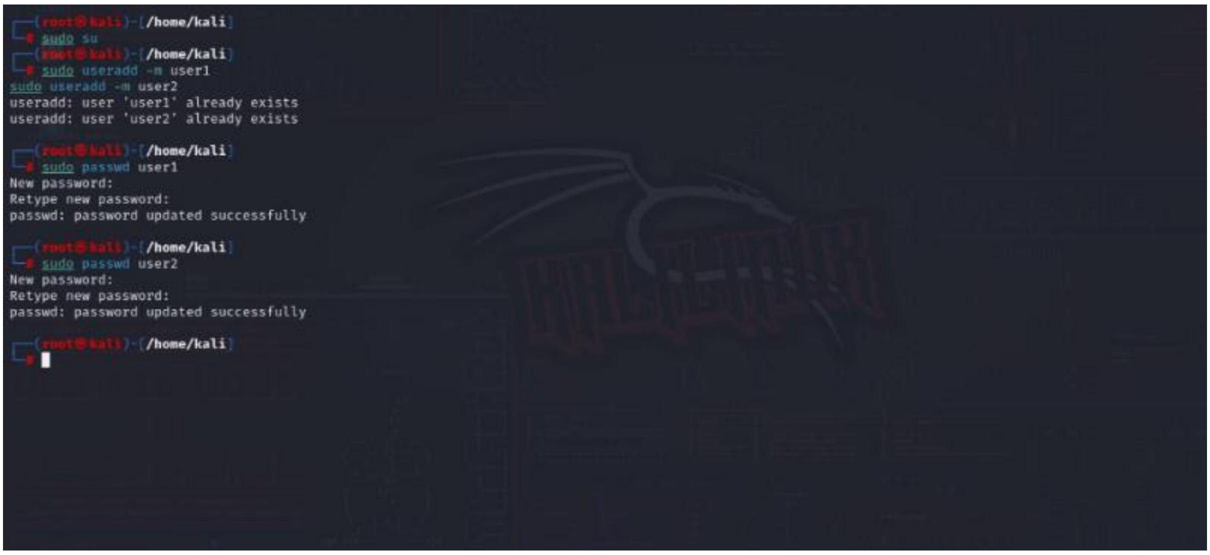
POC TASK 1

1)

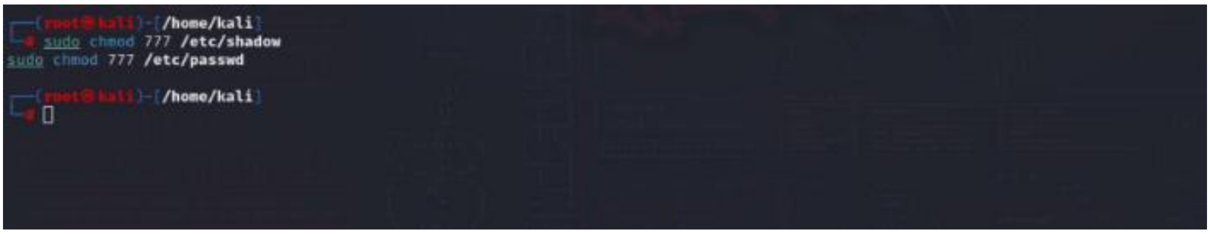


```
┌──(root㉿kali)-[/home/kali]
└─# sudo su
┌──(root㉿kali)-[/home/kali]
└─# sudo useradd -m user1
sudo useradd -m user2
useradd: user 'user1' already exists
useradd: user 'user2' already exists

┌──(root㉿kali)-[/home/kali]
└─# sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[/home/kali]
└─# sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[/home/kali]
└─# █
```

Steps:

- Assign” sudo su”
- Name two users 1 and 2
- Give each user a new passwords
- For example user 1 as kali1 and user 2 as kali2
- By “sudo passwd user”
- We can update the password

2)

