

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, execute the following commands:

```
sudo useradd user1
```

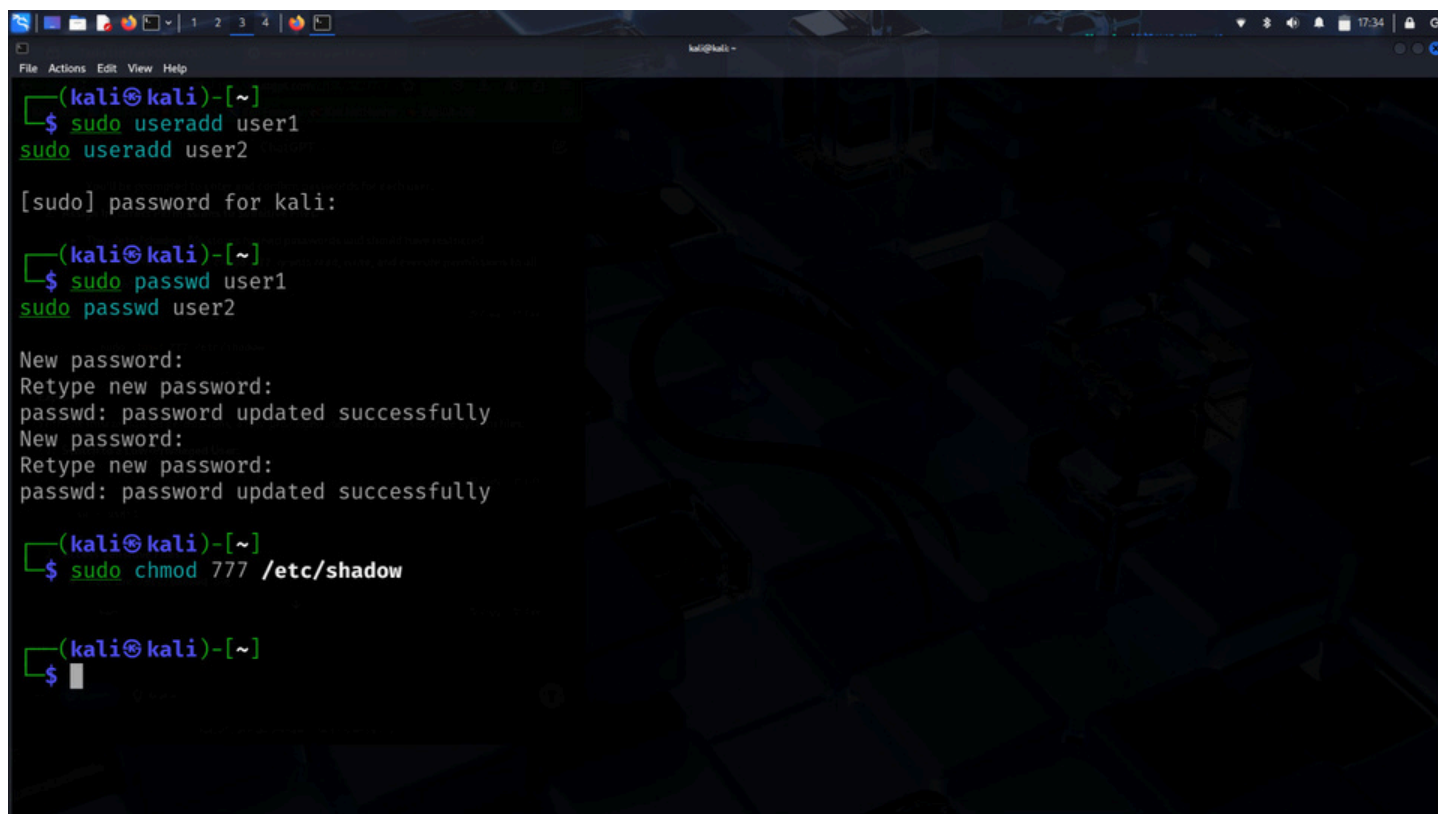
```
sudo useradd user2
```

Set passwords for these users:

```
sudo passwd user1
```

```
sudo passwd user2
```

