OLD DOMINION UNIVERSITY

CYSE 270 LINUX SYSTEM FOR CYBERSECURITY

Assignment #4 Group and User Accounts

John Wilson

01179411

Below is the snippet of a sample lab report.

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.

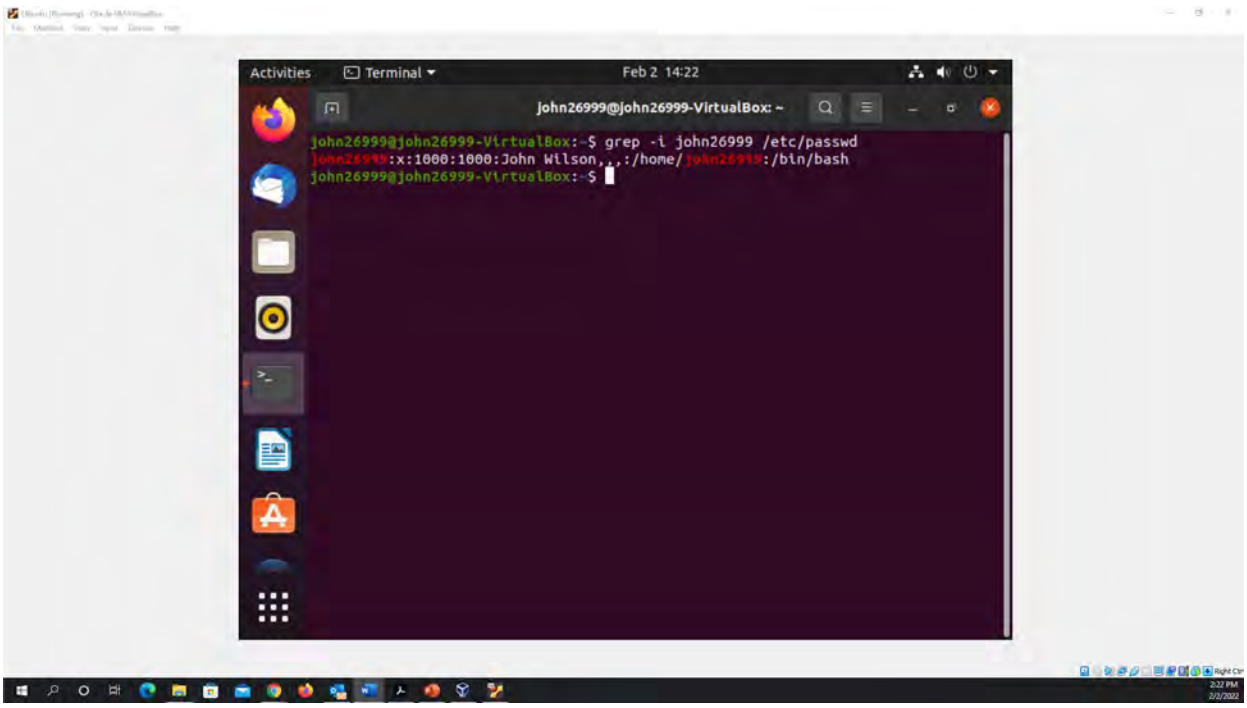

Figure 1 Screenshot of JWILS082 Computer screen for step 1

Above is the screen shot using the command “grep -i john26999 /etc/passwd” that displays the current user account information. “grep” is the command that filter searched for a file of a particular pattern. “-i” is the command that is for case sensitive. “john26999” is the user name I am searching. “/etc/passwd” is where the users group inof is located.

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

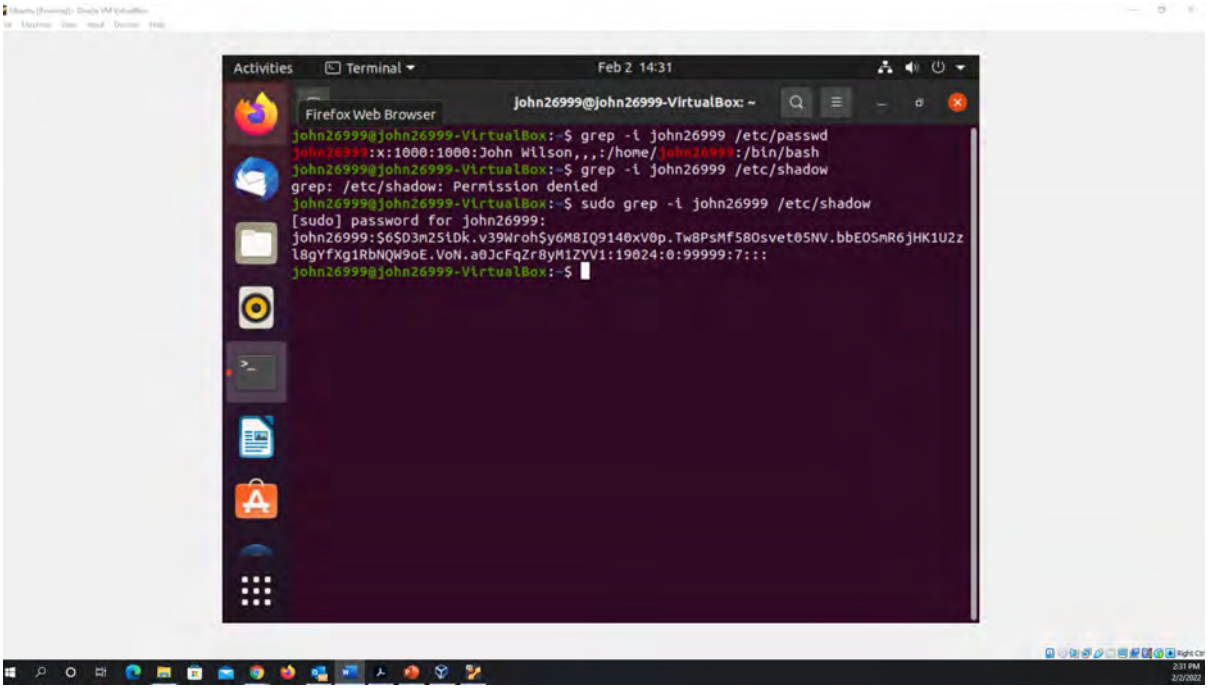

Figure 2 Screenshot of JWILS082 Computer screen for step 2

Above is the screen shot using the command “sudo grep -i john26999 /etc/shadow” that displays the current user account information. “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. “john26999” is the user name I am searching. “/etc/shadow” is where the users group info, including administrators and the group password.

