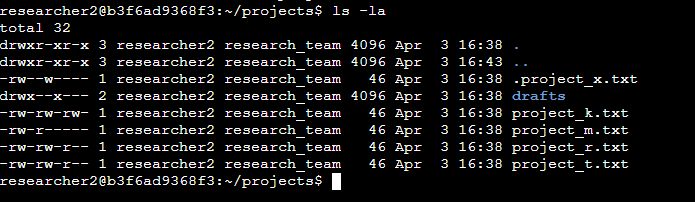
# File permissions in Linux

## Project description

As a Security Professional in our organization I examined the existing permissions on our file system. I determined if the permissions match the authorization given. In this project, I managed to authorize appropriate users and remove any unauthorized access.

## Check file and directory details

First is that I used **ls -la** to find all files including the hidden ones and view their current permissions.



## Describe the permissions string

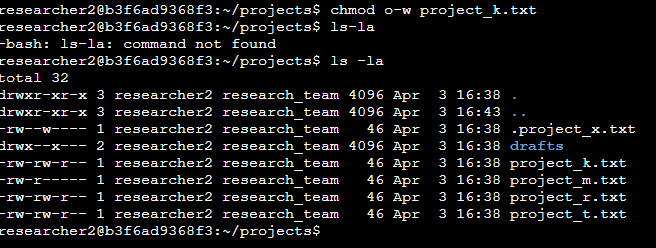
Given that the project\_k.tt for example has the permission “-rw-rw-rw-” which means User has read and write permission but don’t have authorization to execute because it doesnt have the “x” permission which goes for the group and others category.

One of the files that have incorrect permission is the project\_x.txt since this is already an archived file, the group user should not have the permission to write.

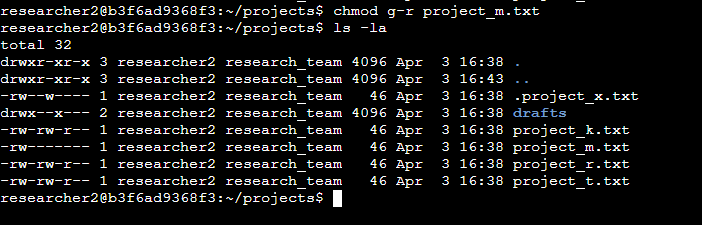
## Change file permissions

The organization does not allow **other** group to have the write authorization to any files.

I removed write access for the **other** group on the file using **chmod** command:



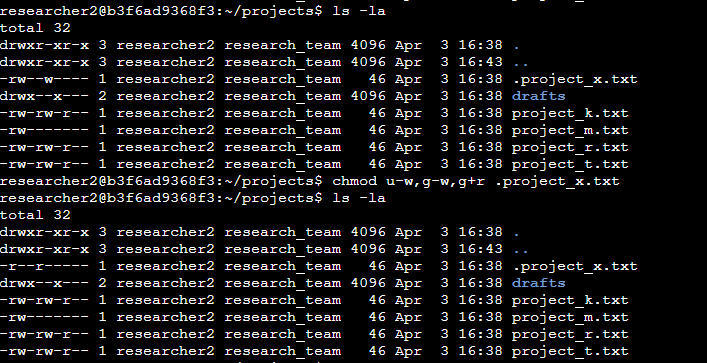
The project\_m.txt is a restricted file and should not be readable or writable by the **group** or **other**. Using **chmod** I removed access to the **group**.



## Change file permissions on a hidden file

I was able to determine the hidden files by using the command **ls -la** and saw that the file .project\_x.txt has been archived and should not be written by anyone.

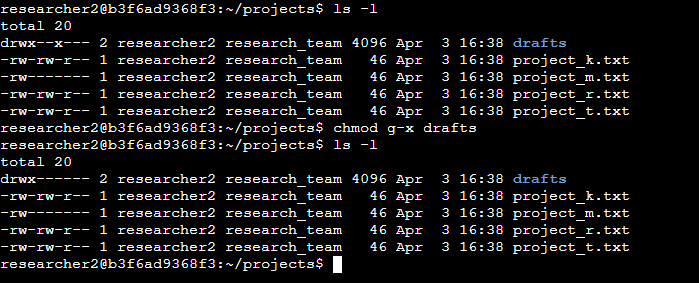
Using ls -la and chmod I was able to correct the given permissions.



## Change directory permissions

After checking the group permissions of the /home/researcher2/projects/draft directory only the researcher2 user should be allowed to access the drafts directory and its contents. Only the user should have execute privileges.

Using **chmod**, I am able to revoke execute access to the **group**.



## Summary

As a cybersecurity analyst, managing file and directory access rights is crucial. For this project, I made sure the organization's filesystem had the appropriate access permissions by using Bash commands. The concept of least privilege was broken by many files, which had more permissions than were necessary. This can be a major security risk since private data may be disclosed to uninvited persons. I was able to view and change access permissions by permission groups using bash commands like ls and chmod, ensuring that every user had the appropriate permissions in accordance with the organization's authorization guidelines.