CYSE 270: Linux System for Cybersecurity

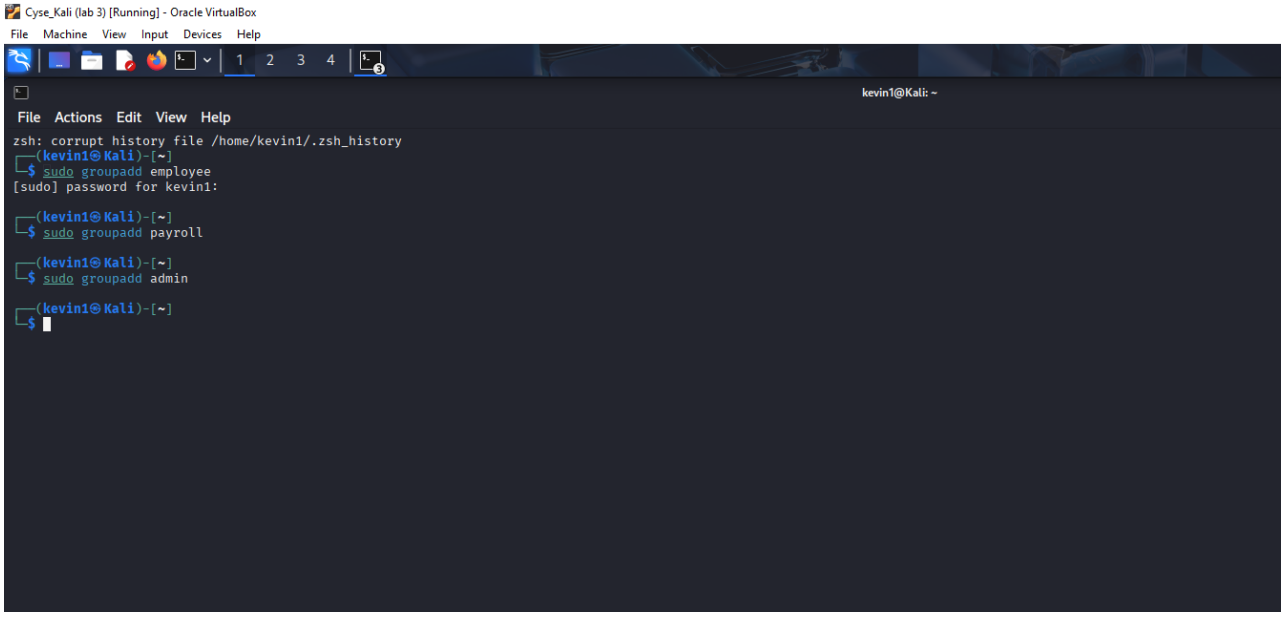
Lab 6 – File Permission

You need to configure the system to allow three users to perform the shared folder actions. Please submit the screenshot for all the steps in a word or pdf file

Task A: Get accounts and groups ready (70 points)

Step 1. Create three groups- **employee**, **payroll**, and **admin**. (You may refer to the slides under Module 2 – Group Management)

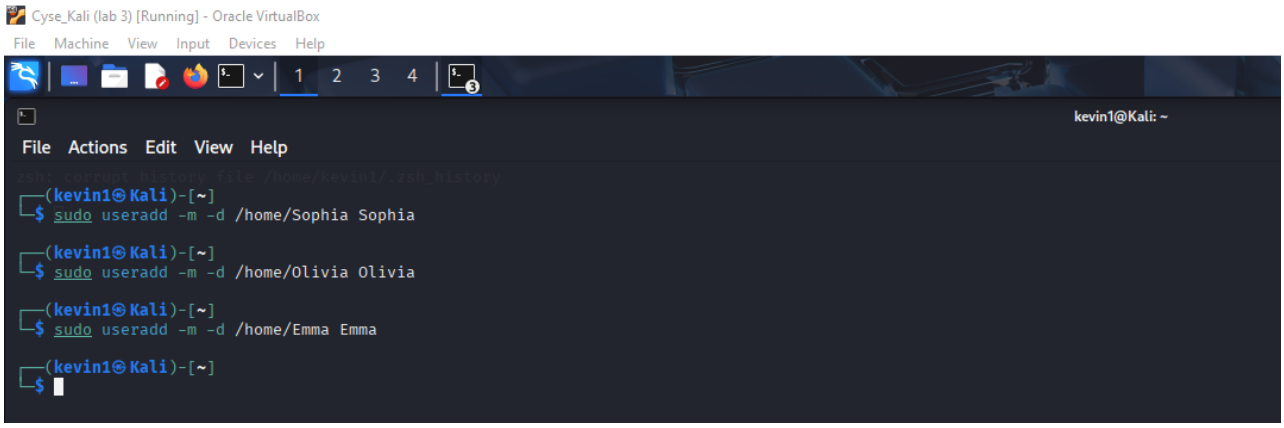
Step 1. To add the three groups, I used “sudo groupadd” to become root user temporally to add the three users.