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

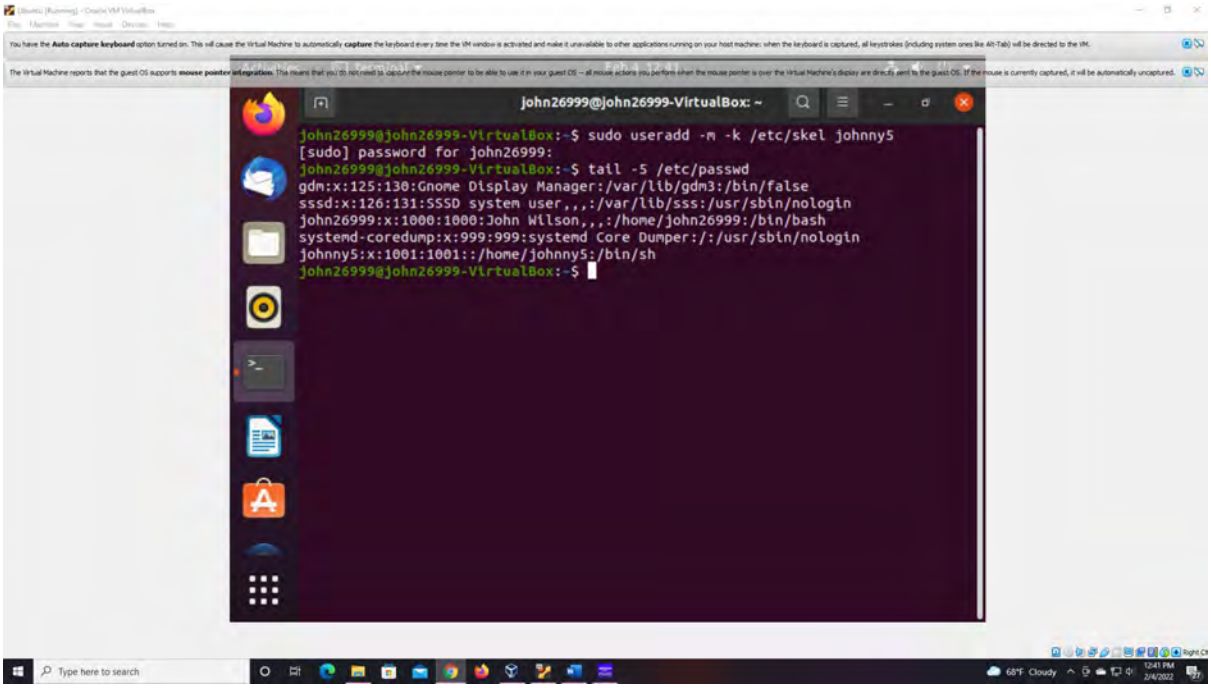

Figure 3 Screenshot of JWILS082 Computer screen for step 3

Above is the screen shot using the command “sudo useradd -m -k /etc/skel johnny5” 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/shadow” is where the users home directotry is located. “johhny5” (the name of the robot from the movie Short Circuit) is the new user name added. I also used the command “tail -5 /etc/passwd” to prove the new user account was created with a home directory.

4. Set a password for the new user.

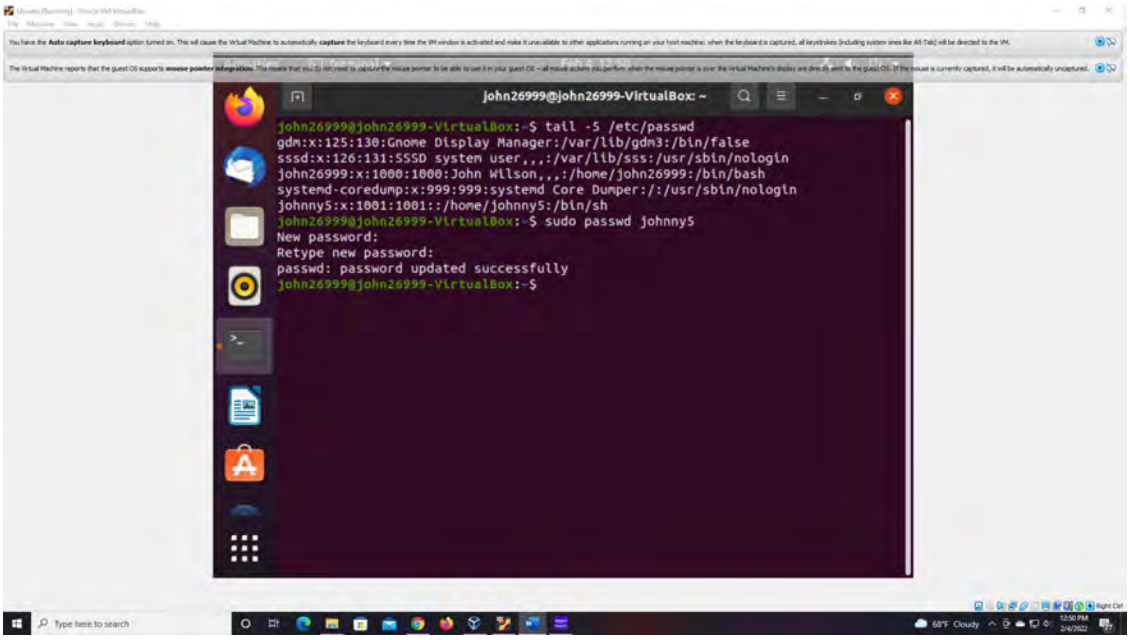

Figure 4 Screenshot of JWILS082 Computer screen for step 4

Above is the screenshot of the command " sudo passwd johnny 5" 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. "johhny5" is the name of new users password that was added or changed.

