# 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. The permissions do not currently reflect the level of authorization that should be given. Checking and updating these permissions will help keep their system secure. To complete this task, I performed the following tasks:

## Check file and directory details

The following code demonstrates how I used Linux commands to determine the existing permissions set for a specific directory in the file system.



I used the command ls -la to list all the items in the project’s directory. The -la option is used to also list all the hidden files which are denoted by a **“.”** in the front of the file name.

## Describe the permissions string

The 10-character string contains information about file access authorization and permissions. Here's what each character represents:

* The first character can be either "d" (denoting a directory) or "-" (indicating a regular file).
* The second to fourth characters represent user permissions: "r" for read, "w" for write, and "x" for execute. If a hyphen "-" appears, it means the corresponding permission is not granted to the user.
* The fifth to seventh characters represent group permissions: "r" for read, "w" for write, and "x" for execute. If a hyphen "-" appears, it means the corresponding permission is not granted to the group.
* The eighth to tenth characters represent other permissions: "r" for read, "w" for write, and "x" for execute. If a hyphen "-" appears, it means the corresponding permission is not granted to others, i.e., users who are neither the owner nor part of the group.

## Change file permissions

The organization determined that other shouldn't have write access to any of their files. To comply with this, I referred to the file permissions that I previously returned. I determined project\_k.txt must have the write access removed for other.

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



Here I used the chmod command to modify file permissions. I used o-w options which indicates that I want to remove write (w) permission of others. I then used ls -la to verify the changes

## 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 used Linux commands to change the permissions:



Here I used the options u-w,g-w,g+r to modify permission for different groups in a single command. Every modification is separated by “,”, the u-w removes the write permission from user. I used g-w to remove write permission from group and then g+r to add read permission for groups.

## Change directory permissions

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

The following code demonstrates how I used Linux commands to change the permissions:



I used the chmod command to remove execution permission from users because researcher2 already has the execution permission.