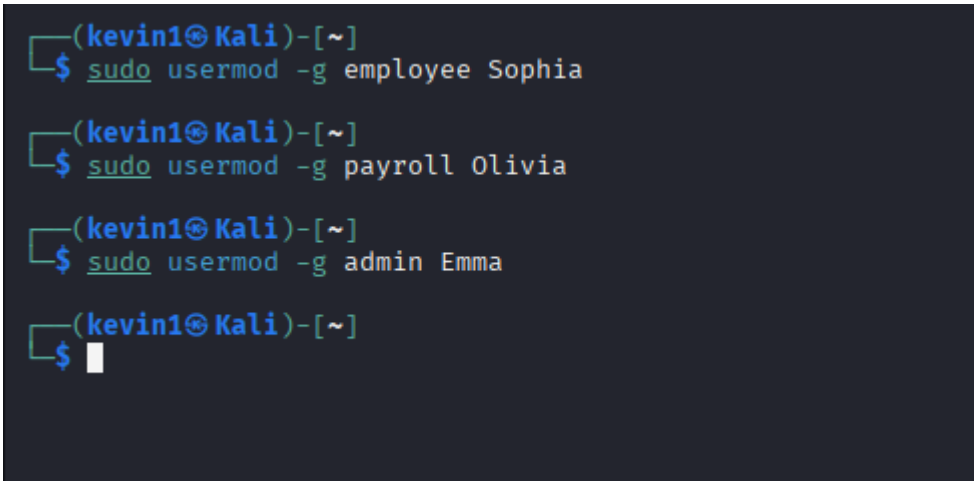
Step 2. Create three user accounts with a specified home directory for **Sophia**, **Olivia**, and **Emma**. Set the primary group for Sophia, Olivia, and Emma to "employee", "payroll", and "admin", respectively.

And change their login shell to /bin/bash. **Don't forget to set their passwords.**

A. “sudo useradd –m –d” would be used to be root user temporally to then add a user with the home directory.



B. "sudo usermod –g" would change the primary group for each of the three users



C. "sudo usermod –s /bin/bash _____ (the three users)" would edit the user information to change their login shell to bin/bash.

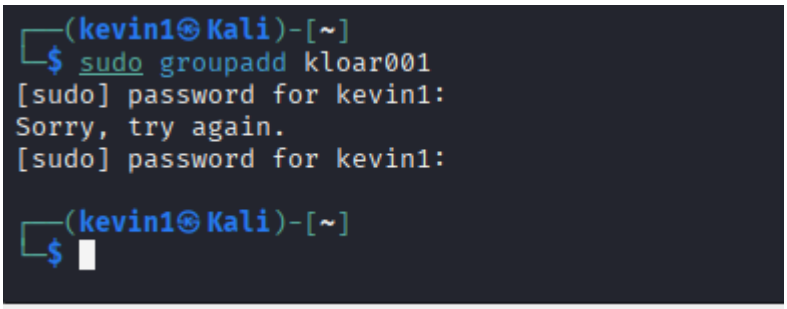
```
┌──(kevin1㉿Kali)-[~]
└─$ sudo usermod -s /bin/bash Sophia

┌──(kevin1㉿Kali)-[~]
└─$ sudo usermod -s /bin/bash Olivia

┌──(kevin1㉿Kali)-[~]
└─$ sudo usermod -s /bin/bash Emma

┌──(kevin1㉿Kali)-[~]
└─$
```

