File permissions in Linux

Project description

As a security analyst at a large organization, I team up with the research crew to make sure users have the right permissions. It's crucial for keeping the system safe. In the Linux environment, my job involves checking the current file system permissions to ensure they match the required authorization. If they don't match, I need to tweak the permissions to allow the right users and get rid of unauthorized access.

Check file and directory details

To check file and directory details in the `projects` I use `ls -la` to display permissions to files and directories, this also will include hidden files.

```
researcher2@74b85d8ce71f:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 04:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 05:48 ..
-rw--w---- 1 researcher2 research_team   46 Aug 30 04:59 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Aug 30 04:59 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Aug 30 04:59 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Aug 30 04:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
researcher2@74b85d8ce71f:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Aug 30 04:59 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Aug 30 04:59 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Aug 30 04:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
researcher2@74b85d8ce71f:~/projects$
```

Describe the permissions string

Permissions are represented by a 10-character string in which each character symbolizes a specific meaning—for example, `drwxrwxrwx`: d=directory r=read w=writable x=execute.
1st character is the file type d=directory or - =regular file.
2nd, 3rd and 4th is the User permissions.
5th, 6th, 7th is the Group permissions.
8th, 9th, 10th is Other permissions.

```
researcher2@74b85d8ce71f:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 04:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 05:48 ..
-rw--w---- 1 researcher2 research_team   46 Aug 30 04:59 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Aug 30 04:59 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Aug 30 04:59 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Aug 30 04:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
```

Change file permissions

The organization does not allow `other` to have write access to any files. In Linux, I would use the command `chmod o-w .project_x.txt` to modify these permissions. The example below shows that I changed the file permissions of `others` for file `.project_x.txt`, by removing permission to read, hence `o-r` followed by the file.

```
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
researcher2@74b85d8ce71f:~/projects$ chmod u=r,g=r .project_x.txt
researcher2@74b85d8ce71f:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 04:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 05:48 ..
-r--r--r-- 1 researcher2 research_team   46 Aug 30 04:59 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Aug 30 04:59 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_k.txt
-rw------- 1 researcher2 research_team   46 Aug 30 04:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
researcher2@74b85d8ce71f:~/projects$ chmod o-r .project_x.txt
researcher2@74b85d8ce71f:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 04:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 05:48 ..
-r--r----- 1 researcher2 research_team   46 Aug 30 04:59 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Aug 30 04:59 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_k.txt
-rw------- 1 researcher2 research_team   46 Aug 30 04:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
```

Change file permissions on a hidden file

The file `.project_x.txt` has been archived by the research team and is therefore a hidden file. It should not have write permissions for anyone, but the user and group should be able to read the file. To change file permissions on hidden file `.project_x.txt`, I use the Linux command `chmod u=r,g=r .project_x.txt` because this command overwrites existing permissions for this file. Using = will assign permissions as specified.

```
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
researcher2@74b85d8ce71f:~/projects$ chmod u=r,g=r .project_x.txt
researcher2@74b85d8ce71f:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 04:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 05:48 ..
-r--r--r-- 1 researcher2 research_team   46 Aug 30 04:59 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Aug 30 04:59 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_k.txt
-rw------- 1 researcher2 research_team   46 Aug 30 04:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug 30 04:59 project_t.txt
```

Change directory permissions

The directories and files in the projects directory are owned by the **`researcher2`** user. Only **`researcher2`** should have access to the **`drafts`** directory and its contents. I would use the Linux command `chmod g-x /home/researcher2/projects/drafts` to adjust the permissions accordingly. Using command chmod with types of owners and permissions rules then the directory path to change directory permissions.

```
researcher2@74b85d8ce71f:~/projects/drafts$ ls -la
total 8
drwx--x--- 2 researcher2 research_team 4096 Aug 30 04:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 04:59 ..
```

```
researcher2@74b85d8ce71f:~/projects/drafts$ chmod g-x /home/researcher2/projec
ts/drafts
researcher2@74b85d8ce71f:~/projects/drafts$ ls -la
total 8
drwx------ 2 researcher2 research_team 4096 Aug 30 04:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug 30 04:59 ..
researcher2@74b85d8ce71f:~/projects/drafts$
```

Summary

As a security professional at a large organization, my role involves ensuring that users have the appropriate permissions to maintain system security. I achieve this by reviewing and modifying file and directory permissions in Linux to align with the organization's access policies. For example, I use commands like `chmod` to remove unauthorized access or restrict permissions, ensuring only designated users and groups can read or modify files, including hidden files and sensitive directories. I also utilize Linux to check details in file permissions with `ls -la`. This process is crucial in preventing unauthorized access and maintaining the integrity of the organization's data.