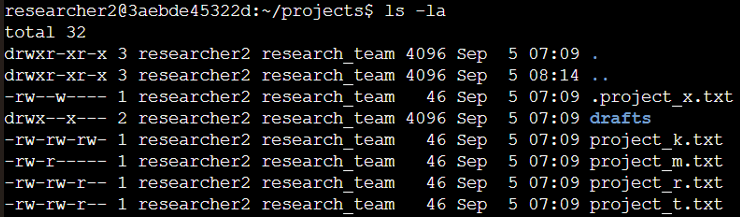
# File permissions in Linux

## Project description

In this scenario, I had to examine and manage the permissions on the files in the /home/researcher2/projects directory for the researcher2 user, including any hidden files, to make sure that permissions align with the authorization that should be given.

## Check file and directory details

First, I went to the projects directory using the cd command: cd /home/researcher2/projects. Then, I used the ls –la command to list the contents (ls) and permissions (-l) of the projects directory, including the hidden files (-a).



## Describe the permissions string

Let’s take the project\_k.txt file to explain the permissions on it:



We can see the –rw-rw-rw- string at the start. The first character indicates the file type, d for directory and – for regular file. Then, we have 3 sets of 3 characters for the read (r), write (w) and execute (x) permissions for the User (u), Group (g) and Other (o).

Therefore, in this string –rw-rw-rw-, we have a regular file - (project\_k.txt), and then rw read and write permissions for the user, group and others. There are no execute (x) permissions for anyone.

## Change file permissions

## The organization does not allow Other to have write access to any files. However, we can see that they have write access in the project\_k.txt file.



The chmod command changes permissions on files and directories.

I used the chmod o-w project\_k.txt command to remove the write (w) permission to Other (o) and then used ls –la again to confirm that the permission was removed:





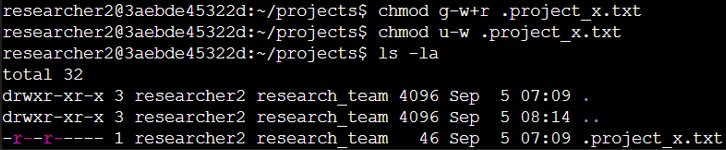
We can see that the w from Other is gone.

## Change file permissions on a hidden file

## The research team has archived .project\_x.txt, which is why it’s a hidden file. This file should not have write permissions for anyone, but the user and group should be able to read the file.



Using the commands chmod g-w+r .project\_x.txt and chmod u-w .project\_x.txt, I removed the write permission and granted the read permission to Group, and also removed the write permission for User from the .project\_x.txt file. Then, I used the ls –la command to list the contents and permissions to confirm the changes.



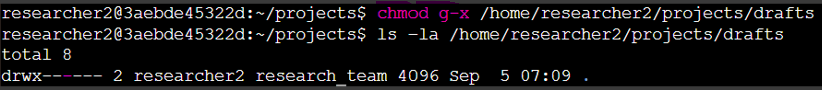
## Change directory permissions

## The files and directories in the projects directory belong to the researcher2 User. Only researcher2 should be allowed to access the drafts directory and its contents.

Using ls-la on the drafts directory, we can see that the User and Group have execute access.

## 

## Therefore, I removed the execute permission for the Group from the drafts directory using chmod g-x /home/researcher2/projects/drafts. Then, I used ls-la again to confirm that the execute permission was correctly removed from the Group.



## Summary

Through a series of commands and checks, I aligned file and directory permissions with the organization's security policies. This process involved securing sensitive files, such as limiting write access to the "Other" type of users, adjusting permissions for hidden files, and ensuring that only the designated user had access to specific directories. The actions taken in this scenario contribute to improved access control and security for the files and directories within the specified directory.