D. "sudo passwd" and the three users would create a password for each specific user.

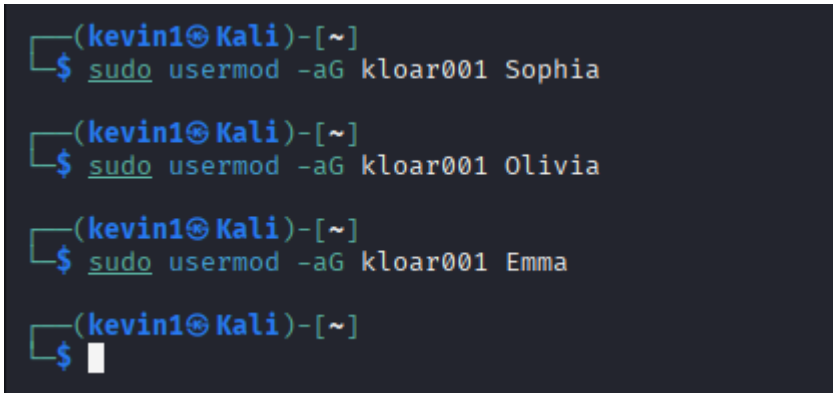
```
┌──(kevin1㉿Kali)-[~]
└─$ sudo passwd Sophia
New password:
Retype new password:
passwd: password updated successfully

┌──(kevin1㉿Kali)-[~]
└─$ sudo passwd Olivia
New password:
Retype new password:
passwd: password updated successfully

┌──(kevin1㉿Kali)-[~]
└─$ sudo passwd Emma
New password:
Retype new password:
passwd: password updated successfully

┌──(kevin1㉿Kali)-[~]
└─$
```

Step 3. Create a shared group called "your_midas" (replace it with your MIDAS name) and set this shared group as the above accounts' secondary group**. After this step, remember to check each user's group profile.**

A. “sudo groupadd kloar001” would create the shared group with my midas name.



B. “sudo usermod –aG kloar001 _____” would add the shared group to the above accounts (and in the blank spot, you would just add each of the users).



C. “id ___” would display each user’s group profile.

```
┌──(kevin1㉿Kali)-[~]
└─$ id Sophia
uid=1013(Sophia) gid=1013(employee) groups=1013(employee),1019(kloar001)

┌──(kevin1㉿Kali)-[~]
└─$ id Olivia
uid=1014(Olivia) gid=1014(payroll) groups=1014(payroll),1019(kloar001)

┌──(kevin1㉿Kali)-[~]
└─$ id Emma
uid=1015(Emma) gid=1015(admin) groups=1015(admin),1019(kloar001)

┌──(kevin1㉿Kali)-[~]
└─$
```

Step 4. Create a directory named /home/cyse_project, which is to be owned by the “your_midas” group which is a shared group). **After this step, remember to check the permission of this shared directory**.

A. “sudo mkdir /home/cyse_project ~/kloar001” would make the directory in the midas shared group.

```
┌──(kevin1㉿Kali)-[~]
└─$ sudo mkdir /home/cyse_project ~/kloar001

┌──(kevin1㉿Kali)-[~]
└─$
```

B. “sudo chgrp kloar001 /home/cyse_project” would make sure that the shared group owns the directory.

```
┌──(kevin1㉿Kali)-[~]
└─$ sudo chgrp kloar001 /home/cyse_project
```

C. “ls -ld /home/cyse_project” would check the permission of the shared directory.

```
┌──(kevin1㉿Kali)-[~]
└─$ ls -ld /home/cyse_project
drwxr-xr-x 2 root kloar001 4096 Oct  7 22:52 /home/cyse_project

┌──(kevin1㉿Kali)-[~]
└─$
```

Step 5. Change the permissions of the /home/cyse_project directory to "**rwxrwx---**" using the octal method so that only the project group members have access to this directory. **After this step, remember to check the permission of this shared directory.**

A. "sudo chmod 770 /home/cyse_project" would change the permission of the home directory to "rwxrwx---".

```
┌──(kevin1㉿Kali)-[~]
└─$ sudo chmod 770 /home/cyse_project

┌──(kevin1㉿Kali)-[~]
└─$
```

