CYSE 270: Linux System for Cybersecurity

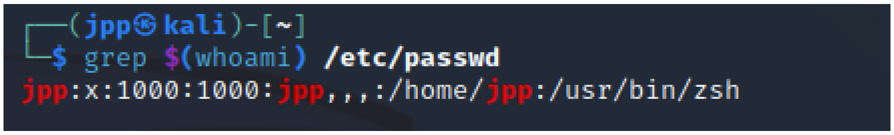
Assignment: Lab 4 – Group and User Accounts

The goal of this lab is to practice basic group and account management. You can choose the Ubuntu VM on your local PC or VMware to complete this assignment.

In this assignment, you should replace xxxxx with your MIDAS ID in all occurrences.

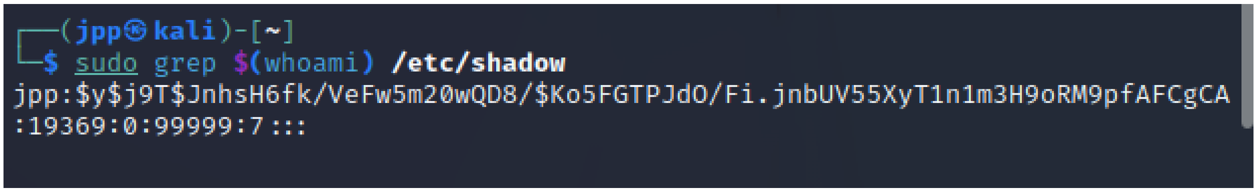
Task A – User Account management (8 * 5 = 40 points)

1. Open a terminal window in VM and execute the correct command to display user account information (including the login shell and home directory) for the current user using grep.



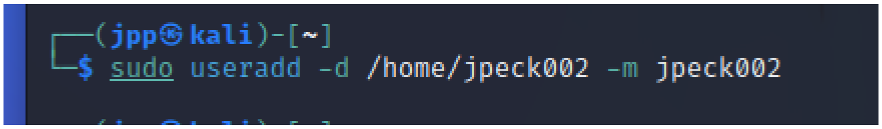
```
┌──(jpp㉿kali)-[~]
└─$ grep $(whoami) /etc/passwd
jpp:x:1000:1000:jpp,,,:/home/jpp:/usr/bin/zsh
```

2. Execute the correct command to display user password information (including the encrypted password and password aging) for the current user using grep.



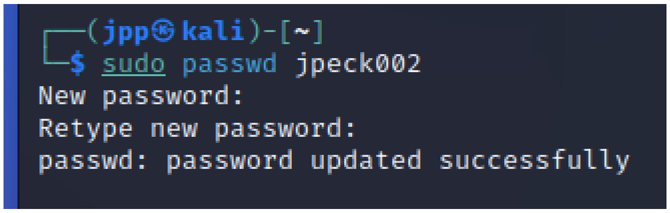
```
┌──(jpp㉿kali)-[~]
└─$ sudo grep $(whoami) /etc/shadow
jpp:$y$j9T$JnhsH6fk/VeFw5m20wQD8/$Ko5FGTPJdO/Fi.jnbUV55XyT1n1m3H9oRM9pfAFCgCA
:19369:0:99999:7:::
```

3. Create a new user named xxxxx and explicitly use options to create the home directory **/home/**xxxxx for this user.



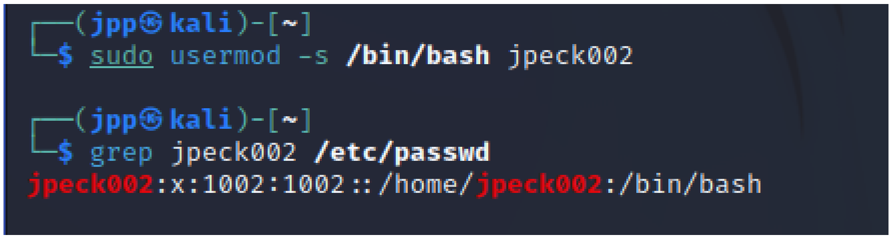
```
┌──(jpp㉿kali)-[~]
└─$ sudo useradd -d /home/jpeck002 -m jpeck002
```

