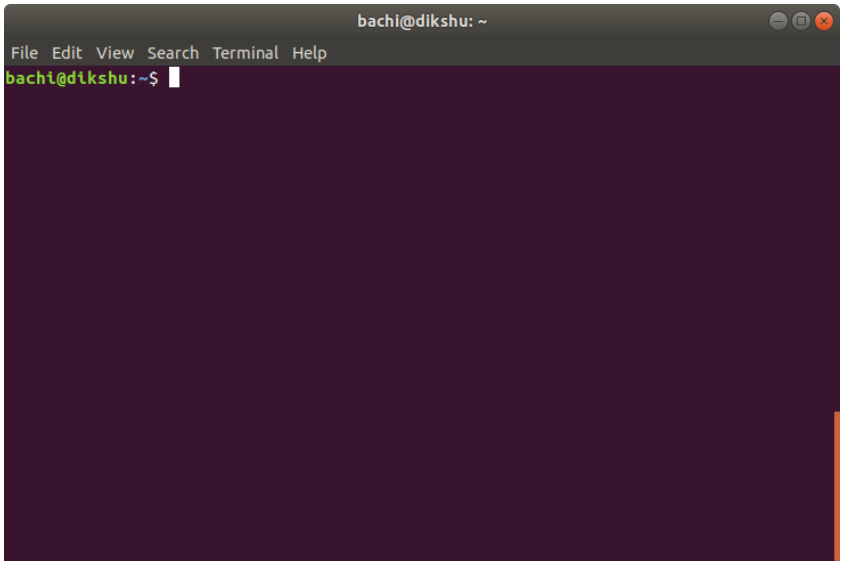
DIKSHITHA VANI V
205001032

UNIX ASSIGNMENT -3

EXERCISE-1:

1. Launch a terminal.



2. Check which group or groups you belong to.

Description: groups command displays the group memberships for the given USERNAME, if no USERNAME is specified, displays for the current user.

```
bachi@dikshu:~$ groups
```

bachi : bachi adm cdrom sudo dip plugdev lpadmin sambashare

3. Use the umask command to set the default permission to 700. What is the default permission for files after this command?

Description: umask command is used to change default permissions of the files. To set the permission to 700, we have to give umask 077 ->this umask value refers to the permissions to be taken away from the default permission 777 of directories.(7-0, 7-7 ,7-7)

```
bachi@dikshu:~$ umask 077
```

4. Create a directory named chapter4 under your home directory.

Description:mkdir is the command used to create directories.

bachi@dikshu:~$ mkdir chapter4

5. Check the default permission of this directory.Is it 700?

   Description: ls -ld command displays the long format of the specified directory. Here, the directory has all the permissions for owner/present user, but users in groups and others have no access permissions. Yes , the permission of this directory is 700.

   bachi@dikshu:~$ ls -ld chapter4

   drwx------ 2 bachi bachi 4096 Oct 28 07:53 chapter4

6. Create a directory under the chapter4 directory (without moving from your home directory) and name it session1.

   bachi@dikshu:~$ mkdir chapter4/session1

7. Check the permission.Is it 700?

   Description:Yes , the permission of this directory is 700.

   bachi@dikshu:~$ ls -ld chapter4/session1

   drwx------ 2 bachi bachi 4096 Oct 28 07:54 chapter4/session1

8. Move to the session1 directory.
   Description : cd command is used to change directories.

   bachi@dikshu:~$ cd chapter4/session1

9. Create a file named hw41 under this directory. Save this file.

   Description: touch command is used to create new files.

   bachi@dikshu:~/chapter4/session1$ touch hw41

10. Check the permission of this file. Is it 700 or 600? Why? Explain the difference between the permissions for files and directories.

    Description: The file permission is 600. This is because the default permission for files is 666 while for directories it is 777. when the new umask value given (113), as already all

execute options are taken from the files, the others users in the file will have only read permission while users in the group will have read and write permission

By default, 666 is given as execute permission on text files can result in weird outputs.

bachi@dikshu:~/chapter4/session1$ ls -l

total 0

-rw------- 1 bachi bachi 0 Oct 28 07:55 hw41

11. Do users in your group have any access to this file? Do other users (outside of your group) have any access to this file?