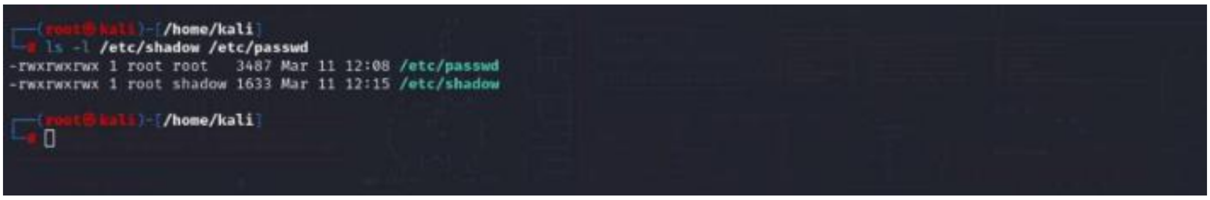


```
┌──(root㉿kali)-[/home/kali]
└─# sudo chmod 777 /etc/shadow
sudo chmod 777 /etc/passwd

┌──(root㉿kali)-[/home/kali]
└─# ▯
```

Steps:

- By sudo chmod 777/etc/shadow we can assign incorrect permisisions.
- chmod 777 /etc/shadow: Makes the password file (/etc/shadow) readable, writable, and executable by all users.
- chmod 777 /etc/passwd: Makes the user information file (/etc/passwd) fully accessible to everyone.

3)

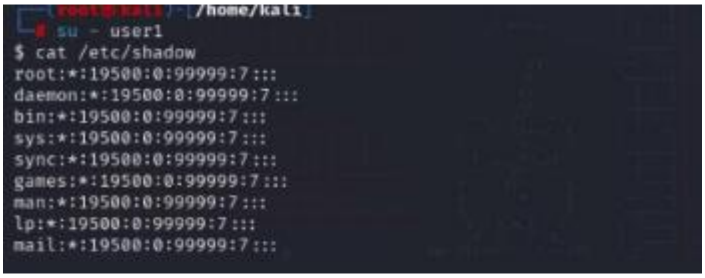


```
┌──(root㉿kali)-[/home/kali]
└─# ls -l /etc/shadow /etc/passwd
-rwxrwxrwx 1 root root   3487 Mar 11 12:08 /etc/passwd
-rwxrwxrwx 1 root shadow 1633 Mar 11 12:15 /etc/shadow

┌──(root㉿kali)-[/home/kali]
└─# ▯
```

Steps:

- By ls -l /etc/shadow/etc/passwd we can verify the permissions.
- Lists the detailed file permissions for /etc/shadow and /etc/passwd.

4)

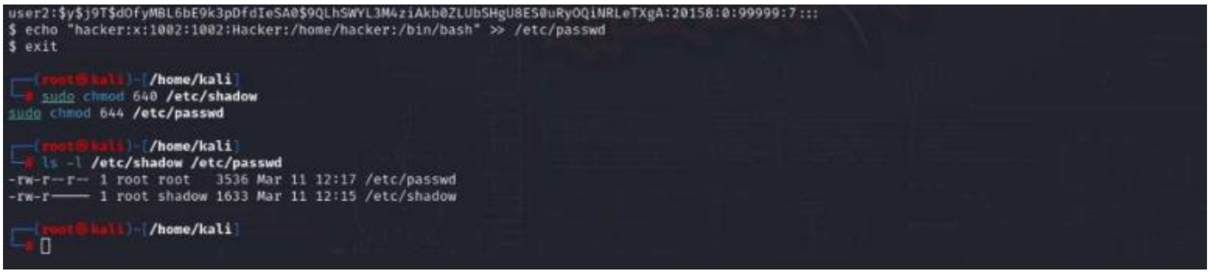


```
┌──(root㉿kali)-[/home/kali]
└─# su - user1
$ cat /etc/shadow
root:*:19500:0:99999:7:::
daemon:*:19500:0:99999:7:::
bin:*:19500:0:99999:7:::
sys:*:19500:0:99999:7:::
sync:*:19500:0:99999:7:::
games:*:19500:0:99999:7:::
man:*:19500:0:99999:7:::
lp:*:19500:0:99999:7:::
mail:*:19500:0:99999:7:::
```

Steps:

- By su - user1 we can switch to Non-root-user
- It can also be done to user2.

