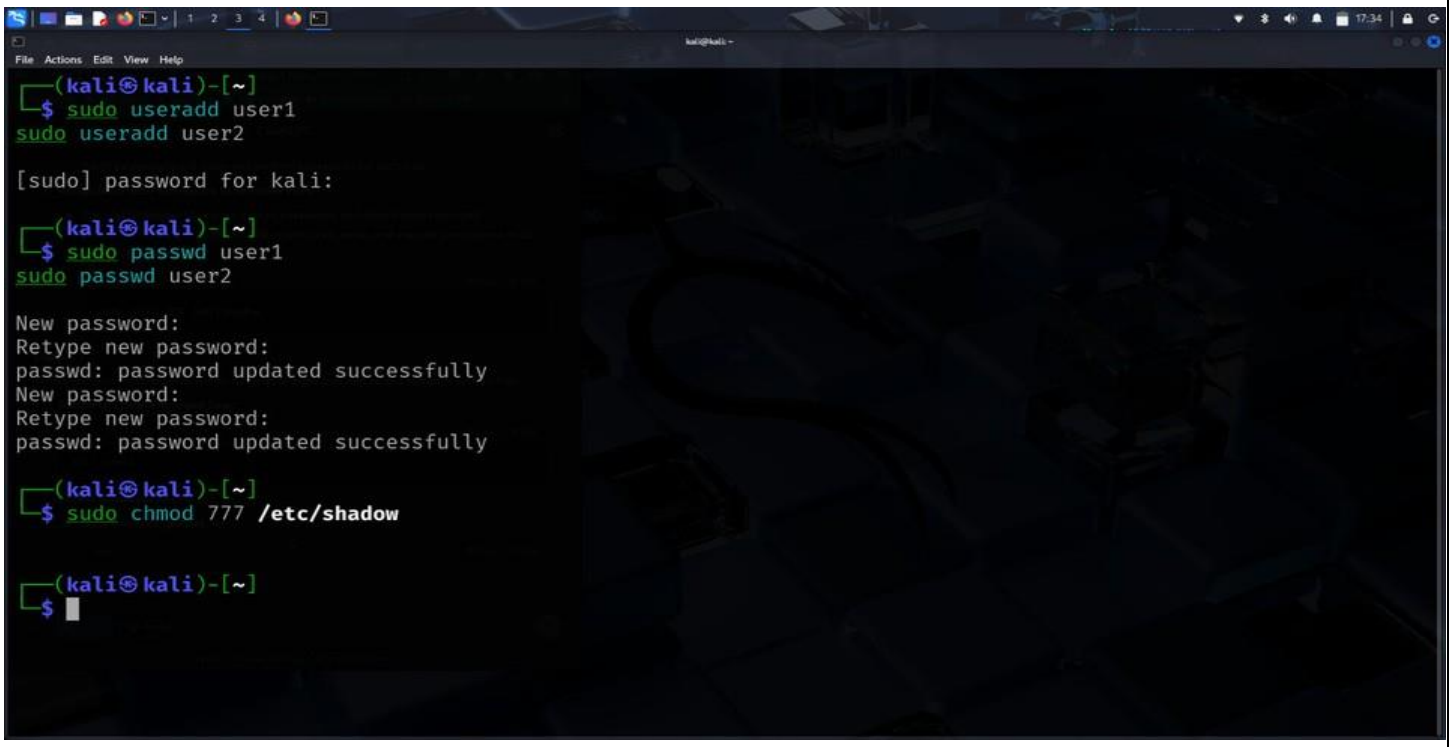
Sudo useradd user1

Sudo useradd user2

- **Set passwords for these users:**

sudo passwd user1

sudo passwd user2



You'll be prompted to enter and confirm passwords for each user.

- **Assign Incorrect Permissions to Sensitive Files:**

The /etc/shadow file is a critical system file that securely stores hashed passwords for all users on a Linux system. It is designed to be accessible only by privileged users (such as root) and should have strict permission settings.

However, assigning chmod 777 to this file grants read, write, and execute permissions to all users making it highly vulnerable to exploitation. This weakens system security by allowing any user to read modify, or delete the password hashes.

```
sudo chmod 777 /etc/shadow
```

- **Exploit:**

  With misconfigured permissions, any low-privileged user on the system can access and manipulate sensitive system files, leading to unauthorized access or privilege escalation.

- **Switch to a Low-Privileged User:**

  A regular user who normally does not have access to sensitive files can now exploit the weak permissions:

```
su - user1
```

- **Access Sensitive Files:**

Since /etc/passwd and /etc/shadow control user authentication, improper permissions allow any user to read them.

