OLD DOMINION UNIVERSITY

CYSE 270 LINUX SYSTEM FOR CYBERSECURITY

Assignment #6 File Permission

John Wilson

01179411

CYSE 270 Assignment #6 File Permission

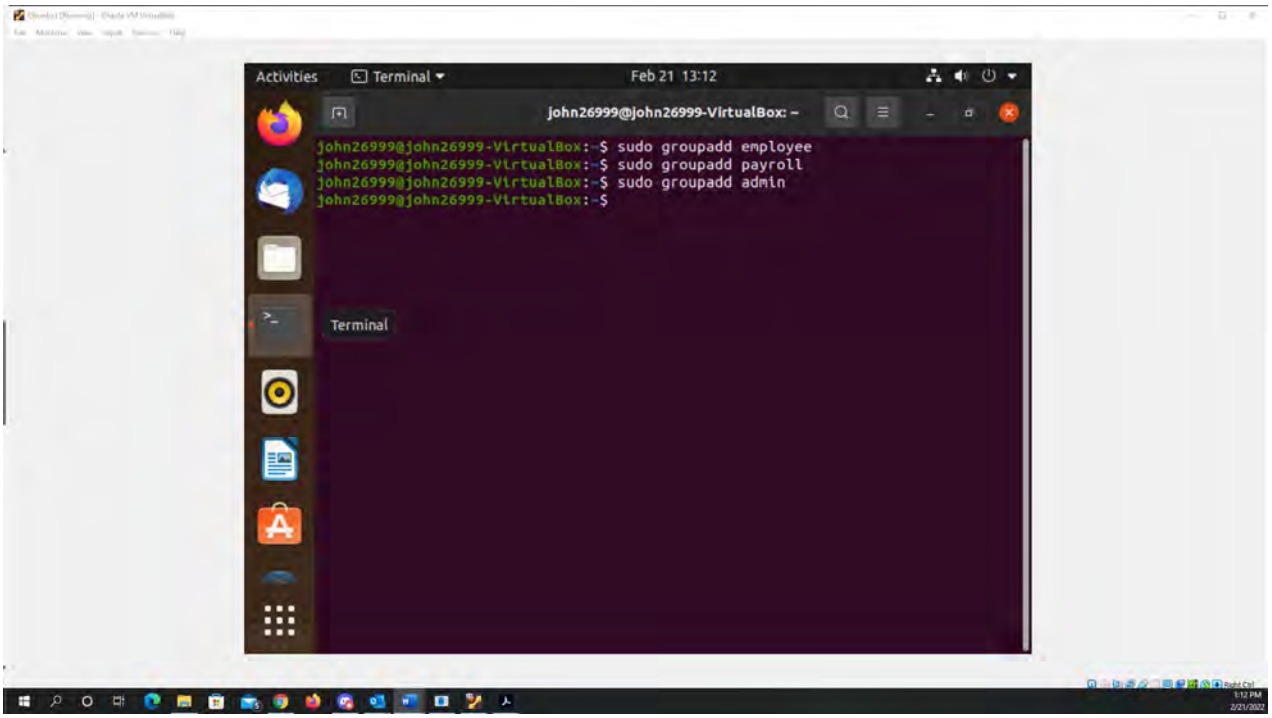
Below is the snippet of a sample lab report.

TASK A:

GET ACCOUNTS AND GROUPS READY

- You need to configure the system to allow three users to perform the shared folder actions.

Step 1. Create three groups, employee, payroll, and admin.



CYSE 270 Assignment #6 File Permission

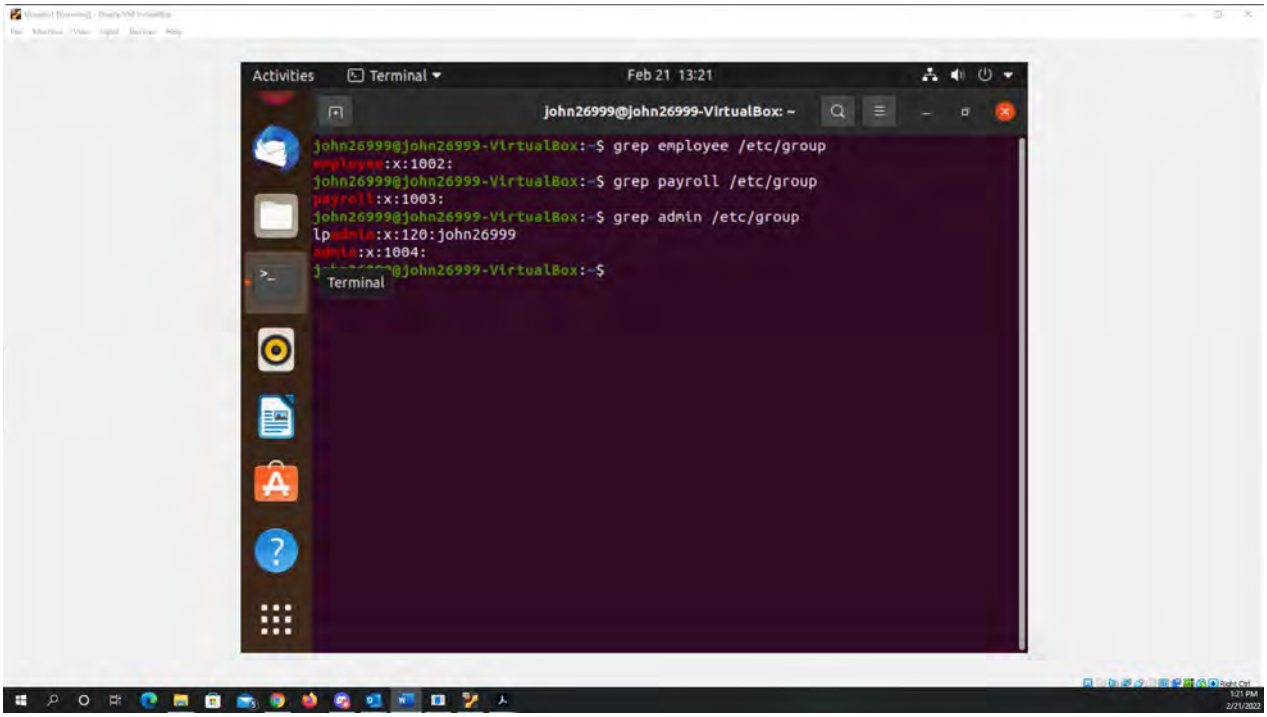


Figure 1 Screenshots of JWILS082 Computer screen for Step 1.

Above is the screen shot using the commands “sudo groupadd XXXXX[1]” three times to add new groups. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “groupadd” is the command adds a group. “XXXXX” is the new group name.

In the second screenshot of Step 1, I then decided to execute the the command “grep XXXXX /etc/group” to validate the the group account information for all three groups (employee, payroll, admin) were implemented correctly.

[1] To keep from writing redundant information in Step 1, when you see “XXXXX” this is actually replaced with the group names of employee, payroll, and admin.

CYSE 270 Assignment #6 File Permission

Step 2.

a. Create three user accounts with a specified home directory for Sophia, Olivia, and Emma.

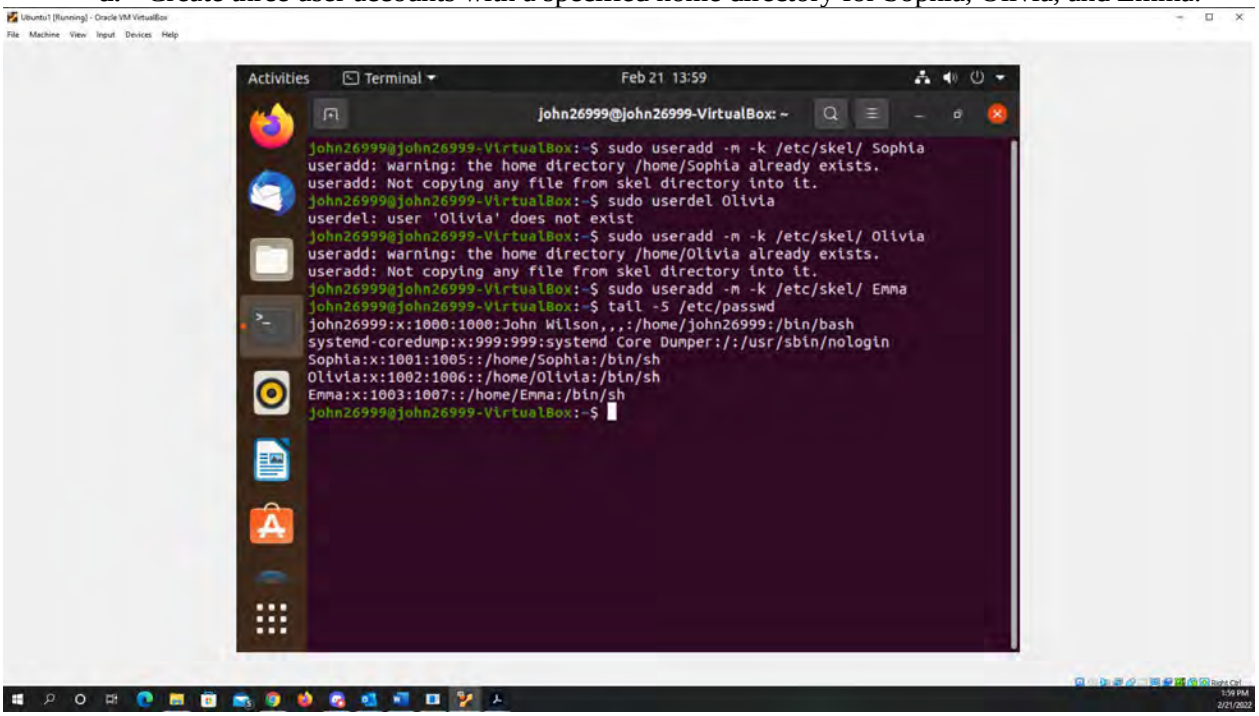


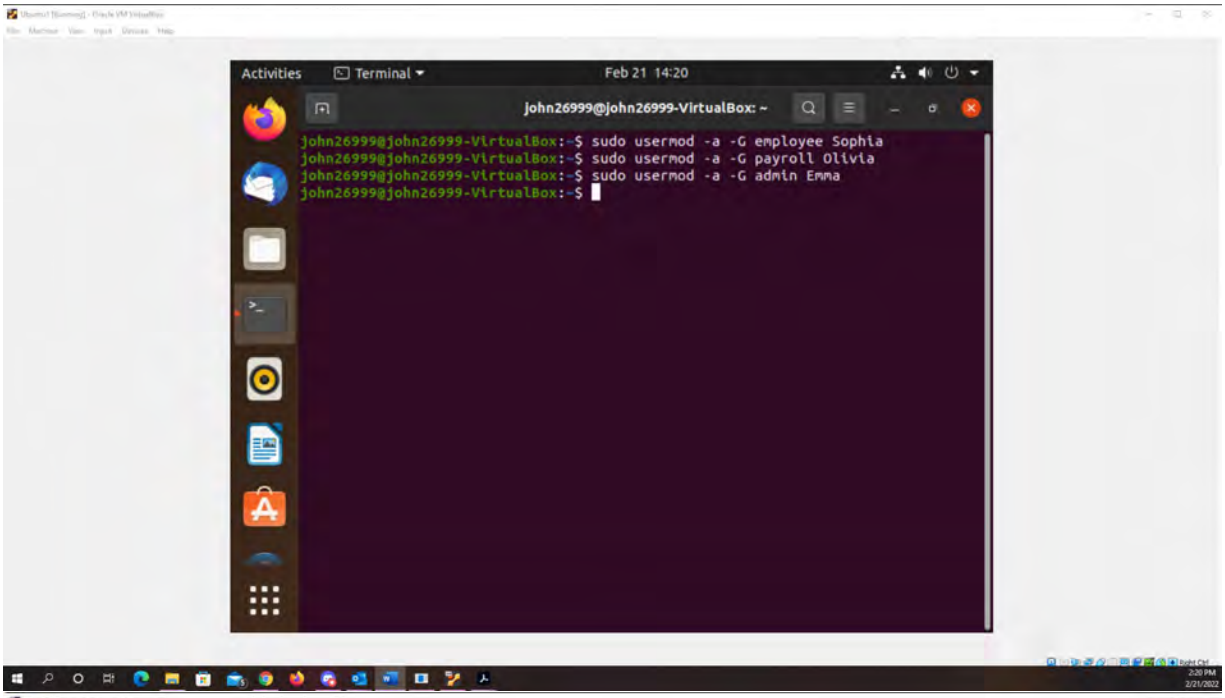
Figure 2 Screenshots of JWILS082 Computer screen for Step 2.a.

Above is the screen shot using the command “sudo useradd -m -k /etc/skel YYYYY[2]” to create a new user with a home directory. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “useradd” is the command that adds a new user profile to the system. “-m” is the command that creates the new user’s home directory. “-k” is the command the uses this skeleton directory. “/etc/skel” is where the users home directotry is located. “YYYYY” is the name of the new user added. In sddition, I also used the command “tail -5 /etc/passwd” to prove the new user account was created with a home directory.

b. Set the primary group for Sophia, Olivia, and Emma to "employee", "payroll", and "admin", respectively.

[2] To keep from writing redundant information in Step 2.a., when you see “YYYYY” this is actually replaced with the user names of Sophia, Olivia, and Emma.

