**Lab 1.**

**Exercise**

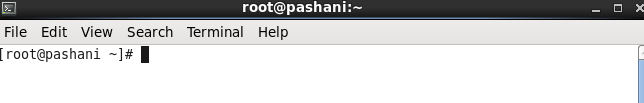


Figure .0

I was able to log in as a privileged user by using the username “root” and the password associated with the root account.

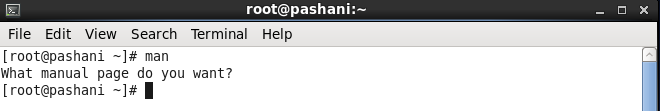


Figure 1.1

The man command works very fine, the figure above shows that the command was asking me what page I wanted to show.

(c-a)

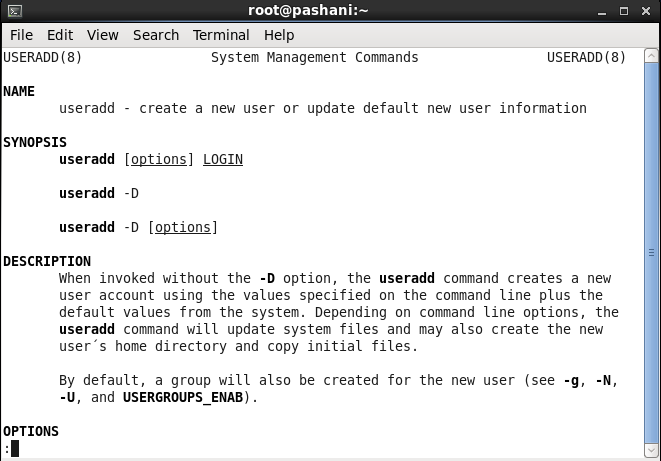


Figure 1.2

The man useradd command, shows the manual for the useradd command, the command is used to create a new user or update new user information, the syntax for adding a user is useradd [option] username, the options that can be used are as follows :

1. -g (start group id).
2. -G admins (adds the user to the admin group).
3. -D (displays the defaults for the useradd command)
4. -s shell name (sets the default shell)
5. -d home directory (sets the home directory for the user)
6. -m (this command creates the user’s home directory if it does not exist)
7. -k PATH (skeleton directory)
8. -e YYYY-MM-DD (sets the account’s expiry date)
9. -f number of days (sets the number of days after the password expires before the account is permanently disabled)

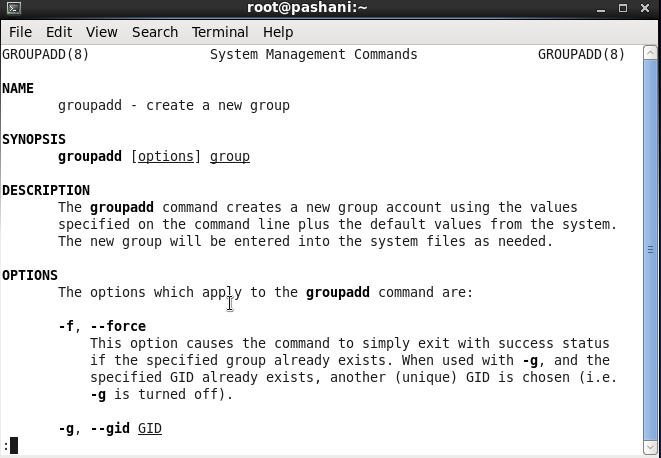
(c-b) 

Figure 1.3

The man groupadd command shows the manual of the groupadd command, it also shows the syntax of the command and the options that can be used when creating a group, the syntax for creating a group is groupadd [options] group.