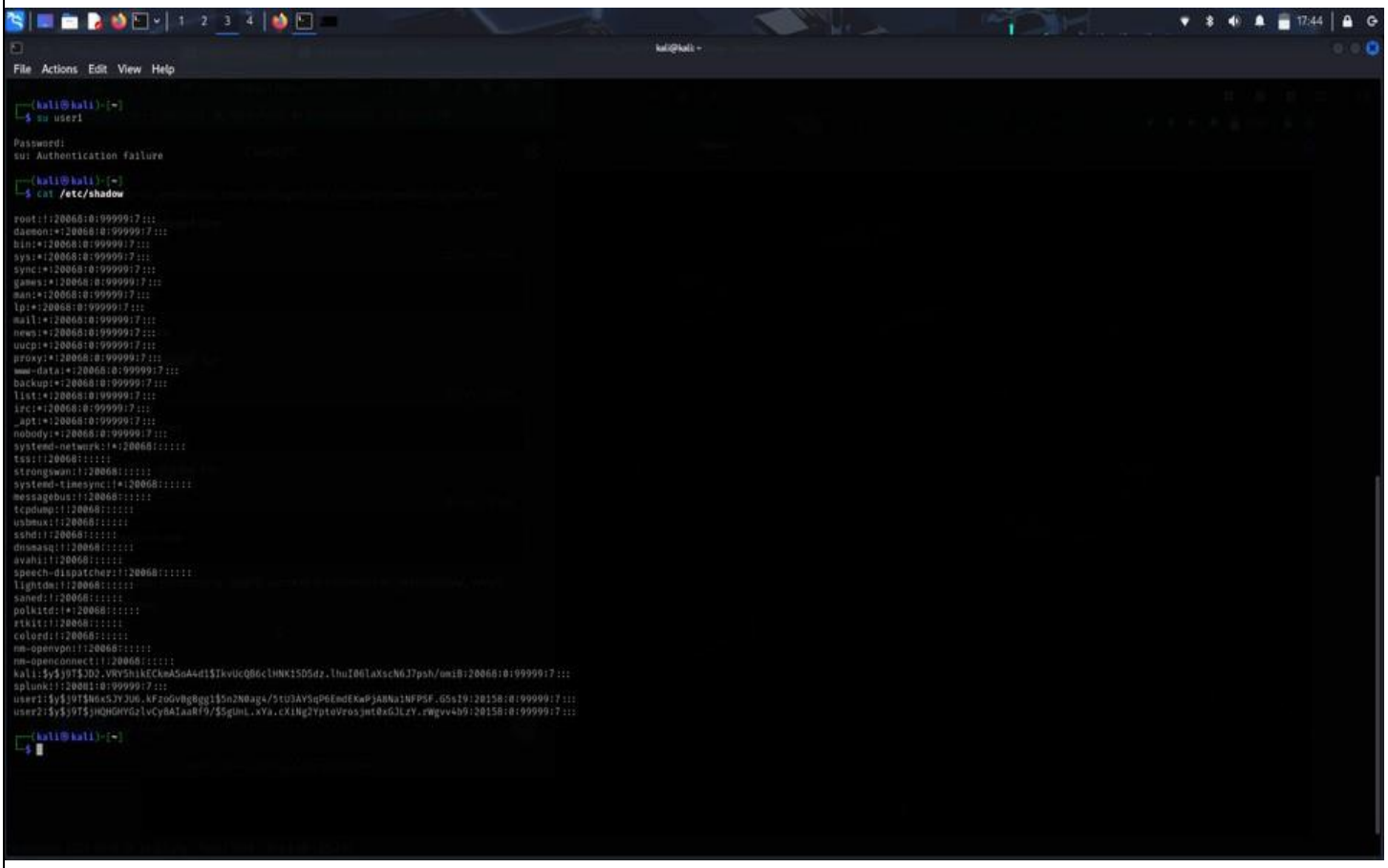
View the /etc/passwd

file: cat /etc/passwd

View the /etc/shadow file:

cat /etc/shadow

Due to the improper permissions, user1 can read the contents of /etc/shadow, which should be restricted.




- **Mitigation:**

  To rectify the permission issues and secure the system, follow these steps:

- **Restrict Permissions on Sensitive Files:**

  Setting appropriate permissions for **/etc/shadow** ensures that only authorized users can access and modify it. The correct permission settings prevent unauthorized access and protect user credentials from being compromised.

  sudo chmod 640 /etc/shadow

- **Verify the permissions:**

  ls -l /etc/shadow

The output should indicate that the file is readable and writable by the owner (root) and readable by the group (shadow), with no permissions for others.