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

A terminal window on a Kali Linux system. The prompt is (kali㉿kali)-[~]. The user runs 'sudo useradd user1' and 'sudo useradd user2'. Then, for each user, they run 'sudo passwd' and are prompted to enter and confirm a password. The output shows 'passwd: password updated successfully' for both. Finally, they run 'sudo chmod 777 /etc/shadow' and the prompt returns to (kali㉿kali)-[~].

```
(kali㉿kali)-[~]
$ sudo useradd user1
sudo useradd user2

[sudo] password for kali:

(kali㉿kali)-[~]
$ sudo passwd user1
sudo passwd user2

New password:
Retype new password:
passwd: password updated successfully
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$ sudo chmod 777 /etc/shadow

(kali㉿kali)-[~]
$
```

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

Assign Incorrect Permissions to Sensitive Files:

The `/etc/shadow` file stores hashed passwords and should have restricted permissions. Assigning `chmod 777` grants read, write, and execute permissions to all users, which is insecure:

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

Exploit:

With the misconfigured permissions, a low-privileged user can access sensitive system files:

Switch to a Low-Privileged User:

```
su - user1
```

Access Sensitive Files:

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.

```
kali@kali: ~  
$ su user1  
Password:  
su: Authentication failure  
kali@kali: ~  
$ cat /etc/shadow  
root!!:20068:0:99999:7:::  
daemon!!:20068:0:99999:7:::  
bin!!:20068:0:99999:7:::  
sys!!:20068:0:99999:7:::  
sync!!:20068:0:99999:7:::  
games!!:20068:0:99999:7:::  
man!!:20068:0:99999:7:::  
lp!!:20068:0:99999:7:::  
mail!!:20068:0:99999:7:::  
news!!:20068:0:99999:7:::  
uucp!!:20068:0:99999:7:::  
proxy!!:20068:0:99999:7:::  
uuuu-data!!:20068:0:99999:7:::  
backup!!:20068:0:99999:7:::  
list!!:20068:0:99999:7:::  
irc!!:20068:0:99999:7:::  
apt!!:20068:0:99999:7:::  
nobody!!:20068:0:99999:7:::  
systemd-networkd!!:20068:0:99999:7:::  
tss!!:20068:0:99999:7:::  
strongswan!!:20068:0:99999:7:::  
systemd-timesyncd!!:20068:0:99999:7:::  
messagebus!!:20068:0:99999:7:::  
tcpdump!!:20068:0:99999:7:::  
usbmuxd!!:20068:0:99999:7:::  
sshd!!:20068:0:99999:7:::  
dnsmasq!!:20068:0:99999:7:::  
avahi!!:20068:0:99999:7:::  
speech-dispatcher!!:20068:0:99999:7:::  
lightdm!!:20068:0:99999:7:::  
sane!!:20068:0:99999:7:::  
polkitd!!:20068:0:99999:7:::  
rtkit!!:20068:0:99999:7:::  
colord!!:20068:0:99999:7:::  
nm-openvpn!!:20068:0:99999:7:::  
nm-openconnect!!:20068:0:99999:7:::  
kali:!:20068:0:99999:7:::  
splunk:!:20068:0:99999:7:::  
user1:$y$9T$NgaS3Y2J06.AF2oGvBg8g1$5n2N0ags/StuIAYSp6EadEKwPJA8Na1NFP5F.G5tI9:20158:0:99999:7:::  
user2:$y$9T$JHQHGHYD2LvcY8A1aaRf9/$5gumL.xYa.cX1Ng2YptoVrosJmt0xGJLzY.rWgvv409:20158:0:99999:7:::  
kali@kali: ~  
$
```

Mitigation:

To rectify the permission issues:

Restrict Permissions on Sensitive Files:

Set appropriate permissions for **/etc/shadow**:

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:

Set the owner and group for `/etc/shadow`:

```
sudo chown root:shadow /etc/shadow
```