(c-c)

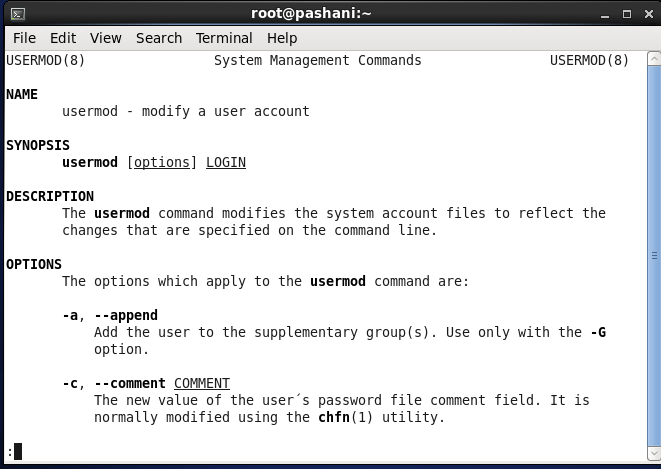


Figure 1.4

The man usermod command shows the manual for modifying system user account files, it shows the syntax of the usermod command and the options that can be used when modifying user information. The syntax is usermod [options] username.

(c-d)

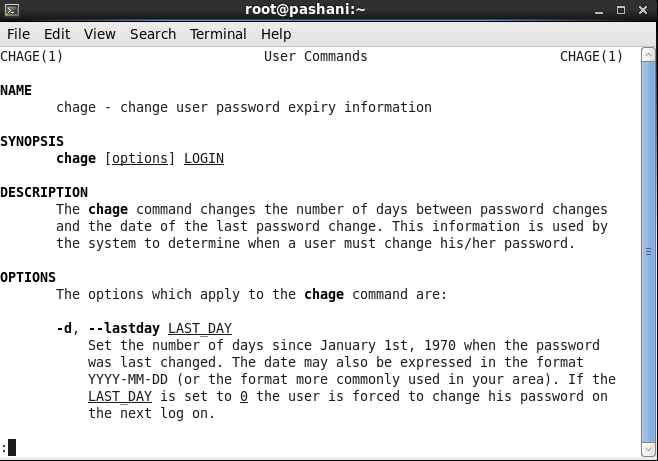


Figure 1.5

The man chage command shows the manual for changing a user’s password expiry information, it shows the syntax and explains the options that can be used with the command, the syntax for changing a user’s password expiry information is chage [options] username.

(c-e)

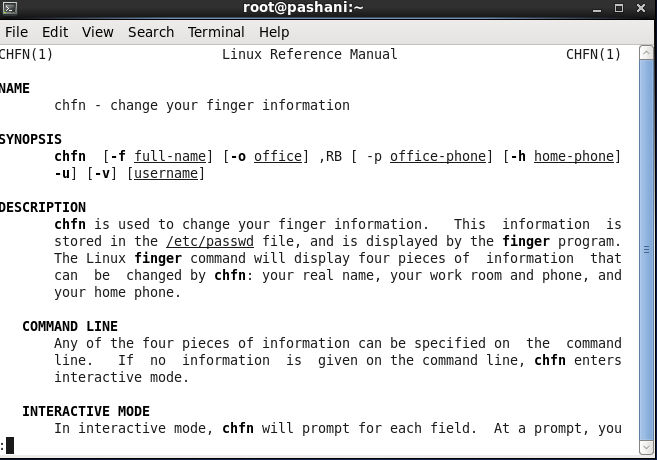


Figure 1.6

The man chfn command shows the manual for the chfn command which is used to change a users finger information, the manual also shows the syntax of the chfn command and the options that can be used with it, the syntax is chfn [options] username

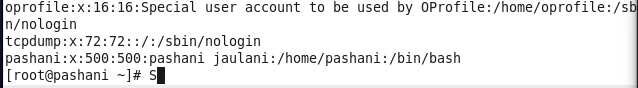
(d-a)

Figure 1.7

The /etc/passwd contains information about the user or accounts on the system, the seven fields are denoted by a colon symbol, the information about a user or account is stored in a single line per user. The information contained in the fields is:

1. Username: the first field shows the username or the account.
2. Password: the second field is for the password; an x character indicates that the password is encrypted.
3. User ID: The third field contains the user ID; each user is assigned a unique user ID. ID 0 is reserved for root.
4. Group ID: the fourth field contains the primary group ID the user belongs to.
5. User ID information: the fifth field is the comment field, it permits you to add extra information about the user such as full name, phone number, etc.
6. Home directory: the sixth field shows the path to the user’s home directory when they successfully log in, if the field is blank then the user's directory becomes /.
7. Default shell: the last field contains the path to the user’s default shell.

(d-b)



Figure 1.8

The /etc/group file contains the group names on the system, it stores the group name, group ID, and the members in the group. The information is stored about a group is stored in a single line per group.

