# File Permissions in Linux Portfolio

## Project Description

In this project, I simulated the responsibilities of a cybersecurity professional managing file permissions for a research team within an organization. My task was to examine the permissions of various files and directories in the projects directory, identify improper access, and use Linux commands to correct these issues. This exercise demonstrates my knowledge of Linux commands for managing file permissions, essential for securing sensitive research data.

## Check File and Directory Details

To check file and directory permissions, I used the following command:

ls -la ~/projects

This command lists all files and directories in long format, including hidden files, and displays details such as ownership, size, modification time, and permissions.

Example output line:

-rw--w---- 1 researcher2 research\_team 46 May 29 18:52 .project\_x.txt

## Describe the Permissions String

Example: -rw--w----  
- - : Regular file.  
- rw- : Owner can read and write.  
- -w- : Group can write but not read.  
- --- : Others have no permissions.  
This string indicates that the file is a regular file, with read and write permissions for the owner, write-only for the group, and no permissions for others.

## Identify and Change File Permissions

I identified that .project\_x.txt had incorrect permissions (group had write access). I used the following command to correct it:

chmod g-w .project\_x.txt

Then, I verified the updated permissions with:

ls -l .project\_x.txt

Updated permissions:

-rw-r----- 1 researcher2 research\_team 46 May 29 18:52 .project\_x.txt

## Change File Permissions on a Hidden File

Since .project\_x.txt should be read-only for user and group, and no access for others, I used:

chmod u-w,g=r,o= .project\_x.txt

Verification:

ls -l .project\_x.txt

Updated permissions:

-r--r----- 1 researcher2 research\_team 46 May 29 18:52 .project\_x.txt

## Change Directory Permissions

The drafts directory should only be accessible by researcher2. I used:

chmod 700 ~/projects/drafts

Verification:

ls -ld ~/projects/drafts

Updated permissions:

drwx------ 2 researcher2 research\_team 4096 May 29 18:52 drafts

## Summary

In this project, I applied Linux file permission management to secure the research team’s files and directories. I used commands such as ls -la to check permissions and chmod to modify them as needed. Specifically, I corrected the permissions on .project\_x.txt to remove unauthorized write access and ensured the drafts directory was restricted to the appropriate user. This portfolio demonstrates my ability to use Linux commands to manage access control, an essential cybersecurity skill.