# File permissions in Linux

## Project description

In this scenario, I am tasked with examining and modifying file and directory permissions on a Linux system to ensure that the authorization of users aligns with the organization's security policies. The primary objective is to review and adjust permissions to enhance the security of the file system.

## Check file and directory details

To check file and directory permissions, I will use the ls -la command. This command provides a detailed listing of files and directories, including their permissions.

ls -la /home/researcher2/projects

## Describe the permissions string

The 10-character string in the permissions output represents various aspects of file permissions:

* The first character represents the file type: (- for regular files, d for directories, and l for symbolic links).
* Characters 2-4 represent the owner's permissions (read, write, and execute).
* Characters 5-7 represent the group's permissions (read, write, and execute).
* Characters 8-10 represent others' permissions (read, write, and execute).

For example, drwxr-xr-x signifies a directory with read, write, and execute permissions for the owner, and read and execute permissions for the group and others.

## Change file permissions

To modify file permissions, I will use the chmod command. In this case, I'll ensure that the "Other" category doesn't have write access to a specific file, as per the organization's policy.

chmod o-w /home/researcher2/projects/project\_m.txt

## Change file permissions on a hidden file

For .project\_x.txt, which is a hidden file, I'll adjust permissions to disallow write access for others but retain read permissions for the user and group.

chmod o-w /home/researcher2/projects/.project\_x.txt

## Change directory permissions

To modify directory permissions, I will use the chmod command. I'll ensure that only the owner (researcher2) can access the drafts directory and its contents.

chmod 700 /home/researcher2/projects/drafts

## Summary

In this task, I examined and adjusted file and directory permissions on a Linux system. I used the ls -la command to inspect permissions, ensuring they align with the organization's security policies. I employed the chmod command to modify permissions for specific files, including hidden files, and directories. This helps maintain a secure file system and access control in line with the organization's requirements.