Jasmyn Wilhelm 02 October 2024

CYSE 270: Linux System for Cybersecurity
Assignment: Lab 4 – User and Group Accounts

Goal:

The goal of this lab is to familiarize students with the fundamental tasks of managing user and group accounts in Linux. By completing this lab, students will gain practical experience in creating, modifying, and deleting accounts, as well as managing group memberships and permissions, which are essential skills in system administration and cybersecurity.

Submission Instructions:

- Complete all tasks in **Task A** and **Task B** on your chosen Ubuntu/Kali VM.
- Take screenshots for each step as evidence of successful command execution.
- Save all your screenshots and results in a single PDF or Word document.
- Ensure that all commands are executed correctly and include detailed explanations for each step taken.

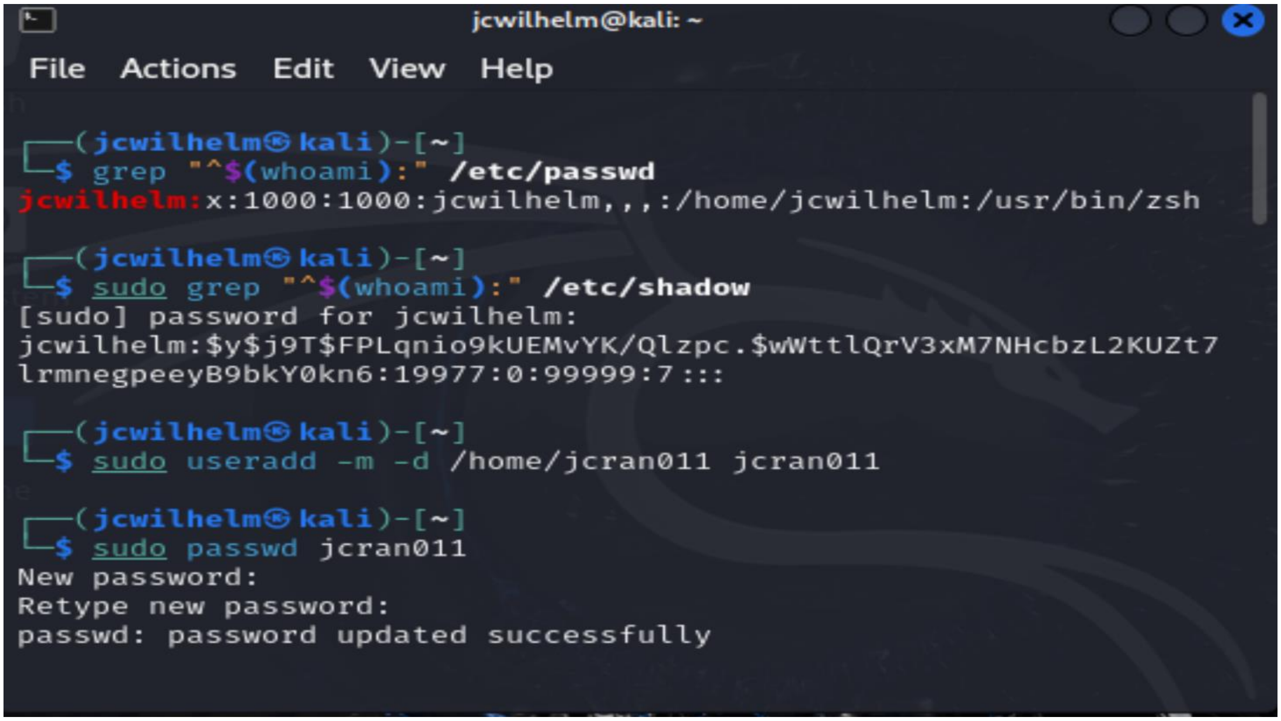
CYSE 270: Linux System for Cybersecurity