CYSE 270 Assignment #6 File Permission



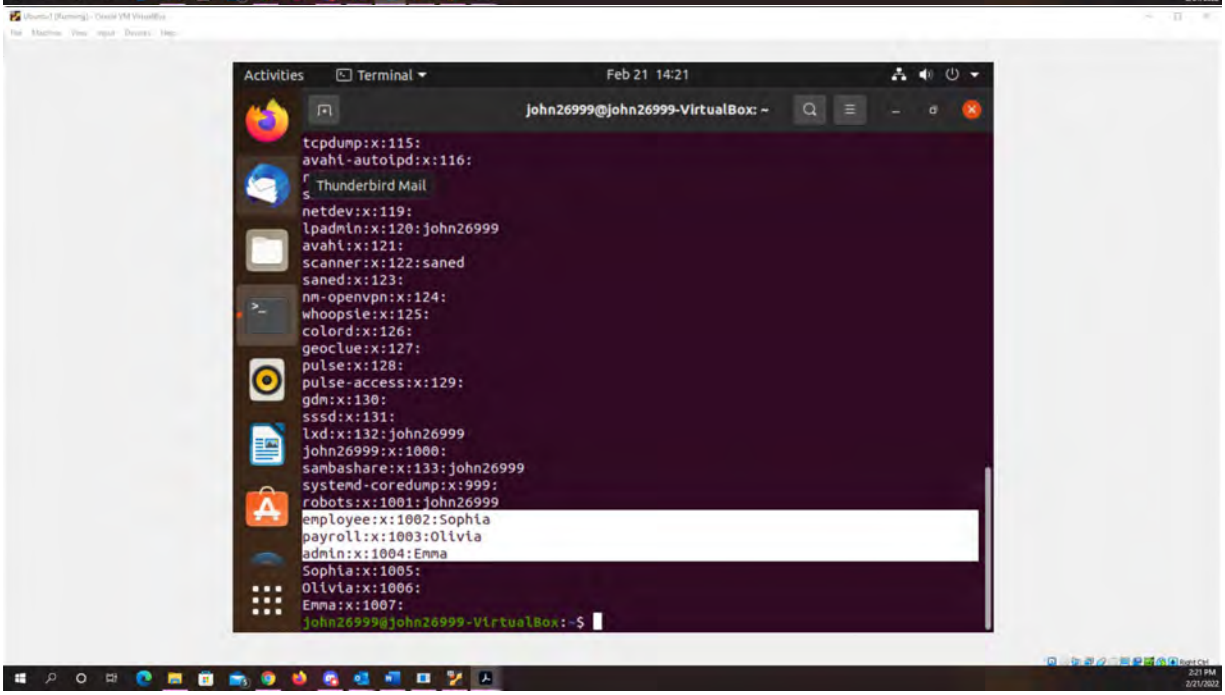


Figure 3 Screenshots of JWILS082 Computer screen for Step 2.b.

Above is the screenshot of the command " sudo usermod -a -G XXXXX[3] YYYYY[4]" that adds the new user to the sudo group without overriding the existing members with the sudo group. "sudo" is the

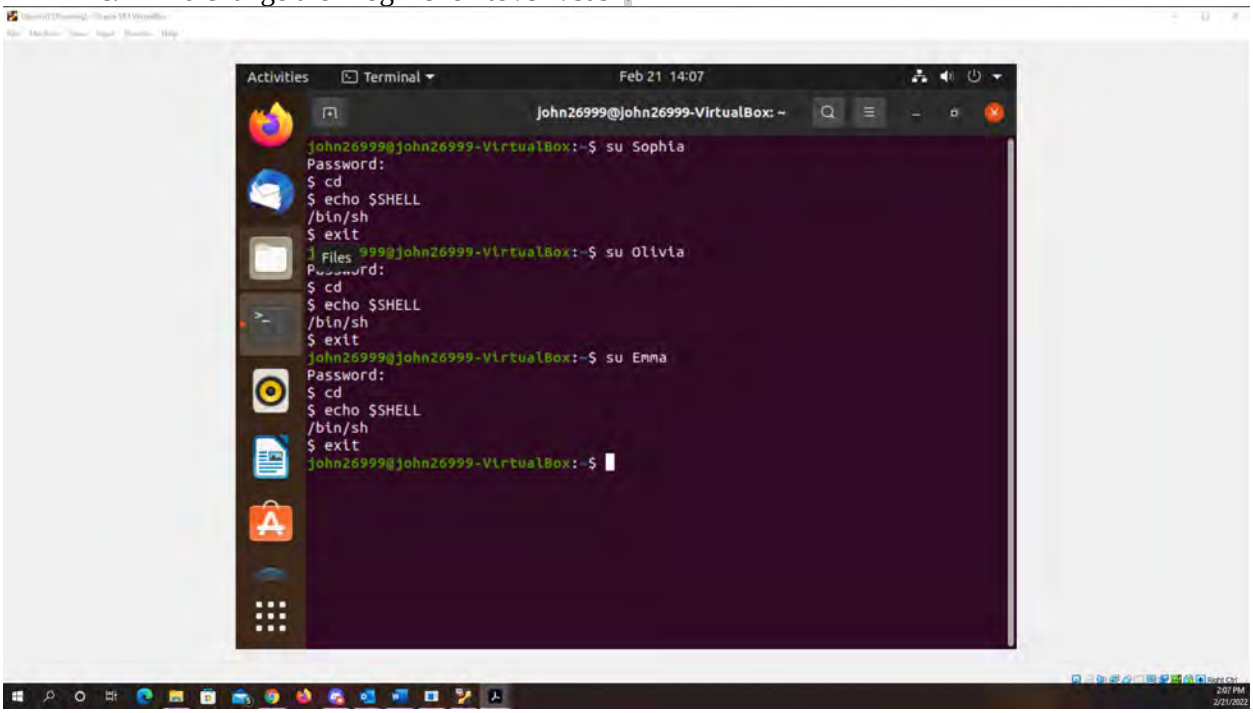
[3] To keep from writing redundant information in Step 1, when you see "XXXXX" this is actually replaced with the group names of employee, payroll, and admin.

[4] To keep from writing redundant information in Step 2.b., when you see "YYYYY" this is actually replaced with the user names of Sophia, Olivia, and Emma.

command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “usermod” is the command that modifies changes to a user. “-a” is the command to append a user to supplemental groups without removing the user from other groups. “-G” new list of supplementary GROUPS. “XXXXX” is the group you want the user to be appended. “YYYYY” is the name of the user attached to the sudo group.

In the second screenshot, I used the command “cat /etc/group” to show the users were successfully added to the group. “cat” is the command to output the contents of a specific place. “/etc/group” is the address to where the information is located.

c. And change their login shell to /bin/bash.



CYSE 270 Assignment #6 File Permission

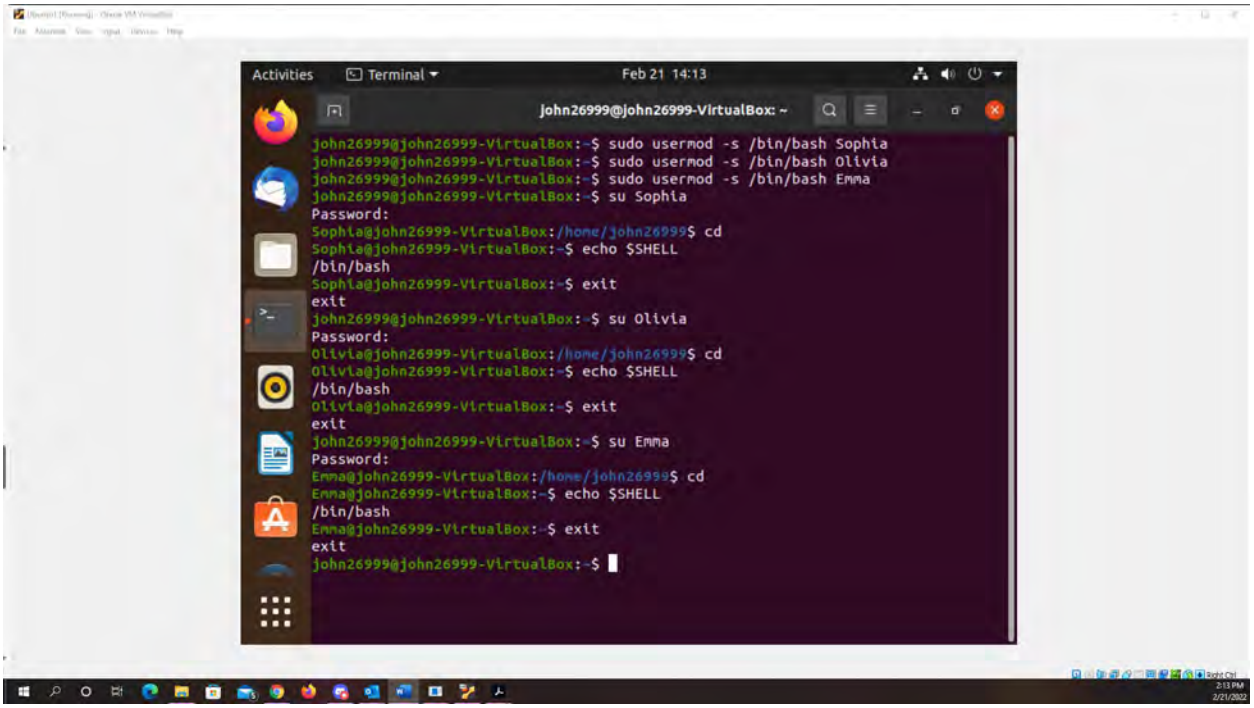


Figure 4 Screenshots of JWILS082 Computer screen for Step 2.c.

The first screenshot is used to show the current shell the users were using

The Second screenshot is the command " sudo usermod -s /bin/bash YYYYY[5]" that changes the shell from /bin/sh to /bin/bash. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "usermod" is the command that modifies changes to a user. "-s" is the command for the new login for the user account. "/bin/bash" is the shell location. "YYYYY" is the users new shell that was changed from "/bin/sh" to "/bin/bash". I also used the command "echo $SHELL" for each user to illustrate the change was correctly made.

d. You can refer to the options in Table 7-4. Don't forget to set their passwords.

[5] To keep from writing redundant information in Step 2.c., when you see "YYYYY" this is replaced with the user names of Sophia, Olivia, and Emma.

CYSE 270 Assignment #6 File Permission

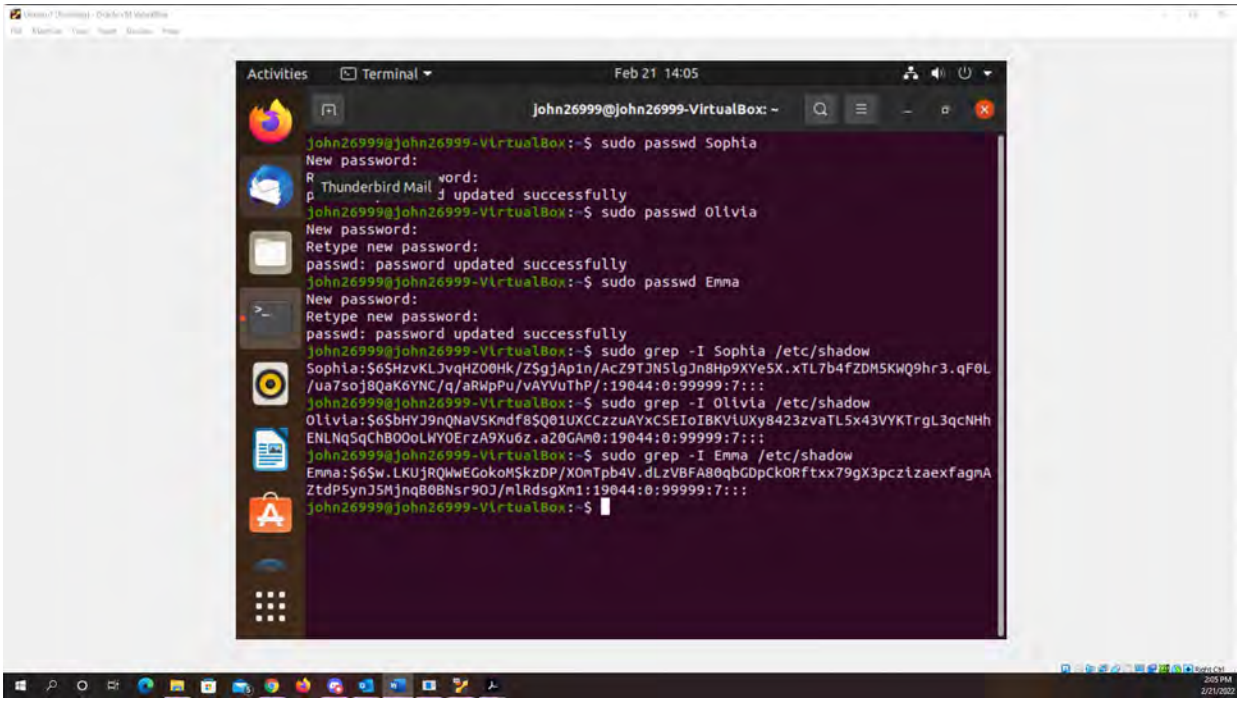


Figure 5 Screenshots of JWILS082 Computer screen for Step 2.d.

