File Permissions in Linux

Project Description:

As a security professional with Cisco Labs, my main responsibility is to ensure that users on the research team are authorized with the appropriate permissions. This ensures the continued operations and the security of the overall system.

We will first begin by examining the existing permissions on the file system through the command-line interface and then determine whether the permissions match the authorization that should be given to them as per the organization's policies and guidelines.

If the permissions do not match, We will need to modify the permissions to authorize the appropriate users and remove any unauthorized access.

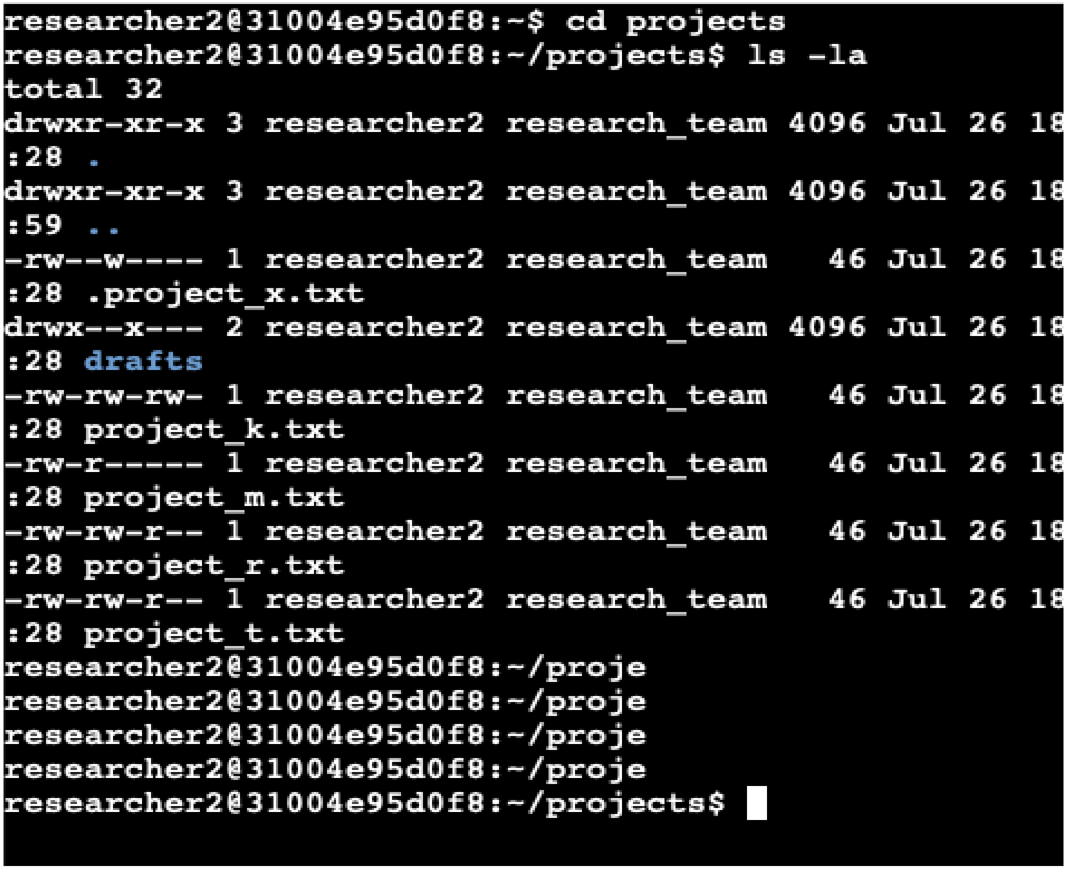
Check File & Directory Details:

We will examine and manage the permissions on the files in the /home/researcher2/projects directory of the "researcher2" user.

In the /home/researcher2/projects directory, there are five files with the following names and permissions.

To determine this, we first navigated to the projects directory and listed out all the contents and the permissions of the project directory.

