# File permissions in Linux

## Project description

As a security analyst, I am responsible to manage proper authorization and permissions in an ongoing research study from a safety perspective. The permissions of who gets to read or make changes to certain files in the project folder for one of the researchers, and in some cases even hidden assets, are not set as they should be. Correcting this will help to keep their system more secure.

Below follows a brief description on how I did it.

## Check file and directory details

I used the command pwd to display in which directory I am, and then the command ls to display the content, i.e., the project subdirectory.

The command cd projects then changed directory.

The commands ls -l and ls -la then revealed all files and their permission structure.

See attached file: permissions of the files in the projects directory to view the commands, and their resulted output.

## Describe the permissions string

Each files, or directory, has a 10-character string before it.

One example taken from the screenshot Permissions of the files in the project’s directory:

-rw-rw-rw- for project\_k.txt

where (from left to right):

- = simple file (a directory would have been a d)

r = read permission (for user researcher2)

w = writing permission, i.e., make changes to file (for user researcher2)

- = no permission given to execute any executable function (for user researcher2)

r = permission to read the file (for any other member of research\_team)

x = writing permission, i.e., make changes to file (for any other)

- = no permission given to execute any executable function (for any other)

r = permission to read the file (for any other)

w = permission to read the file (for any other)

- = no permission to given to execute any executable function (for any other)

This is of course a simple txt file, but it could have been an executable file (such as .exe, .xlsm, or even a python file .py)

## Change file permissions

The organization determined that none outside the research team should have access to change any of their files. To comply with this, I first listed all files, with command ls -la, and noticed that project\_.txt fell short of this. I corrected this by typing chmod o-w project\_.txt command.

See attached file: writing permissions for others.png

## Change file permissions on a hidden file

The research team recently archived the file project\_x.txt. No further changes should be made, but both the user and wider research team should be able to read it.

I performed this in two (2) steps.

See attached file: correcting permissions for a hidden file.png

## Change directory permissions

There is subdirectory named drafts in the projects folder that none other then then researcher2 should have any access to, according to my organization. It noticed that the research team had access – that is privilege level x – so I removed it with the chmod command.

See attached file: permissions for the drafts folder.png

## Summary

I changed permissions for multiple files to get the level of authorization my organization desired to match reality in the current project folder, for one of the researchers. Usually that required using the Linux commands ls -l or ls -la to check permission status. Then I changed permissions using the Linux command chmod in appropriate forms as needed.