4. Set a password for the new user.



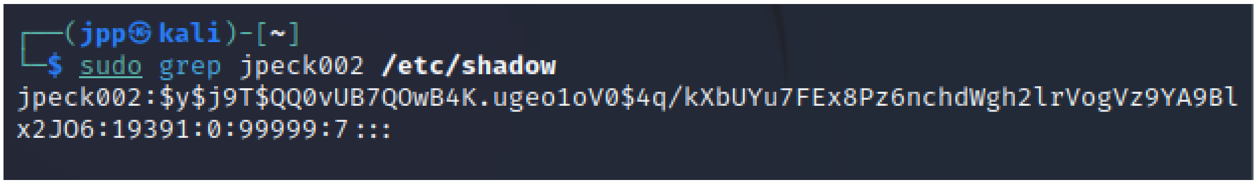
```
┌──(jpp㉿kali)-[~]
└─$ sudo passwd jpeck002
New password:
Retype new password:
passwd: password updated successfully
```

5. Set bash shell as the default login shell for the new user xxxxx, then verify the change.



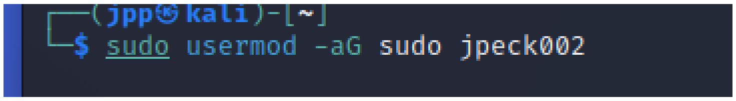
```
┌──(jpp㉿kali)-[~]
└─$ sudo usermod -s /bin/bash jpeck002

┌──(jpp㉿kali)-[~]
└─$ grep jpeck002 /etc/passwd
jpeck002:x:1002:1002::/home/jpeck002:/bin/bash
```

6. Execute the correct command to display user password information (including the encrypted password and password aging) for the new user xxxxx using grep.



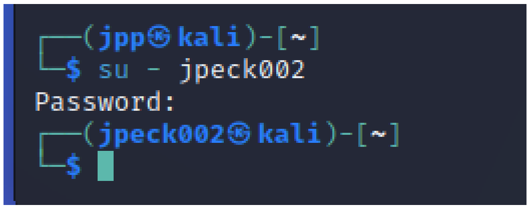
```
┌──(jpp㉿kali)-[~]
└─$ sudo grep jpeck002 /etc/shadow
jpeck002:$y$j9T$QQ0vUB7QOwB4K.ugeo1oV0$4q/kXbUYu7FEx8Pz6nchdWgh2lrVogVz9YA9Bl
x2JO6:19391:0:99999:7:::
```

7. Add the new user xxxxx to sudo group without overriding the existing group membership.



```
┌──(jpp㉿kali)-[~]
└─$ sudo usermod -aG sudo jpeck002
```

8. Switch to the new user's account.

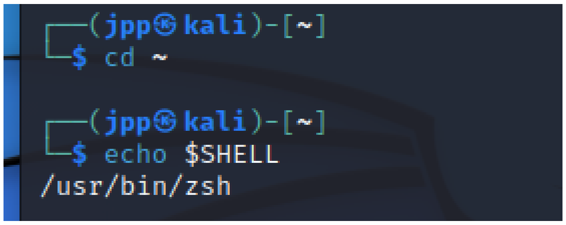


```
┌──(jpp㉿kali)-[~]
└─$ su - jpeck002
Password:
┌──(jpeck002㉿kali)-[~]
└─$ 
```

Task B – Group account management (12 * 5 = 60 points)

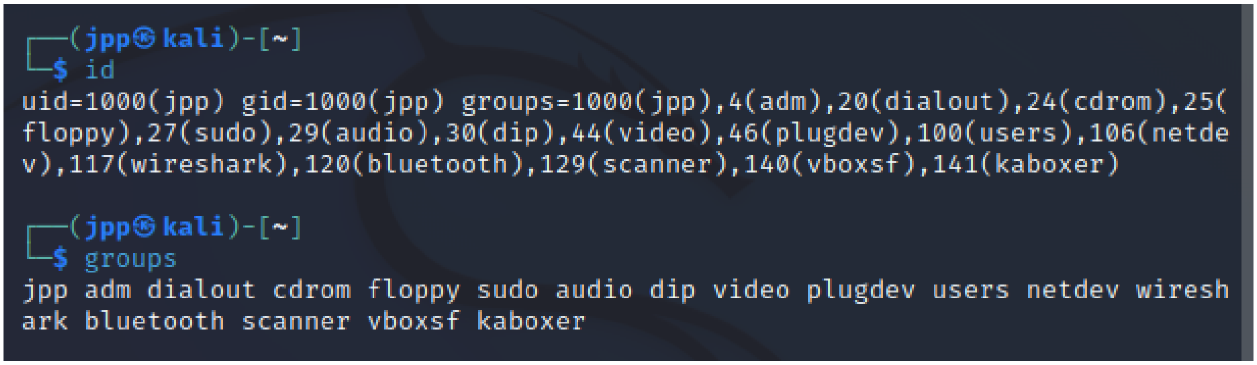
Use Linux commands to execute the following tasks:

1. Return to your home directory and determine the shell you are using.



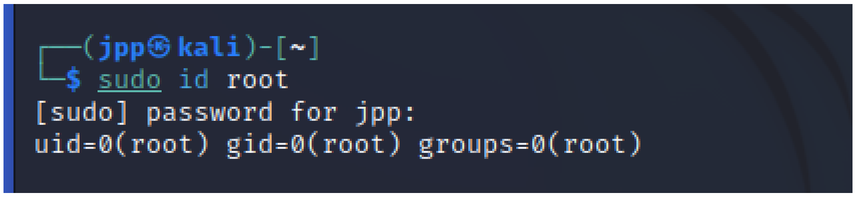
```
┌──(jpp㉿kali)-[~]
└─$ cd ~

┌──(jpp㉿kali)-[~]
└─$ echo $SHELL
/usr/bin/zsh
```

2. Display the current user's ID and group membership.



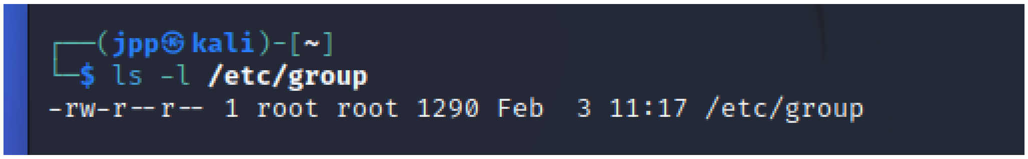
```
┌──(jpp㉿kali)-[~]
└─$ id
uid=1000(jpp) gid=1000(jpp) groups=1000(jpp),4(adm),20(dialout),24(cdrom),25(
floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netde
v),117(wireshark),120(bluetooth),129(scanner),140(vboxsf),141(kaboxer)

┌──(jpp㉿kali)-[~]
└─$ groups
jpp adm dialout cdrom floppy sudo audio dip video plugdev users netdev wiresh
ark bluetooth scanner vboxsf kaboxer
```

3. Display the group membership of the root account.



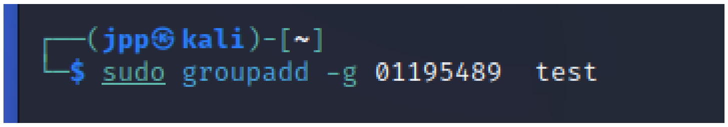
```
┌──(jpp㉿kali)-[~]
└─$ sudo id root
[sudo] password for jpp:
uid=0(root) gid=0(root) groups=0(root)
```

4. Run the correct command to determine the user owner and group owner of the /etc/group file.



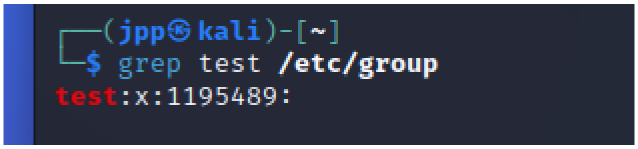
```
┌──(jpp㉿kali)-[~]
└─$ ls -l /etc/group
-rw-r--r-- 1 root root 1290 Feb  3 11:17 /etc/group
```

5. Create a new group named **test** and use your UIN as the GID.



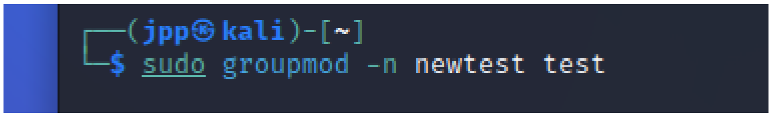
```
┌──(jpp㉿kali)-[~]
└─$ sudo groupadd -g 01195489  test
```

