File permissions in Linux

Project description

This project focuses on managing file and directory permissions in Linux, using commands to ensure that files are accessible and editable only by authorized users. By utilizing commands like chmod and ls -la, the goal is to ensure that critical files do not have write permissions for unauthorized users and that sensitive directories are accessible only by the designated owner. This is crucial in collaborative environments where data security and integrity are priorities.

Check file and directory details

```
researcher2@dc9a4228dc82:~$ pwd
/home/researcher2
researcher2@dc9a4228dc82:~$ ls
projects
researcher2@dc9a4228dc82:~$ cd projects
researcher2@dc9a4228dc82:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:14 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:34 ..
-rw--w---- 1 researcher2 research_team   46 Jan  7 18:14 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan  7 18:14 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jan  7 18:14 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jan  7 18:14 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_t.txt
```

Describe the permissions string

I will take the example of the permissions string for one of the listed files, such as `-rw-rw-r--` for the file `project_r.txt`. I will break down the 10-character string that represents file permissions in Linux:

Permissions String: -rw-rw-r--

First character (-):

This indicates the type of file. A dash (-) means it's a regular file. If it were a d, it would indicate a directory.

Next three characters (rw-):

These represent the permissions for the file owner.

r: The owner has read permission.

w: The owner has write permission.

-: There is no execute permission for the owner.

Next three characters (rw-):

These represent the permissions for the group the file belongs to.

r: The group has read permission.

w: The group has write permission.

-: There is no execute permission for the group.

Last three characters (r--):

These represent the permissions for other users (everyone else).

r: Others have read permission.

-: Others do not have write permission.

-: Others do not have execute permission.

The complete string `-rw-rw-r--` tells me that `project_r.txt` is a regular file where the owner and the group can read and write, but not execute, and other users can only read. This permission structure is common for files that need to be editable by the owner and group but only visible to others.

Change file permissions

Considering that the organization does not allow others to have write access to any files, I will modify the permissions accordingly. To achieve this, I will use the chmod command.
After executing the `ls -la` command, we observed that the only file with incorrect permissions was `project_k.txt`.

The chmod command is used to modify the permissions of files and directories in Linux systems, playing a crucial role in managing who can read, write, or execute them to ensure proper security and access control. It requires two main arguments: the first specifies the new permission settings to be applied, and the second identifies the file or directory whose permissions are to be changed. This command structure allows precise adjustment of access levels for different users or groups, ensuring that only authorized individuals can interact with the files in specified ways.

I applied the following command to modify the permissions

```
researcher2@dc9a4228dc82:~/projects$ chmod o-w project_k.txt
```

I verify that it has been applied correctly:

```
researcher2@dc9a4228dc82:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:14 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:34 ..
-rw--w---- 1 researcher2 research_team   46 Jan  7 18:14 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan  7 18:14 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jan  7 18:14 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_t.txt
```

Change file permissions on a hidden file

The research team has archived .project_x.txt, which is why it's a hidden file. This file should not have write permissions for anyone, but both the user and the group should be able to read it.

Previously, we noted that .project_x.txt has the following permissions:

```
-rw--w---- 1 researcher2 research_team   46 Jan  7 18:14 .project_x.txt
```

- The user has read and write permissions but not execute.
- The group has write permission but not read or execute.
- Others have no permissions for read, write, or execute.

I need to remove the write permissions for both the user and the group.

```
researcher2@dc9a4228dc82:~/projects$ chmod u-w,g-w .project_x.txt
researcher2@dc9a4228dc82:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:14 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:34 ..
-r-------- 1 researcher2 research_team   46 Jan  7 18:14 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan  7 18:14 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jan  7 18:14 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_t.txt
```

Additionally, I need to grant read permissions to the group.

```
researcher2@dc9a4228dc82:~/projects$ chmod g+r .project_x.txt
```

```
researcher2@dc9a4228dc82:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:14 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:34 ..
-r--r----- 1 researcher2 research_team   46 Jan  7 18:14 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan  7 18:14 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jan  7 18:14 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_t.txt
```

Change directory permissions

The files and directories within the projects directory are owned by the user researcher2. Only researcher2 should have access to the drafts directory and its contents.

Considering the following permissions:

```
researcher2@dc9a4228dc82:~$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:34 .
drwxr-xr-x 1 root        root          4096 Jan  7 18:14 ..
-rw------- 1 researcher2 research_team  210 Jan  7 19:09 .bash_history
-rw-r--r-- 1 researcher2 research_team  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 researcher2 research_team 3574 Jan  7 18:14 .bashrc
-rw-r--r-- 1 researcher2 research_team 3574 Jan  7 18:14 .profile
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:14 projects
```

I use the following Linux command to modify the permissions so that only researcher2 can access the drafts directory and its contents.

```
researcher2@dc9a4228dc82:~/projects$ chmod u+rwx,go-rwx /home/researche
r2/projects/drafts
researcher2@dc9a4228dc82:~/projects$
researcher2@dc9a4228dc82:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:14 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  7 18:34 ..
-r--r----- 1 researcher2 research_team   46 Jan  7 18:14 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Jan  7 18:14 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jan  7 18:14 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan  7 18:14 project_t.txt
```

Summary

In this project, the permissions of various files and directories were adjusted to comply with the organization's security policies, ensuring that only specific users can modify or access them. Incorrect permissions were corrected on files such as project_k.txt, and exclusive access to the drafts directory was configured for the user researcher2. These measures were implemented to uphold effective security practices and safeguard sensitive information.