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

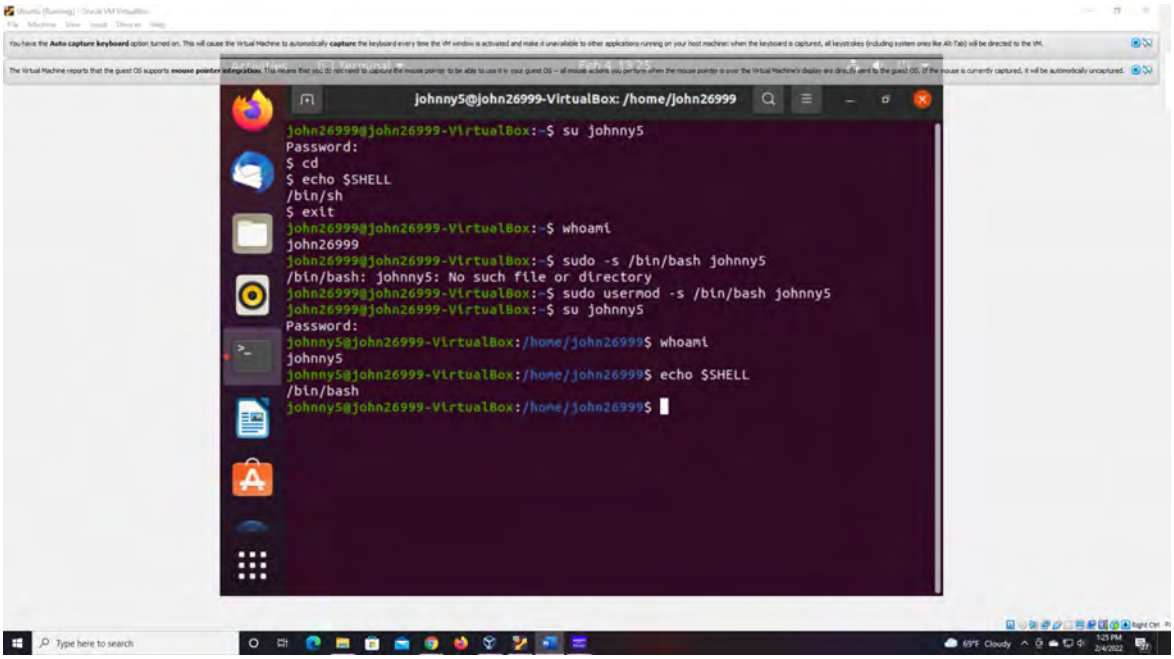

Figure 5 Screenshot of JWILS082 Computer screen for step 5

Above is the screenshot of the command " sudo usermod -s /bin/bash johnny5" 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. "johhny5" is the users new shell that was changed from "/bin/sh" to "/bin/bash". I also used the command "echo $SHELL" to show that the change was made.

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

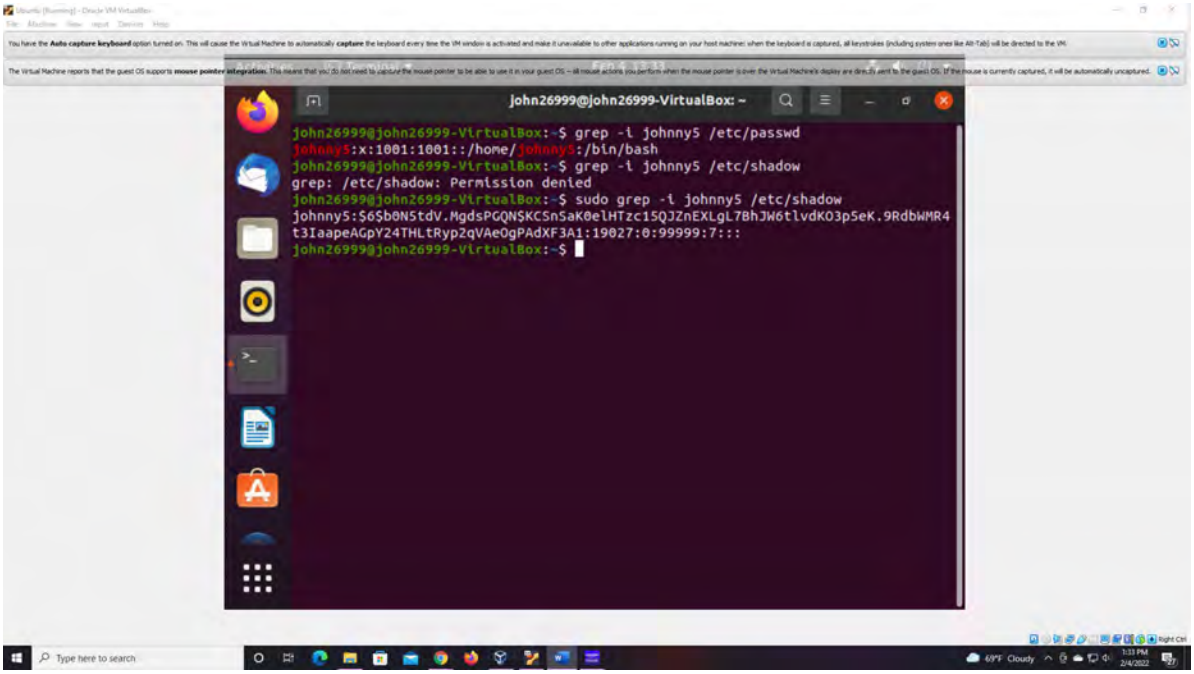

Figure 6 Screenshot of JWILS082 Computer screen for step 6

Above is the screenshot of the command " sudo grep -I johnny5 /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. "johnny5" is the user name I am searching. "/etc/shadow" is where the users group info, including administrators and the group password.