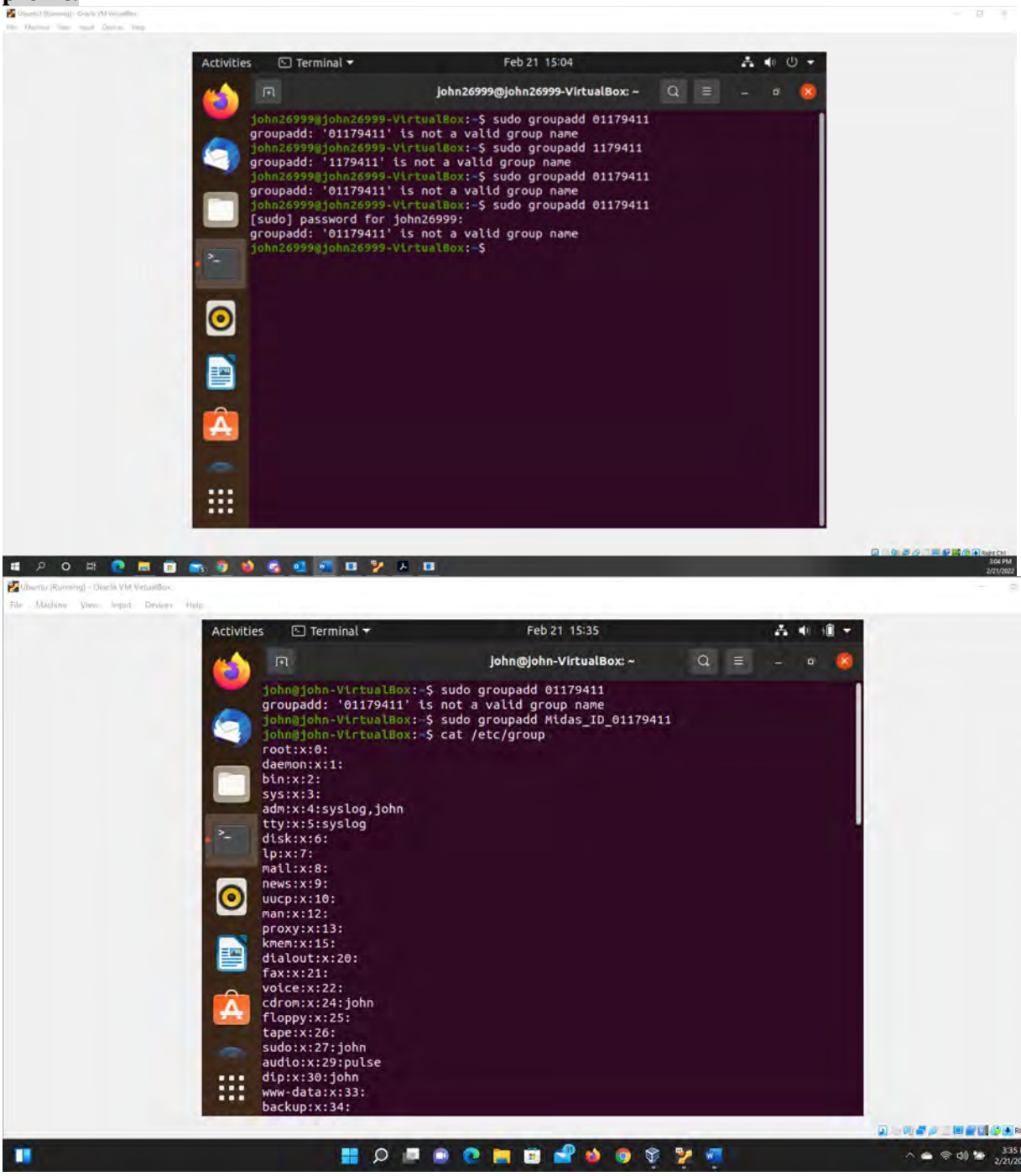
Above is the screenshot of the command " sudo passwd YYYYY[6]" that changes the new user password. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "passwd" is the command that changes the password for a user. "YYYYY" is the name of new users password that was added or changed.

In addition, I used the command " sudo grep -I YYYYY /etc/shadow" that displays the user password information including the encrypted password and password aging. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "grep" is the command that filter searched for a file of a particular pattern. "-i" is the command that is for case sensitive searches. "YYYYY" is the user name I am searching. "/etc/shadow" is where the users group info, including administrators and the group password.

[6] To keep from writing redundant information in Step 2.d., when you see "YYYYY" this is replaced with the user names of Sophia, Olivia, and Emma.

CYSE 270 Assignment #6 File Permission

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



CYSE 270 Assignment #6 File Permission

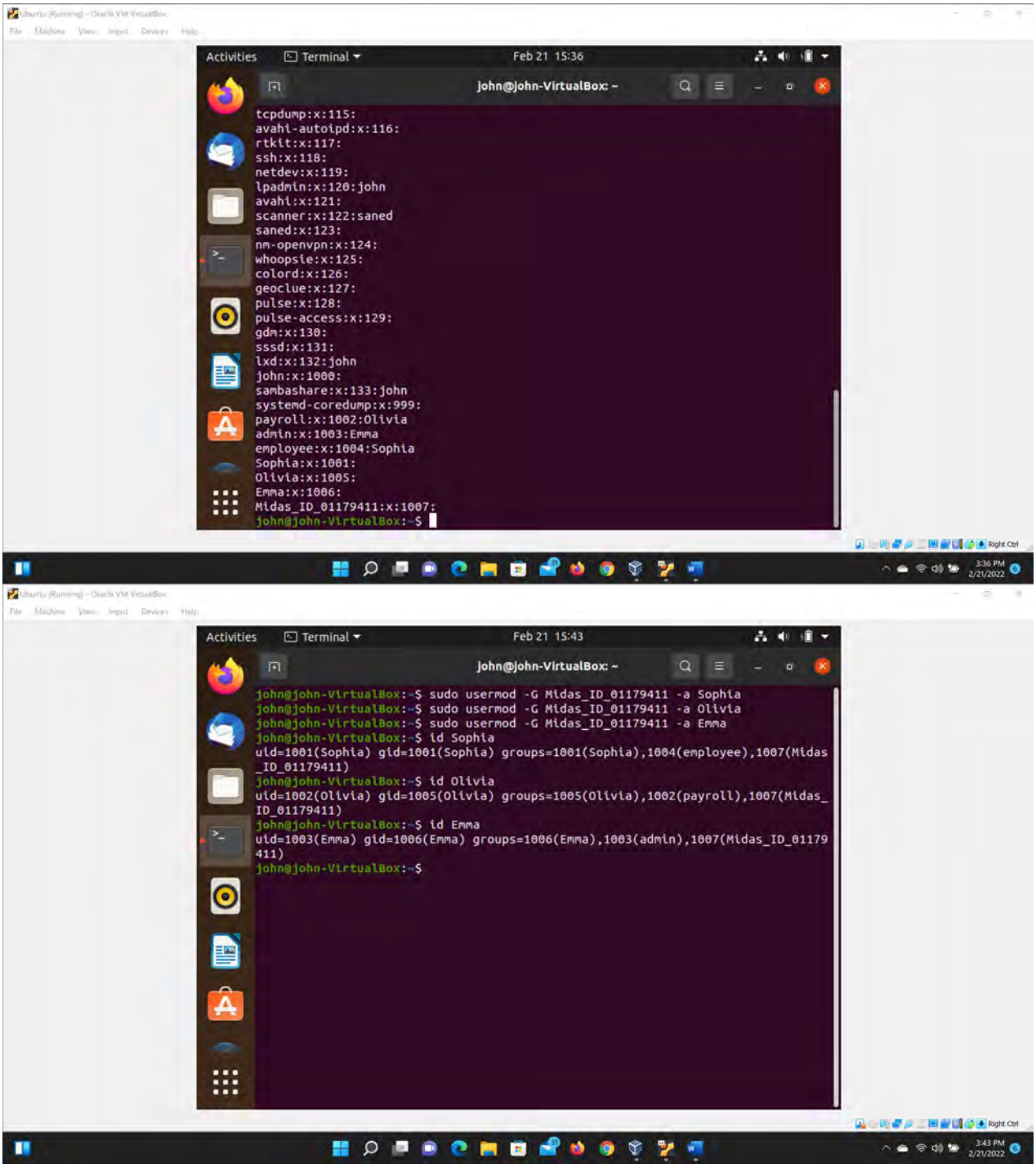


Figure 6 Screenshots of JWILS082 Computer screen for Step 3.

In the first shot I wanted to show that my system did not like just using my MIDAS ID as a group name. And then my Unbuntu crashed. Lol. So from here on out I am going to use my other (backup) Unbutu off of my spare laptop. So the screenshots might look alittle different.

The second screen shot uses the commands “sudo groupadd Midas_ID_01179411” to add a new group for users secondary use. “sudo” is the command that allows you to run programs with the security privileges

of another user (otherwise known as a super user). “groupadd” is the command adds a group. “sudo groupadd Midas_ID_01179411” is the new group name.

In addition, I used the command “cat /etc/group” to validate the the group account information was created.

In the fourth screen shot I used the command “sudo usermod -G Midas_ID_01179411 -a YYYYY[7]” to add the this directory to the three users as a secondary directoty.

[7] To keep from writing redundant information in Step 2.d., when you see “YYYYY” this is replaced with the user names of Sophia, Olivia, and Emma.

CYSE 270 Assignment #6 File Permission

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

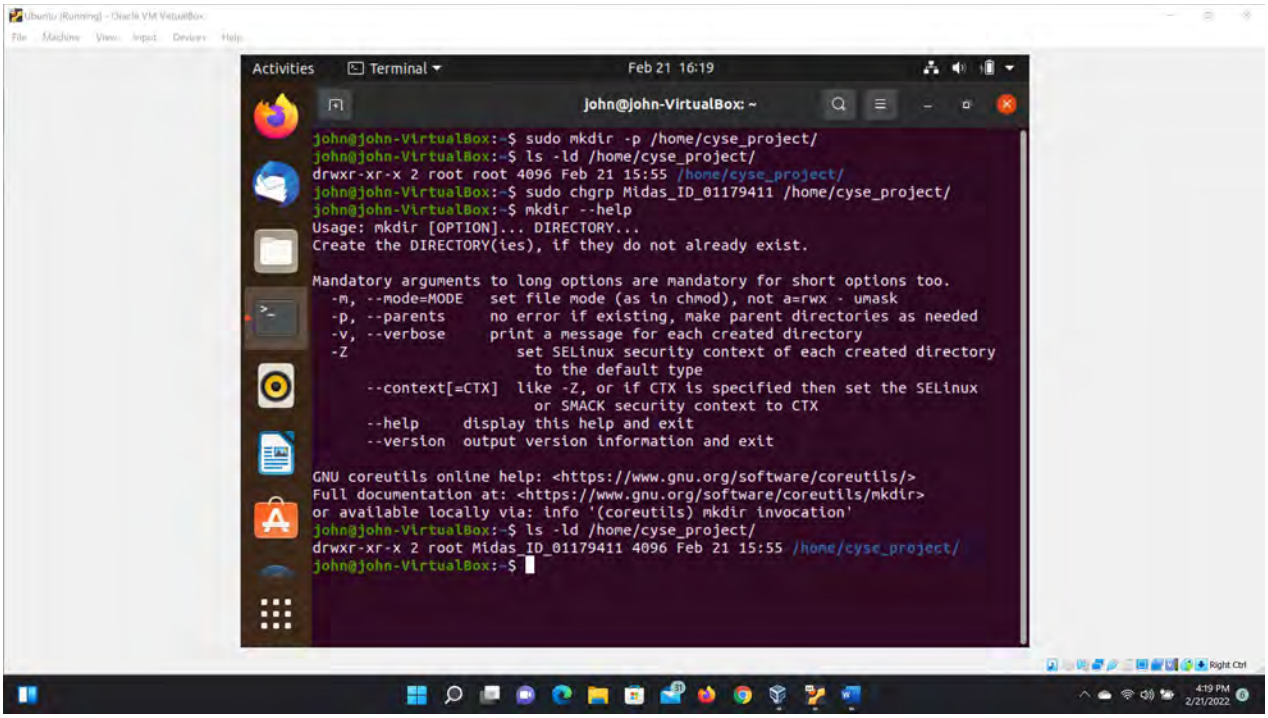


Figure 7 Screenshots of JWILS082 Computer screen for Step 4.

Above is the screenshot of the command " sudo mkdir -p /home/cyse_project" that makes a new directory called cyse_project. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "mkdir" is the command that makes a new directory. "-p" says to make it a parent directory if not already made. "/home/cyse_project" is the address of the new directory.

In addition, I used the command "sudo chgrp Midas_ID_01179411 /home/cyse_project" that changed the group owner to Midas_ID_01179411. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "chgrp" is the command that changes the group ownership of a file or directory. "Midas_ID_01179411" is the name of the group I am changing ownership. "/home/cyse_project" is where the directory where the group will own.

In addition, I used the command "ls -ld /home/cyse_project" to check the permissiond of the directory.

