Mawlana Bhashani Science and Technology University

Lab-Report

Report No:04

Course code:ICT-3110

Course title:Operating Systems Lab

Date of Performance:04-09-2020

Date of Submission:16-09-2020

Submitted by

Name:Meraz Ahmed

ID:IT-18005

3rd year 1st semester

Session: 2017-2018

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment No: 04

Experiment Name: File operation and permission

Objective :

To learn about file permission and operation in a linux pc and be able to use them in real live scenario and understand why they are needed and what could be done with them .

File Permission :

On Linux and other Unix-like operating systems, there is a set of rules for each file which defines who can access that file, and how they can access it. These rules are called file permissions or file modes. The command name chmod stands for "change mode", and it is used to define the way a file can be accessed.

In general, chmod commands take the form:

chmod options permissions filename

Each file on a system has associated with it a set of permissions which are used to protect files: a file's permissions determine which users may access that file, and what type of access they have to it.
There are three general classes of users:

- The user who owns the file ("User")
- Users belonging to the file's defined ownership group ("Group")
- Everyone else ("Other")

In turn, for each of these classes of user, there are three types of file access:

- The ability to look at the contents of the file ("Read")
- The ability to change the contents of the file ("Write")
- The ability to run the contents of the file as a program on the system ("Execute")

So, for each of the three classes of user, there are three types of access. Taken together, this information makes up the file's permissions.
There are two ways to represent a file's permissions: symbolically (using symbols like "r" for read, "w" for write, and "x" for execute) or with an octal numeric value.

- 4 stands for "read",
- 2 stands for "write",

- 1 stands for "execute", and
- 0 stands for "no permission."

So 7 is the combination of permissions 4+2+1 (read, write, and execute), 5 is 4+0+1(read, no write, and execute), and 4 is 4+0+0 (read, no write, and no execute).

Commands :

ls – l :This command shows all the file in the current directory with there permission

```
meraz@meraz-VirtualBox:~$ ls -l
total 60
drwxr-xr-x 2 meraz meraz 4096 সেপ্টে 12 19:16 Desktop
drwxr-xr-x 4 meraz meraz 4096 সেপ্টে 12 22:09 Documents
drwxr-xr-x 2 meraz meraz 4096 ফেব্রু 26  2020 Downloads
-rw-r--r-- 1 meraz meraz 8980 ফেব্রু 25  2020 examples.desktop
drwxr-xr-x 2 meraz meraz 4096 মার্চ  2  2020 java
drwxr-xr-x 2 meraz meraz 4096 সেপ্টে 12 21:07 karim
-rw-r--r-- 1 meraz meraz   22 সেপ্টে 12 21:01 meraz
drwxr-xr-x 2 meraz meraz 4096 ফেব্রু 26  2020 Music
drwxr-xr-x 2 meraz meraz 4096 ফেব্রু 26  2020 Pictures
drwxr-xr-x 2 meraz meraz 4096 ফেব্রু 26  2020 Public
drwxr-xr-x 2 meraz meraz 4096 সেপ্টে 12 19:12 python
drwxr-xr-x 2 meraz meraz 4096 ফেব্রু 26  2020 Templates
drwxr-xr-x 2 meraz meraz 4096 ফেব্রু 26  2020 Videos
```

Permission for a particular file could be seen by typing the file name after the existing command

```
meraz@meraz-VirtualBox:~$ ls -l hello.txt
ls: cannot access 'hello.txt': No such file or directory
```

Conclusion :

This is one of the most important lab so far as we learnt about various kinds of users and operations and how to set permission for different users , how to add or remove different set of permissions for a or a set of users .