CYSE 270: Linux System for Cybersecurity

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.

Step 1. Create three groups- employee, payroll, and admin. (You may refer to the slides for week-4 – Group Management)

To create the three groups, I used the sudo groupadd command to create the employee, payroll, and admin groups.

```
┌──(sulaiman㉿kali)-[~]
└─$ sudo groupadd employee

┌──(sulaiman㉿kali)-[~]
└─$ sudo groupadd payroll

┌──(sulaiman㉿kali)-[~]
└─$ sudo groupadd admin
```

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.

I used the sudo useradd -m -k /etc/skel command to create each user. To set the passwords, I used the sudo passwd command to set the password for each user. Next, to change their login shell, I used the sudo usermod -s /bin bash command for each user. For the final part, I used the sudo usermod -g command to set the primary group of each user to employee, payroll, and admin respectively.

```
zsh: corrupt history file /home/sulaiman/.zsh_history
┌──(sulaiman㉿kali)-[~]
└─$ sudo useradd -m -k /etc/skel Sophia
[sudo] password for sulaiman:
Sorry, try again.
[sudo] password for sulaiman:

┌──(sulaiman㉿kali)-[~]
└─$ sudo useradd -m -k /etc/skel Olivia

┌──(sulaiman㉿kali)-[~]
└─$ sudo useradd -m -k /etc/skel Emma

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

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

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

```
┌──(sulaiman㉿kali)-[~]
└─$ tail -3 /etc/passwd
Sophia:x:1001:1001::/home/Sophia:/bin/sh
Olivia:x:1002:1002::/home/Olivia:/bin/sh
Emma:x:1003:1003::/home/Emma:/bin/sh

┌──(sulaiman㉿kali)-[~]
└─$ sudo usermod -s /bin/bash Sophia

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

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

┌──(sulaiman㉿kali)-[~]
└─$ tail -3 /etc/passwd
Sophia:x:1001:1001::/home/Sophia:/bin/bash
Olivia:x:1002:1002::/home/Olivia:/bin/bash
Emma:x:1003:1003::/home/Emma:/bin/bash
```

```
┌──(sulaiman㉿kali)-[~]
└─$ sudo groupadd employee

┌──(sulaiman㉿kali)-[~]
└─$ sudo groupadd payroll

┌──(sulaiman㉿kali)-[~]
└─$ sudo groupadd admin

┌──(sulaiman㉿kali)-[~]
└─$ sudo usermod -g employee Sophia

┌──(sulaiman㉿kali)-[~]
└─$ sudo usermod -g payroll Olivia

┌──(sulaiman㉿kali)-[~]
└─$ sudo usermod -g admin Emma
```

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

I created a shared group called msula001 using the sudo groupadd msula001 command and set it up as the secondary group for the created users using the sudo usermod -aG msula001 command for each user. I used the id Sophia, id Emma and id Olivia commands to verify changes.

```
┌──(sulaiman㉿kali)-[~]
└─$ sudo groupadd msula001

┌──(sulaiman㉿kali)-[~]
└─$ sudo usermod -aG msula001 Sophia

┌──(sulaiman㉿kali)-[~]
└─$ sudo usermod -aG msula001 Olivia

┌──(sulaiman㉿kali)-[~]
└─$ sudo usermod -aG msula001 Emma
```

```
┌──(sulaiman㉿kali)-[~]
└─$ id Sophia
uid=1001(Sophia) gid=1004(employee) groups=1004(employee),1007(msula001)

┌──(sulaiman㉿kali)-[~]
└─$ id Olivia
uid=1002(Olivia) gid=1005(payroll) groups=1005(payroll),1007(msula001)

┌──(sulaiman㉿kali)-[~]
└─$ id Emma
uid=1003(Emma) gid=1006(admin) groups=1006(admin),1007(msula001)
```

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.

To create the /home/cyse_project directory, I used the sudo mkdir /home/cyse_project command and to change the ownership, I used the sudo chgrp msula001 /home/cyse_project command. Finally, to check the permission, I used the ls -ld /home/cyse_project command.

```
┌──(sulaiman㉿kali)-[~]
└─$ sudo mkdir /home/cyse_project
[sudo] password for sulaiman:

┌──(sulaiman㉿kali)-[~]
└─$ sudo chgrp msula001 /home/cyse_project

┌──(sulaiman㉿kali)-[~]
└─$ ls -ld /home/cyse_project
drwxr-xr-x 2 root msula001 4096 Feb 20 16:56 /home/cyse_project
```

Step 5. Change the permissions of the /home/cyse_project directory to "drwxrwx---" 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.

To change the permission of the /home/cyse_project directory to drwxrwx---, I used the octal method using the sudo chmod 770 /home/cyse_project command and to check the changes I used the ls -ld /home/cyse_project command.