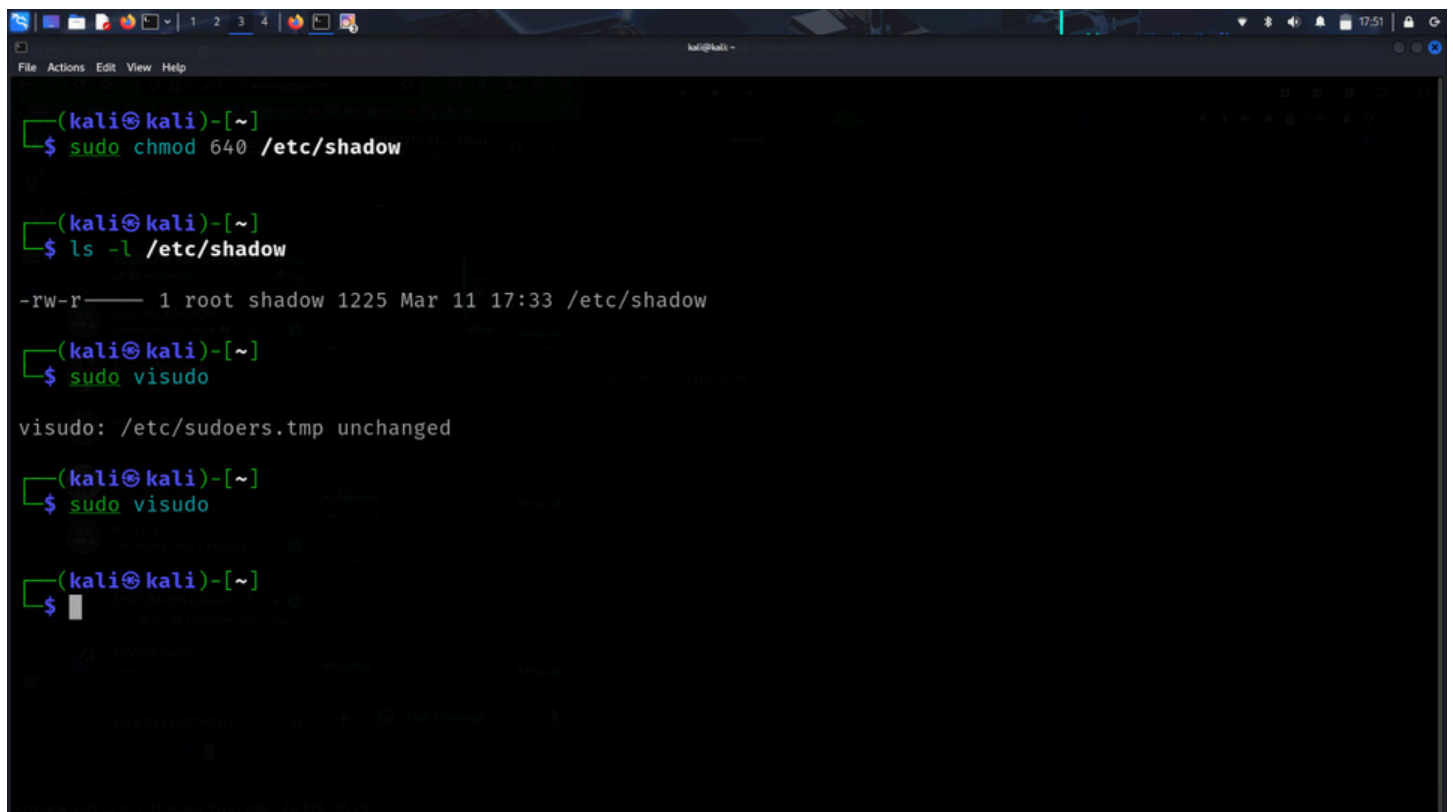
Configure Proper sudo Privileges:

Edit the sudoers file to grant specific permissions:

```
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
```



```
(kali㉿kali)-[~]
$ sudo chmod 640 /etc/shadow

(kali㉿kali)-[~]
$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1225 Mar 11 17:33 /etc/shadow

(kali㉿kali)-[~]
$ sudo visudo
visudo: /etc/sudoers.tmp unchanged

(kali㉿kali)-[~]
$ sudo visudo

(kali㉿kali)-[~]
$
```

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