- **Ensure Correct Ownership:**

  The /etc/shadow file must have strict ownership settings to prevent unauthorized modifications The correct owner should be root, and the group should be shadow to ensure only privileged system processes can access it.

  sudo chown root:shadow /etc/shadow

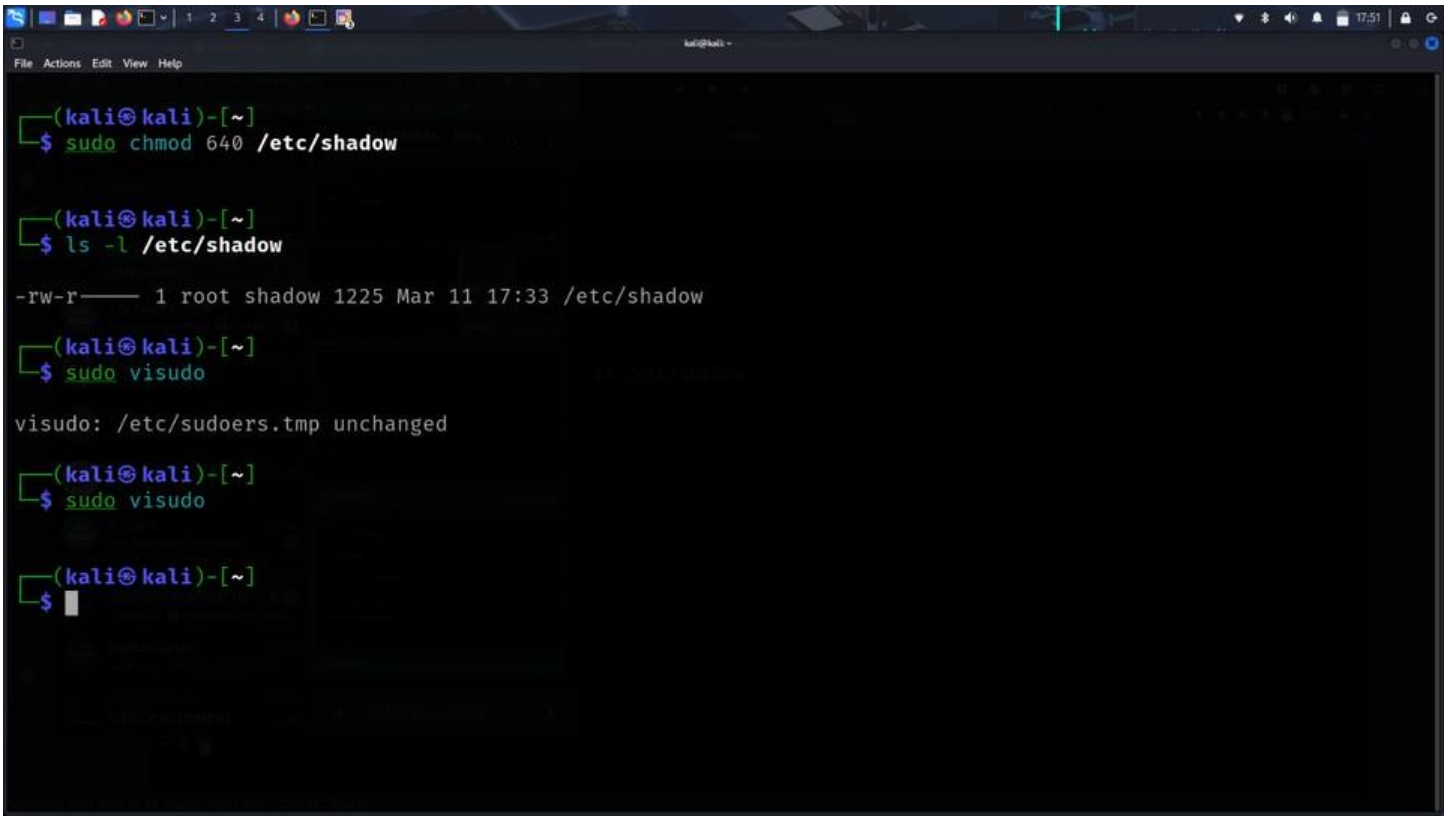
- **Configure Proper sudo Privileges:**

  To prevent unauthorized users from executing administrative commands, ensure **only trusted users** have sudo access:

  sudo visudo

  Add or modify lines to ensure only authorized users have elevated privileges. For example, to grant user1 specific permissions:

  user1  ALL=(ALL)  /usr/bin/apt-get




This line allows user1 to run apt-get with sudo without granting full administrative rights.