5)

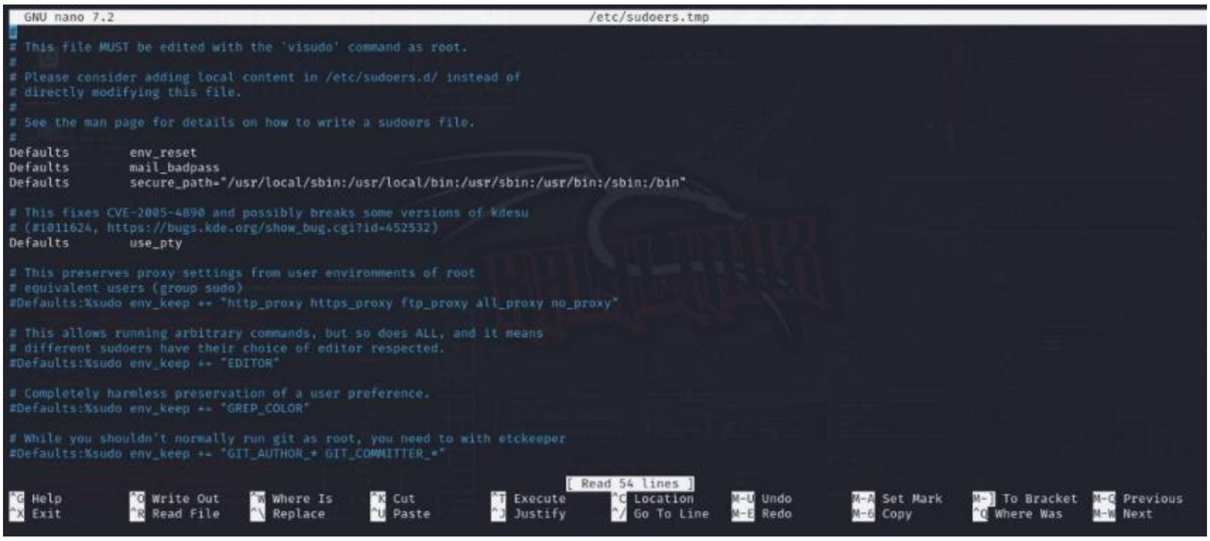


```
user2:$y$j9T$dOfyMBL6bE9k3pDfdIeSA0$9QLhSWYL3M4ziAkb0ZLUbSHgU8ES0uRyOQiNRLeTXgA:20158:0:99999:7:::
$ echo "hacker:x:1002:1002:Hacker:/home/hacker:/bin/bash" >> /etc/passwd
$ exit

┌──(root㉿kali)-[/home/kali]
└─# sudo chmod 640 /etc/shadow
sudo chmod 644 /etc/passwd

┌──(root㉿kali)-[/home/kali]
└─# ls -l /etc/shadow /etc/passwd
-rw-r--r-- 1 root root   3536 Mar 11 12:17 /etc/passwd
-rw-r----- 1 root shadow 1633 Mar 11 12:15 /etc/shadow

┌──(root㉿kali)-[/home/kali]
└─# 
```

Steps:

- By typing echo and the above command we can come back from server switching.
- The sudo chmod 640 /etc/shadow and /etc/passwd we can verify correct permissons.
- -rw-r----- 1 root shadow <date> /etc/shadow
- -rw-r--r-- 1 root root <date> /etc/passwd
- It shows that the permissons in fixed.

6)



```
  GNU nano 7.2                                              /etc/sudoers.tmp
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

                                        [ Read 54 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket M-Q Previous
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was   M-W Next
```

Steps:

- By “sudo visudo” command we can configure file for editing.
- It can secure sudo access.