# File permissions in Linux

## Project description

In this scenario, as a security professional working with the research team in a large organization, I was tasked with ensuring that users had appropriate permissions on the file system to maintain security. Through Linux commands, I examined existing permissions, ensured they aligned with authorized access, and modified permissions as needed to remove unauthorized access.

## Check file and directory details

To check file and directory details, I used the ls -la command in Linux. This command displayed all permissions, including hidden files and directories.

## Describe the permissions string

The 10-character string represents file permissions in Linux. The first character indicates the file type, while the next three characters represent permissions for the owner, followed by permissions for the group, and finally, permissions for others.

## Change file permissions

To modify file permissions, I used the chmod command followed by the desired permissions and the file name. For example, to remove write permissions for others on a file named example.txt, I used chmod o-w example.txt.

## Change file permissions on a hidden file

To assign appropriate permissions to a hidden file, such as .project\_x.txt, I used the chmod command similarly to changing permissions on regular files. For instance, to allow only read access for the user and group, I used chmod ug=r, o= .project\_x.txt.

## Change directory permissions

To modify directory permissions, I used the chmod command with the -R option to recursively change permissions for all files and directories within the specified directory. For example, to restrict access to the drafts directory to only the researcher2 user, I used chmod -R 700 drafts.

## Summary

In this portfolio document, I demonstrated proficiency in managing file permissions using Linux commands. By checking, interpreting, and modifying permissions, I ensured that authorized users had appropriate access while unauthorized access was restricted, contributing to the overall security of the organization's file system.