File permissions in Linux

Project description

The research team at my organization needs to update the file permissions for certain files and directories within the projects directory. Since the current permissions do not reflect the level of authorization that should be given, I will be checking and updating them.

Check file and directory details

```
researcher2@069311f8e4f4:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Oct  1 12:37 .
drwxr-xr-x 3 researcher2 research_team 4096 Oct  1 13:10 ..
-rw--w---- 1 researcher2 research_team   46 Oct  1 12:37 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Oct  1 12:37 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Oct  1 12:37 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Oct  1 12:37 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct  1 12:37 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct  1 12:37 project_t.txt
researcher2@069311f8e4f4:~/projects$ chmod o-w project_k.txt
```

First, I typed the command ls -la to show file and directory details (including hidden files). The output of this command indicates that there is one directory called drafts, five regular files, and one hidden file called .project_x.txt.

Describe the permissions string

As shown in the picture above, the initial 10 character string is the permissions string.
*The first character can be either a d or a (-), indicating whether we are referring to a directory or a file respectively.
*The 2nd-4th characters indicate the read (r), write (w) and execute (x) permissions for the user. A (-) indicates that the permission is not granted to the user.
*The 5th-7th characters indicate the read (r), write (w) and execute (x) permissions for the group. A (-) indicates that the permission is not granted to the group.
*The 8th-10th characters indicate the read (r), write (w) and execute (x) permissions for other. A (-) indicates that the permission is not granted to other.

Change file permissions

A requirement I was given was to make sure that other shouldn't have access to any of their files. To do so, I used the command `chmod o-w project_k.txt`. I also made some other modifications to follow security best practices. In the following code, you can see the resulting permissions after the change, shown by the command `ls -la`.

```
researcher2@069311f8e4f4:~/projects$ chmod o-w project_k.txt
researcher2@069311f8e4f4:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Oct  1 12:37 .
drwxr-xr-x 3 researcher2 research_team 4096 Oct  1 13:10 ..
-rw--w---- 1 researcher2 research_team   46 Oct  1 12:37 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Oct  1 12:37 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Oct  1 12:37 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Oct  1 12:37 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct  1 12:37 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct  1 12:37 project_t.txt
```

Change file permissions on a hidden file

Another requirement given to me was to make sure nobody had permissions to write `project_x`, but the user and group should have read access. This can also be done using `chmod`, the only difference is the use of the `.` symbol right before the name of the hidden file (see picture below for reference).

```
researcher2@069311f8e4f4:~/projects$ chmod -w .project_x.txt
chmod: .project_x.txt: new permissions are r---w----, not r--------
researcher2@069311f8e4f4:~/projects$ chmod g-w .project_x.txt
researcher2@069311f8e4f4:~/projects$ chmod g+r .project_x.txt
```

Change directory permissions

Lastly, my organization only wanted `researcher2` to have access to the `drafts` directory and its contents. To ensure this, I simply typed the command using `chmod g-x drafts`. Note that the procedure is the same as a regular file, but without the need to type extensions like .txt.

Summary

After the previous steps and considering the principle of least privilege (to grant access in a need to know basis), we enhanced the security of the `projects` directory, its subdirectories, and files to minimize risks in case of a potential attack.