CYSE 270 Assignment #6 File Permission

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

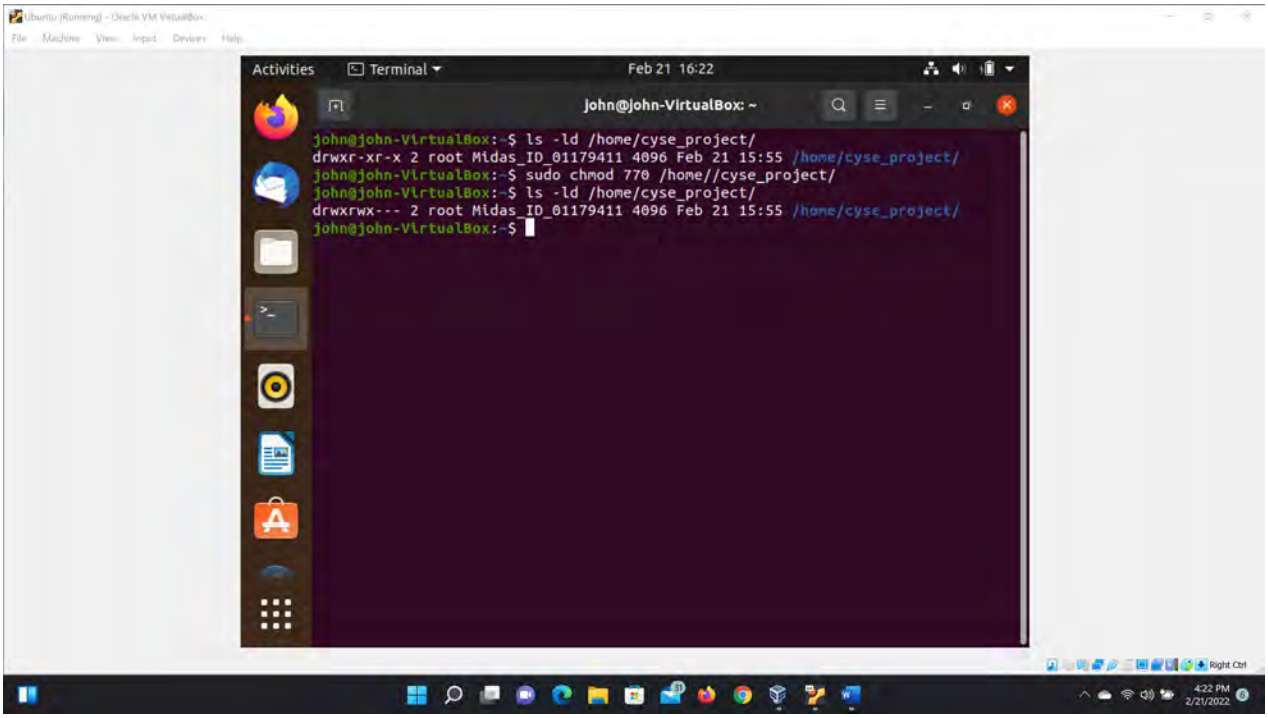


Figure 8 Screenshots of JWILS082 Computer screen for Step 5.

Above is the screenshot of the command " sudo chmod 770 /home/cyse_project" to change the directory permissions from drwxr-xr-x to drwxrwx---. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "chmod" is the command that changes the file or directory permissions. "770" are the permissions that you want to file to be. "/home/cyse_project" is te directory you want the permissions chaged.

In addition, I used the command "ls -ld /home/cyse_project" that displays the permission information of the directory cyse_project.

CYSE 270 Assignment #6 File Permission

Step 6. Switch to Sophia's account. Change the default permissions 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.**

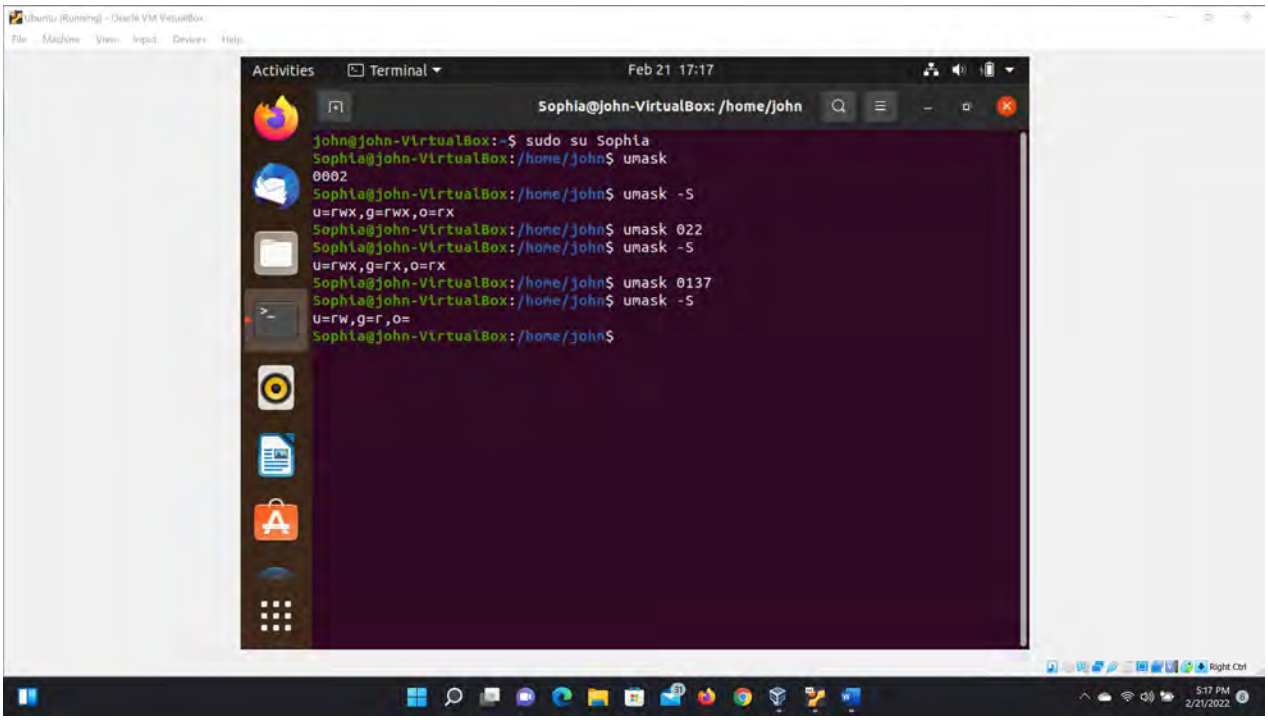


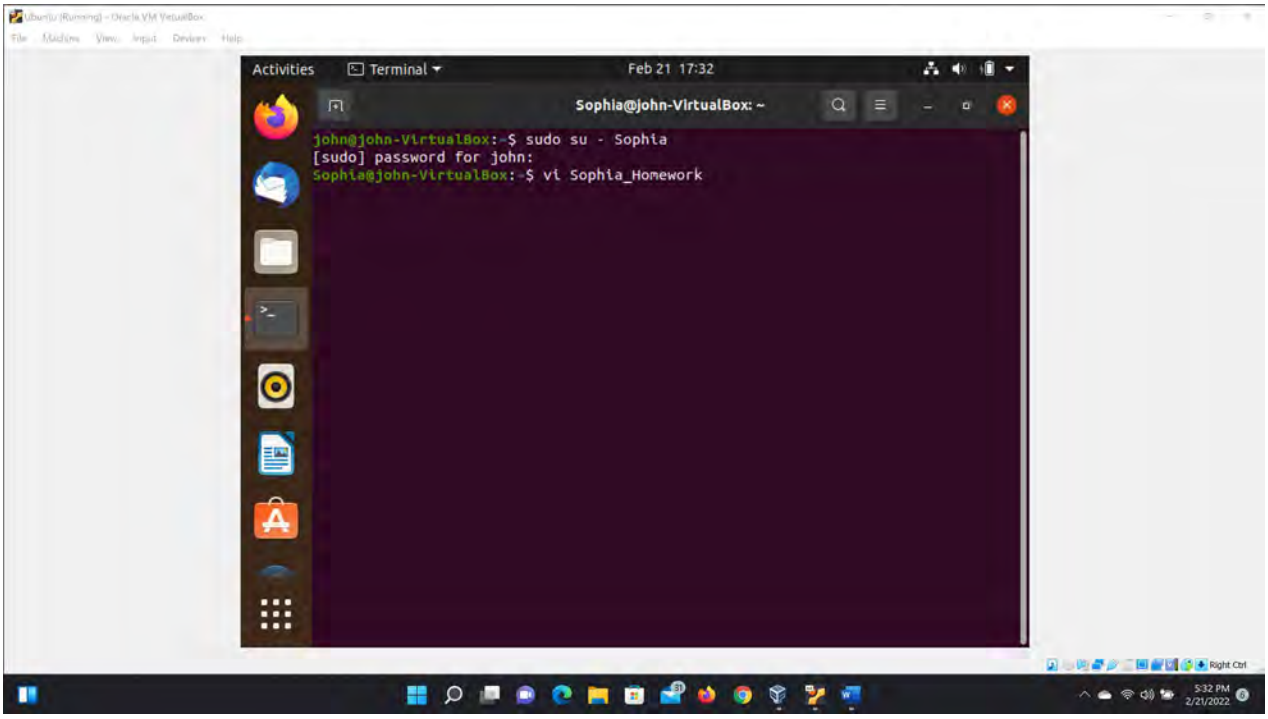
Figure 9 Screenshots of JWILS082 Computer screen for Step 6.

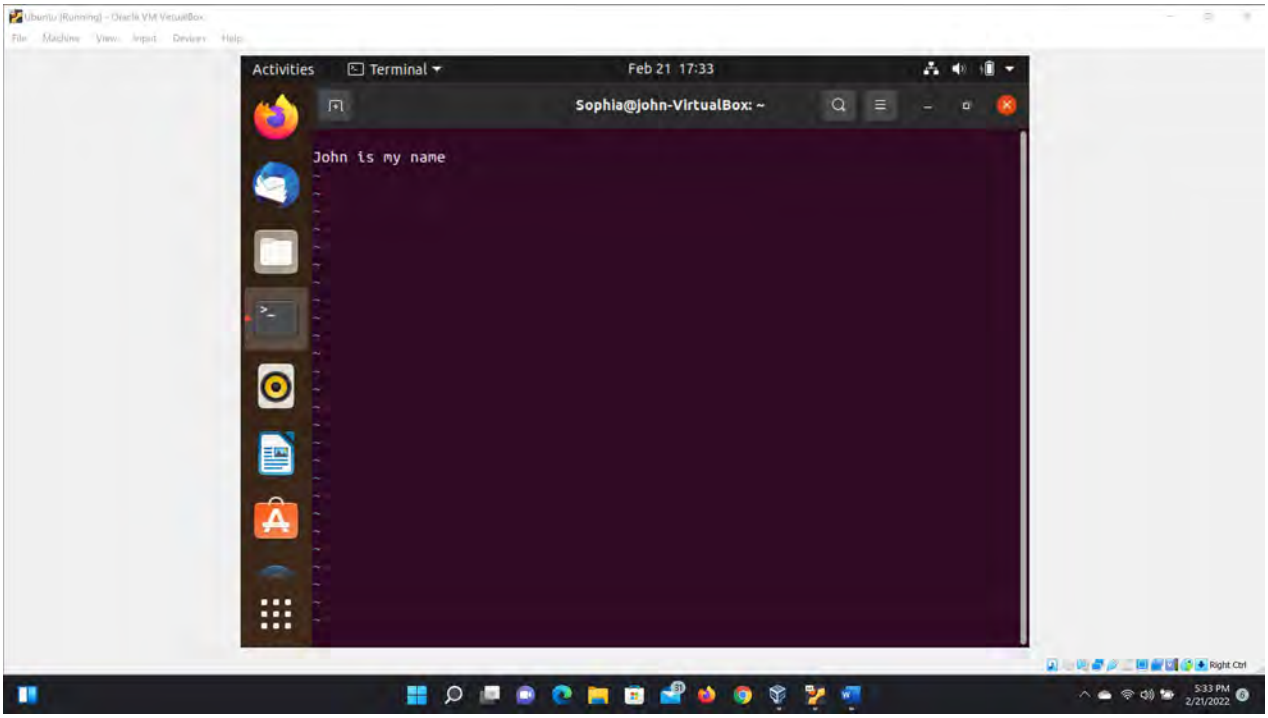
Above is the screenshot of the command " sudo su Sophia" that switches to account Sophia. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "su" is the command that allows users to run commands with another users privileges. "Sophia" is the user name that you want to switch.

In addition, I used the command "umask" that displays the users default permissions for new files created. Becsaue the users default permissions were set to 0002 it only gave permissions for anyone to read and write for new files created. To change the permissions to "-rw-r-----" I had to do some quick math. -rw-r----- = 640 -> (777-640 = 137). 137 is the numer you want to change the permissions to "-rw-r-----" So, I gave the command "umask 137" to update the permissions and I also did the command "umask -S" to show the outuput in letter notation.

