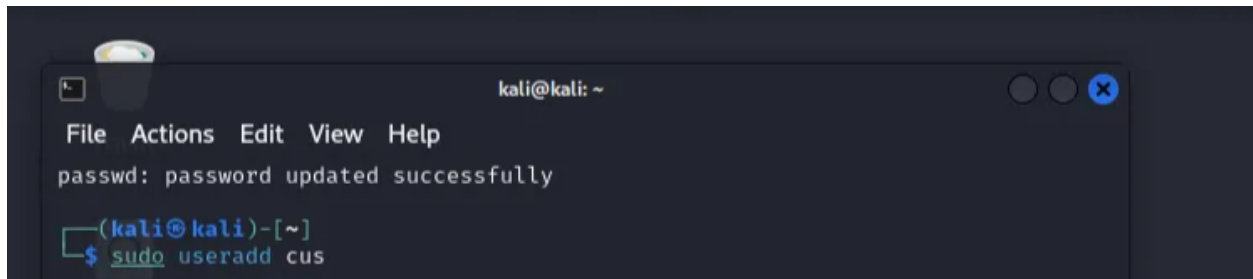


TASK 1

Task 1: User & Permission Misconfigurations

User permission and system misconfigurations:

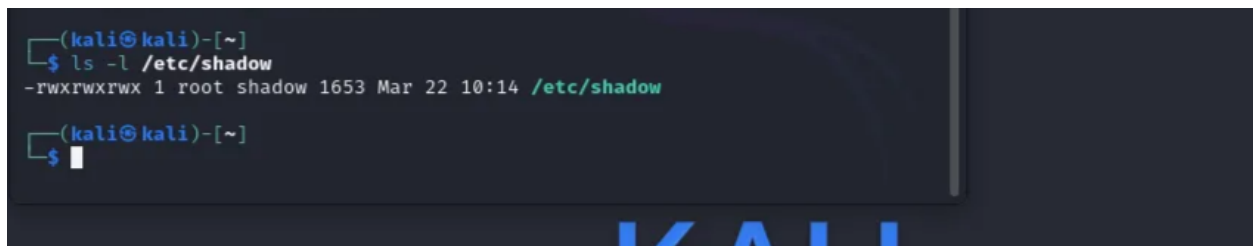
1.First, we create a user named "cus" using the **sudo useradd** command.



```
kali@kali: ~  
File Actions Edit View Help  
passwd: password updated successfully  
  
(kali@kali)-[~]  
$ sudo useradd cus
```

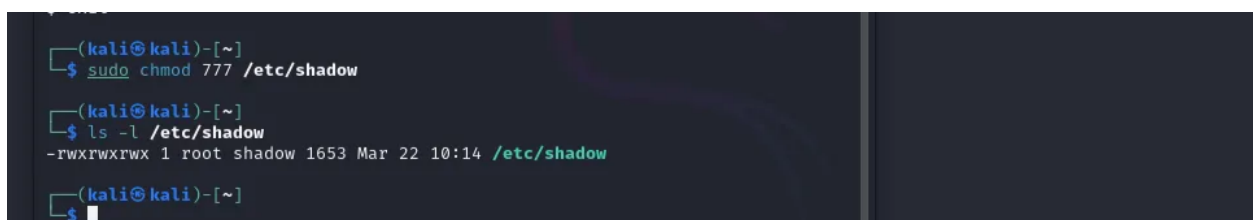
2.We assign the password "4739" by using the **echo** command to write it into the password file **chpassword** , with elevated privileges via **sudo** .

3.We examine the permissions of the password file to identify and exploit any misconfigurations



```
(kali@kali)-[~]  
$ ls -l /etc/shadow  
-rwxrwxrwx 1 root shadow 1653 Mar 22 10:14 /etc/shadow  
  
(kali@kali)-[~]  
$
```

4.We modify the permissions of the shadow file using the **sudo chmod 777** command to grant full access. Then, we verify the updated permissions to confirm the ability to view the file.



```
(kali@kali)-[~]  
$ sudo chmod 777 /etc/shadow  
  
(kali@kali)-[~]  
$ ls -l /etc/shadow  
-rwxrwxrwx 1 root shadow 1653 Mar 22 10:14 /etc/shadow  
  
(kali@kali)-[~]  
$
```

5.As observed, we can now view the contents of the **/etc/shadow** file, which contains hashed passwords, even with normal user privileges.

```
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
$ su user
Password:
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
$ exit

(kali@kali)-[~]
```

6. We have successfully configured **/etc/shadow** to be accessible by normal users.

Securing permissions:

1.We secure the password file by setting its permissions to **640** using the **chmod** command. This ensures that only the root user and members of the shadow group can access it. The root user's password remains viewable only under superuser privileges.

We modify the permissions of the **/etc/passwd** file using **sudo chmod 644** and set its ownership to **root:root** with **sudo chown root:root**. This ensures that regular users can read the file but cannot modify it.

```
—$ sudo chmod 644 /etc/shadow
sudo chown root:shadow /etc/shadow
```

3.Finally, we use Sudo visudo to check permissions.

Summary of Steps:

Step	Command	Purpose
Create Users	sudo useradd user1	Add new users
Set Passwords	<code>`echo "user1: pass" sudo chpasswd`</code>	
Break Security	sudo chmod 777 /etc/shadow	Make shadow file world-readable (BAD)

Exploit	su user1 && cat /etc/shadow	Access passwords as normal user
Fix Permissions	sudo chmod 640 /etc/shadow	Secure shadow file
Secure /etc/passwd	sudo chmod 644 /etc/passwd	Prevent unauthorized edits
Fix sudo Privileges	sudo visudo	Restrict sudo access