

Nick Carpenter

CYSE 270

Lab 4

6/4/2024

Step 1:

Command: Grep -i Nick /etc/passwd

```
File Actions Edit View Help
(nick@kali)-[~]
└─$ grep -i Nick /etc/passwd
nick:x:1000:1000:,,,:/home/nick:/usr/bin/zsh
```

Step 2:

Command: Grep -i Nick /etc/shadow (access denied)

Second Command: sudo grep -i Nick /etc/shadow

```
(nick@kali)-[~]
└─$ sudo grep -i Nick /etc/shadow
[sudo] password for nick:
nick:$y$j9T$Sp/.EXf.oyBs0LWdlWEnu0$50DwcLevkvb9dalQtCQmfqIsrsZRhPlPDgVZyx54F1:19856:0:99999:7:
::
```

Step 3:

Command: Sudo useradd -m -k/etc/skel ncap006 (was done previously when I was attempting the lab)

```
(nick@kali)-[~]
└─$ sudo useradd -m -k/etc/skel ncarp006
useradd: user 'ncarp006' already exists
```

```
(nick@kali)-[~]
└─$ tail -1 /etc/passwd
ncarp006:x:1001:1001::/home/ncarp006:/bin/sh
```

(shows that the user was added)

Step 4:

Command: sudo passwd ncarp006

```
(nick@kali)-[~]
└─$ sudo passwd ncarp006
New password:
Retype new password:
passwd: password updated successfully
```

Step 5:

Command: sudo usermod -s /bin/bash ncarp006

```
(nick@kali)-[~]
└─$ sudo usermod -s /bin/bash ncarp006
```

Command: echo tail -1 /etc/passwd

```
(nick@kali)-[~]
└─$ tail -1 /etc/passwd
ncarp006:x:1001:1001::/home/ncarp006:/bin/bash
```

Step 6:

Command: sudo grep -i ncarp006 /etc/shadow

```
(nick@kali)-[~]
└─$ sudo grep -i ncarp006 /etc/shadow
ncarp006:$y$j9T$myacdJpyfidPEa0ZZb06f/$xlrY2LM/6ICSidd1LDzDvr.51BCik6y2zmL4FyKzh3B:19878:0:9999
9:7:::
```

Step 7:

Command: sudo usermod -a -G sudo ncarp006

```
(nick@kali)-[~]
└─$ sudo usermod -a -G sudo ncarp006
```

Step 8:

Command: sudo su ncarp006

```
(nick@kali)-[~]
└─$ sudo su ncarp006
(ncarp006@kali)-[/home/nick]
└─$
```

Task B:

Step 1:

Echo \$SHELL

```
(ncarp006@kali)-[~/home/nick]
└─$ echo $SHELL
/bin/bash
```

Step 2:

Id

Command: groups

```
(ncarp006@kali)-[~/home/nick]
└─$ id
uid=1001(ncarp006) gid=1001(ncarp006) groups=1001(ncarp006),27(sudo)

(ncarp006@kali)-[~/home/nick]
└─$ groups
ncarp006 sudo
```

Step 3:

Command: groups nick

```
(ncarp006@kali)-[~/home/nick]
└─$ groups nick
nick : nick adm dialout cdrom floppy sudo audio dip video plugdev users netdev wireshark blueto
oth scanner vboxsf kaboxer
```

Step 4:

Command: ls -l /etc/group

```
(ncarp006@kali)-[~/home/nick]
└─$ ls -l /etc/group
-rw-r--r-- 1 root root 1309 Jun  6 16:27 /etc/group
```

Step 5:

Command: sudo groupadd -g 01207867 test

```
(ncarp006@kali)-[~/home/nick]
└─$ sudo groupadd -g 01207867 test
[sudo] password for ncarp006:
```

Step 6:

Command: `grep test /etc/group`

```
(ncarp006@kali)-[/home/nick]
└─$ grep test /etc/group
test:x:1207867:
```

Step 7:

Command: `sudo groupmod -n newtest test`

I also used `grep newtest /etc/group` to make sure the information was changed.

```
(ncarp006@kali)-[/home/nick]
└─$ sudo groupmod -n newtest test
```

```
(ncarp006@kali)-[/home/nick]
└─$ grep newtest /etc/group
newtest:x:1207867:
```

Step 8:

Commands: `sudo usermod -G newtest ncarp006` (done previously when attempting the lab)

I used `grep newtest /etc/group` to make sure my MIDAS was in the new group

```
(ncarp006@kali)-[/home/nick]
└─$ grep newtest /etc/group
newtest:x:1207867:ncarp006
```

Step 9:

Commands:

`sudo touch newfile.txt`

`sudo chgrp newtest newfile.txt`

`sudo ls -l`

```
(ncarp006@kali)-[/home/nick]
└─$ sudo touch newfile.txt
[sudo] password for ncarp006:

(ncarp006@kali)-[/home/nick]
└─$ sudo chgrp newtest newfile.txt
```

```

(ncarp006@kali)-[/home/nick]
└─$ sudo ls -l
total 44
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Desktop
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Documents
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Downloads
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Music
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Pictures
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Public
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Templates
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Videos
-rw-r--r-- 1 nick nick 5471 May 28 19:52 copyright_cyse270
drwxr-xr-x 2 nick nick 4096 May 20 20:25 data
-rw-r--r-- 1 root newtest 0 Jun 6 16:53 newfile.txt

```

Step 10:

Commands: sudo groupdel newtest

My UIN has taken the place of the group owner.

```

(ncarp006@kali)-[/home/nick]
└─$ sudo groupdel newtest

(ncarp006@kali)-[/home/nick]
└─$ sudo ls -l
total 44
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Desktop
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Documents
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Downloads
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Music
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Pictures
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Public
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Templates
drwxr-xr-x 2 nick nick 4096 May 13 17:33 Videos
-rw-r--r-- 1 nick nick 5471 May 28 19:52 copyright_cyse270
drwxr-xr-x 2 nick nick 4096 May 20 20:25 data
-rw-r--r-- 1 root 1207867 0 Jun 6 16:53 newfile.txt

```

Step 11:

commands:

kill -9 16013 to stop the process to be able to delete the user.

Sudo userdel -r ncarp006

```

(nick@kali)-[~]
└─$ sudo userdel -r ncarp006
[sudo] password for nick:
userdel: ncarp006 mail spool (/var/mail/ncarp006) not found

```