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

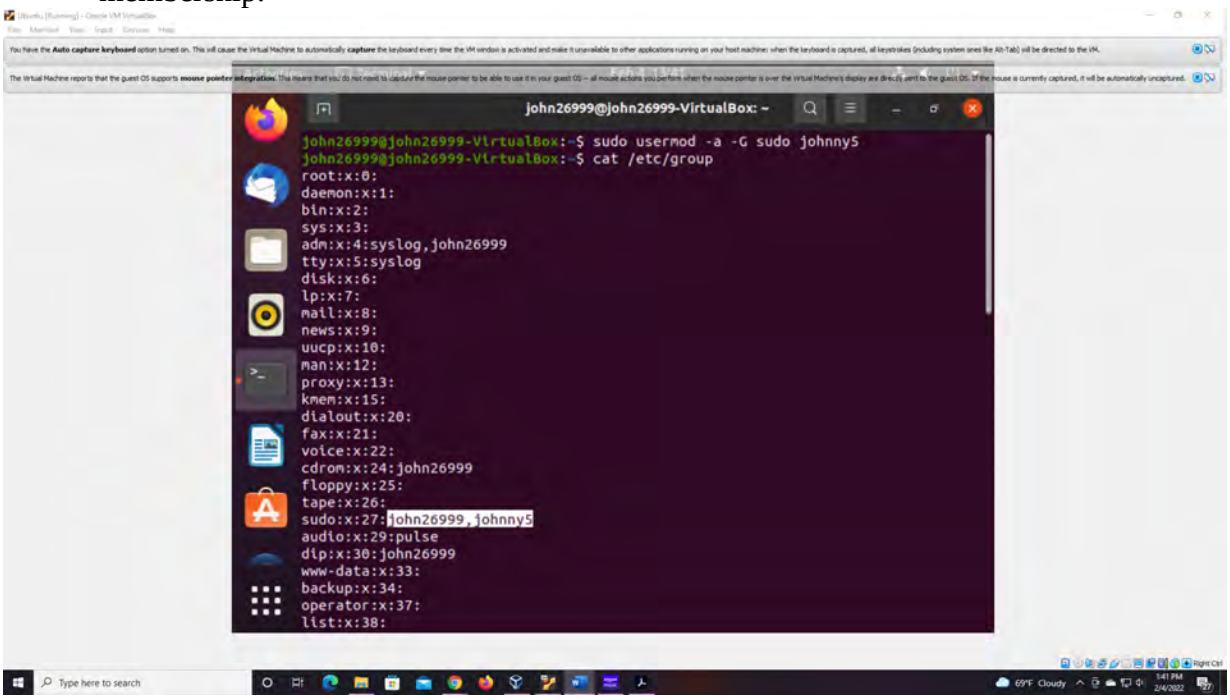

Figure 7 Screenshot of JWILS082 Computer screen for step 7

Above is the screenshot of the command " sudo usermod -a -G sudo johnny5" that adds the new user to the sudo group without overriding the existing members with the sudo group. "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. "-a" is the command to append a user to supplemental groups without removing the user from other groups. "-G" new list of supplementary GROUPS. "sudo" is the group you want the user to be appended. "johhny5" is the name of the user attached to the sudo group.

8. Switch to the new user's account.

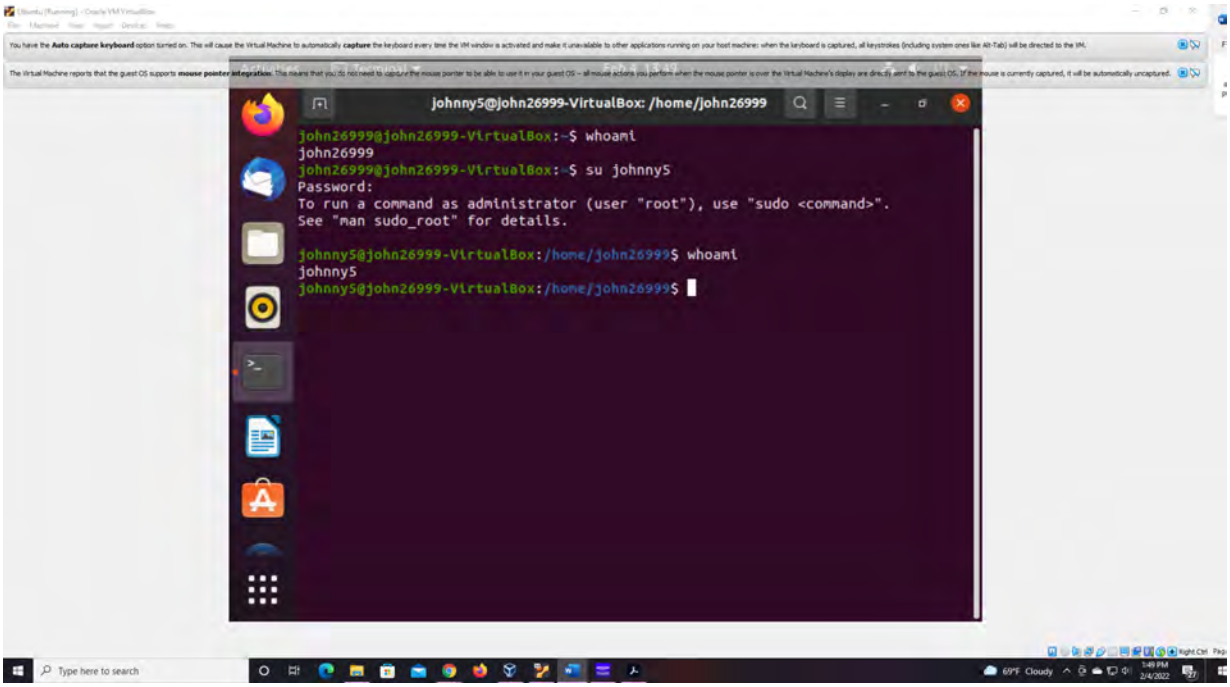

Figure 8 screenshot of JWILS082 Computer screen for step 8

Above is the screenshot of the command "su johnny5". "su" is the command to switch the user. "johnny5" is the name of the new user you want to switch from "john26999" to "johnny5". I also did the command "whoami" to porve that the user were switched from "john26999" to "johnny5"

TASK B

GROUP ACCOUNT MANAGEMENT (12 * 5 = 60 POINTS)

1. Return to your home directory and determine the shell you are using.
2. Display the current user's ID and group membership.

