# File permissions in Linux

## Project description

In this project scenario, the research team needs to update the file and directory permissions within the projects directory. Current permissions do not reflect the level of authorization that should be given in alignment with the principle of least privilege. Checking and updating these permissions will help keep their system secure. To complete this task, I performed the following tasks using Linux commands:

## Check file and directory details:

A screen shot of a computer program

Description automatically generated

To check file and directory details, I ran the “*ls -la”* command as highlighted in the screenshot above. Below it, is the output of the command showing the contents of the projects directory including a hidden file (. *project\_x.txt*) and a directory (*drafts*). Running the *ls* command with the -*la* option ensured file and directory full details including the permission levels and any hidden content was included in the output.

## Describe the permissions string

A screenshot of a computer program

Description automatically generated

The 10-character permissions string is highlighted in the above screenshot. It shows who is authorized to access the file and their specific permissions. The characters and what they represent are as follows:

* **1st character**: This character is either a d or hyphen (-) and indicates the file type. If it’s a d, it’s a directory. If it’s a hyphen (-), it’s a regular file.
* **2nd-4th characters**: These characters indicate the read (r), write (w), and execute (x) permissions for the user. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted to the user.
* **5th-7th characters:** These characters indicate the read (r), write (w), and execute (x) permissions for the group. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted for the group.
* **8th-10th characters:** These characters indicate the read (r), write (w), and execute (x) permissions for other. This owner type consists of all other users on the system apart from the user and the group. When one of these characters is a hyphen (-) instead, that indicates that this permission is not granted for other.

## Change file permissions

A screenshot of a computer program

Description automatically generated

The outlined policy does not allow write access to any files for other. As can be seen from previous screenshots, the *project\_k.txt* file had write access granted to other. I changed this by running the *“chmod o-w project\_k.txt”* command to set the appropriate permission as seen in above screenshot. The “chmod” commands changes the permissions on files and directories. The “o-w” argument indicates what permission is being changed (o = other, - = remove, w = write access) on the file “project\_k.txt”.

A screenshot of a computer program

Description automatically generated

Also, the organization wanted read and write access to the project\_m.txt file for the user and no access for the group or other. To implement this, I ran “*chmod g-r project\_m.txt”* command to remove the read access initially granted to the group.

## Change file permissions on a hidden file

A screenshot of a computer program

Description automatically generated

The research team recently archived project\_x.txt file and wanted read access for user and group only with no write or execute access for anybody. To set the required permissions, I ran the command “*chmod u-w,g+r-w .project\_x.txt”* removing write access for user and group and granting read access to the group.

## Change directory permissions

A screenshot of a computer screen

Description automatically generated

The organization wants only the researcher2 who is the owner to have access to the drafts directory. I ran the command “*chmod g-x drafts”* to remove the execute access initially granted to the group ensuring no one has access to the directory but researcher2.

## 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 was using “ls -la” to check the file and directory permissions, then using “chmod” with the appropriate arguments to set the permissions.