CYSE 270 Assignment #6 File Permission

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





CYSE 270 Assignment #6 File Permission

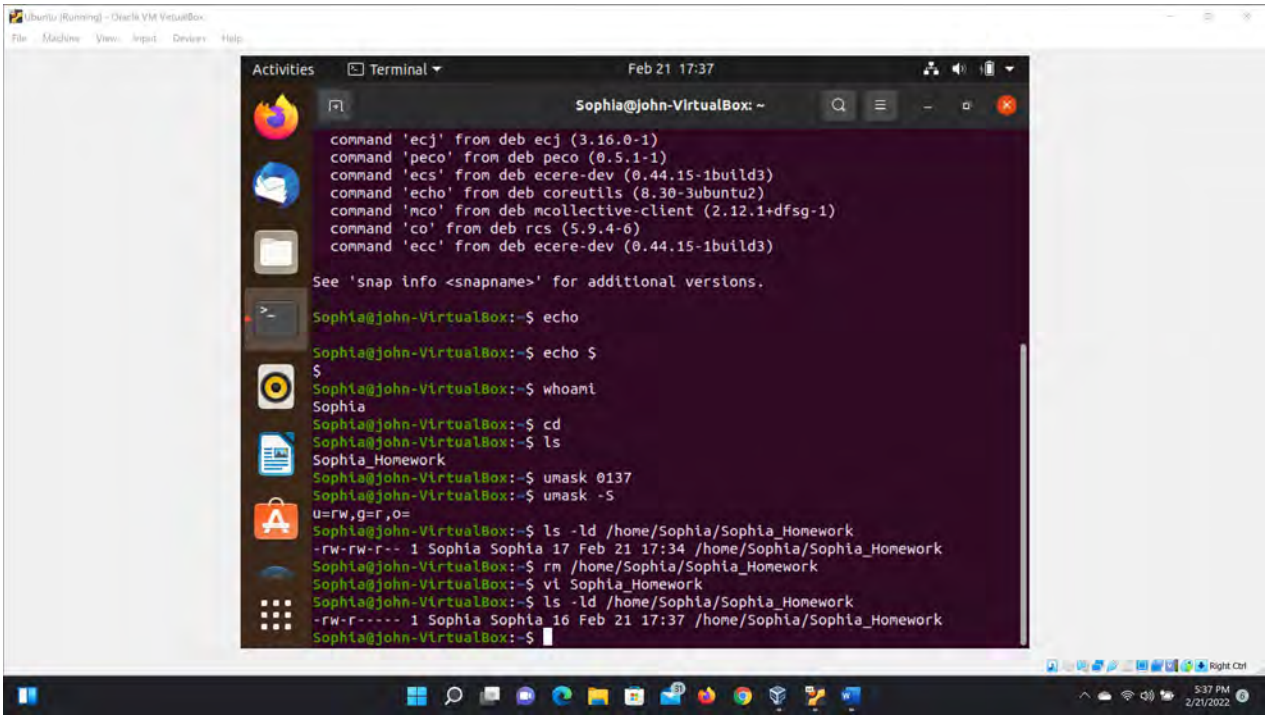


Figure 10 Screenshots of JWILS082 Computer screen for Step 7.

Above is the screenshot of the command " sudo su - Sophia" that changes to the new user Sophia. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "su" is the command that allows users to run commands with another users privileges. "Sophia" is the user name that you want to switch.

I also ran the command "vi Sophia_Homework" so that I could create a file name Sophia_Homework in Sophia's home directory. "vi" is the command for the vi word processor program thingy. "Sophia_Homework" is the name of the file. Once the vi file was open I added my name. saved asn closed the file.

I then made sure the permissions were appropriate for the file. By using the command "umask" that displays the users default permissions for new files created. Becsaue the users default permissions were set to 0002 it only gave permissions for anyone to read and write for new files created. To change the permissions to "-rw-r-----" I had to do some quick math. -rw-r----- = 640 -> (777-640 = 137). 137 is the numer you want to change the permissions to "-rw-r-----" So, I gave the command "umask 137" to update the permissions and I also did the command "umask -S" to show the outuput in letter notation.

CYSE 270 Assignment #6 File Permission

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.**

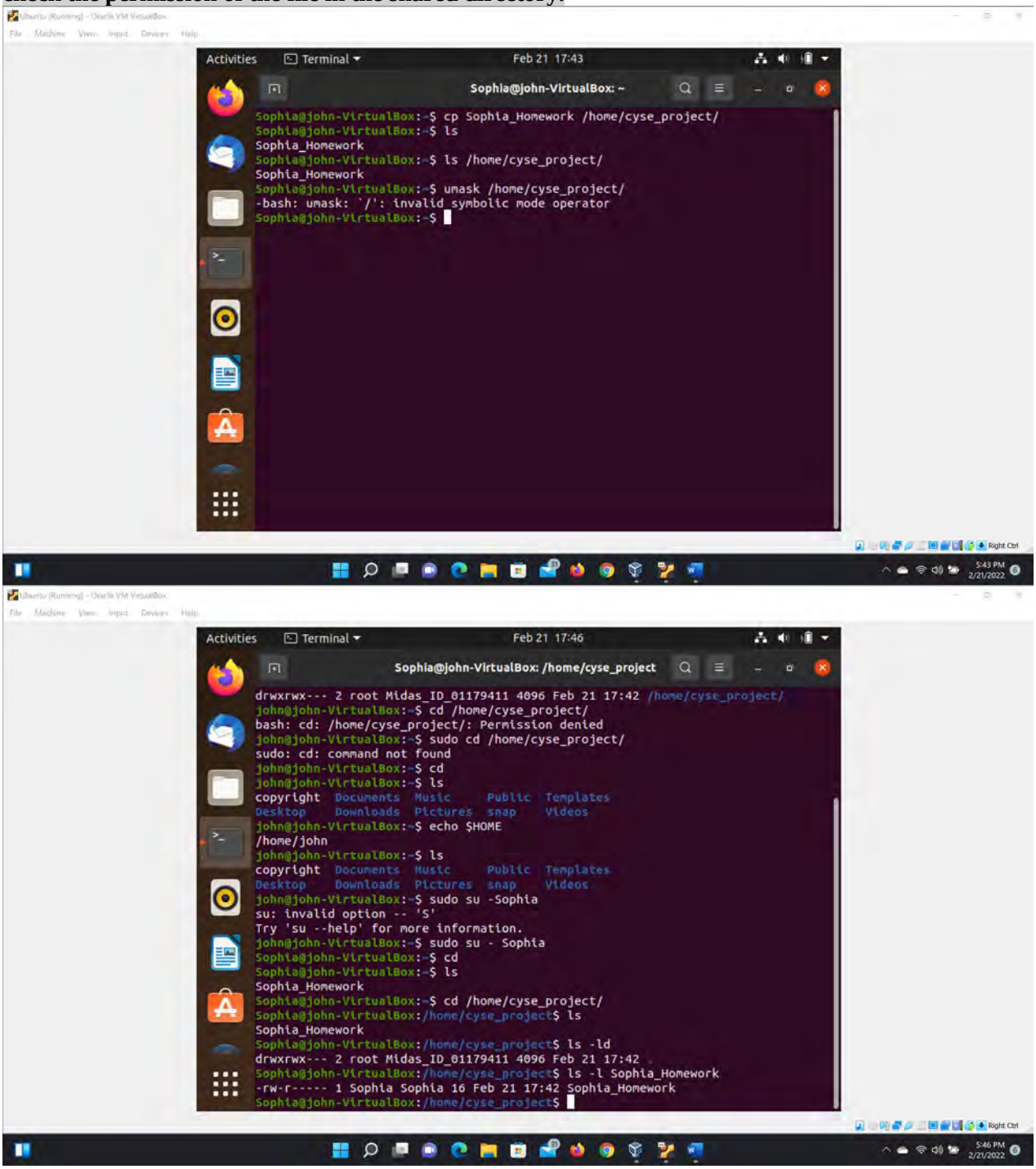


Figure 11 Screenshots of JWILS082 Computer screen for Step 8.

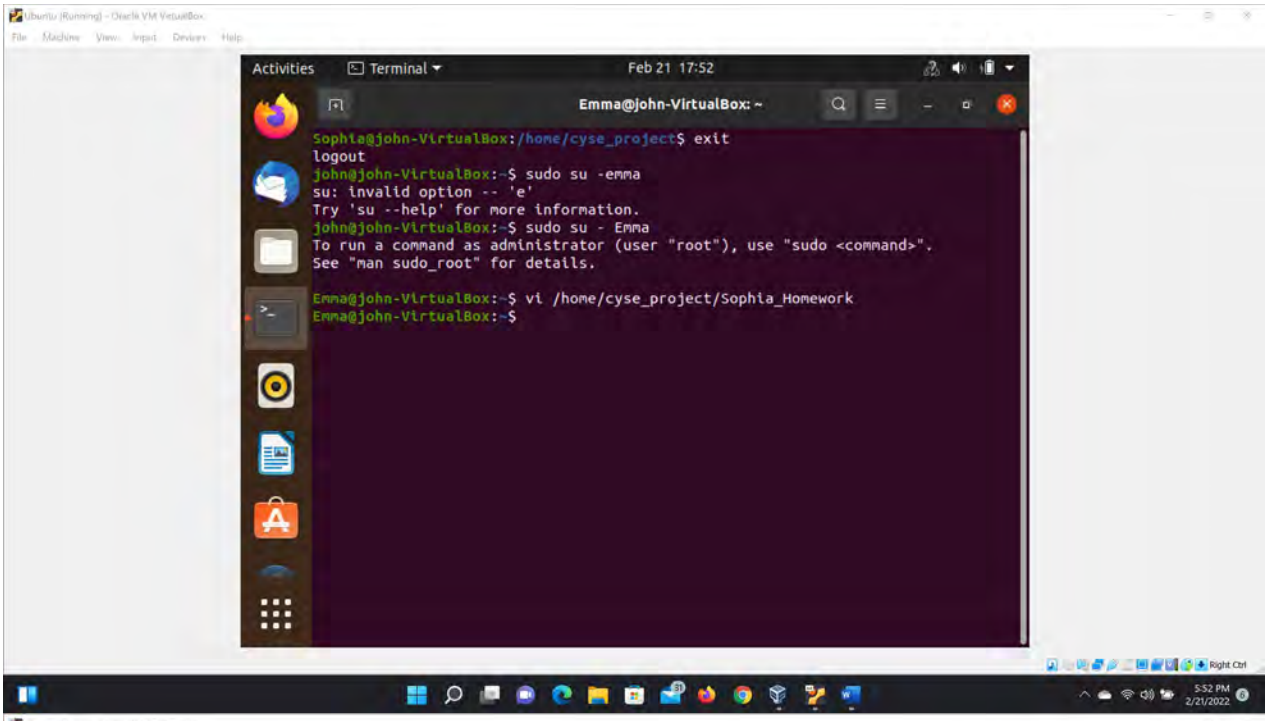
Above is the screenshot of the command “cp Sophia_Homework /home/cyse_project” that copies the file Sophia-Homework and places the file in the /home/cyse_project directory. “cp” is the command to copy. “Sophia_Homework” is the file to be copied. “/home/cyse_project” is the path address where the copied file is to be placed.

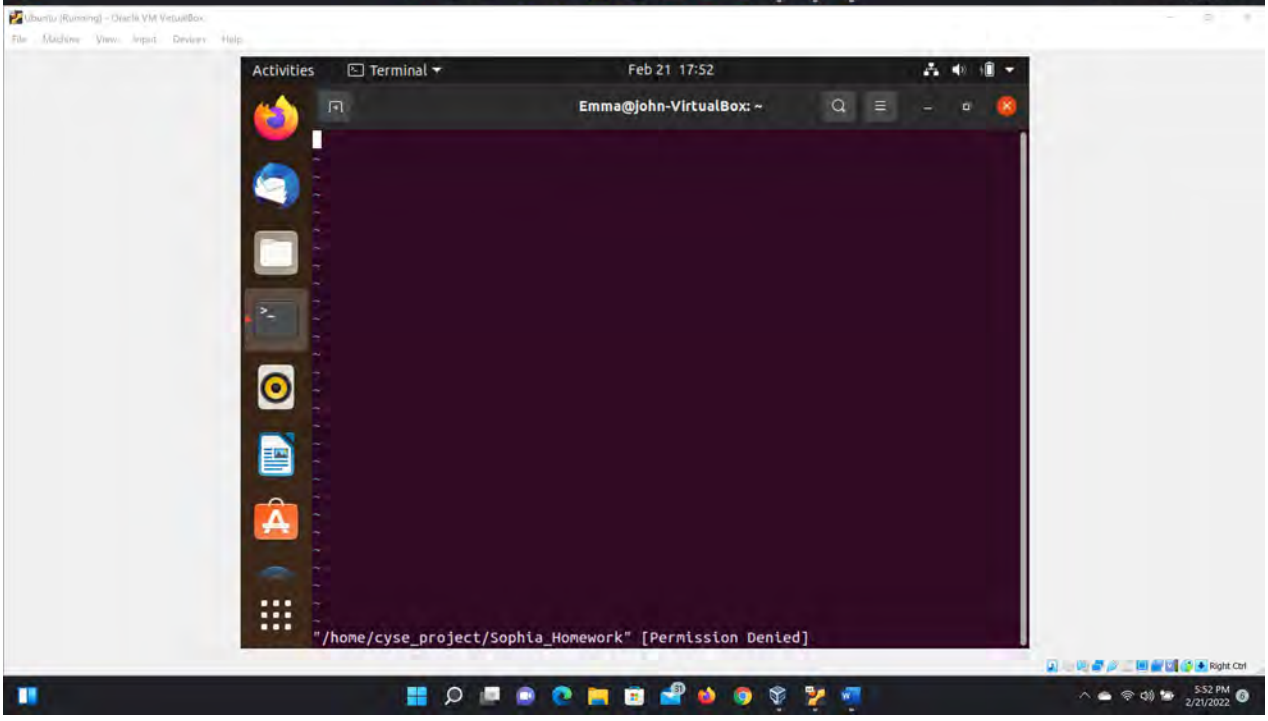
CYSE 270 Assignment #6 File Permission

I also used the command “cd /home/cyse_project” to chage the directory to cyse_project. Then I used the command “ls -l Sophia_Homework” to check on the permissions of the file Sophia_Homework. I took me a minute to get there and did.