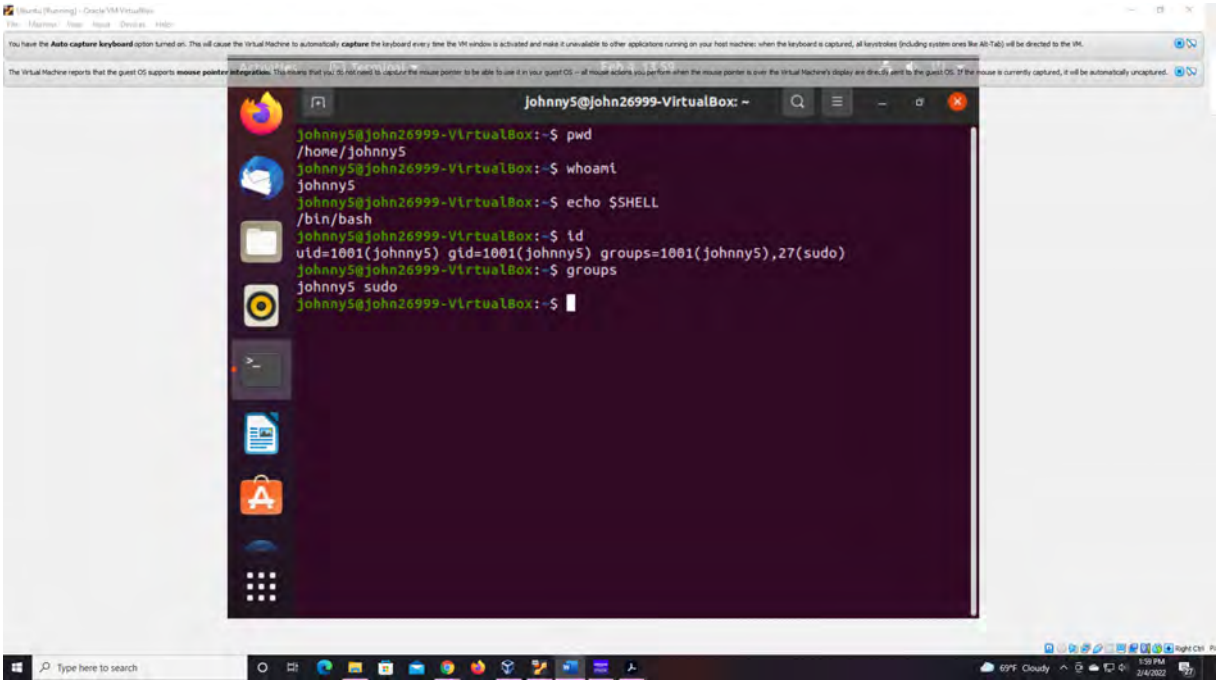

Figure 9 screenshot of JWILS082 Computer screen for step 1 and 2

Above is the screenshot of the command "pwd" that illustrates I am in my home directory. I also used the command "whoami" to show the user. I used the command "echo $SHELL" to determine the shell the user is utilizing. I used the comman "id" to show all the groups that johnny 5 is a part of. And I used the command "groups" to show the group membership for usr johnny5.

3. Display the group membership of the root account.

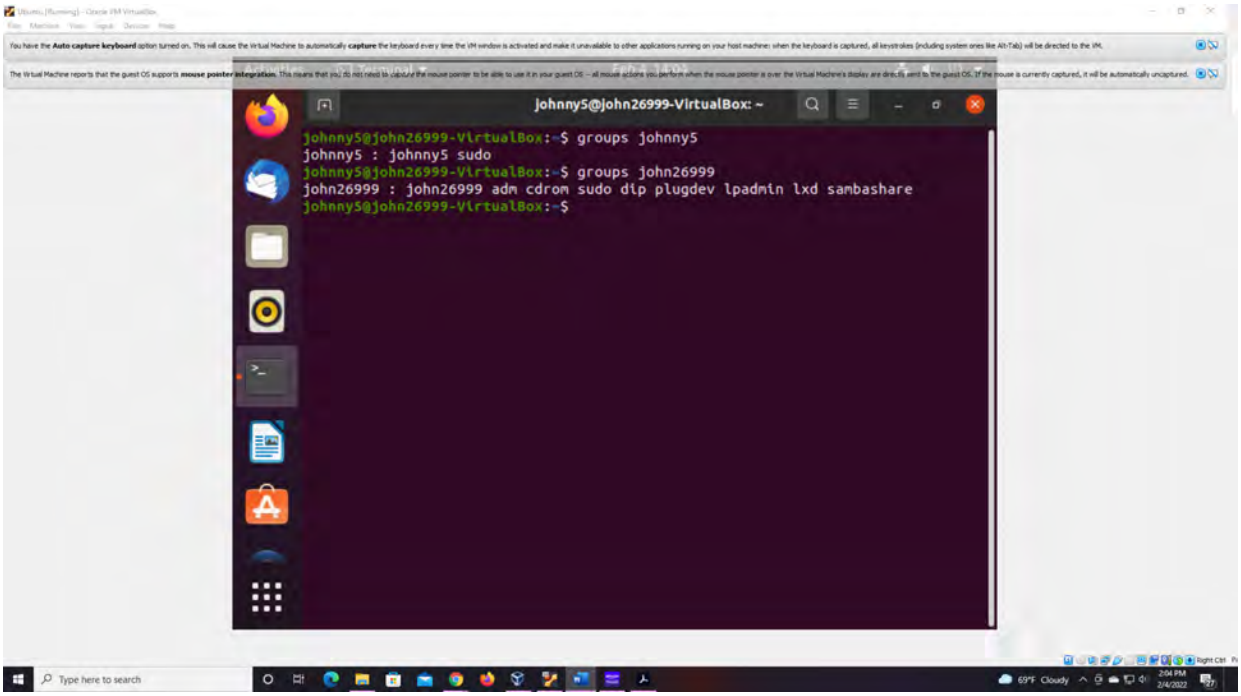

Figure 10 screenshot of JWILS082 Computer screen for step 3

Above is the screenshot of the command “groups johnny5” and groups john26999” that displays the group membership of the root account. ”groups” to show the group membership for usr johnny5. I did the smathing for user “john26999”.

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

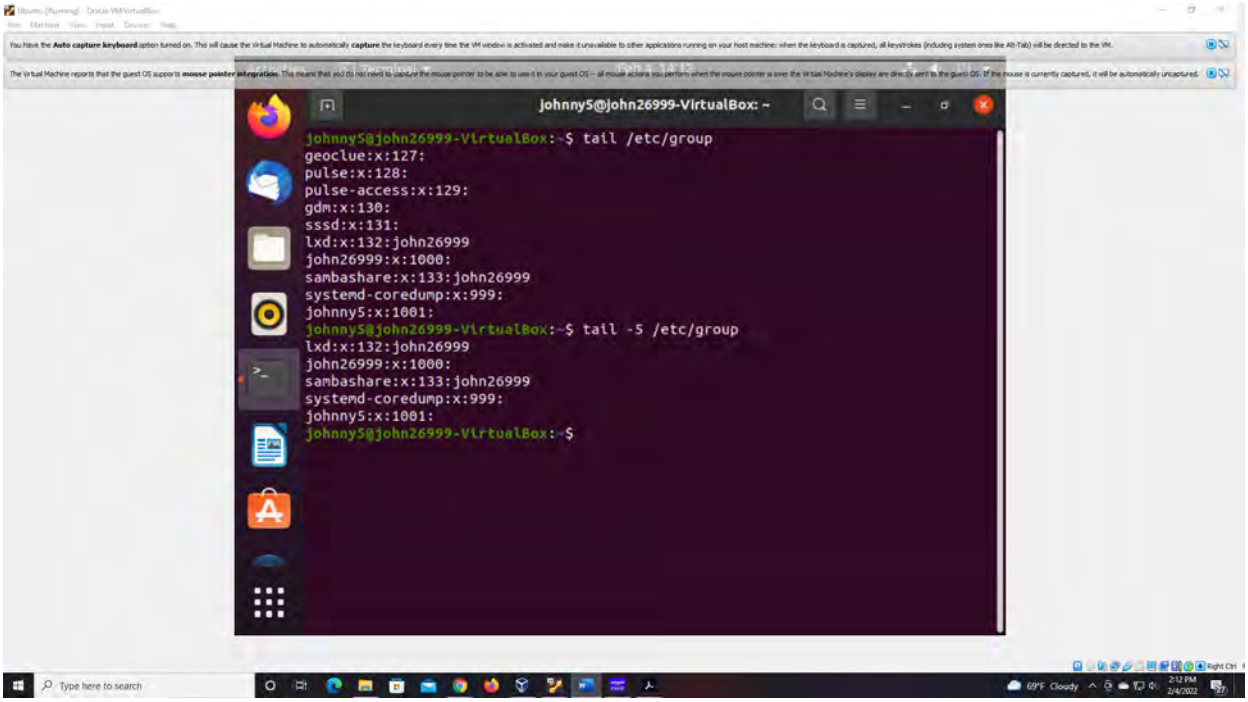

Figure 11 screenshot of JWILS082 Computer screen for step 4

Above is the screenshot of the command “tail -5 /etc/group” that shows the uer owner and group owner of the “/etc/group”. “tail” is the command that shows the information at the end. “-5” is the command the says it only wants five lines. “/etc/group”0 is the place to look.

