

POC TASK - 1

TASK 1: User & Permission Misconfigurations

1.1) Create Multiple Users

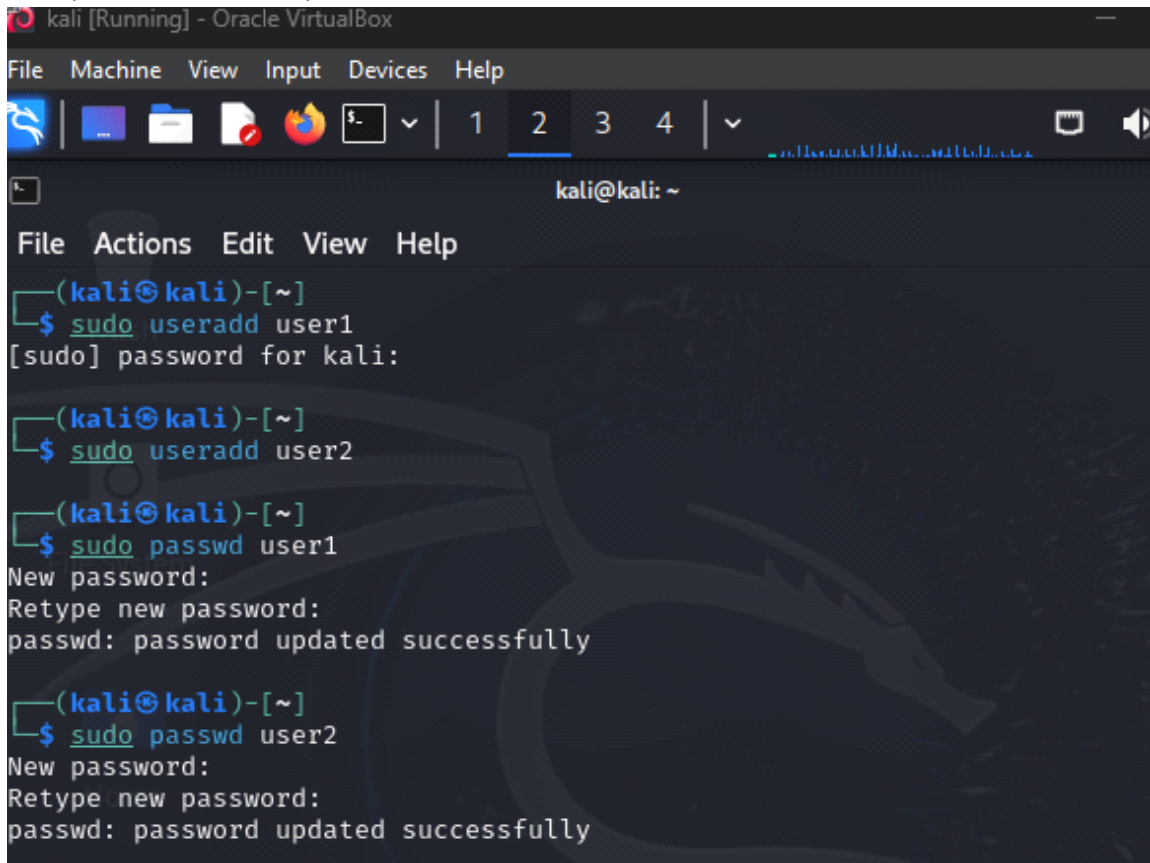
create user1 and user2:

```
sudo useradd -m user1
```

```
sudo useradd -m user2
```

```
sudo passwd user1 # Set password
```

```
sudo passwd user2 # Set password
```

A screenshot of a Kali Linux terminal window running inside an Oracle VM VirtualBox. The terminal shows the following commands and output:

```
(kali㉿kali)-[~]  
$ sudo useradd user1  
[sudo] password for kali:  
  
(kali㉿kali)-[~]  
$ sudo useradd user2  
  
(kali㉿kali)-[~]  
$ sudo passwd user1  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(kali㉿kali)-[~]  
$ sudo passwd user2  
New password:  
Retype new password:  
passwd: password updated successfully
```

 The terminal window has a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. The title bar says 'kali [Running] - Oracle VM VirtualBox'. The terminal background features a faint dragon logo.

