File permissions in Linux

Project description

The existing permissions on the filesystem are to be examined. Upon examination, they are to be determined if they match the authorization that should be granted. If they do not match, then the permissions are to be updated to authorize appropriate users, and to remove any unauthorized access.

Check file and directory details

In order to change the current working directory to the directory where permissions need examining, the following command is executed in the bash shell.

```
 cd  /home/researcher2/projects
```

In order to display the contents of this directory, as well as the permissions and hidden files. The following command is executed.

```
ls -la
```

The output of this command is as follows:

```
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 19 16:29 .
drwxr-xr-x 3 researcher2 research_team 4096 May 19 17:22 ..
-rw--w---- 1 researcher2 research_team   46 May 19 16:29
.project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 19 16:29 drafts
-rw-rw-rw- 1 researcher2 research_team   46 May 19 16:29 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 19 16:29 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 19 16:29 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 19 16:29 project_t.txt
```

The 10-character string at the start of every line of the items in this directory indicate their permissions.

Describe the permissions string

Below is the 10-character permissions string for the `.project_x.txt` file

```
-rw--w----
```

The 10-character permissions string is composed of 4 segments.

The first segment denotes the type of the item and is 1-character in length. For example, in the permissions string above, the `-` denotes that this item in the directory is a file.
The last three segments are all 3-characters in length, and they state the read, write, and execute permissions of the item which are denoted by r, w, and x. The first of these segments corresponds to the permissions for the user, the second corresponds to the permissions for the group, and the third corresponds to the permissions for others. If `-` is displayed, this means that this permission is not granted.
Therefore, in the permissions string above, the user has access to read and write to the file, the group has access to write to the file, and others have no permissions to access the file whatsoever.

Change file permissions

The organization does not allow other to have write access to any files. Therefore, the `project_k.txt` file needs updating, to remove other write access.
This is done with the following command:
`chmod o-w project_k.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 the user and group should be able to read the file. Therefore, a command has to be executed to: remove user write access, remove group write access, and add group read access.
This is done with the following command:
`chmod u-w,g-w,g+r .project_x.txt`

Change directory permissions

The files and directories in the projects directory belong to the *researcher2* user. Only *researcher2* should be allowed to access the *drafts* directory and its contents.
Currently, the group has access to execute, which needs to be removed. This is done with the following command:
`chmod g-x drafts`

Summary

I changed multiple permissions to match the level of authorization wanted for files and directories in the projects directory. The first step in this was using ls -la to check the permissions for the directory. This informed my decisions in the following steps. I then used the chmod command multiple times to change the permissions on files and directories.