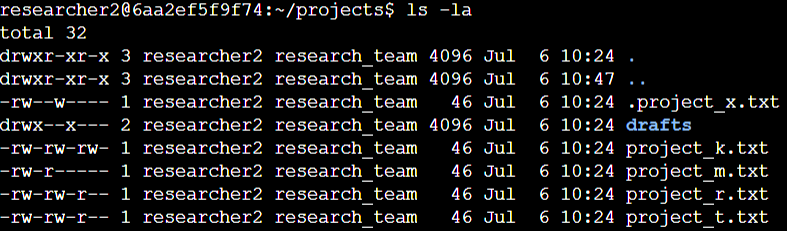
# File permissions in Linux

## Project description

In this scenario, I am tasked with examining and modifying the permissions of files and directories on a linux system to ensure that the authorization of the users, groups, and others aligns with the organization’s security policies. The primary goal of this project is to review and modify permissions to enhance the security of the file system.

## Check file and directory details

To check file and directory permission details, ls -la command should be used. This command provides a detailed list of all files and directories(including hidden files and directories) and their permissions.



Or we could use ls -la /home/researcher2/projects from the root directory.

## Describe the permissions string

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

* The first character represents the file type it is denoted by (-) for regular files, (d) for directories and (l) for symbolic links.
* The characters 2-4 represent the user’s(or owner) permissions(read,write and execute).
* The characters 5-7 represent the group’s permissions(read,write and execute).
* The characters 8-10 represent the other’s permissions(read,write and execute).

In linux, read is represented as (r), write is represented as (w) and execute is represented as (x).

For example, the file permissions for project\_t.txt are -rw-rw-r--. Since the first character is a hyphen (-), this indicates that project\_t.txt is a file. The second, fifth, and eighth characters are all r, which indicates that user, group, and other all have read permissions. The third and sixth characters are w, which indicates that only the user and group have write permissions. No one has execute permissions for project\_t.txt.

## Change file permissions

To change/modify or remove file permissions, the chmod command is used. In this scenario, I will ensure that the “Other” category does’'t have write permissions to a specific file called project\_k.txt, as per organization’s policy. 

To ls -la command is used after the chmod command to verify the changes made.

Output:



## Change file permissions on a hidden file

The file .project\_x.txt is a hidden file that has been archived and should not be written to by anyone. (The user and group should still be able to read this file.). So by following the policy, The permission needs to be modified using chmod command to disable write access for others but retain read permissions for the user and group.



Output:

## Change directory permissions

In case of drafts directory, Only the researcher2 user should be allowed to access the drafts directory and its contents. (This means that only researcher2 should have execute privileges.), since the group also has execute permission, the chmod command is used to remove the execute privilege of the group.



Output:



## Summary

For this task, I examined and modified the file and directory permissions on a linux system. I used the ls -la command to view the permissions, to match the level of authorization my organization wanted for files and directories in the projects directory. I also used the chmod command to modify permissions for specific files and directories which needed to be modified based on the policies. This helps the organization to maintain a secure file system and secure access control thus reducing the vulnerabilities which can be exploited.