CYSE 270 Assignment #6 File Permission

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





CYSE 270 Assignment #6 File Permission

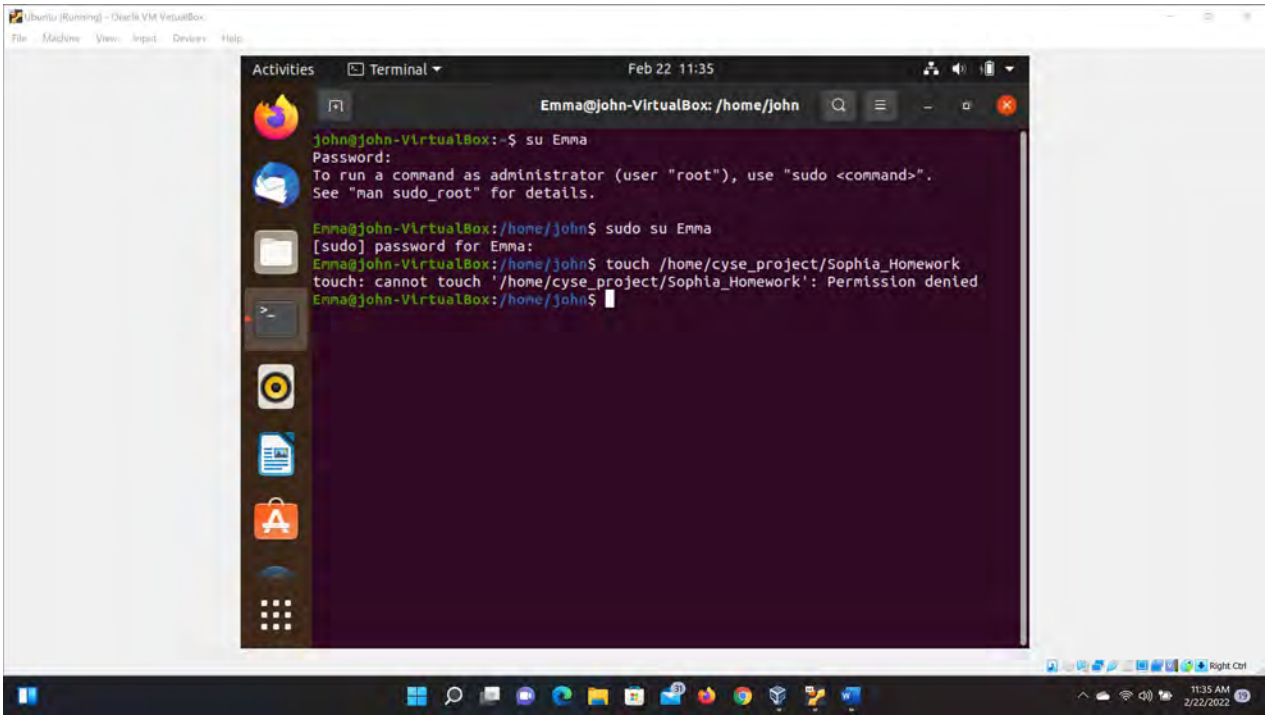


Figure 12 Screenshots of JWILS082 Computer screen for Step 9.

Above is the screenshot of the command “sudo su - Emma” that changes to the user account Emma. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “su” is the command that allows users to run commands with another users privileges. “Emma” is the user name that you want to switch.

I also ran the command “vi /home/cyse_project/Sophia_Homework” to see if I could access the file and I got a “permission denied” banner.

I also used the command “touch /home/cyse_project/Sophia_Homework” to see if I had the permissions to get into the file in this way. But was also denied access.

CYSE 270 Assignment #6 File Permission

TASK B:

SET SGID PERMISSION

Step 1. Switch to 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 give the group user read permission.

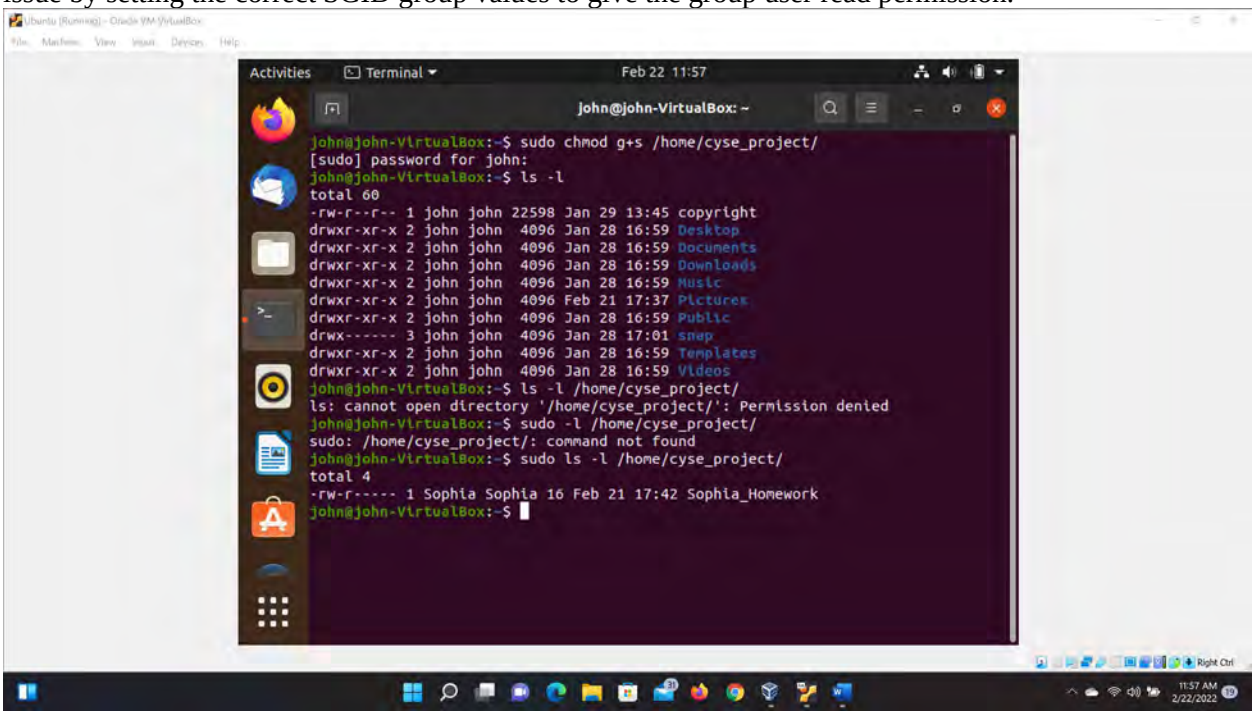


Figure 13 Screenshots of JWILS082 Computer screen for Step 1.

Above is the screenshot of the command “sudo chmod g+s /home/cyse_project” that changes or Sets the Group ID (SGID). “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “chmod” is the command that changes the file or directory permissions. “g+s” affects the files group Id but does not affect the owner ID. “/home/cyse_project” is the address of the directory you want the permissions or ID changed.

CYSE 270 Assignment #6 File Permission

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

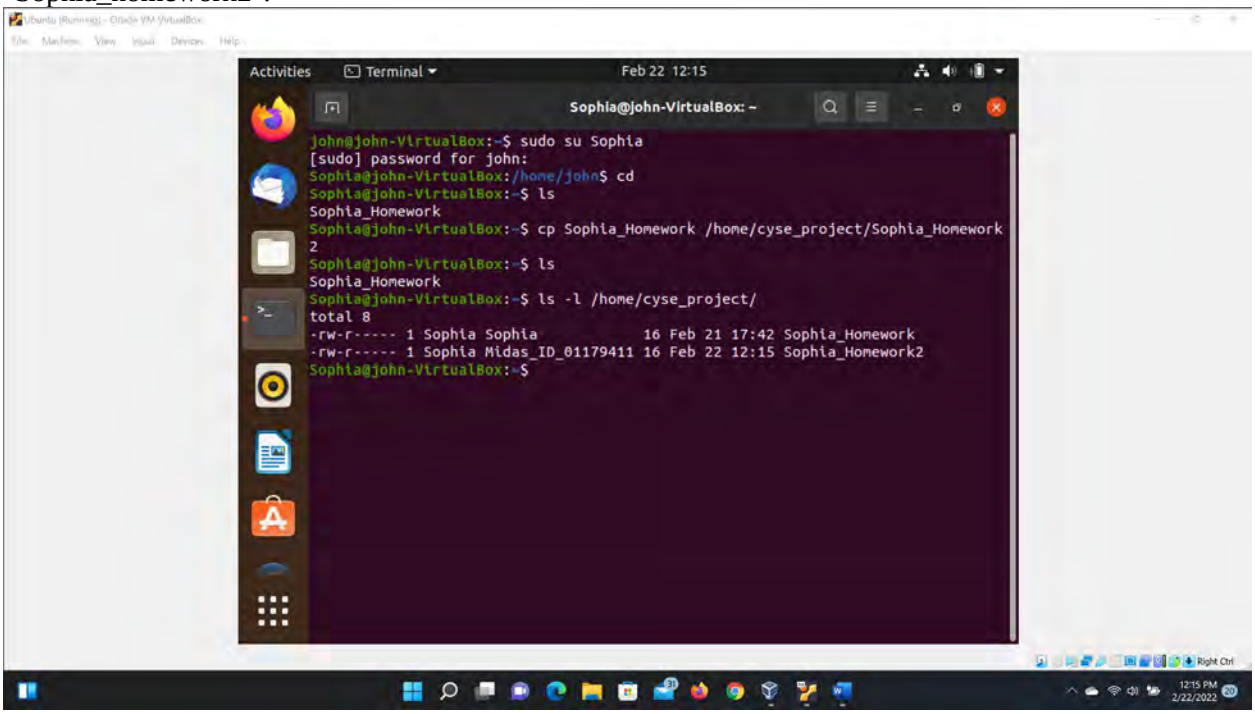


Figure 14 Screenshots of JWILS082 Computer screen for Step 2.

Above is the screenshot of the command “cp Sophia_Homework /home/cyse_project/Sophia_Homework2” that will copy the file Sophia_Homework and rename it to Sophia_Homework2 and place it in the directory cyse_project. “cp” is the command to copy a file. “Sophia_Homework” is the file that is copied. “/home/cyse_project/Sophia_Homework2” is the address of the dierectory to place the file. And because there is no file already named Sophia_Homeowrk2, the file is automatically created.

I also did the command “ls -l /home/cyse_project” to validate the file was created in the directory specficied.

CYSE 270 Assignment #6 File Permission

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

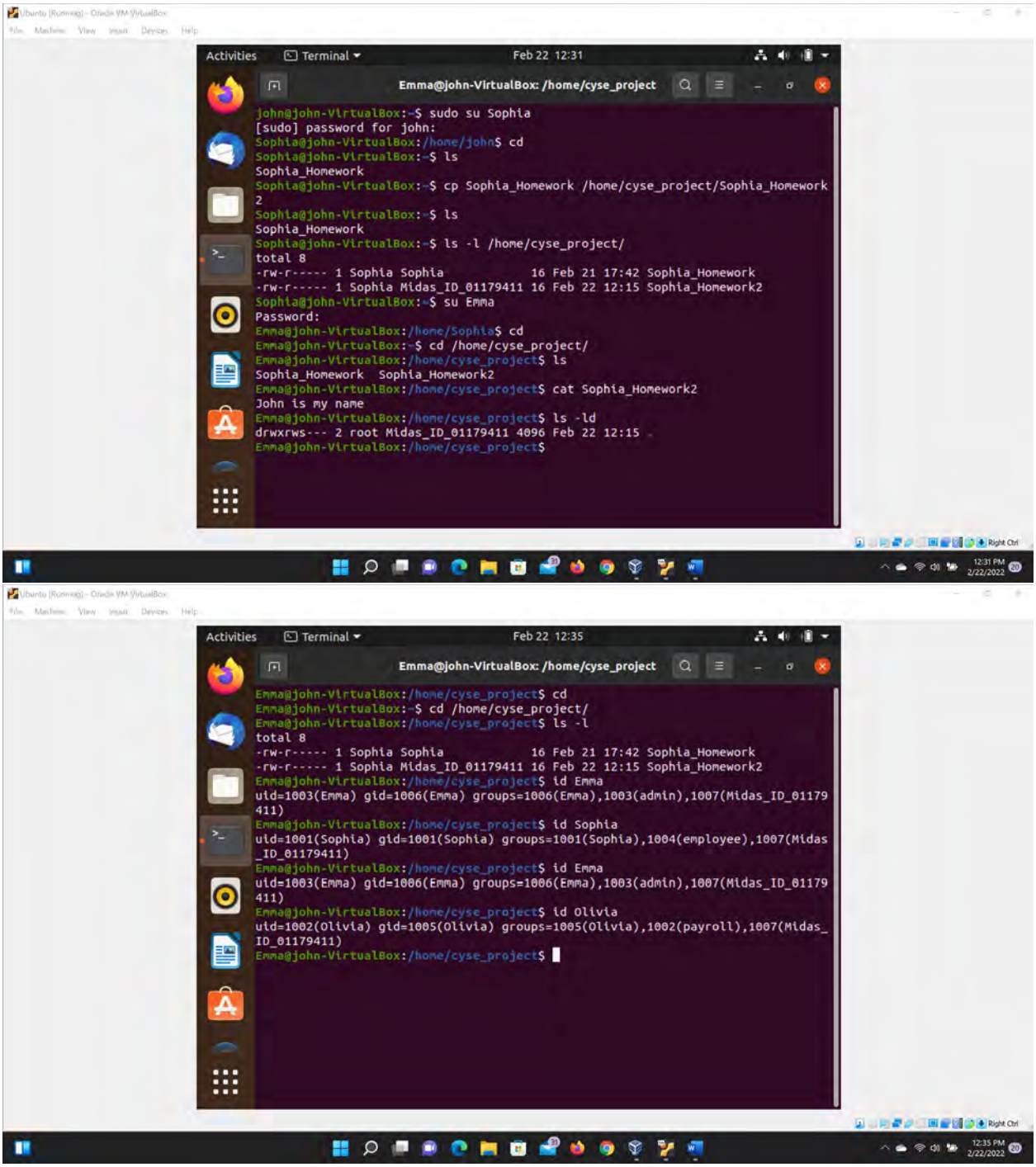


Figure 15 Screenshots of JWILS082 Computer screen for Step 3.

