File permissions in Linux

Project description

Reviewed and corrected file and directory permissions within the projects directory to ensure they follow the principle of least privilege. Identified permission misconfigurations, verified actual access levels, and updated permissions to prevent unauthorized access and improve system security.

Check file and directory details

Command I use for checking permission set for a specific directory in the file system.

```
researcher2@72858695d848:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 12 17:43 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 12 18:11 ..
-rw--w---- 1 researcher2 research_team   46 Jan 12 17:43 .project_x.
txt
drwx--x--- 2 researcher2 research_team 4096 Jan 12 17:43 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jan 12 17:43 project_k.t
xt
-rw-r----- 1 researcher2 research_team   46 Jan 12 17:43 project_m.t
xt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_r.t
xt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_t.t
xt
```

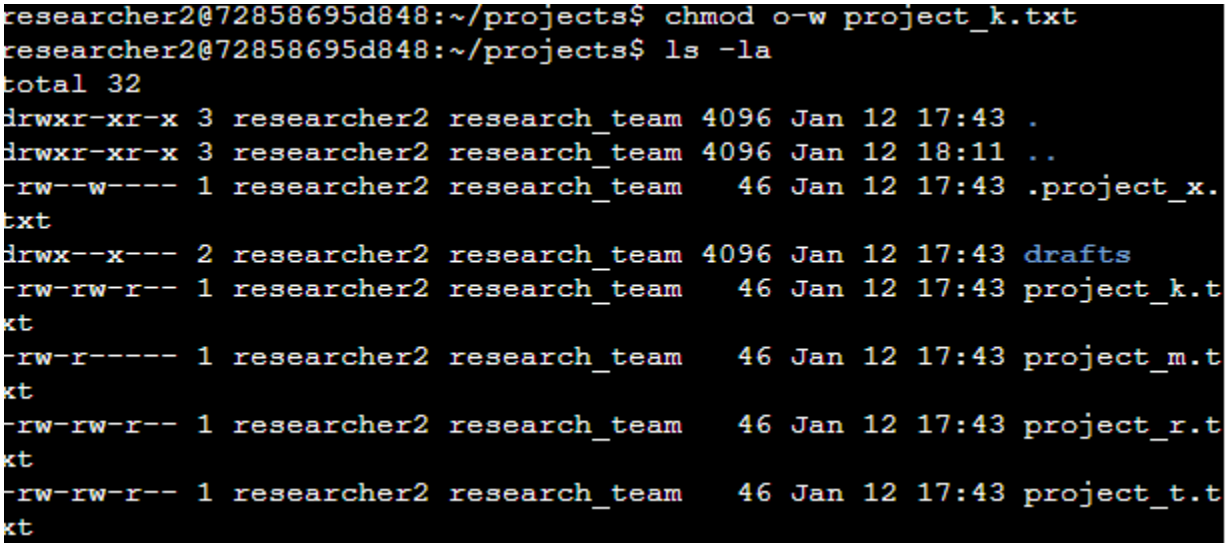
The first line of the screenshot displays the command I entered, and the other lines display the output. The code lists all contents of the projects directory. I used the ls command with the -la option to display a detailed listing of the file contents that also returned hidden files. The output of my command indicates that there is one directory named drafts, one hidden file named .project_x.txt, and five other project files. The 10-character string in the first column represents the permissions set on each file or directory.

Describe the permissions string

The 10-character permission string drwxrwxrwx indicates a directory that is readable, writable, and executable by the owner, group, and all other users. The leading d denotes a directory (a - would indicate a regular file). The first three characters represent the owner's permissions, the next three the group's permissions, and the final three the permissions for all other users.

This configuration poses a critical security risk, as it allows any user on the system to create, modify, or delete files within the directory, violating the principle of least privilege.

Change file permissions



The first two lines show the commands used to fix the file permissions. Using chmod, I removed write permissions for other users on the project_k.txt file. Next, I used ls -la to verify that the permission changes were correctly applied to the relevant files.

Change file permissions on a hidden file

As requested, the project_x.txt file must not have write permissions, and only the user and the group are allowed to have read access. The image below shows the commands used to modify the file permissions accordingly. The dot (.) before project_x.txt indicates that the file is hidden.

```
researcher2@72858695d848:~/projects$ chmod u-w,g-w,g+r .project_x.tx
t
researcher2@72858695d848:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 12 17:43 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 12 18:11 ..
-r--r----- 1 researcher2 research_team   46 Jan 12 17:43 .project_x.
txt
drwx--x--- 2 researcher2 research_team 4096 Jan 12 17:43 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_k.t
xt
-rw------- 1 researcher2 research_team   46 Jan 12 17:43 project_m.t
xt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_r.t
xt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_t.t
xt
researcher2@72858695d848:~/projects$
```

Change directory permissions

The team wants the user researcher2 to have access to the drafts directory and its contents. No other users should have execute permissions. The image below shows the commands used to apply these changes.

```
researcher2@72858695d848:~/projects$ chmod g-x drafts
researcher2@72858695d848:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 12 17:43 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 12 18:11 ..
-r--r----- 1 researcher2 research_team   46 Jan 12 17:43 .project_x.
txt
drwx------ 2 researcher2 research_team 4096 Jan 12 17:43 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_k.t
xt
-rw------- 1 researcher2 research_team   46 Jan 12 17:43 project_m.t
xt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_r.t
xt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 12 17:43 project_t.t
xt
researcher2@72858695d848:~/projects$
```

First two lines are the command I entered, and either lines display the output of the second command. I use the chmod command to remove them.

Summary

I changed multiple permissions to match the level of authorization my organization 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.