(d-c)



Figure 1.9

The /etc/shadow is a text-based file that holds information about the system’s user's password, it contains one line per entry with each line representing an account.

The entries a denoted by a colon, these denotations hold the information in this order:

1. Username
2. Encrypted password
3. Last date the password was changed
4. Minimum age of the password
5. Maximum age of the password
6. Password warning period
7. Number of days after expiration of the password before account is permanently disabled
8. The expiration date of the password
9. The last field is ignored and mostly reserved for future use

(d-d)

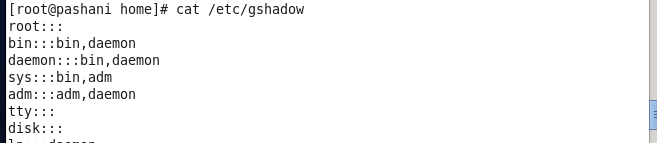


Figure 1.10

The /etc/gshadow contains shadowed information for group accounts. To maintain security this file should only be read-only. This file contains :

1. The group’s name.
2. Encrypted password for the group
3. Group administrators.
4. Group members.

(d-e)



Figure 1.11

The /etc/gpasswd is used to administer the /etc/passwd and the /etc/shadow files

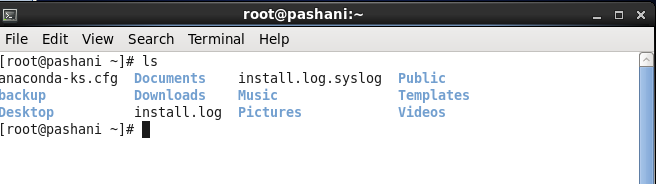


Figure 1.12

ls command is used to list computer files, when it is typed without any arguments or options, it lists the files in the current working directory, as shown above, it listed all the files in the root’s home directory because that was the current directory.

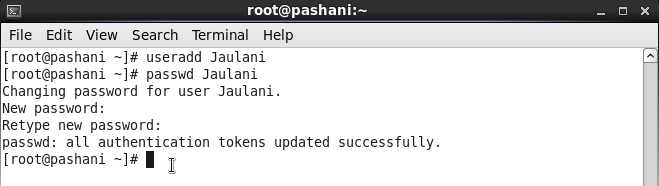


Figure 1.13

The useradd command added a new user and I also added a password to the user account for encryption.



Figure 1.14

The new account was successfully added, the /etc/passwd file has been updated with a new entry, that has information that is separated by a colon, the first field shows the username, second field the password which is encrypted because of the x character, third field the user’s ID, fourth the group ID, the fifth field is empty because I did not add any finger information about the user, the sixth field shows the users home directory and the last field shows the users default shell.



Figure 1.15

The /etc/group file has been updated with the new user showing the user's default group ID



Figure 1.16

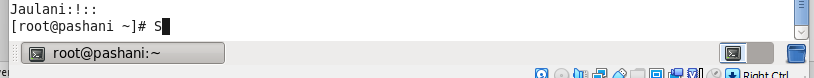
The /etc/shadow file has been updated showing the username, the encrypted password, account aging information, the aging information is the accounts expiry date, and the password expiration date. 

Figure 1.17

The /etc/gshadow file

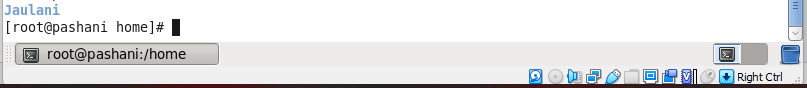


Figure 1.18

The /home directory has a new folder named after the created username





Figure 1.19

The testuser has been added to the user's group which has a group id of 502

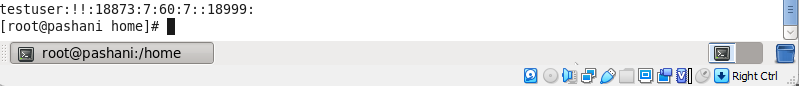
1. 

Figure 1.20

The account’s password aging information has been configured successfully, the aging information is stored in the /etc/shadow file.