Description: Only owner has all permissions to the source directory and read -write permissions for the file. Users in the groups don't have access to the file,

bachi@dikshu:~$ ls -ld chapter4/session1

drwx------ 2 bachi bachi 4096 Oct 28 07:54 chapter4/session1

bachi@dikshu:~/chapter4/session1$ ls -l

total 0

-rw------- 1 bachi bachi 0 Oct 28 07:55 hw41

12. Change the permissions to allow users in your group only to copy this file to their own directories. Is there a need to change the permission of any directories? If yes, make necessary changes.

Description: Read and execute permission is given to all users in the group for chapter4 directory and session1 directory.

bachi@dikshu:~/chapter4/session1$ cd

bachi@dikshu:~$ chmod g=rx chapter4

bachi@dikshu:~$ chmod g=rx chapter4/session1

bachi@dikshu:~$ ls -ld chapter4

drwxr-x--- 3 bachi bachi 4096 Oct 28 07:54 chapter4

bachi@dikshu:~$ ls -ld chapter4/session1

drwxr-x--- 2 bachi bachi 4096 Oct 28 07:55 chapter4/session1

13. Let a user in your group copy this file into her home directory. Was the copy successful? If not, find the reason and take the appropriate action(s) to correct it. Then try again with the other user in your group.

Description: Copy was not successful.So the permissions of the group is changed to read to enable the users in the group to read the file.

bachi@dikshu:~$ chmod g=r chapter4/session1/hw41

bachi@dikshu:~$ ls -ld chapter4/session1/hw41

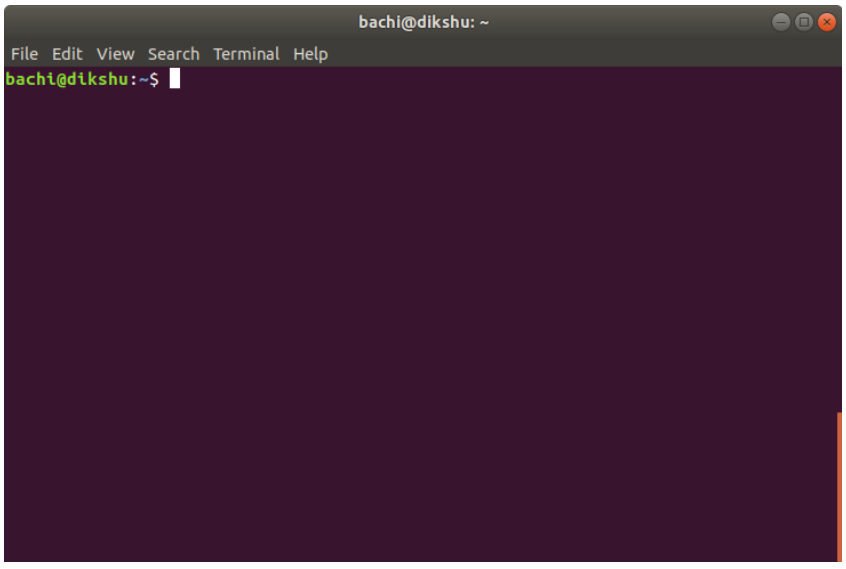
-rw-r----- 1 bachi bachi 0 Oct 28 07:55 chapter4/session1/hw41

dikshitha@dikshu:~$ cp /home/bachi/chapter4/session1/hw41 ~/copyhw41.txt

14. .Quit the terminal.