By using the ls -la, we not only listed out the contents but also the permissions and any hidden files as well.



```
researcher2@31004e95d0f8:~$ cd projects
researcher2@31004e95d0f8:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jul 26 18
:28 .
drwxr-xr-x 3 researcher2 research_team 4096 Jul 26 18
:59 ..
-rw--w---- 1 researcher2 research_team   46 Jul 26 18
:28 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jul 26 18
:28 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jul 26 18
:28 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 26 18
:28 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18
:28 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18
:28 project_t.txt
researcher2@31004e95d0f8:~/proje
researcher2@31004e95d0f8:~/proje
researcher2@31004e95d0f8:~/proje
researcher2@31004e95d0f8:~/proje
researcher2@31004e95d0f8:~/projects$ █
```

As per the results shown out above, .project_x.txt is a hidden file on the system.

There are 5 files which include project_k.txt, project_m.txt, project_r.txt, project_t.txt, .project_x.txt.

There is also one subdirectory inside the projects directory named drafts.

Describe the Permissions String:

This is how file & directory permissions work in Linux:

A 10 character string begins each entry and indicates the permissions on the files & directories

1. The first character indicates the file type - d indicates it's a directory. When the character is a hyphen (-), it's a regular file.
2. 2nd-4th characters indicate the read(r), write(w), execute(x) permissions for the user. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted to the user.

3. The 5th-7th characters indicate the read(r), write(w), and execute(x) permissions for the group. Same rules apply for the hyphen as mentioned above.
4. The 8th-10th indicate the read(r), write(w), and execute(x) permissions for the owner type of other - all other users on the system apart from the user and the group.

As per the screenshot above, there are five files with the following names and permissions:

1. project_k.txt
   a. User = Read, Write
   b. Group = Read, Write
   c. Other = Read, Write
2. Project_m.txt
   a. User = Read, Write
   b. Group = Read
   c. Other = None
3. Project_r.txt
   a. User = read,write
   b. Group = read,write
   c. Other = read
4. Project_t.txt
   a. User = read,write
   b. Group = read,write
   c. Other = read
5. .project_x.txt
   a. User = read, write
   b. Group = write
   c. Other = none

Subdirectory - drafts
Permissions:
User = Read, Write, Execute
Group = Execute
Other = None

Change file permissions:

First Flag: As per the organization's security policies, the owner type or other should not have write permissions for any files in the projects directory. Our examination of the current file permissions on the system indicates that the file project_k.txt has write permissions for the owner type of "other".

To change the permissions of the file identified above, we will have to use the chmod command followed by the owner type, + or - (depending on whether we're giving or removing permissions), and the first letter of the permission type we're giving (read, write, execute).

```
chmod o-w project_k.txt
```

O = Other
(-) = Remove
W = Write

Second Flag: The file project_m.txt is restricted and should not be readable or writable by the group or other. Only the user should have these permissions on the file.

Currently, the group has read permissions on this file.

To remove that, we'll type in;

```
chmod g-r project_m.txt
```

Change file permissions on a hidden file:

The file .project_x.txt is a hidden file that has been archived and should not be written to by anyone (The user and group should still be able to read this file).

The group and the user have write permissions for the hidden file.

To change this, we'll still use the chmod command.

```
chmod g-w .project_x.txt
chmod u-w .project_x.txt
```

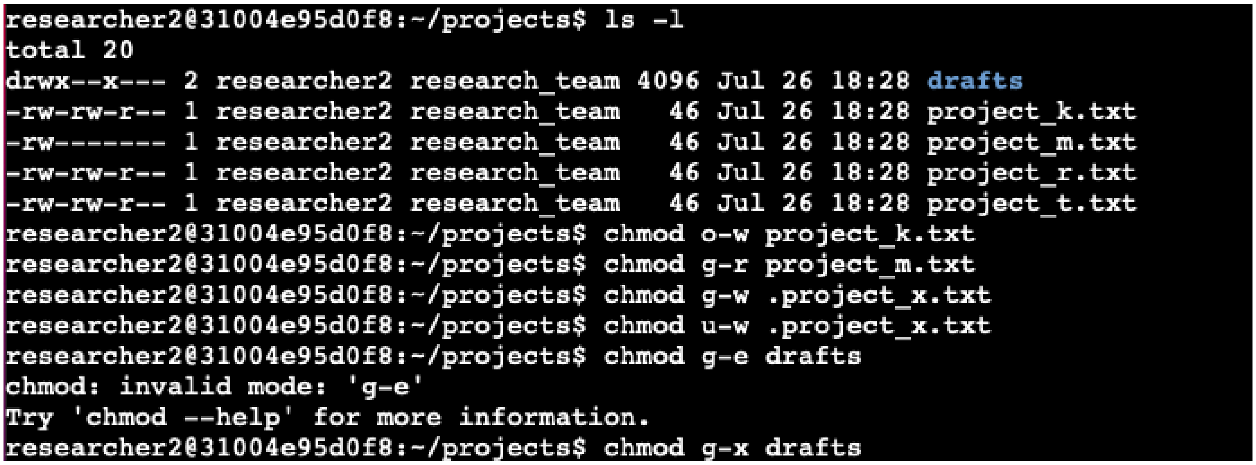
Change directory permissions:

Inside the projects folder, we have the drafts subdirectory. As per the organizations' policies, only the "researcher2" user should be allowed to access the drafts directory and its contents. This includes the execute privilege as well.

Currently, the group has read, write & execute permissions.

To change this, we'll type in this command:

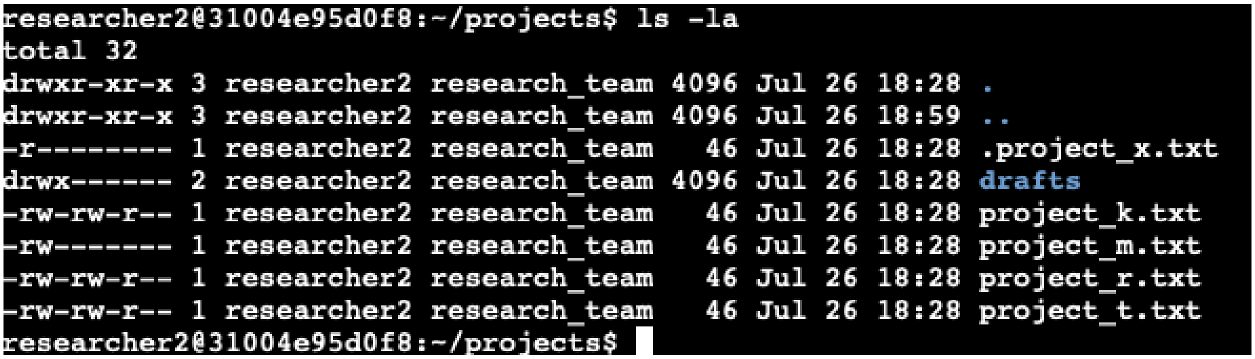
chmod g-e drafts



```
researcher2@31004e95d0f8:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Jul 26 18:28 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18:28 project_k.txt
-rw------- 1 researcher2 research_team   46 Jul 26 18:28 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18:28 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18:28 project_t.txt
researcher2@31004e95d0f8:~/projects$ chmod o-w project_k.txt
researcher2@31004e95d0f8:~/projects$ chmod g-r project_m.txt
researcher2@31004e95d0f8:~/projects$ chmod g-w .project_x.txt
researcher2@31004e95d0f8:~/projects$ chmod u-w .project_x.txt
researcher2@31004e95d0f8:~/projects$ chmod g-e drafts
chmod: invalid mode: 'g-e'
Try 'chmod --help' for more information.
researcher2@31004e95d0f8:~/projects$ chmod g-x drafts
```

Summary:

After making the appropriate changes to the file & directory permissions in Linux, we'll now list out the files and contents of the projects folder inside the **"researcher2"** user using the ls -la command.



```
researcher2@31004e95d0f8:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jul 26 18:28 .
drwxr-xr-x 3 researcher2 research_team 4096 Jul 26 18:59 ..
-r-------- 1 researcher2 research_team   46 Jul 26 18:28 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Jul 26 18:28 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18:28 project_k.txt
-rw------- 1 researcher2 research_team   46 Jul 26 18:28 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18:28 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 26 18:28 project_t.txt
researcher2@31004e95d0f8:~/projects$ 
```

This screenshot confirms that the file permissions of "researcher2" projects directory is in compliance with the organization's security policies.