B. "ls -ld /home/cyse_project" would check the permission of the shared directory.

```
┌──(kevin1㉿Kali)-[~]
└─$ ls -ld /home/cyse_project
drwxrwx--- 2 root kloar001 4096 Oct  7 22:52 /home/cyse_project

┌──(kevin1㉿Kali)-[~]
└─$
```

Step 6. Switch to Sophia's account. Change the default permissions using octal method with umask command, to "**rw-r-----**" for Sophia when she creates a file or directory. **Check the value of umask, and permission of a new file after this step.**

A. "su - Sophia" would switch to that user account

```
┌──(kevin1㉿Kali)-[~]
└─$ su - Sophia
Password:
┌──(Sophia㉿Kali)-[~]
└─$
```

B. “umask 027” would set the permission to the "rw-r-----".

```
zsh: corrupt history file /home/kevin1/.zsh_history
┌──(Sophia㉿Kali)-[~]
└─$ umask 027

┌──(Sophia㉿Kali)-[~]
└─$
```

C. “touch file1” and then “umask” & “ls -ld file1” creates the file, displays the umask value, and shows permissions.

```
┌──(Sophia㉿Kali)-[~]
└─$ touch file1

┌──(Sophia㉿Kali)-[~]
└─$ umask
0027

┌──(Sophia㉿Kali)-[~]
└─$ ls -ld file1
-rw-r----- 1 Sophia employee 0 Oct  7 23:11 file1

┌──(Sophia㉿Kali)-[~]
└─$
```

Step 7. Create a new file called "Sophia_homework" in the home directory of Sophia and put your name in the file as content. **After this step, remember to check the content and the permission of the new file. (ls -l Sophia_homework)**

A. “touch Sophia_homework” creates the file.

```
┌──(Sophia㉿Kali)-[~]
└─$ touch Sophia_homework

┌──(Sophia㉿Kali)-[~]
└─$
```

B. “vim Sophia_homework” would allow me to edit the file in which I had put my name in.

```
┌──(Sophia㉿Kali)-[~]
└─$ vim Sophia_homework

┌──(Sophia㉿Kali)-[~]
└─$
```

C. “cat Sophia_homework” & “ls -l Sophia_homework” checks the content in the file and the permission of the file.

```
┌──(Sophia㉿Kali)-[~]
└─$ cat Sophia_homework
Kevin

┌──(Sophia㉿Kali)-[~]
└─$ ls -l Sophia_homework
-rw-r----- 1 Sophia employee 6 Oct  7 23:29 Sophia_homework

┌──(Sophia㉿Kali)-[~]
└─$
```

Step 8. Copy "Sophia_homework" to the /home/cyse_project directory**. After this step, remember to check the permission of the file in the shared directory.**

A. “cp Sophia_homework /home/cyse_project” would copy the file to the shared directory.

```
┌──(Sophia㉿Kali)-[~]
└─$ cp Sophia_homework /home/cyse_project

┌──(Sophia㉿Kali)-[~]
└─$
```

B. “ls -al /home/cyse_project” would display all the files in the shared directory which would show Sophia_homework.

```
zsh: corrupt history file /home/kevini/.zsh_history
┌──(Sophia㉿Kali)-[~]
└─$ ls -al /home/cyse_project
total 12
drwxrwx---  2 root   kloar001 4096 Oct  7 23:33 .
drwxr-xr-x 20 root   root     4096 Oct  7 22:52 ..
-rw-r-----  1 Sophia employee    6 Oct  7 23:33 Sophia_homework

┌──(Sophia㉿Kali)-[~]
└─$
```

Step 9. Switch to Emma's account. Try to read "Sophia_homework" in the /home/cyse_project Directory.