1.2) Assign Incorrect Permissions to Sensitive Files

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

```
sudo chmod 777 /etc/passwd
```

```
ls -l /etc/shadow /etc/passwd
```

```
(kali㉿kali)-[/home/kali]
PS> sudo chmod 777 /etc/shadow

(kali㉿kali)-[/home/kali]
PS> ls -l /etc/shadow
-rwxrwxrwx 1 root shadow 1615 Mar 24 19:22 /etc/shadow

(kali㉿kali)-[/home/kali]
PS> sudo chmod 777 /etc/passwd

(kali㉿kali)-[/home/kali]
PS> ls -l /etc/passwd
-rwxrwxrwx 1 root root 3286 Mar 24 19:21 /etc/passwd
```

1.3) Exploit: Access Sensitive System Files as Low-Privileged User

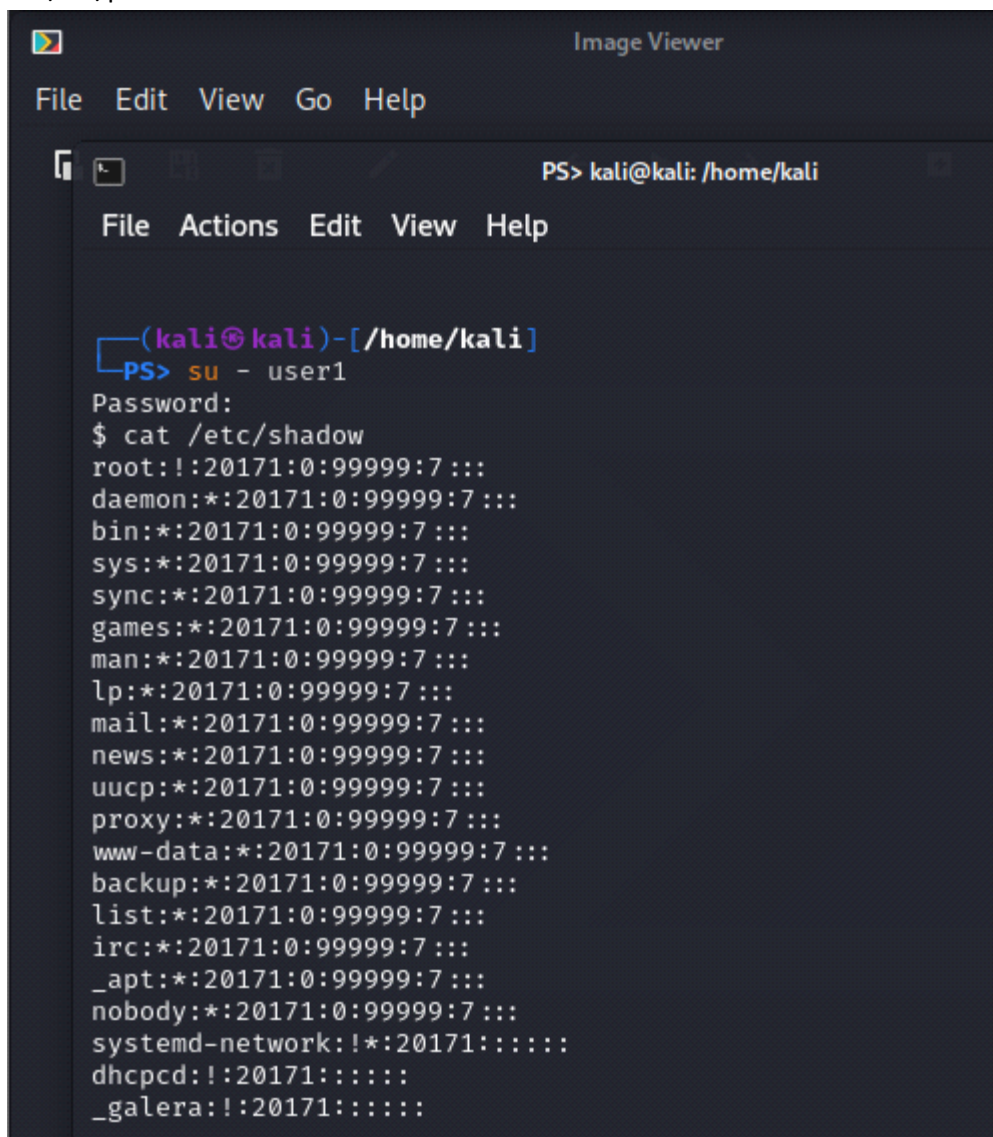
1.3.1) Switch to user1 (Low Privilege User)