6. Display the group account information for the test group using grep.



```
┌──(jpp㉿kali)-[~]
└─$ grep test /etc/group
test:x:1195489:
```

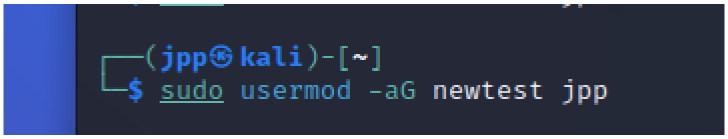
7. Change the group name of the test group to **newtest**.



```
┌──(jpp㉿kali)-[~]
└─$ sudo groupmod -n newtest test
```

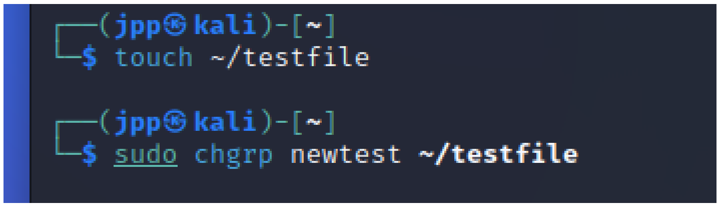
8. Add the current account (xxxxx) as a secondary member of the **newtest** group without overriding

this user's current group membership.



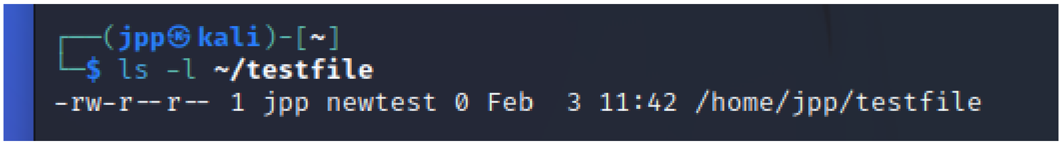
```
┌──(jpp㉿kali)-[~]
└─$ sudo usermod -aG newtest jpp
```

9. Create a new file testfile in the account’s home directory, then change the group owner to **newtest**.



```
┌──(jpp㉿kali)-[~]
└─$ touch ~/testfile

┌──(jpp㉿kali)-[~]
└─$ sudo chgrp newtest ~/testfile
```

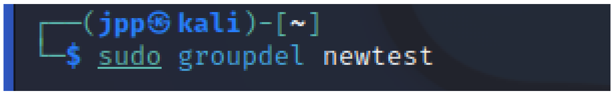
10. Display the user owner and group owner information of the file **testfile**.



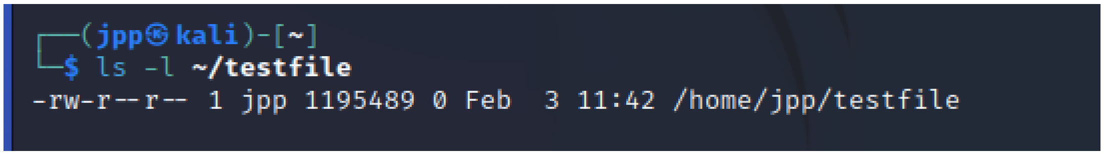
```
┌──(jpp㉿kali)-[~]
└─$ ls -l ~/testfile
-rw-r--r-- 1 jpp newtest 0 Feb  3 11:42 /home/jpp/testfile
```

11. Delete the **newtes**t group, then repeat the previous step. What do you find?

I found that the file testfile no longer has a group owner.

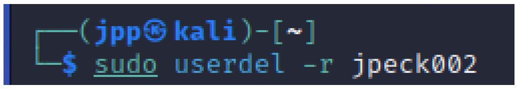


```
┌──(jpp㉿kali)-[~]
└─$ sudo groupdel newtest
```



```
┌──(jpp㉿kali)-[~]
└─$ ls -l ~/testfile
-rw-r--r-- 1 jpp 1195489 0 Feb  3 11:42 /home/jpp/testfile
```

12. Delete the user xxxxx along with the home directory using a single command.



```
┌──(jpp㉿kali)-[~]
└─$ sudo userdel -r jpeck002
```