A. "su - Emma" would go to Emma's account

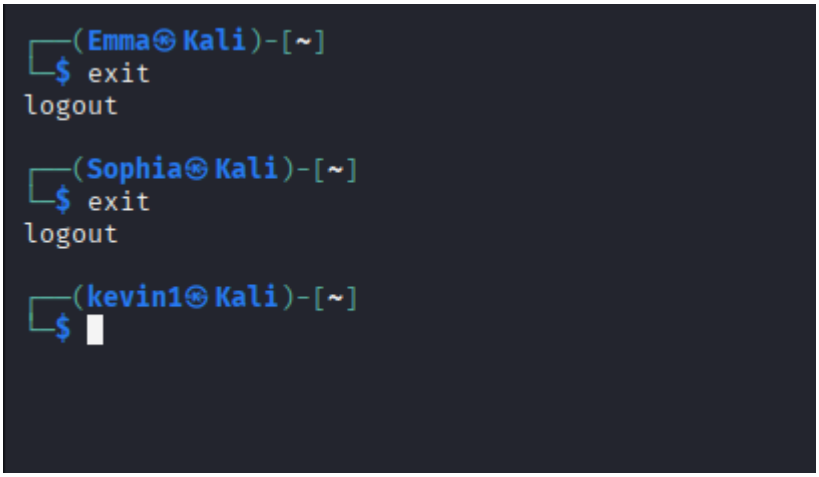
```
┌──(Sophia㉿Kali)-[~]
└─$ su - Emma
Password:
┌──(Emma㉿Kali)-[~]
└─$
```

B. "cat /home/cyse_project/Sophia_homework" would be the command to try to read the file but since we don't have permission, it is denied.

```
┌──(Emma㉿Kali)-[~]
└─$ cat /home/cyse_project/Sophia_homework
cat: /home/cyse_project/Sophia_homework: Permission denied

┌──(Emma㉿Kali)-[~]
└─$
```

Step 10. Exit out of Emma's account and Sophia's account.

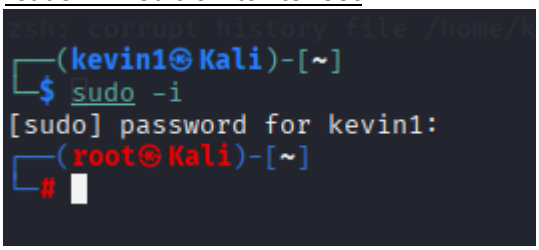
Using the command "exit" for both accounts exits it.



Task B: Set SGID permission (15 points)

Step 1. Switch to root or the regular user's account. To allow group members to access the files shared in the shared directory, you need to fix the sharing issue by setting the correct **SGID** group values to **/home/cyse_project** directory.

A. "sudo -i" would switch to root



B. "chmod g+s /home/cyse_project" would allow others to see the files in the shared directory.

```
┌──(root㉿Kali)-[~]
└─# chmod g+s /home/cyse_project

┌──(root㉿Kali)-[~]
└─#
```

Step 2. Switch to Sophia's account. Copy "Sophia_homework" to the /home/cyse_project directory as "Sophia_homework**2**".

A. "su - Sophia" would switch to that account.

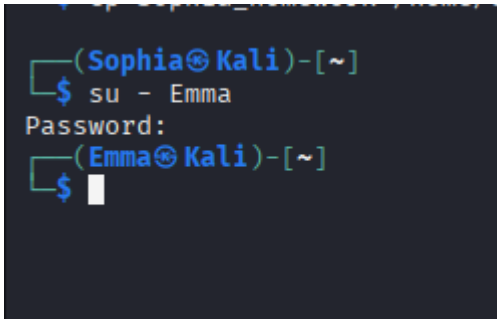
```
┌──(root㉿Kali)-[~]
└─# su - Sophia
┌──(Sophia㉿Kali)-[~]
└─$
```

B. "cp Sophia_homework Sophia_homework2" & "cp Sophia_homework2 /home/cyse_project" would copy the first file to a new name in the /home/cyse_project directory.

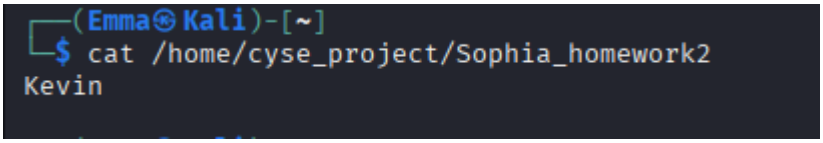
```
┌──(Sophia㉿Kali)-[~]
└─$ cp Sophia_homework Sophia_homework2

┌──(Sophia㉿Kali)-[~]
└─$ cp Sophia_homework2 /home/cyse_project

┌──(Sophia㉿Kali)-[~]
└─$
```

Step 3. Switch to Emma's account. Try to read "Sophia_ homework2" in the /home/cyse_project directory.