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.

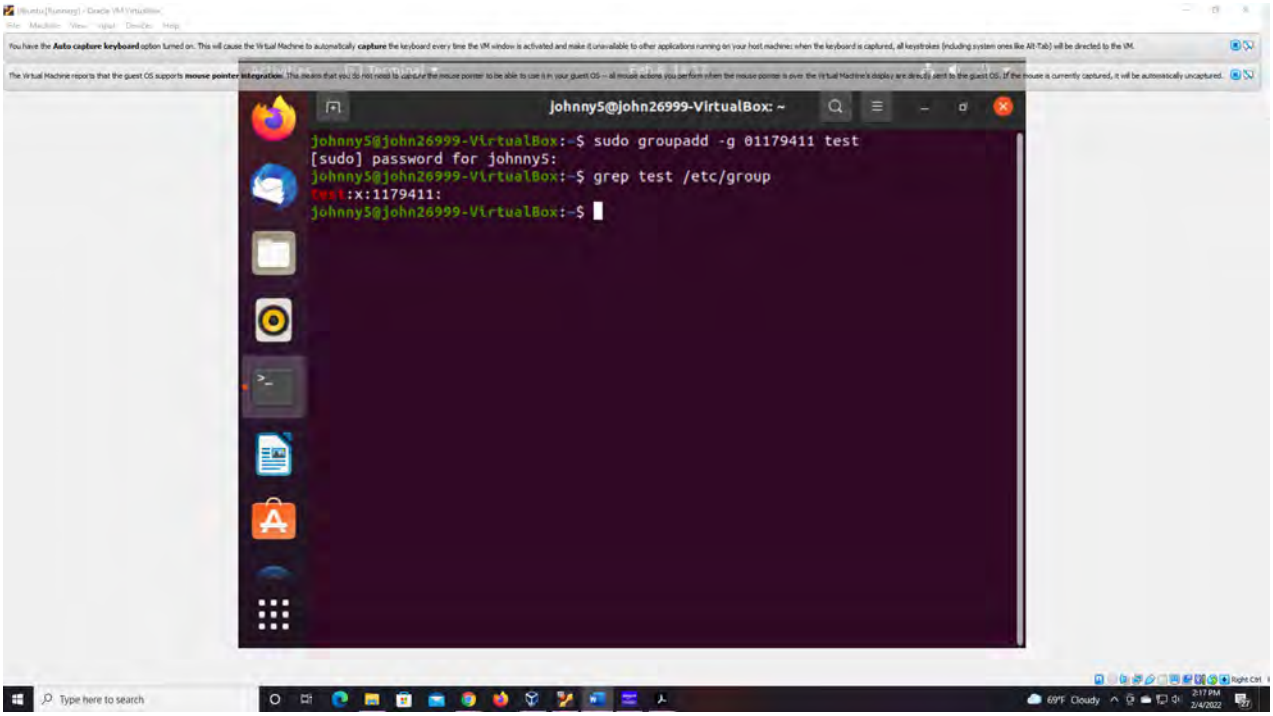

Figure 12 screenshot of JWILS082 Computer screen for step 5 and 6

Above is the screenshot of the command “sudo gropuadd -g 01179411 test” that crates a group named test and uses my UIN as the group ID (GID). “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. “-g” is the command to assign a GID for the new group ID. “01179411” is the name of the new GID. “test” is the new group name. I then did the command “grep test /etc/group” to display the group account information for the test group to show it was executed correctly.

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

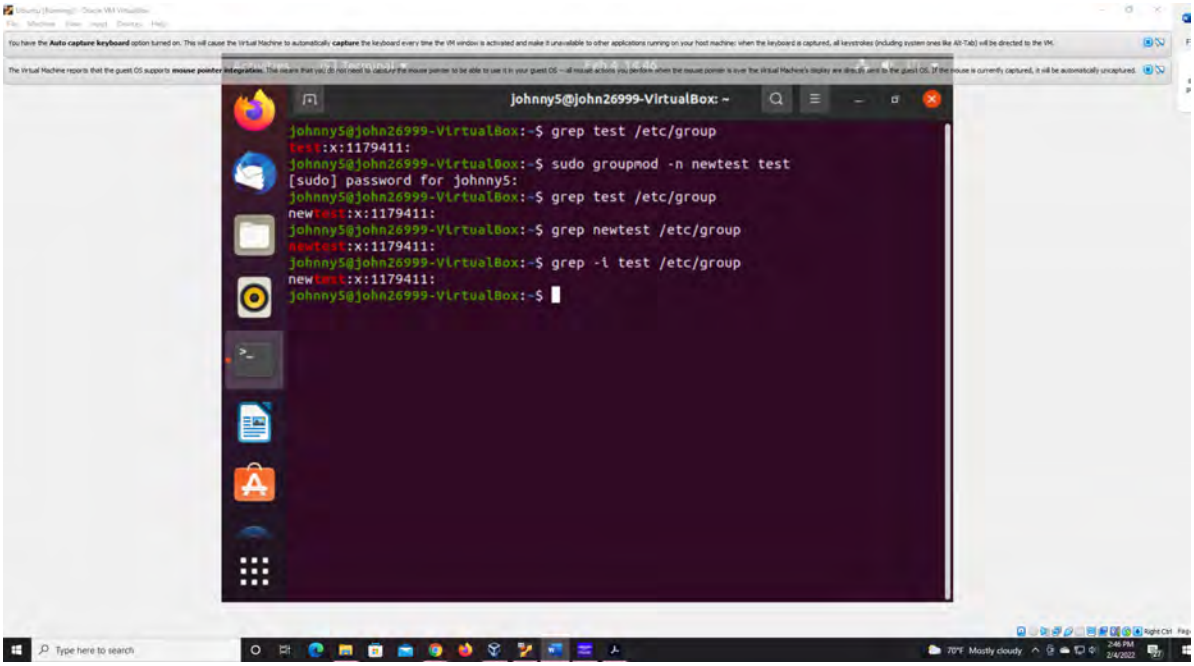

Figure 13 screenshot of JWILS082 Computer screen for step 7

Above is the screenshot of the command “sudo groupmod -n newtest test” to change the group name from test to newtest. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “groupmod” is the command that modifies changes to a group. “-n” is the command to change the name of a group. “newtest” is the new name for the group. “test” is the name of the group that will be changed. I also did the command “grep newtest /etc/group” to display the group account information for the test group to show the name change was executed correctly.