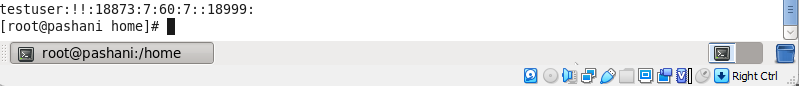


Figure 1.21

Aging information has been configured successfully.

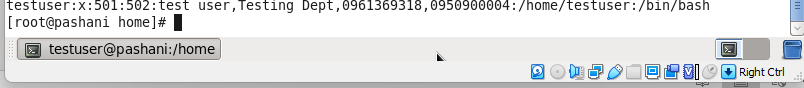


Figure 1.22

Finger information about the user was added successfully, I was able to verify by checking

The /etc/shadow file’s contents.

II)



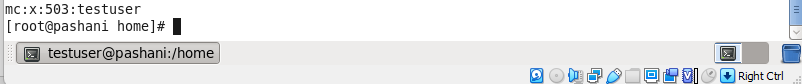


Figure 1.23

The testuser account has been added to the mc group.



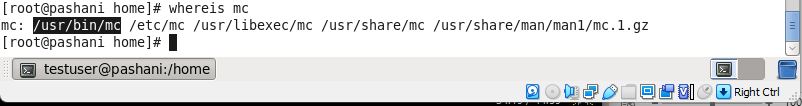


Figure 1.24

The mc program is located in the /usr/bin/mc directory





Figure 1.25





Figure 1.26

I gave ownership of the mc program to the mc group using the chown command,

The left side of the colon accepts individual accounts while the right side accepts group accounts that you want to give ownership of a directory.



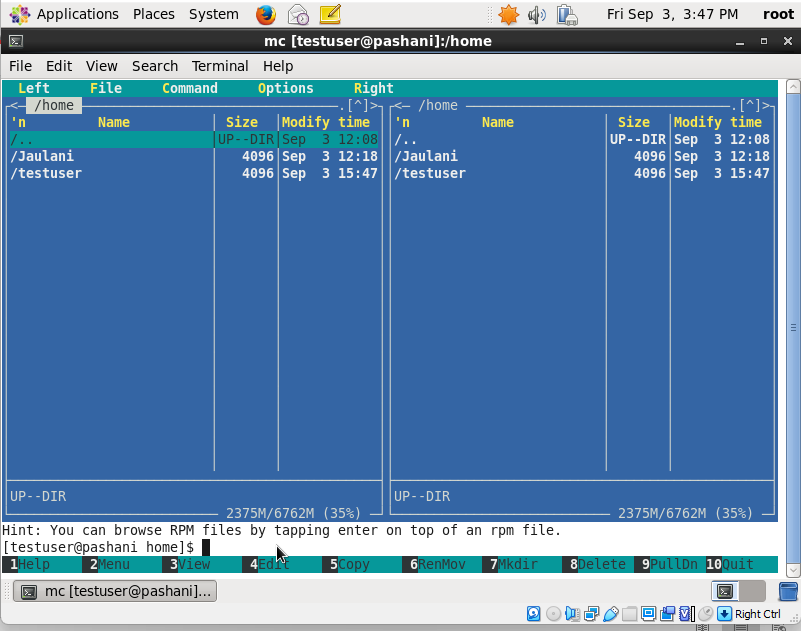


Figure 1.27

The mc program has worked correctly because the testuser belongs to the mc group which has ownership of the mc program.



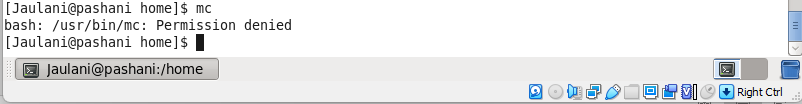


Figure 1.28

Access to the mc program was denied from this user account because it doesn’t belong to the mc group.

**Task**

****

Figure 1.29

To add a user without using the useradd command, I added an entry to the /etc/passwd file

about the new user, with the username being newbee, user\_id 502, group id 504, home directory /home/newbee, and the default bash /bin/home. To edit the /etc/passwd I used the vi editor.



Figure 1.30

Creating a group for the newbee user by adding a group and a group id to the /etc/group file using vi editor.



Figure 1.31

I created the home directory for the newbee user using the mkdir command



Figure 1.32

I gave permission to the newbee home directory to the newbee user account



Figure 1.33

To remove the password and enable account aging information, I added an entry to the /etc/shadow file to satisfy the requirements of the task using vi editor.