EXERCISE-2:

1. Launch a terminal.



2. Check which group or groups you belong to.

Description: groups command displays the group memberships for the given USERNAME, if no USERNAME is specified, displays for the current user.

bachi@dikshu:~$ groups

bachi : bachi adm cdrom sudo dip plugdev lpadmin sambashare

3. Check your default mask.

   Description: umask command sets the user file-creation mask to mode. If mode is not given, prints the current value of the mask.

   bachi@dikshu:~$ umask

   0002

4. Create a directory called garbage under your home directory.

   Description: mkdir command creates the directory(ies), if they do not already exist.

   bachi@dikshu:~$ mkdir garbage

5. Check the permission of this directory. Make a note of it.

Description: ls -ld command displays the long format of the specified directory. Here, the directory has all the permissions for groups but others have only read and execute permissions.

bachi@dikshu:~$ ls -ld garbage

drwxrwxr-x 2 bachi bachi 4096 Oct 28 08:28 garbage

6. Change your default mask so that the default permission is 664.

   Description: umask command sets the user file-creation mask to the given mode. If mode is not given,prints the current value of the mask.

bachi@dikshu:~$ umask 113

What is the default permission for directories after you make this change?

Answer: The default permission for directories: 664 (rw-rw-r--)

7. Check the permission for the garbage directory. *Has it been changed after setting the default mask? Why or why not?*

Answer: No, the permissions haven't changed because the directory was created before change in the umask.

bachi@dikshu:~$ ls -ld garbage

drwxrwxr-x 2 bachi bachi 4096 Oct 28 08:28 garbage

8. Delete this directory.
   Description: rmdir is used to remove directories that are empty.

   bachi@dikshu:~$ rmdir garbage

9. Create a directory called session2 under the chapter4 directory.

   bachi@dikshu:~$ mkdir chapter4/session2

10. Check the permission of this directory and make a note of it.

    Description: ls -ld command displays the long format of the specified directory.

bachi@dikshu:~$ ls -ld chapter4/session2

drw-rw-r-- 2 bachi bachi 4096 Oct 28 08:31 chapter4/session2

11. Remove the x permission for the user from this directory.

Description: chmod command changes the file mode bits of each given file according to mode, a symbolic representation of changes to make in the bit pattern for the new mode bits (- means to remove and + means to add a particular permission).

bachi@dikshu:~$ chmod u-x chapter4/session2

12. Move to the session2 directory.

    bachi@dikshu:~$ cd chapter4/session2

bash: cd: chapter4/session2: Permission denied

You should have a problem. Do you know what the problem is? Fix the problem.

Answer: The problem is that we can't read directories without giving execute permission to it. To resolve this we add the execute permission to the directory using chmod command (+x).

bachi@dikshu:~$ chmod u+x chapter4/session2

bachi@dikshu:~$ cd chapter4/session2

13. Create a file named hw42 under this directory. Save this file.

    bachi@dikshu:~/chapter4/session2$ touch hw42

14. Check the permissions of this file.Can users in your group copy this file? Can they change this file? Can users outside your group copy this file? Can they change this file? Is this file executable?

Answer: Users inside and outside the group cannot copy this file, as they are denied execute permissions for the source directory. If execute permission is granted, for session directory,Users inside the group can read and modify the file, but not execute it.

Other users can not read,modify or execute it as they do not have read and execute access to the chapter4 directory.

bachi@dikshu:~/chapter4/session2$ ls -l hw42

-rw-rw-r-- 1 bachi bachi 0 Oct 28 08:34 hw42

bachi@dikshu:~/chapter4/session2$ ls -ld

drwxrw-r-- 2 bachi bachi 4096 Oct 28 08:

bachi@dikshu:~$ ls -ld chapter4

drwxr-x--- 4 bachi bachi 4096 Oct 28 08:31 chapter4

15. Change the permissions of this file so that every user can read, modify, but not execute this file.

Description:The access of chapter4 is changed to give execute and read permissions to other users.

chmod command changes the file mode bits of each given file according to mode, an octal number representing the bit pattern for the new mode bits. Here, hw42 is set to 666 (only read and write permission to users, groups and others).

bachi@dikshu:~$ chmod o+rx chapter4

bachi@dikshu:~$ ls -ld chapter4

drwxr-xr-x 4 bachi bachi 4096 Oct 28 08:31 chapter4

bachi@dikshu:~/chapter4/session2$ chmod 666 hw42

bachi@dikshu:~/chapter4/session2$ ls -l hw42

-rw-rw-rw- 1 bachi bachi 0 Oct 28 08:34 hw42

16. Quit the terminal.