8. Add the current account (xxxxx) as a secondary member of the **newtest** group without overriding this user's current group membership

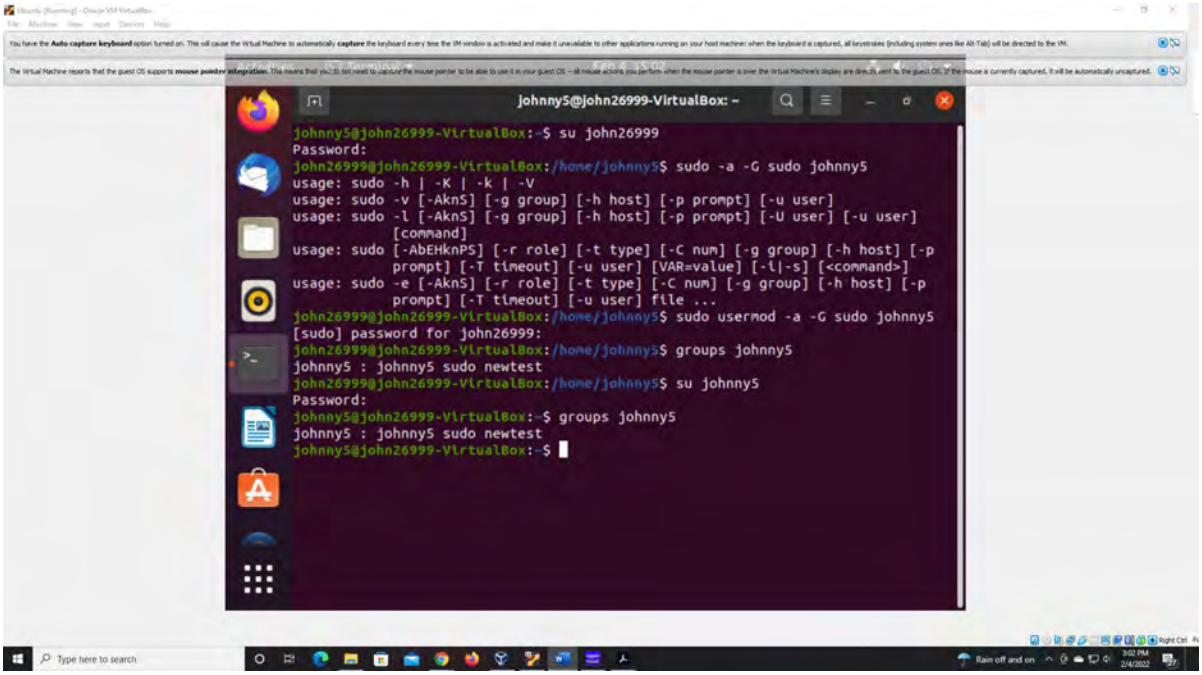

Figure 14 screenshot of JWILS082 Computer screen for step 8

Above is the screenshot of the command " sudo usermod -a -G newtest johnny5" that adds a user to the sudo group without overriding the existing members with the sudo group. "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. "-a" is the command to append a user to supplemental groups without removing the user from other groups. "-G" new list of supplementary GROUPS. "sudo" is the group you want the user to be appended. "johhny5" is the name of the user attached to the sudo group. I also did the command "groups johnny5" to show the groups were not changed.

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.

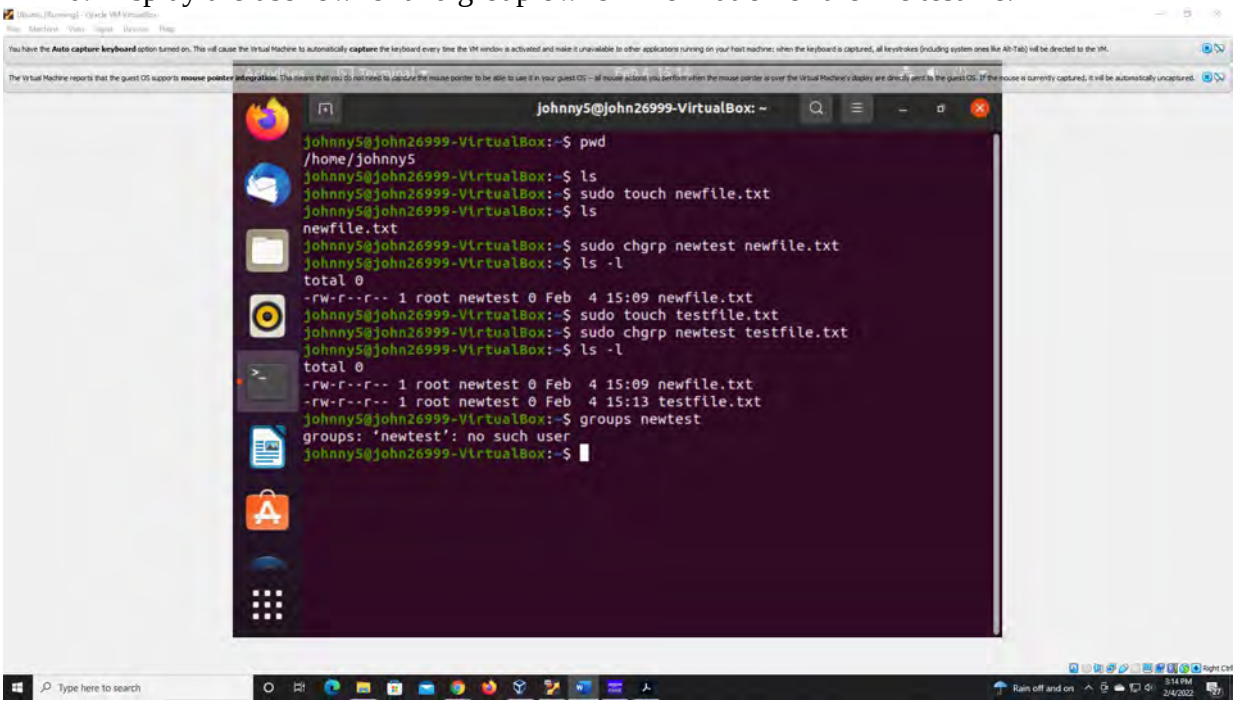

Figure 15 screenshot of JWILS082 Computer screen for step 9 and 10

Above is the screenshot of the command " sudo touch testfile.txt" that creates a new file named testfile in the account's 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). "touch" is the command that creates anew file. "testfile" is the name of the file created.