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

Jasmyn Wilhelm 02 October 2024

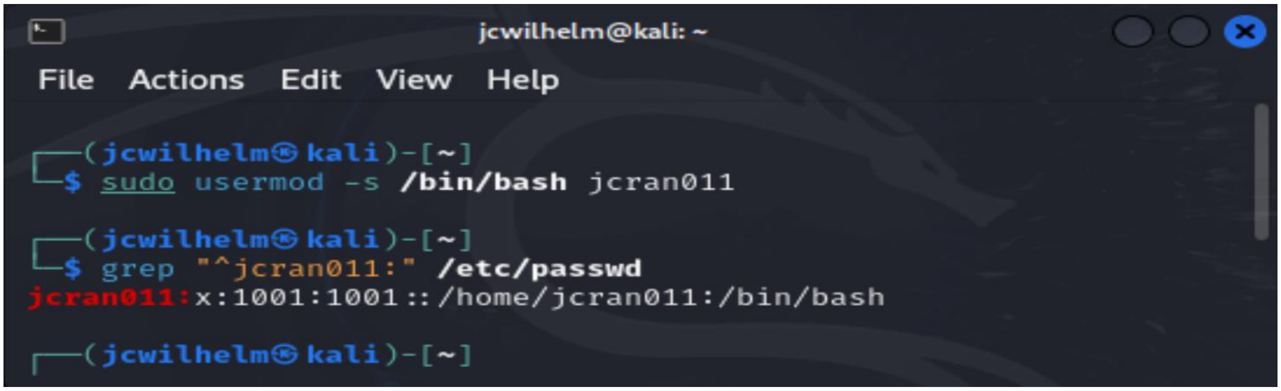
Task A – User Account management (8 * 5 = 40 points)

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.
2. Execute the correct command to display user password information (including the encrypted password and password aging) for the current user using grep.
3. Create a new user named xxxxx and explicitly use options to create the home directory **/home/xxxxx** for this user.
4. Set a password for the new user.



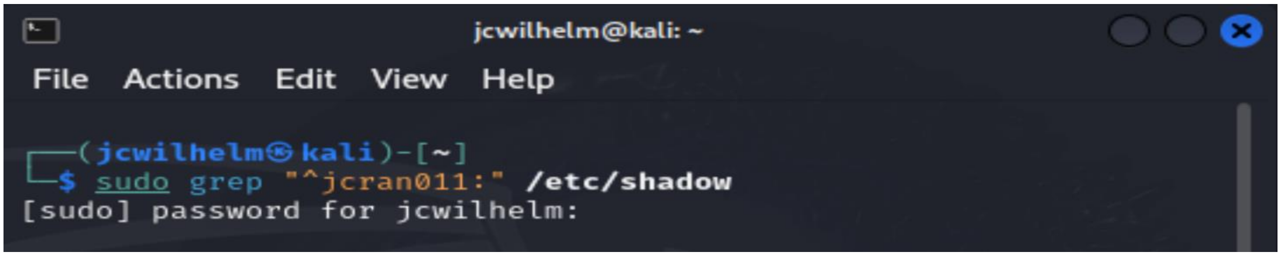
```
┌──(jcwilhelm㉿kali)-[~]
└─$ grep "^$(whoami):" /etc/passwd
jcwilhelm:x:1000:1000:jcwilhelm,,,:/home/jcwilhelm:/usr/bin/zsh

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo grep "^$(whoami):" /etc/shadow
[sudo] password for jcwilhelm:
jcwilhelm:$y$j9T$FPLqnio9kUEMvYK/Qlzpc.$wWttlQrV3xM7NHcbzL2KUZt7
lrmnegpeeyB9bkY0kn6:19977:0:99999:7:::

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo useradd -m -d /home/jcran011 jcran011

┌──(jcwilhelm㉿kali)-[~]
└─$ sudo passwd jcran011
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.



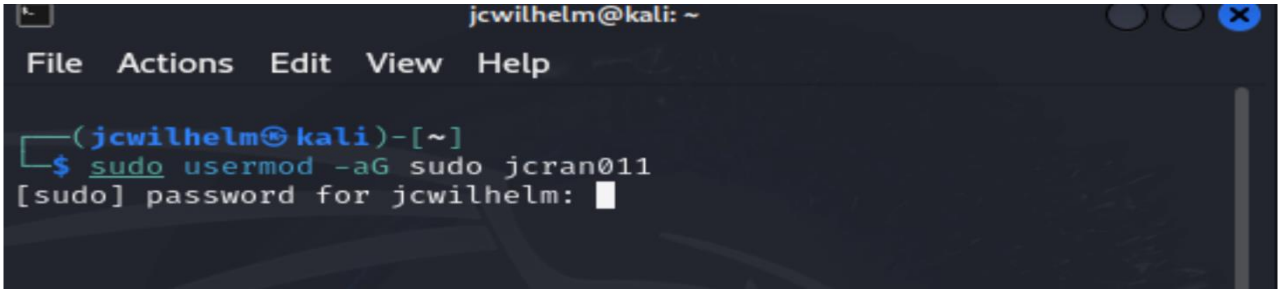
```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo usermod -s /bin/bash jcran011

