

File permissions in Linux

Project description

My organization's research team wants to update their file and directories permissions within the "project" directory. As a security analyst, I will ensure users on this team are authorized with the appropriate permissions to keep the system secure. I will examine the permissions and determine if the permissions are granted appropriately. I will also ensure that our organization uses the least privilege for permissions to ensure security. To check and update permissions for the files and directories, I did the following tasks:

Check file and directory details

The following screenshot shows how I used the "ls -la" command to figure out existing permissions for all the files and directories within the projects subdirectory. The command I entered is "ls -la". This command lists all the permissions of the files/directories in my current working directory (projects), including the hidden files. There is one directory within the projects directory and there are five text files. The first 10 letters of the output lines represent the permissions. This is what I plan to examine.

```
researcher2@0cd75ee3ef7b:~$ ls
projects
researcher2@0cd75ee3ef7b:~$ cd projects/
researcher2@0cd75ee3ef7b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:38 .
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:42 ..
-rw--w---- 1 researcher2 research_team  46 May 30 14:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 30 14:38 drafts
-rw-rw-rw- 1 researcher2 research_team  46 May 30 14:38 project_k.txt
-rw-r----- 1 researcher2 research_team  46 May 30 14:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_t.txt
researcher2@0cd75ee3ef7b:~/projects$
```

Describe the permissions string

Knowing how to read the permission string is important because it tells you who has what permissions. To know the full permission for a file or directory, we need to examine all 10 letters.

- The first letter: The first letter can be **d** or a hyphen(-). The letter **d** suggests that the permission string represents a directory. A **hyphen** suggests that the permission string represents a file.

- The 2nd, 3rd, and 4th letter: The next three letters describe the permissions for the user. The 2nd letter can be **r** or **-**. If it's an **r**, then the user has read permission, if it's a hyphen(-), then the user does not have read permission. The 3rd letter can be **w(write permission)** or hyphen(-) and the 4th letter can be **x(execution permission)** or hyphen(-).
- The 5th, 6th, and 7th letter: The next three letters describe the permissions for the group. The 5th letter can be **r** or **-**. If it's an **r**, then the user has read permission, if it's a hyphen(-), then the user does not have read permission. The 6th letter can be **w(write permission)** or hyphen(-) and the 7th letter can be **x(execution permission)** or hyphen(-).
- The 8th, 9th, and 10th letter: The next three letters describe the permissions for others. The 8th letter can be **r** or **-**. If it's an **r**, then the user has read permission, if it's a hyphen(-), then the user does not have read permission. The 9th letter can be **w(write permission)** or hyphen(-) and the 10th letter can be **x(execution permission)** or hyphen(-).

If we look at the permission for the drafts directory, we can see that it is `drwx- - x - - -`. The first letter says that the permission string is for a directory and “drafts” is a directory. The next three letters show that users have all three permissions(read, write and execute). The next three letters show that groups only have execute permissions. The last three letters show that others don't have any permission.

Change file permissions

The Organization specified that “others” should not have write permissions for any of the files or directories. Based on our previous screenshot, we see that `project_k.txt` grants write permission to others.

```
researcher2@0cd75ee3ef7b:~/projects$ chmod o-w project_k.txt
researcher2@0cd75ee3ef7b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:38 .
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:42 ..
-rw--w---- 1 researcher2 research_team  46 May 30 14:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 30 14:38 drafts
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_k.txt
-rw-r----- 1 researcher2 research_team  46 May 30 14:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_t.txt
researcher2@0cd75ee3ef7b:~/projects$
```

This screenshot shows how I modified the permission for the `project_k.txt` text file. The `chmod` command alters the permission for the file and the specification of `o-w` means that others don't get the write permissions. I later used the `ls -la` command to ensure that the permissions for the file are updated.

Change file permissions on a hidden file

The organization also specified that the `.project_x.txt` file should not grant write access to anyone, but should grant read access to the user and the group. This file is special because it is a hidden file. Hidden files start with a period.

The screenshot shows how I updated the permissions of the `.project_x.txt` file.

```
researcher2@0cd75ee3ef7b:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@0cd75ee3ef7b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:38 .
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:42 ..
-r--r----- 1 researcher2 research_team  46 May 30 14:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 30 14:38 drafts
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_k.txt
-rw-r----- 1 researcher2 research_team  46 May 30 14:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_t.txt
researcher2@0cd75ee3ef7b:~/projects$
```

The first two lines of the screenshot are the commands that I typed. The first command I typed was to change the permissions for the `.project_x.txt` file. I removed write permission to the user and the group as the file cannot be modified by anyone. Then I added read permission to the group. The second command lists the updated permissions for the `.project_x.txt`.

Change directory permissions

My organization also specified how they only want the user named `researcher2` to have access to the `drafts` directory and its files/subdirectories. This really means that no one should have execute permissions for the directory other than `researcher2`.

Currently, both the group and the user have execute permission. The screenshot shows the linux commands I typed to disable the group from having execute permission.

```
researcher2@0cd75ee3ef7b:~/projects$ chmod g-x drafts/
researcher2@0cd75ee3ef7b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:38 .
drwxr-xr-x 3 researcher2 research_team 4096 May 30 14:42 ..
-r--r----- 1 researcher2 research_team  46 May 30 14:38 .project_x.txt
drwx----- 2 researcher2 research_team 4096 May 30 14:38 drafts
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_k.txt
-rw-r----- 1 researcher2 research_team  46 May 30 14:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 May 30 14:38 project_t.txt
researcher2@0cd75ee3ef7b:~/projects$
```

The first command I typed was `chmod g-x drafts/`. This command alters the permission for the `drafts` directory. It takes away the execute permission for the group. The next command lists

the updated permissions for the drafts directory to see if my commands were executed properly.

Summary

In this activity, I changed the permissions for multiple files and directories to match the organization's requirements. The first command that I used was `ls -la`, which lists all the permissions for the files. Using this command, I was able to check the permissions for each type of owner. Then, I changed the permissions based on my organization's specifications.