I also did the command "sudo chgrp newtest testfile.txt" to change the group owner to newtest. "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 to change the group. "newtest" us the name of the group that is not the owner. "testfile.txt" is the file that chged groups.

11. Delete the newtest group, then repeat the previous step. What do you find?

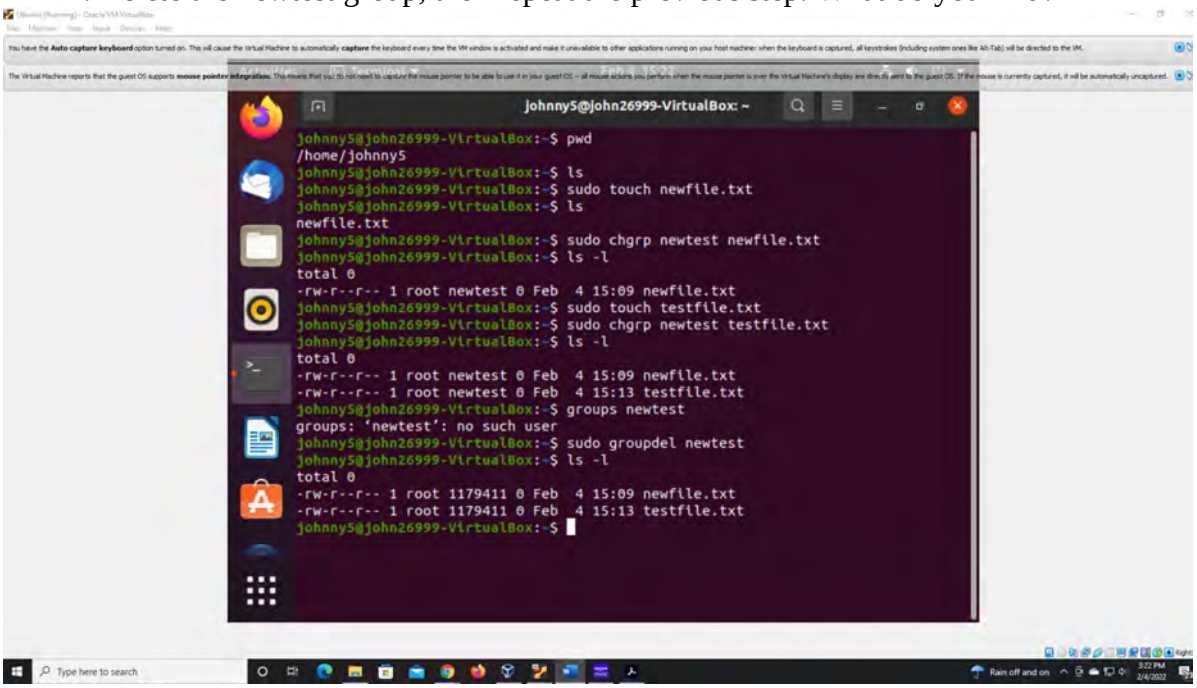

Figure 16 screenshot of JWILS082 Computer screen for step 11

Above is the screenshot of the command " sudo groupdel newtest" that deletes the group newtest. "sudo" is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). "groupdel" is the command that deletes a group. "newtest" is the name of the group deleted. I also did the command "ls -l" to show the new owners of testfile.txt which is the root.

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

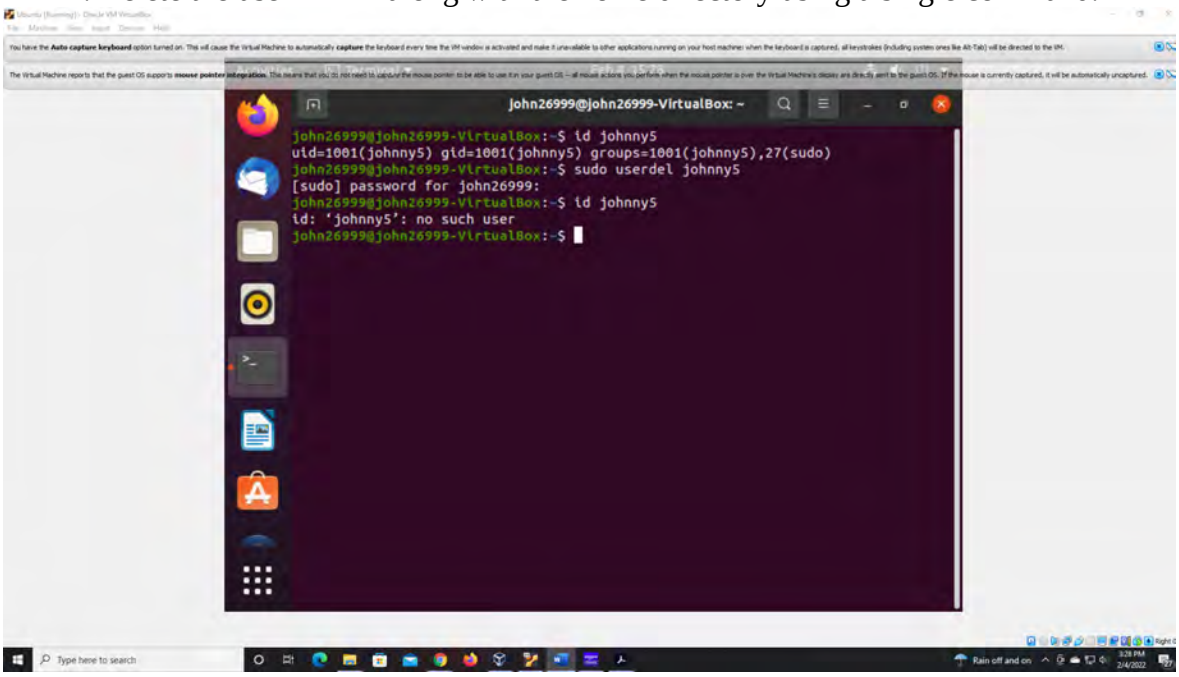

Figure 17 screenshot of JWILS082 Computer screen for step 12

Above is the screenshot of the command " sudo userdel johnny5" that deletes the user and the 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). "userdel" is the command that deletes a user. "johnny5" is the name of the user deleted. I also did the command "id johnny5" to show the user was deleted successfully.