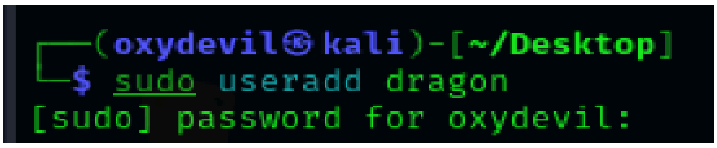
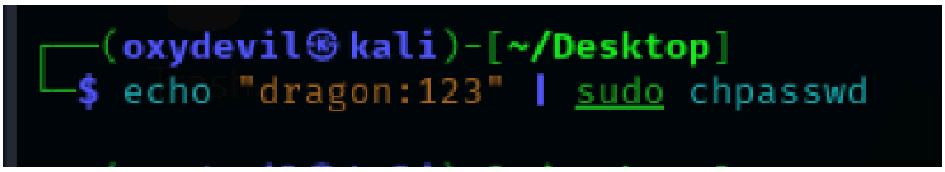
TASK 1:

User permission and system misconfigurations ⚙ :



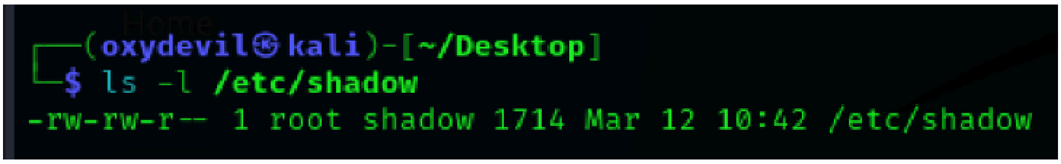
```
┌──(oxydevil㉿kali)-[~/Desktop]
└─$ sudo useradd dragon
[sudo] password for oxydevil:
```

1. First, we use the sudo useradd <username> command to create a user named “dragon.”



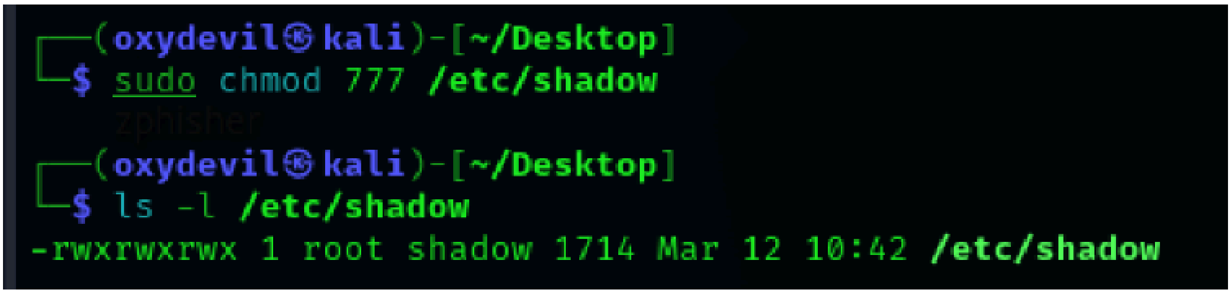
```
┌──(oxydevil㉿kali)-[~/Desktop]
└─$ echo "dragon:123" | sudo chpasswd
```

2. We set the password to “1234” using the echo command and update the password file with elevated privileges via sudo chpasswd.



```
┌──(oxydevil㉿kali)-[~/Desktop]
└─$ ls -l /etc/shadow
-rw-rw-r-- 1 root shadow 1714 Mar 12 10:42 /etc/shadow
```

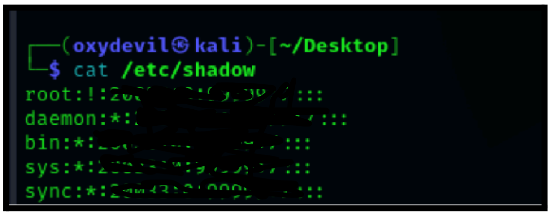
3. We check the password file’s permissions to detect and exploit any misconfigurations.



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

┌──(oxydevil㉿kali)-[~/Desktop]
└─$ ls -l /etc/shadow
-rwxrwxrwx 1 root shadow 1714 Mar 12 10:42 /etc/shadow
```

4. We use the sudo chmod 777 command to modify the shadow file’s permissions, granting full access. Then, we verify the changes to confirm readability.

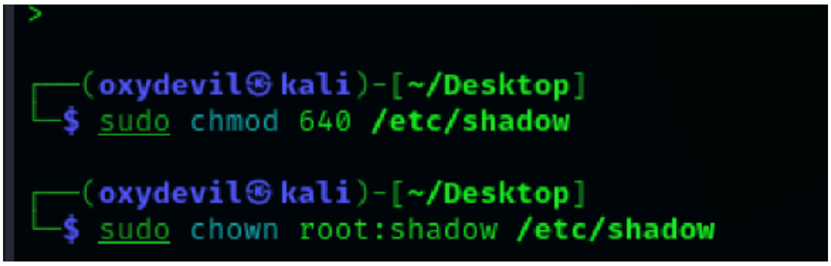


```
┌──(oxydevil㉿kali)-[~/Desktop]
└─$ cat /etc/shadow
root:!:[redacted]:::
daemon:*:
bin:*:
sys:*:
sync:*:
```

5. We can now access the contents of the /etc/shadow file, which stores hashed passwords, even with normal user privileges.

6. We have successfully modified /etc/shadow to allow access for normal users.

Securing permissions 🔒:



```
>
┌──(oxydevil㉿kali)-[~/Desktop]
└─$ sudo chmod 640 /etc/shadow

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

1. We secure the password file by setting its permissions to 640 using the chmod command. This restricts access to the root user and members of the shadow group, ensuring that the root user's password is only viewable with superuser privileges.

2. We set the permissions of the /etc/passwd file to 644 using sudo chmod 644 and assign ownership to root:root with sudo chown root:root. This allows regular users to read the file while preventing modifications.

3. Finally, we use sudo visudo to review and verify permissions.

Summary of Steps:

Step	Command	Purpose
Create Users	`sudo useradd user1`	Add new users
Set Passwords	`echo "user1:pass" | sudo chpasswd`	Set user passwords
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