┌──(jcwilhelm㉿kali)-[~]
└─$ grep "^jcran011:" /etc/passwd
jcran011:x:1001:1001::/home/jcran011:/bin/bash

┌──(jcwilhelm㉿kali)-[~]
```

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



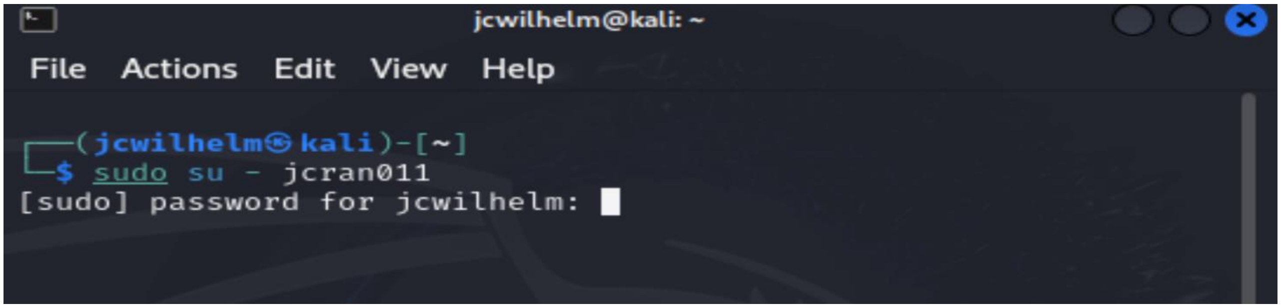
```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo grep "^jcran011:" /etc/shadow
[sudo] password for jcwilhelm:
```

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