su - user1

1.3.2) Now, as user1, try accessing the system files:

cat /etc/shadow

cat /etc/passwd



```
Image Viewer
File Edit View Go Help

PS> kali@kali: /home/kali

File Actions Edit View Help

(kali㉿kali)-[/home/kali]
PS> su - user1
Password:
$ cat /etc/shadow
root:!:20171:0:99999:7:::
daemon:!:20171:0:99999:7:::
bin:!:20171:0:99999:7:::
sys:!:20171:0:99999:7:::
sync:!:20171:0:99999:7:::
games:!:20171:0:99999:7:::
man:!:20171:0:99999:7:::
lp:!:20171:0:99999:7:::
mail:!:20171:0:99999:7:::
news:!:20171:0:99999:7:::
uucp:!:20171:0:99999:7:::
proxy:!:20171:0:99999:7:::
www-data:!:20171:0:99999:7:::
backup:!:20171:0:99999:7:::
list:!:20171:0:99999:7:::
irc:!:20171:0:99999:7:::
_apt:!:20171:0:99999:7:::
nobody:!:20171:0:99999:7:::
systemd-network:!:20171:0:99999:7:::
dhcpcd:!:20171:0:99999:7:::
_galera:!:20171:0:99999:7:::
```

1.4) Mitigation: Fix Permission Issues & Secure Privileges

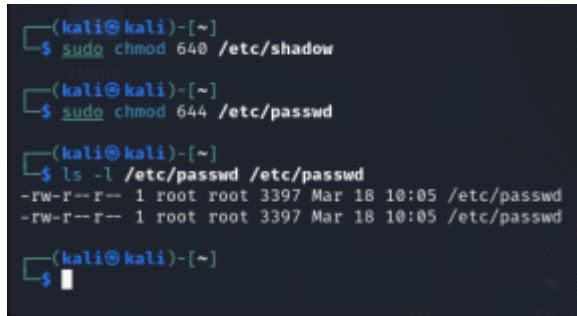
1.4.1) Restrict Permissions on System Files

Switch back to root and fix permissions:

```
sudo chmod 640 /etc/shadow
```

```
sudo chmod 644 /etc/passwd
```

```
ls -l /etc/shadow /etc/passwd
```

A terminal window with a dark background and light green text. The prompt is '(kali㉿kali)-[~]'. The user enters '\$ sudo chmod 640 /etc/shadow'. The prompt is '(kali㉿kali)-[~]'. The user enters '\$ sudo chmod 644 /etc/passwd'. The prompt is '(kali㉿kali)-[~]'. The user enters '\$ ls -l /etc/passwd /etc/passwd'. The output shows two lines: '-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd' and '-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd'. The prompt is '(kali㉿kali)-[~]'. The user enters '\$' and a cursor is visible.

```
(kali㉿kali)-[~]  
$ sudo chmod 640 /etc/shadow  
  
(kali㉿kali)-[~]  
$ sudo chmod 644 /etc/passwd  
  
(kali㉿kali)-[~]  
$ ls -l /etc/passwd /etc/passwd  
-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd  
-rw-r--r-- 1 root root 3397 Mar 18 10:05 /etc/passwd  
  
(kali㉿kali)-[~]  
$
```

1.4.1) Use chown to Assign Proper Ownership

Ensure system files are owned by root:

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

```
sudo chown root:root /etc/passwd
```