# Changing user permissions in Linux

## Project description

The aim of this project is to verify current user access permissions for the research group and to modify them as needed following the least privilege principle.

## Check file and directory details

The **pwd** command is used to display the working directory.

The **ls** command is used to display the existing files and sub-directories in the working directory.

Using the **cd projects** command allows us to navigate into the “projects” directory.

With the **ls** command we see the files and the sub-directories in the “projects” directory.

A computer screen shot of a program

Description automatically generated

## Describe the permissions string

The **ls** command and the **-la** option are used to display current permissions for both visible and hidden files and directories.

A computer screen shot of a program

Description automatically generated

## Change file permissions

The **chmod o-w project\_k.txt** command takes away the write permission (w) from other users (o) for the project\_k.txt file.

The **chmod g-r project\_m.txt** command takes away the read permission (r) from the group (g) for the project\_m.txt file.

A computer screen shot of a program

Description automatically generated

## Change file permissions on a hidden file

The **chmod u-w,g=r .project\_x.txt** takes away the write (w) permission from the user (u) and establishes that the group have read (r) permission for the hidden file called **.project\_x.txt**

A computer screen shot of a program

Description automatically generated

## Change directory permissions

The **chmod g-x drafts** takes away the execute (x) permission for the group (g) for the “drafts” directory.

A computer screen shot of a program

Description automatically generated

## Summary

During this exercise, a list of current access permissions for a number of files and directories has been displayed. Then, permissions have been modified to appropriately meet security requirements establishing that users should only have access to the resources that they require in order to carry out their tasks.

Below, the updated list of user permissions following the modifications:

A computer screen shot of a program

Description automatically generated