A. "su - Emma" would switch to Emma's account.



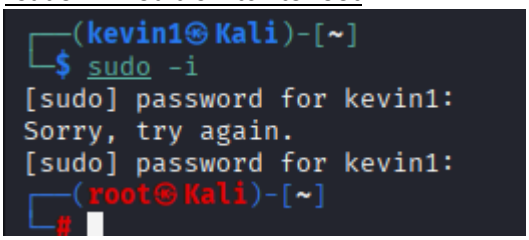
B. "cat /home/cyse_project/Sophia_homework2" reads the file.



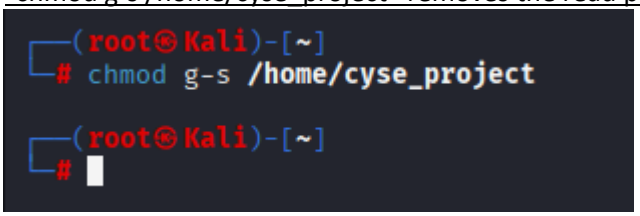
Task C: Unset SGID permissions (15 points)

Step 1. Switch to root the regular user's account. To disallow group members to access the files in the shared folder, you need to fix the sharing issue by setting the correct **SGID** group values to **/home/cyse_project** directory to remove the group user read permission.

A. "sudo -i" would switch to root

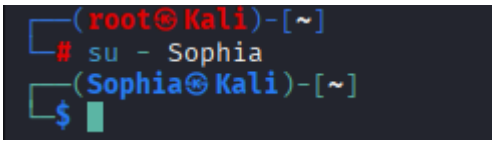


B. "chmod g-s /home/cyse_project" removes the read permissions.

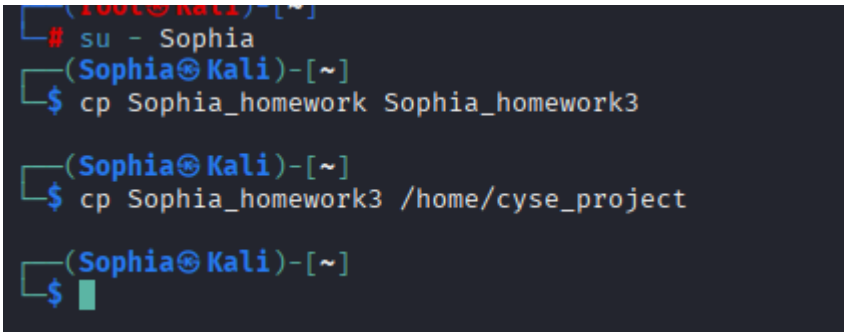


Step 2. Switch to Sophia's account. Copy "Sophia_homework" to the /home/cyse_project directory as "Sophia_homework3".

A. "su - Sophia" would switch to that account

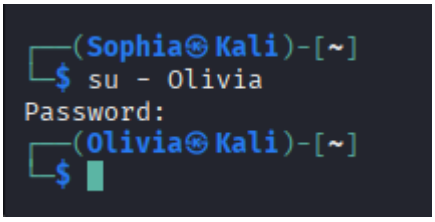


B. "cp Sophia_homework Sophia_homework3" & "cp Sophia_homework3 /home/cyse_project" would copy the file into the new file into that directory.

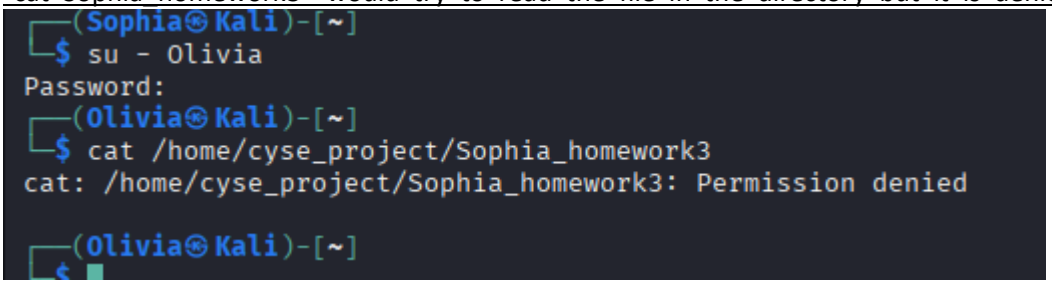


Step 3. Switch to Olivia's account. Try to read "Sophia_home3" in the /home/cyse_project directory.