```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo usermod -aG sudo jcran011
[sudo] password for jcwilhelm:
```

8. Switch to the new user's account.

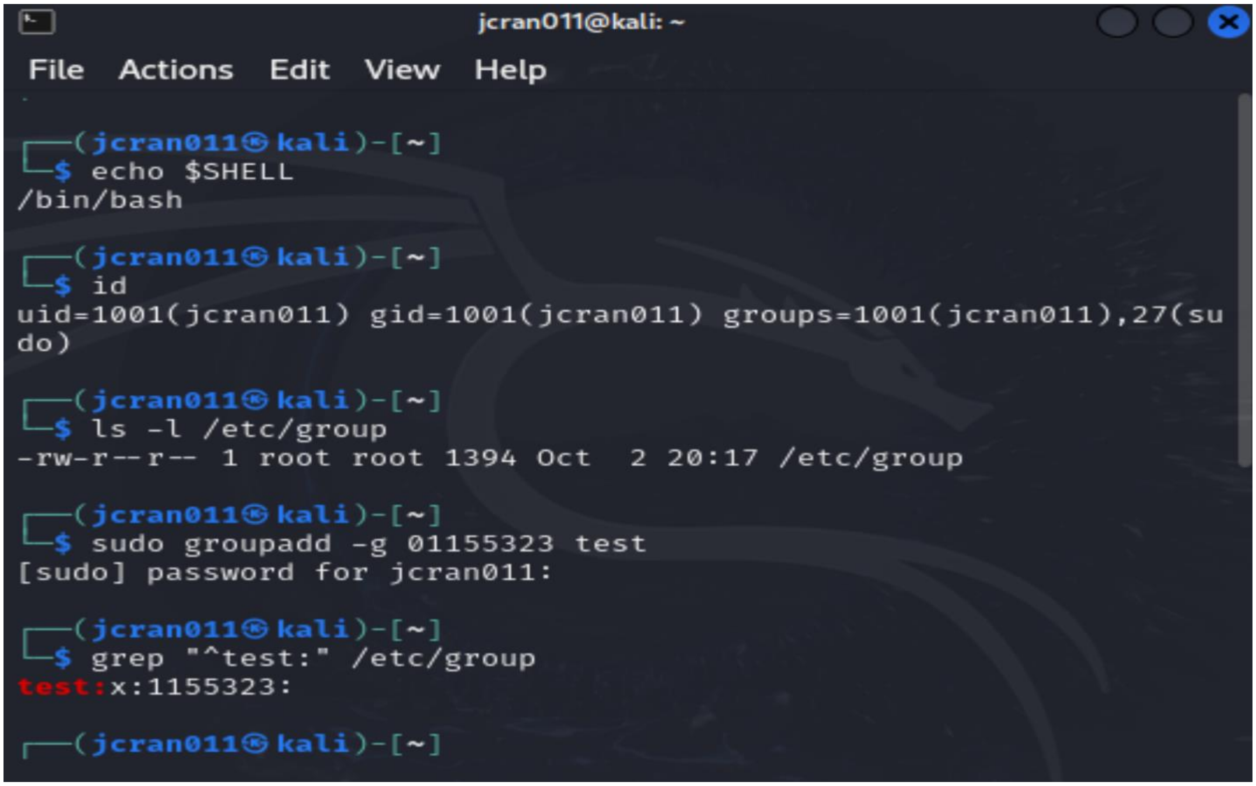