```
┌──(sulaiman㉿kali)-[~]
└─$ ls -ld /home/cyse_project
drwxr-xr-x 2 root msula001 4096 Feb 20 16:56 /home/cyse_project

┌──(sulaiman㉿kali)-[~]
└─$ sudo chmod 770 /home/cyse_project
[sudo] password for sulaiman:

┌──(sulaiman㉿kali)-[~]
└─$ ls -ld /home/cyse_project
drwxrwx--- 2 root msula001 4096 Feb 20 16:56 /home/cyse_project
```

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

I used the su Sophia command to switch to Sophia's account and changed the default permission using the umak 027 command.

```
┌──(Sophia㉿kali)-[~]
└─$ umask 027

┌──(Sophia㉿kali)-[~]
└─$ umask
0027
```

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)

To create a file, I used the touch Sophia_homework command and added my name as content using the echo "Sulaiman." >> Sophia_homework command. Finally, to check the content I used the cat Sophia_homwork command. I revealed the permission using the ld -l Sophia_homework command.

```
┌──(Sophia㉿kali)-[/home/cyse_project]
└─$ ls

┌──(Sophia㉿kali)-[/home/cyse_project]
└─$ touch Sophia_homework

┌──(Sophia㉿kali)-[/home/cyse_project]
└─$ echo "Sulaiman." >> Sophia_homework

┌──(Sophia㉿kali)-[/home/cyse_project]
└─$ cat Sophia_homework
Sulaiman.

┌──(Sophia㉿kali)-[/home/cyse_project]
└─$ ls -l
total 4
-rw-r----- 1 Sophia employee 10 Feb 21 17:32 Sophia_homework

┌──(Sophia㉿kali)-[/home/cyse_project]
└─$ ls -l Sophia_homework
-rw-r----- 1 Sophia employee 10 Feb 21 17:32 Sophia_homework
```

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.

I used the cp command to copy Sophia_homework to the /home/cyse_project. And to check the permission, I used the ld -l command.

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

I switched to Emma's account using the su Emma command. I tried reading the file using the cat /home/cyse_project/Sophia_homework but the permission was denied.

```
┌──(Sophia㉿kali)-[~]
└─$ su Emma
Password:
┌──(Emma㉿kali)-[/home/Sophia]
└─$ cat Sophia_homework

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

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

I exited from both accounts using the exit command.

Task B: Set SGID permission (15 points)

Step 1. Switch to the root account. To allow group members to access this file, you need to fix the sharing issue by setting the correct SGID group values to /home/cyse_project directory, to give the group users read permission.

I used the sudo chmod g+s /home/cyse_project command to give the group read permission.

```
┌──(sulaiman㉿kali)-[~]
└─$ sudo chmod g+s /home/cyse_project

┌──(sulaiman㉿kali)-[~]
└─$ ls -ld /home/cyse_project
drwxrws--- 2 root msula001 4096 Feb 21 17:31 /home/cyse_project
```

Step 2. Switch to Sophia's account. Copy "Sophia_homework" to the /home/cyse_project directory as "Sophia_homework2".

I copied the file using the cp command and named it Sophia_homework1.

```
-rw-r----- 1 Sophia employee 10 Feb 21 17:32 Sophia_homework
-rw-r----- 1 Sophia msula001 10 Feb 22 14:55 Sophia_homework1
```

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

I switched to Emma's account using the su Emma command and to read the file, I used the ls -l followed by cat Sophia_homework1 and I was able to read the content.

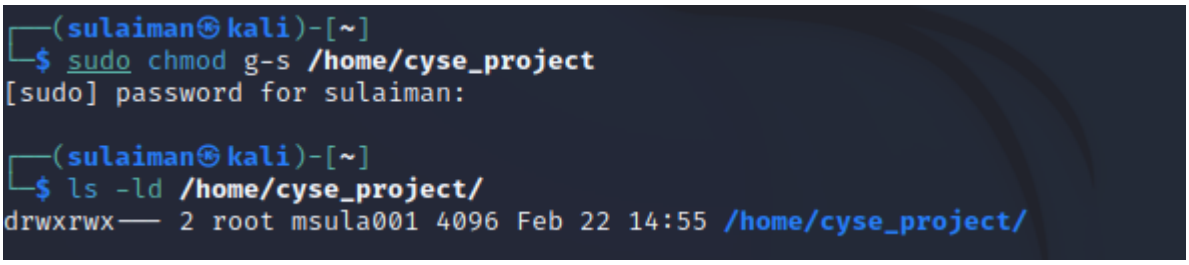
```
┌──(Emma㉿kali)-[/home/cyse_project]
└─$ ls -l
total 8
-rw-r----- 1 Sophia employee 10 Feb 21 17:32 Sophia_homework
-rw-r----- 1 Sophia msula001 10 Feb 22 14:55 Sophia_homework1

┌──(Emma㉿kali)-[/home/cyse_project]
└─$ cat Sophia_homework1
Sulaiman.
```

Task C: Unset SGID permissions (15 points)

Step 1. Switch to root 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.

I removed the SGID permissions using the sudo chmod g-s /home/cyse_project command.



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

I copied the document using the cp command to /home/cyse_project and named it as Sophia_homework3.

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

I switched to Olivia's account using the su command and was not able to read the file. "permission denied."

CYSE 270: Linux System for Cybersecurity

Extra credit: Sticky Bit (10 points)

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

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

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