A. "su - Olivia" would switch to that account.



B. "cat Sophia_homework3" would try to read the file in the directory but it is denied this time.

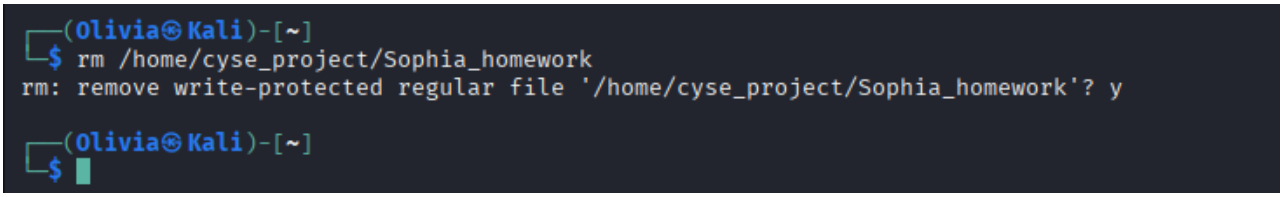


Extra credit: Sticky Bit (10 points)

Step 1. Switch to Olivia' account. Delete "Sophia_ homework" in the /home/cyse_project directory.

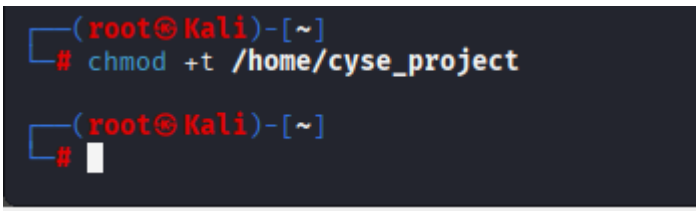
A. "su - Olivia" would switch to that account.

B. "rm /home/cyse_project/Sophia_homework" removes the file.



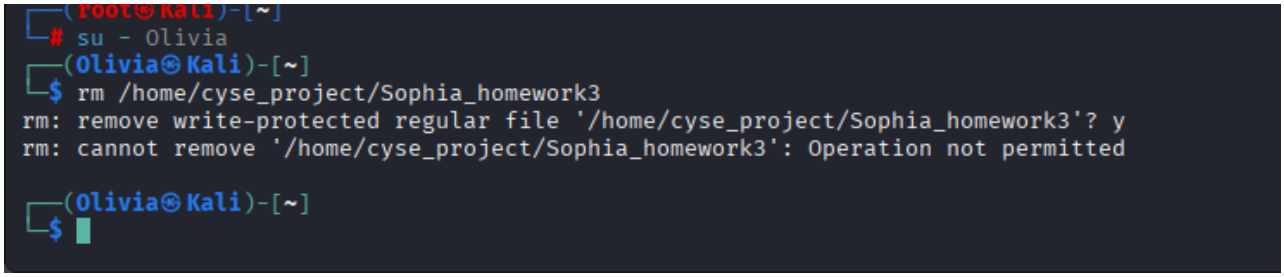
Step 2. Switch to root account. Set the sticky bit permission, to make files can only be removed by the owner of the file.

A. "chmod +t /home/cyse_project" adds the sticky bit permission.



Step 3. Switch to Olivia' account. Try to delete "Sophia_ homework3" in the /home/cyse_project directory. Can you delete it this time? Why?

This time it does not allow us to remove the file since we change it in the last step, so that only the owner can do it.



Reflection

After completing the lab, I learned how to add new users, create a password for them, etc. The information is very useful as this could be replicated in real life to edit the different user's permission depending on the group that they're placed in. There were some challenges when completing the lab such as when I placed some of the users in the wrong spot or setting the wrong number in "chmod" for them to read the files.