Above is the screenshot of the command “su Emma” that changes to the user account to Emma.

CYSE 270 Assignment #6 File Permission

I also used the command “cd /home/cyse_project” to chage the current directory. “cd” is the command to chage the current directory. “/home/cyse_project/” is the address of the directory you want to access. I used the command “ls” to list the files in the cyse_project directory.

To read the file Sophia_Homework2, I used the command “cat Sophia_Homework2”. “cat” is the command that reads the contents of a fike and outputs it on the screen. “ Sophia_Homework2” is the name of the file you want to read.

CYSE 270 Assignment #6 File Permission

TASK C:

UNSET SGID PERMISSIONS

Step 1. Switch to root account. To disallow group members to access the files in this folder, you need to fix the sharing issue by setting the correct SGID group values to remove the group user read permission.

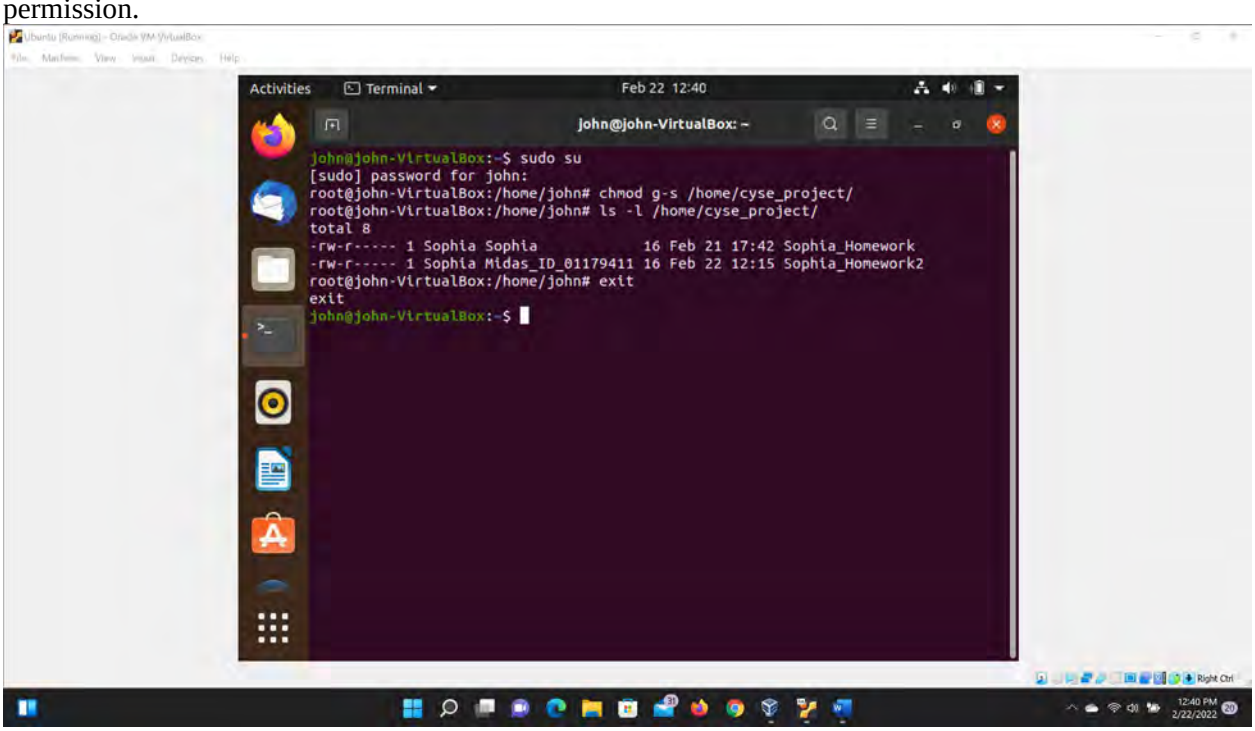


Figure 16 Screenshots of JWILS082 Computer screen for Step 1.

Above is the screenshot of the command “sudo su “ that changes to the root account for user account john. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “su” is the command that allows users to run commands with another users privileges.

I also did the command “chmod g-s /home/cyse_project” to change or unset the SGID permissions. “chmod” is the command that changes the file or directory permissions. “g-s” affects the files group Id but does not affect the owner ID. “/home/cyse_project” is the address of the directory you want the permissions or ID changed.

CYSE 270 Assignment #6 File Permission

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

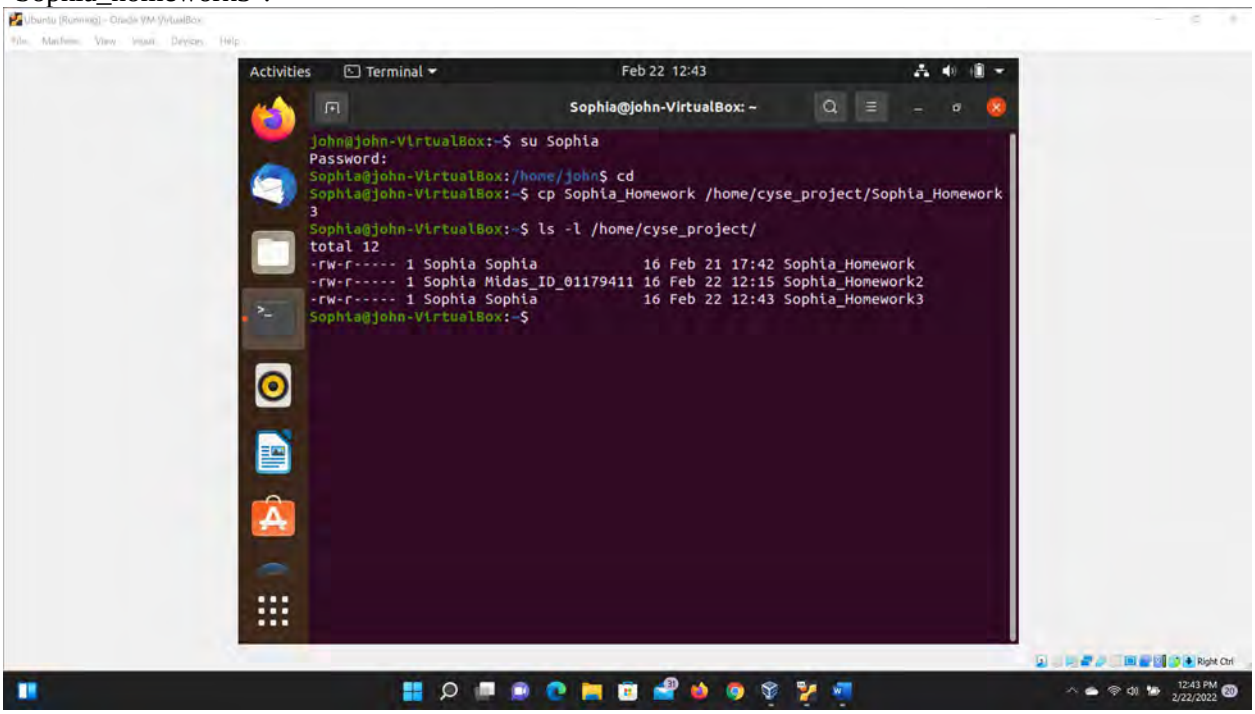


Figure 17 Screenshots of JWILS082 Computer screen for Step 2.

Above is the screenshot of the command “su Sophia” that changes to the user account to Sophia. “su” is the command that allows users to run commands with another users privileges. “Sophia” is the user name that you want to switch.

I also executed the command “cp Sophia_Homework /home/cyse_project/Sophia_Homework3” that will copy the file Sophia_Homework and rename it to Sophia_Homework3 and place it in the directory cyse_project. “cp” is the command to copy a file. “Sophia_Homework” is the file copied. “/home/cyse_project/Sophia_Homework3” is the address of the dierectory to place the file. And because there is no file already named Sophia_Homework3, the file is automatically created.

I also did the command “ls -l /home/cyse_project” to validate the file was created in the directory specficied.

CYSE 270 Assignment #6 File Permission

Step 3. Switch to Olivia's account. Try to read "Sophia_home3" in the /home/cyse_project directory. CYSE 270: Linux System for Cybersecurity.

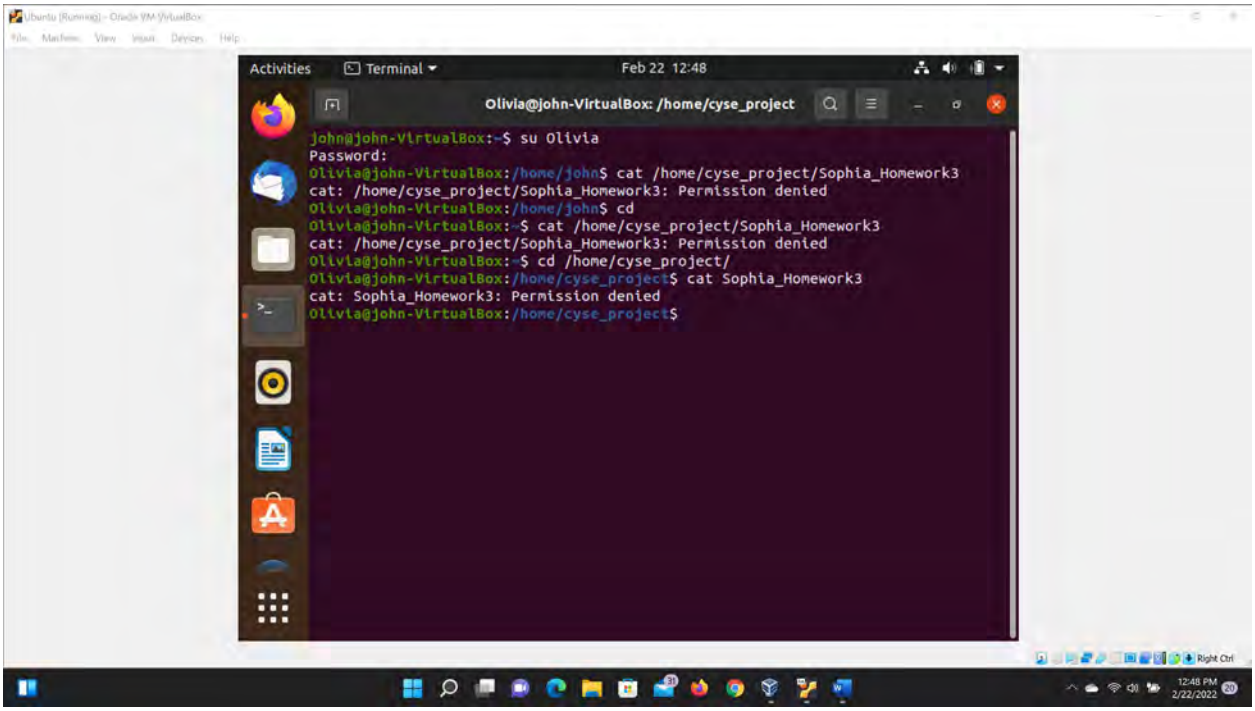


Figure 18 Screenshots of JWILS082 Computer screen for Step 3.

Above is the screenshot of the command “su Olivia” that changes to the user account Olivia. “su” is the command that allows users to run commands with another users privileges. “Olivia” is the user name that you want to switch.

To read the file Sophia_Homework3, I used the commands “cat Sophia_Homework3”. “cat” is the command that reads the contents of a fike and outputs it on the screen. “ Sophia_Homework3” is the name of the file you want to read.

I received that access to the file was denied.

