# File permissions in Linux

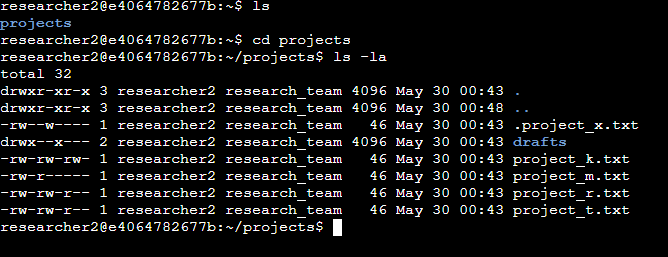
## Project description

The research team at my organization needs to update the file permission for certain files and directories within the projects directory.The permissions do not currently reflect the level of authorization that should be given.CHecking and updating these permission will help keep their

System [secur](http://secure.to)e. To complete this task, i performed the following tasks:

## Check file and directory details

The following code demonstrates how I used linux commands to determine the existing permissions set for a specific directory in the file system.



The first line shows the list of directories under the current parent folder and it shows our projects folder on which we need to work. After that we navigate to the projects directory and check permissions for all contents inside it using ls -la command the file content returned had 3 different users who had various access over different files and directories in the project directory. There was also a hidden file in this .project\_x.txt and five other project files. The 10 character string in the first column represents the permissions set on each file or directory.

## Describe the permissions string

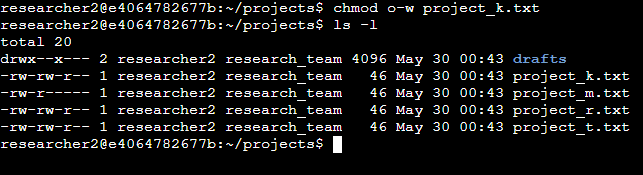
The 10-character string can be deconstructed to determine who is authorized to access the file and their specific permissions. The characters and what they represent are as follows:

* **1st character**: This character is either a d or hyphen (-) and indicates the file type. If it’s a d, it’s a directory. If it’s a hyphen (-), it’s a regular file.
* **2nd-4th characters**: These characters indicate the read (r), write (w), and execute (x) permissions for the user. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted to the user.
* **5th-7th characters:** These characters indicate the read (r), write (w), and execute (x) permissions for the group. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted for the group.
* **8th-10th characters:** These characters indicate the read (r), write (w), and execute (x) permissions for other. This owner type consists of all other users on the system apart from the user and the group. When one of these characters is a hyphen (-) instead, that indicates that this permission is not granted for other.

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, not a directory. 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

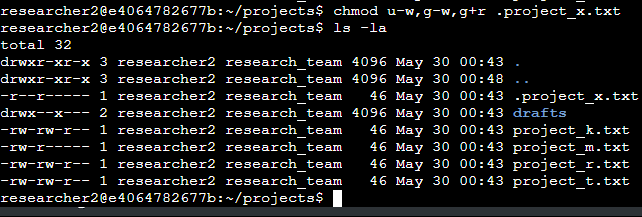
Now as per the organisations norms others should not have the access to write on any files so we remove the write permission for all the other owners in the project file



Now no other owners have the write permissions to content in the projects directory,

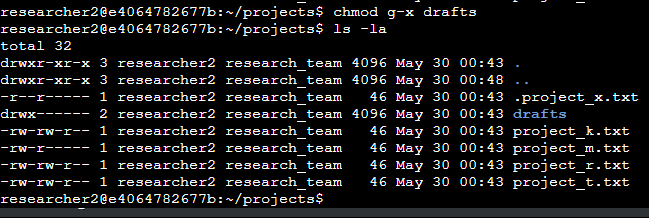
## Change file permissions on a hidden file

Now the hidden file should not have write permissions for anyone , but the user and group should be able to read the file. For this i ran the following commands



## Change directory permissions

Now the directory project should only have executable access to researcher2 and as we can see the drafts directory within the projects directory has -x permission so we have to change that so that only researcher2 has the permission



The output here displays the permission listing for several files and directories. Line 1 indicates the current directory (projects), and line 2 indicates the parent directory (home). Line 3 indicates a regular file titled .project\_x.txt. Line 4 is the directory (drafts) with restricted permissions. Here you can see that only researcher2 has execute permissions. It was previously determined that the group had execute permissions, so I used the chmod command to remove them. The researcher2 user already had execute permissions, so they did not need to be added.

## 

## Summary

I changed multiple permissions to match the level of authorization my organization wanted for files and directories in the projects directory. The first step in this was using ls -la to check the permissions for the directory. This informed my decisions in the following steps. I then used the chmod command multiple times to change the permissions on files and directories.