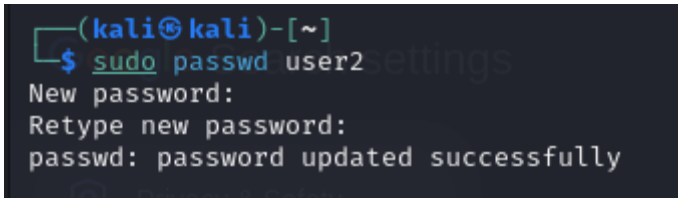
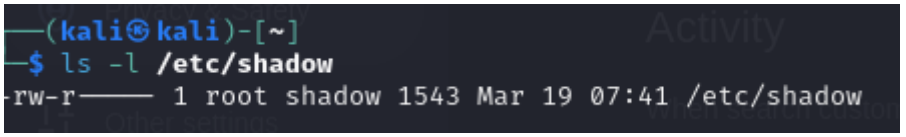
TASK :1 User & Permission Misconfigurations

1.First step ,we created a user “**user2**” with the use of the command **sudo useradd** <username>.

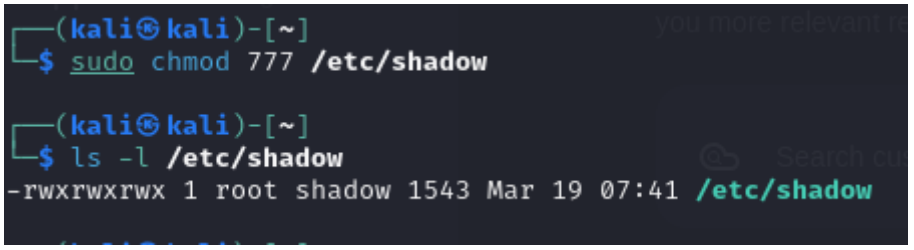
2.Then next we assigned the password user2 by using **sudo passwd <username>.**



3.we examine the permissions to identify and exploit.



4.After we modified the permissions of the shadow file using the command **sudo chmod777** and we verify the updated permissions to confirm the ability to view the file.



5.we can see the contents of the **/etc/shadow file**. It contains hashed passwords even with normal user privileges.

SECURING PERMISSIONS:

Set the password file's permissions to **640** using the chmod command. This allows only the **root user** and members of the **shadow group** to access it. The root user's password can only be viewed with **superuser privileges**.

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod 777 /etc/shadow

┌──(kali㉿kali)-[~]
└─$ sudo chown root:shadow /etc/shadow
```

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod 644 /etc/passwd

┌──(kali㉿kali)-[~]
└─$ sudo chown root:root /etc/shadow
```

SUMMARY OF STEPS:

STEPS	COMMANDS	PURPOSE
Create users	sudo useradd user1	It adds new users
Set passwords	Echo “username:pass	Sudo chpasswd (helps to assign the psd)
Break security	Sudo chmod 777 /etc/shadow	Make shadow file
Exploit	Su username && cat/etc/shadow	Helps to access the password
Fix permissions	Sudo chmod 640 /etc/shadow	Secure the shadow file
Secure /etc/passwd	Sudo chmod 644/etc/passwd	Prevent unauthorized edits
Fix sudo privileges	Sudo visudo	Restrict sudo access