CYSE 270 Assignment #6 File Permission

Extra credit: Sticky Bit

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

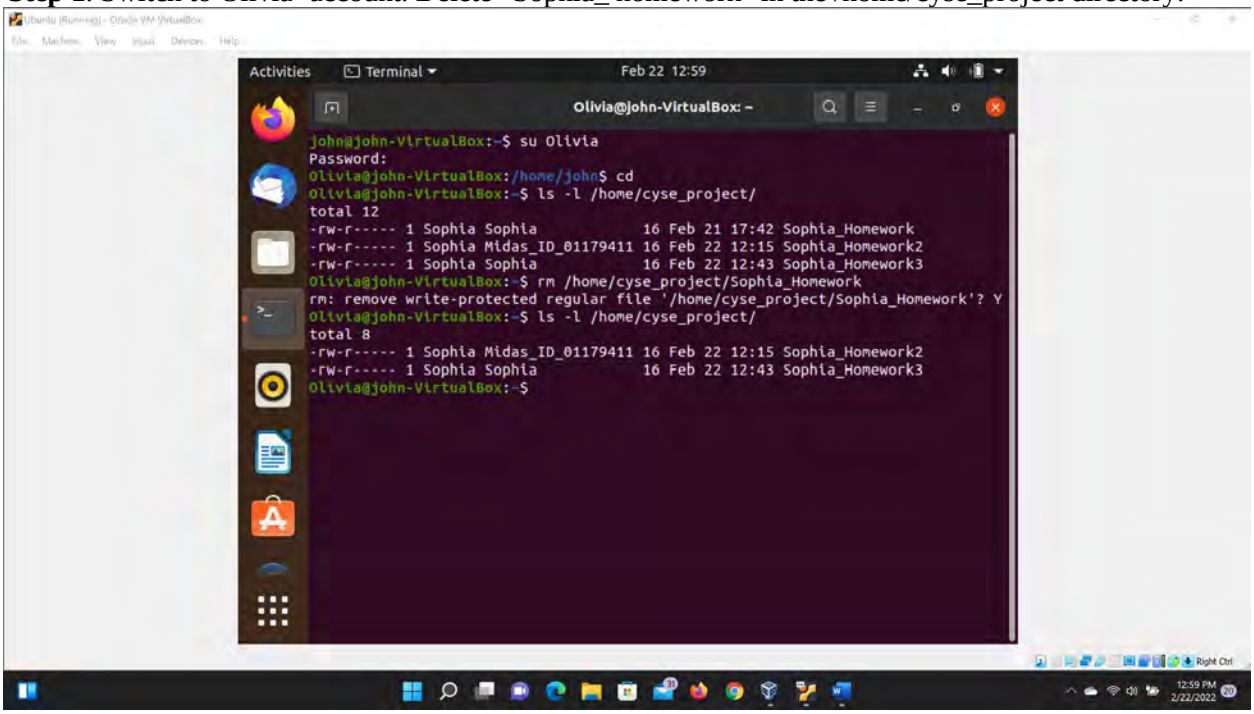


Figure 19 Screenshots of JWILS082 Computer screen for Extra Credit Step 1.

Above is the screenshot of the command "su Olivia" that changes to the user account Olivia. "su" is the command that allows users to run commands with another users privileges. "Olivia" is the user name that you want to switch.

I also used the command "ls -l /home/cyse_project" to list the files in the cyse_project directory.

I used the command "rm /home/cyse_project/Sophia_Homework" to delete the file Sophia-Homework. "rm" is the command to remove or delete a file. "/home/cyse_project/Sophia_Homework" is the command that gives the address of the file Sophia_Homework that was deleted.

I also used the command "ls -l /home/cyse_project" to list the files in the cyse_project directory to validate the file was deleted or removed.

CYSE 270 Assignment #6 File Permission

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

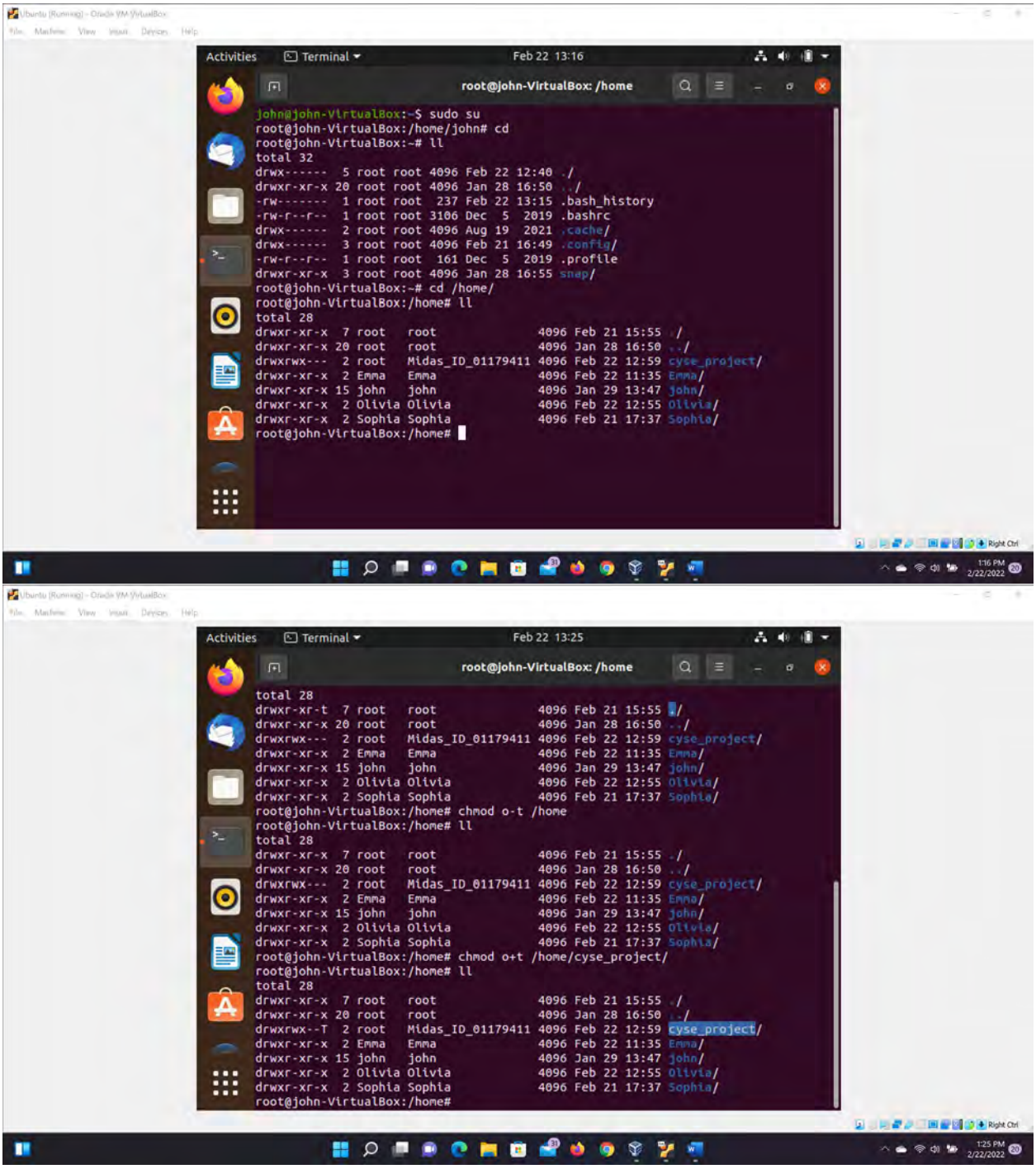


Figure 20 Screenshots of JWILS082 Computer screen for Extra Credit Step 2.

Above is the screenshot of the command “sudo su “ that changes to the root account for user account john. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “su” is the command that allows users to run commands with another users privileges.

JOHN WILSON
2/22/22

CYSE 270 Assignment #6 File Permission

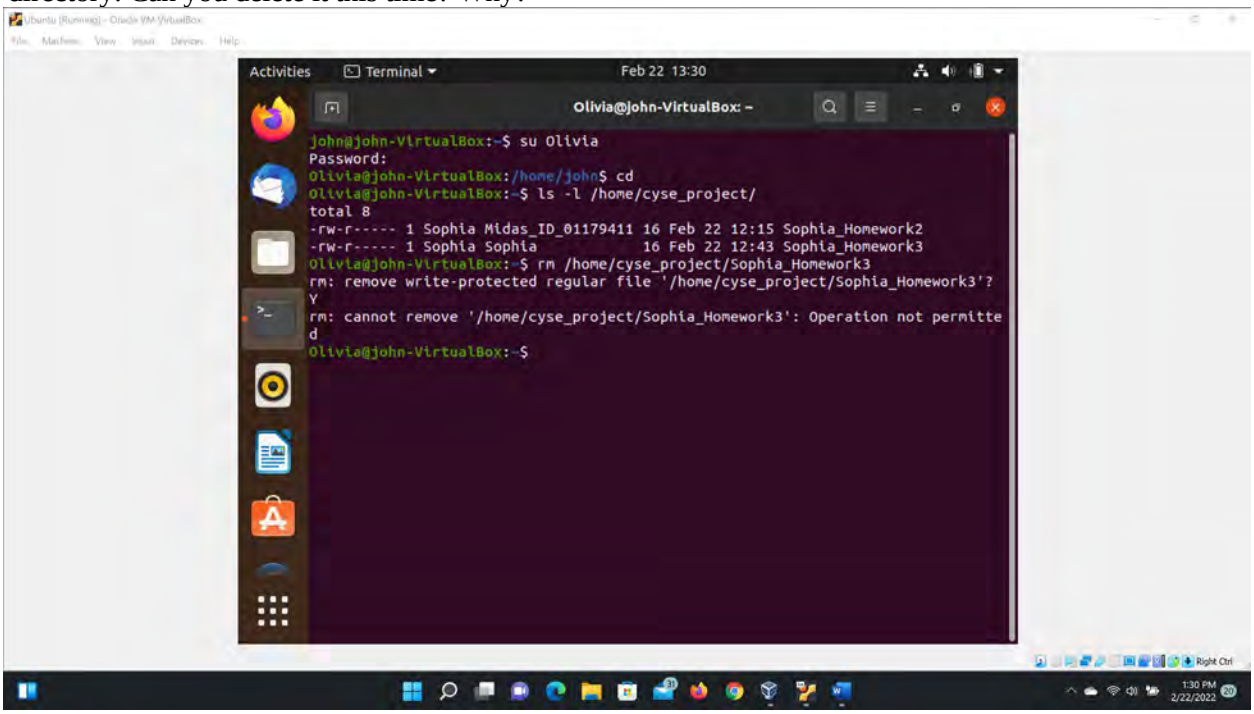
I also executed the command “cd /home” to change to the home directory. I also did the command “ll” to show the current permissions of the directories prior to using the stickbit command.

I used the commands “chmod o+t /home/cyse_project” that changes home directory permissions to sticky bit permission set. “chmod” is the command that changes the file or directory permissions. “o+t” affects allows the users to add a file to the directory but will not allow the user to delete it. “/home/cyse_project” is the address of the directory you want to place the sticky bit permissions.

I then used the “ll” to show the permission of the directories updated after executing the stickbit command. And you can see this as a T instead of an x in the last line of the permissions.

CYSE 270 Assignment #6 File 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?



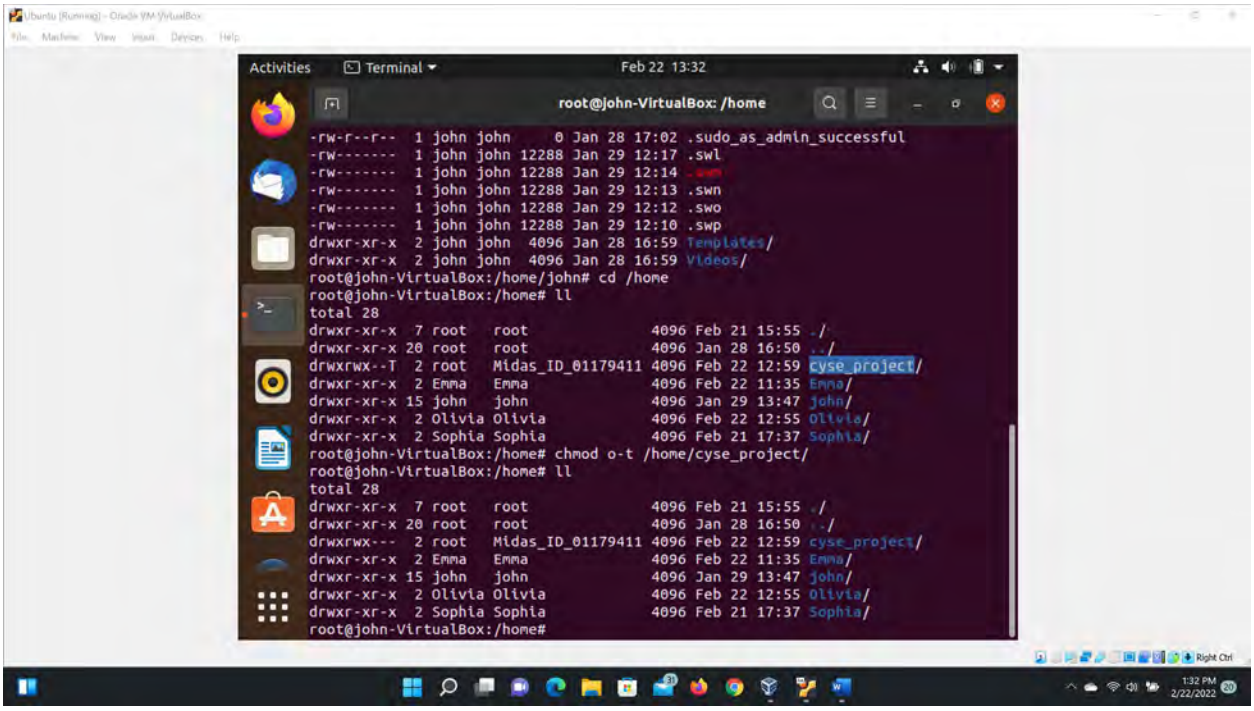


Figure 21 Screenshots of JWILS082 Computer screen for Extra Credit Step 3.

Above is the screenshot of the command "su Olivia" that changes to the user account Olivia. "su" is the command that allows users to run commands with another users privileges. "Olivia" is the user name that you want to switch.

CYSE 270 Assignment #6 File Permission

I also used the command “ls -l /home/cyse_project” to list the files in the cyse_project directory.

I used the command “rm /home/cyse_project/Sophia_Homework3” to delete the file Sophia-Homework. “rm” is the command to remove or delete a file. “/home/cyse_project/Sophia_Homework” is the command that gives the address of the file Sophia_Homework that was deleted.

The deletion of the file was denied. So the sticky bit permission worked.

And I removed the stickybit permissions after all of this.

Sources