File permissions in Linux

Project description

The Organization I work for has tasked me to update the file permissions for certain files and directories within the projects directory. The current directory does not reflect the proper level of authorization that should be given. Checking the permissions and updating them to reflect the proper level of authorization will help in maintaining their system secure. To complete the task, I performed the following changes:

Check file and directory details

The following Linux command demonstrates and shows the existing permissions set for a specific directory and its contents.

```
researcher2@aa00cac580fb:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 19:41 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 20:37 ..
-rw--w---- 1 researcher2 research_team   46 Jun 27 19:41 .project_x.t
xt
drwx--x--- 2 researcher2 research_team 4096 Jun 27 19:41 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jun 27 19:41 project_k.tx
t
-rw-r----- 1 researcher2 research_team   46 Jun 27 19:41 project_m.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 19:41 project_r.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 19:41 project_t.tx
t
researcher2@aa00cac580fb:~/projects$
```

The first line of the screenshot displays the command I entered, and the other lines display the output.What you see in the output is the list of all content inside of the projects directory. I used the ls command with the -la option to display all of the content inside of the projects directory. It returned several items like files, directories, and a hidden file called .project_x.txt. The 10-character string in the first column represents the permission set on each file and directory.

Describe the permissions string

The 10-character string consists of 3 types who can access the content. User, Group, and Other. Each type has 3 character strings which include read(r),write(w),and execute(x). The first character in the string consists of either a d or a hyphen(-) which tells us if it's a directory(d) or a file(-). That only pertains to the first character. What follows after the first character is the user and their access which can consist of read(r),write(w), and execute(x) which would display like this drwx- - - - - -. If the user has no permission for any type of access to read,write, or execute the letter would be replaced with a hyphen(-) which indicates that they are not granted permission for that string. This applies to both Group and Other.

For example: The project_t.txt has the permission as -rw-rw-r--. Since the first character is a hyphen(-), this indicates that project_t.txt is a file. The 2nd-4th character indicates the user can read(r),write(w), but not execute for the reason being there is a hyphen(-) on the 4th character. The 5th-7th character indicates that the group(g) has read(r) and write(w) permissions as well but the 7th character again, is a hyphen(-) indicating no execute permission. The 8th-10th characters indicate that other can only read(r) the file and not write(w) or execute(x) which is represented by the two hyphens(--) following the read(r).

Change file permissions

The organization has determined that other shouldn't have write access to any of their files. In order to comply with their request we will need to run the command ls with the -la option to display a detailed listing of the file contents and hidden content as well.

The following code demonstrates how i used Linux commands to do this:

```
researcher2@da25e560d02b:~/projects$ chmod o-w project_k.txt
researcher2@da25e560d02b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 21:10 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 22:05 ..
-rw--w---- 1 researcher2 research_team   46 Jun 27 21:10 .project_x.t
xt
drwx--x--- 2 researcher2 research_team 4096 Jun 27 21:10 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_k.tx
t
-rw-r----- 1 researcher2 research_team   46 Jun 27 21:10 project_m.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_r.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_t.tx
t
researcher2@da25e560d02b:~/projects$
```

The first two lines display the commands I entered, and the other lines display the output of the second command. The chmod command changes the permissions on files and directories. As previously mentioned, the other is represented by (o) and the write is represented by (w). When we use the command chmod followed by o-w project_k.txt, the first argument indicates what permission should be changed, and the second argument specifies the file or directory. In this example, i removed the write permission from other for the project_k.txt file. After this, the second command i used ls -la to review the updates i made. It now shows other cannot write(w) on project_k.txt.

Change file permissions on a hidden file

The research team at my organization recently archived project_x.txt. They do not want anyone to have write access to this project, but the user and group should have read access.

The following code demonstrates how i use Linux commands to change the permission:

```
researcher2@da25e560d02b:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@da25e560d02b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 21:10 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 22:05 ..
-r--r----- 1 researcher2 research_team   46 Jun 27 21:10 .project_x.t
xt
drwx--x--- 2 researcher2 research_team 4096 Jun 27 21:10 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_k.tx
t
-rw------- 1 researcher2 research_team   46 Jun 27 21:10 project_m.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_r.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_t.tx
t
researcher2@da25e560d02b:~/projects$
```

The first two lines display the commands I entered to remove and display the full information from the files and directories inside. As you can see .project_x.txt is a hidden folder due to starting with a (.) which indicates the folder is hidden. From the first command I used chmod to remove the write from the user with u-w and following after i used the command to remove write from group (g-w). Following after I added read to group in order to be able to read the content inside the file with the command (g+r). To confirm everything worked i used the command ls -la which displays the files, directories, and hidden folders with all their information listed.

Change directory permissions

THe organization only wants the researcher2 user to have access to the drafts directory and its contents. This means no one other than researcher2 should have execute permissions.

The following code shows how i used Linux commands to change the permission:

```
researcher2@da25e560d02b:~/projects$ chmod g-x drafts
researcher2@da25e560d02b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 21:10 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 27 22:05 ..
-r--r----- 1 researcher2 research_team   46 Jun 27 21:10 .project_x.t
xt
drwx------ 2 researcher2 research_team 4096 Jun 27 21:10 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_k.tx
t
-rw------- 1 researcher2 research_team   46 Jun 27 21:10 project_m.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_r.tx
t
-rw-rw-r-- 1 researcher2 research_team   46 Jun 27 21:10 project_t.tx
t
researcher2@da25e560d02b:~/projects$
```

The first two lines are input commands which show i used chmod to remove execute from group which is represented by (g-x) from drafts. The second input displays the output with files and directories inside of projects showing us who can read(r),write(w), execute(x), who is the user, what group has permission, date and time and full name of file or directory. Which as you can see drafts no longer allows anyone else but researcher2 to be able to execute drafts.

Summary

I changed multiple permissions to match the level of authorization the organization wanted for files and directories in the projects directory. The first step was to ls -la to check the permissions for the drectory. Following that command this informed my decisions as to what files needed modifications. I then used chmod to remove write(w), read(r), or execute(x) from a user(u),group(g), or other(o). This gives security to the company from having un-authorized users from reading(r),writing(w), or executing(x) files.