```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo su - jcran011
[sudo] password for jcwilhelm:
```

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

Use Linux commands to execute the following tasks:

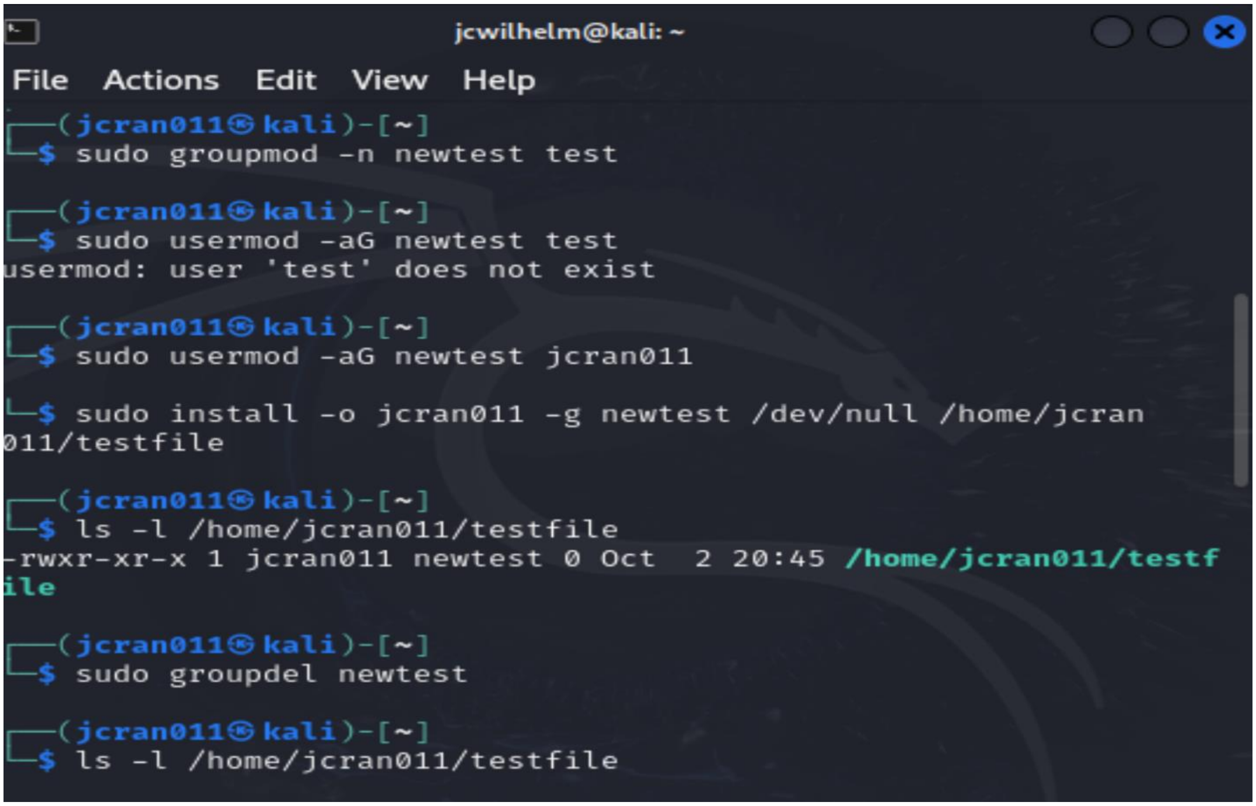
1. Return to your home directory and determine the shell you are using.
2. Display the current user's ID and group membership.
3. Display the group membership of the root account.
4. Run the correct command to determine the user owner and group owner of the /etc/group file.
5. Create a new group named **test** and use your UIN as the GID.



```
┌──(jcran011㉿kali)-[~]
└─$ echo $SHELL
/bin/bash

┌──(jcran011㉿kali)-[~]
└─$ id
uid=1001(jcran011) gid=1001(jcran011) groups=1001(jcran011),27(su
do)

┌──(jcran011㉿kali)-[~]
└─$ ls -l /etc/group
-rw-r--r-- 1 root root 1394 Oct  2 20:17 /etc/group

┌──(jcran011㉿kali)-[~]
└─$ sudo groupadd -g 01155323 test
[sudo] password for jcran011:

┌──(jcran011㉿kali)-[~]
└─$ grep "^test:" /etc/group
test:x:1155323:

┌──(jcran011㉿kali)-[~]
```

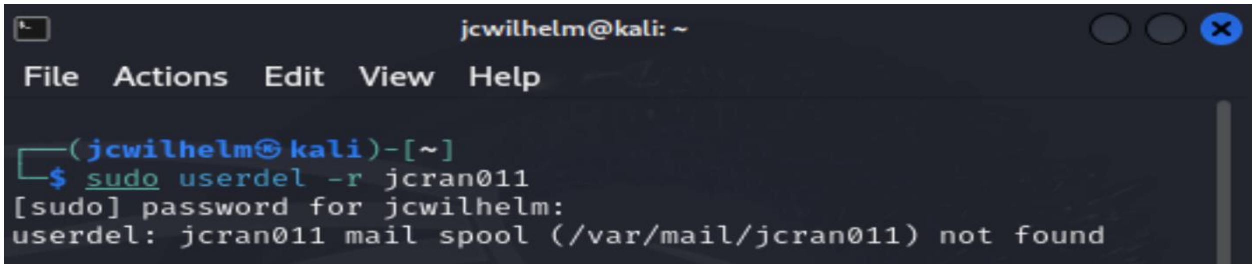
6. Display the group account information for the test group using grep.
7. Change the group name of the test group to **newtest**.
8. Add the current account (xxxxx) as a secondary member of the **newtest** group without overriding this user's current group membership.
9. Create a new file testfile in the account's home directory, then change the group owner to **newtest**.
10. Display the user owner and group owner information of the file **testfile**.

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