Figure 1.34

For the user to login into the newbee account, I had to copy the skeleton for a user account from the /etc/skel directory to the /home/newbee directory, the skel is used to initiate the home directory when the user is first created.

**Testing**



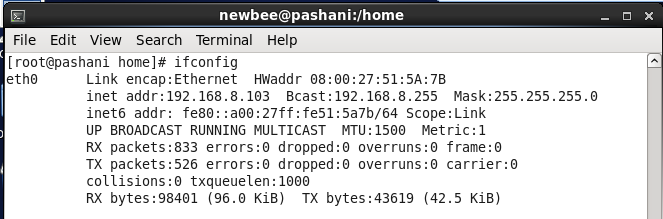
****

Figure 1.35





Figure 1.36



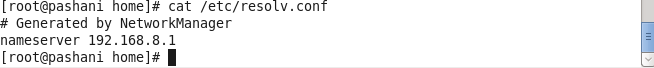


Figure 1.37



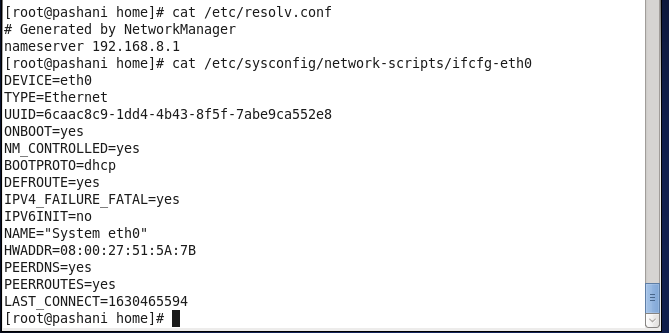


Figure 1.38





Figure 1.39



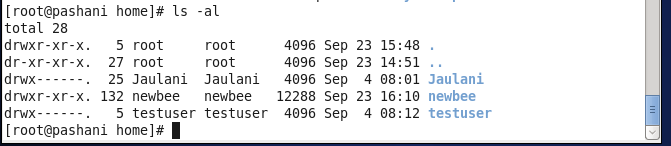


Figure 1.40

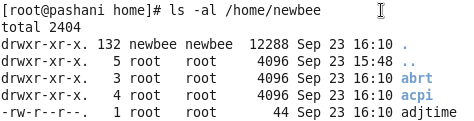


Figure 1.41





Figure 1.42





Figure 1.43





Figure 1.44

**Conclusion**

I aim to critically reflect on my learning experience in this lab using the Rolfe model of reflective writing, I was able to log in as a root user and use the man command which provided a detailed manual for various programs and commands on Linux, using the cat program (concatenate) I was able to view account information that is stored in various files e.g /etc/passwd, /etc/group, and /etc/shadow.

I added a new user account after reading and understanding the manual for the useradd command, the account was also added to a specific group with account password aging information using the chage command. Using yum I installed the mc program which is a graphical orthodox cross-platform file manager, to change permissions for the mc program, I had to find the location of the executable command of the mc program using the whereis command, I gave the mc group permission to the mc program to read, write and execute it, other accounts and groups did not have permission to the program and were not able to run it.

For the task, I was required to add a new user to the system without using the useradd, usermod,groupadd, chage, or chfn commands, the approach I took was editing the /etc/passwd, /etc/group and /etc/shadow files and making a home directory for the user using the mkdir command. to edit these files I used the vi editor which proved to be easy to work with, I successfully added the user and added account password aging information correctly.

The challenge I faced was editing the /etc/shadow file because this is a read-only file, I was able to overcome this challenge by giving only the root user full ownership to this file to prevent any user to tamper with other accounts. Secondly, after adding a new user by editing the said above files, I was not able to login to the account because it lacked certain files like the .bash\_logout, .bash\_profile, these files are called the skeleton and are found in the /etc/skel directory, using the cp command, I copied the contents of the /etc/skel directory to the home directory on the user account. Afterward, then I was able to log in to the account.

This lab has expanded my knowledge of the Linux operating system, I can confidently add a new user to the system without any challenges, I know exactly where user account information is stored and how to manipulate it.