```
┌──(jcran011㉿kali)-[~]
└─$ sudo groupmod -n newtest test

┌──(jcran011㉿kali)-[~]
└─$ sudo usermod -aG newtest test
usermod: user 'test' does not exist

┌──(jcran011㉿kali)-[~]
└─$ sudo usermod -aG newtest jcran011

└─$ sudo install -o jcran011 -g newtest /dev/null /home/jcran
011/testfile

┌──(jcran011㉿kali)-[~]
└─$ ls -l /home/jcran011/testfile
-rwxr-xr-x 1 jcran011 newtest 0 Oct  2 20:45 /home/jcran011/testf
ile

┌──(jcran011㉿kali)-[~]
└─$ sudo groupdel newtest

┌──(jcran011㉿kali)-[~]
└─$ ls -l /home/jcran011/testfile
```

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



```
┌──(jcwilhelm㉿kali)-[~]
└─$ sudo userdel -r jcran011
[sudo] password for jcwilhelm:
userdel: jcran011 mail spool (/var/mail/jcran011) not found
```

If attempting to use this command under the user meant to be deleted, an error will occur stating the account is being used in a process even if using the root user. If separate terminals are not used or the terminal of the new account is listed as being terminated, the error will occur. This does not mean the account was not deleted but meant that it was still active at the time of the deletion request. This screenshot represents what happens after the command is entered and the error occurs, showing the account was deleted but could not be completed until the terminal used was closed.

CYSE 270: Lab 4 - User and Group Accounts

2 October 2024

Task A

1. Display user account information (login and home directory) for the Current user using grep, showing the Correct Command.
2. Display user password information (including the encrypted password and aging) for the current user using grep, showing the Correct Command.
3. Create a new user named xxXXx and use options to create the home directory /home/xxxxx for this user.
4. Set a password for the new user
5. Set bash Shell as the default login Shell for the new user xxxxx, then verify.
6. Execute Correct Command to display user password information (include password encrypted and aging) for the new user xxxxx using grep
7. Add the new user xxxxx to Sudo group without overriding the existing group membership.
8. Switch to the new user's account

Task B

1. Return to your home directory and determine the Shell you are using.
2. Display the Current user's ID and group membership.
3. Display the group membership of the root account.
4. Run the Correct Command to determine the user owner and group owner of the /etc/group file
5. Create a new group named test and use your UIN as the GID.
6. Display the group account information for the test group using grep.

Jasmyn Wilhelm ID: 01155323

7. Change the group name of the test group to newtest
8. Add the current account (xxxxx) as a Secondary member of the newtest group without overriding this User's current group membership.
9. Create a new file testfile in the account's home directory, then Change the group owner to newtest.
10. Display the user owner and group owner information of the file testfile.
11. Delete the newtest group, then repeat the previous step. what was found?
12. Delete the user xxxxx along with the home directory using a single command.

```
1. grep "^$(whoami):" /etc/passwd
2. Sudo grep "^$(whoami):" /etc/shadow
3. sudo useradd -m -d /home/Jcran011   Jcran011
4 Sudo passwd Jcran011          Password
5. sudo usermod -s /bin/bash Jcran011 ; grep "^Jcran011:"/etc/passw
6. Sudo grep "^Jran011:" /etc/shadow
7. Sudo usermod -aG Sudo Jran011
8. sudo su - Jcran011
```

```
9. echo $SHELL
10. id
11. id root      or   groups root
12. ls -l /etc/group
13. Sudo groupadd -g 01155323 test
14. grep "^test:" /etc/group
15. sudo groupmod -n newtest test
16. sudo usermod -aG newtest Jcran011
17. Sudo install -o Jcran011 -g newtest /dev/null /home/Jcran011/testfile
18. ls -l /home/Jcran011/testfile
19. sudo groupdel newtest ;ls -l /home/Jcran011/testfile
20. sudo userdel -r Jcran011
```