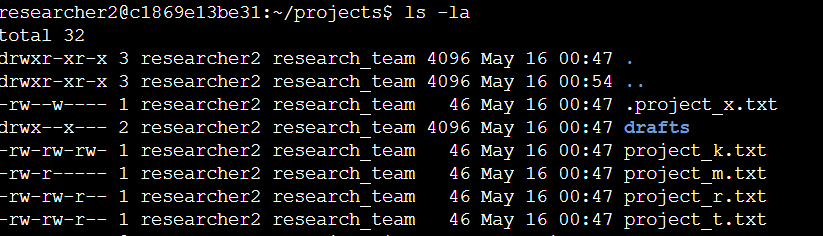
# File permissions in Linux

## Project description

On this project , I as a cybersecurity student realized there are several files and directories that have wrong permissions. It is important to keep everything in a system safe by using least privilege to allow certain users to fully access files and deny unauthorized access users from gaining full access to important files. I have changed permissions on several files to keep everything safe.

## Check file and directory details

I navigated to /home/researcher2/projects .I have used the command line ls -la to check permissions on the files and directories inside the current directory including hidden files. The following picture shows the permissions of all files. 

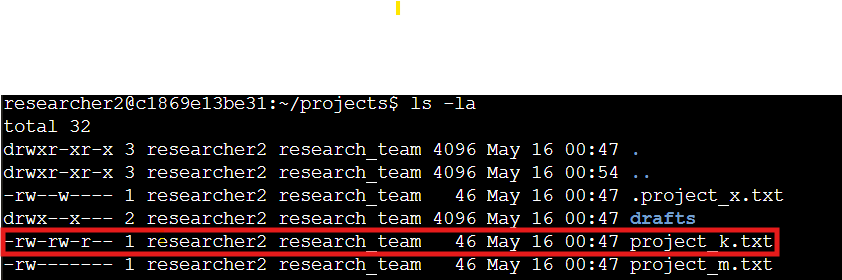
## Describe the permissions string

According to the image above . The first block shows a 10-character string for each of the files and directories. the 1st character indicates the file type; if it is (d) it means it's a directory, whereas the hyphen (-) indicates it is a file. The 2nd to 4th character shows the user permissions , 5th to 7th shows the group permissions, last, the 8th to 10th character shows the other permissions. The letters (r,w,x) in the string show what type of permissions they are. The ( r ) letter stands for Reading, ( w ) stands for writing and ( x ) stands for execute, for example , the .project\_x.txt indicates that the user grants permissions for read and write , while the group has access to write only, whereas the other have no access to the file.

## Change file permissions

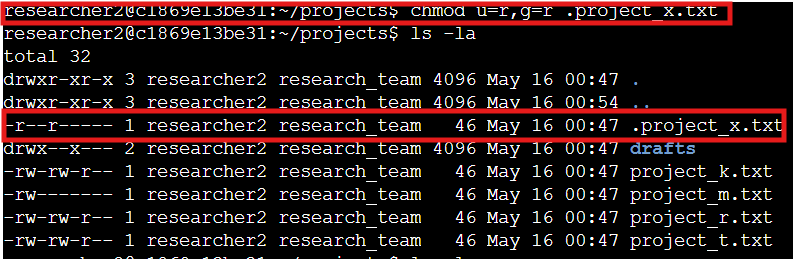
The other users are not allowed to write on any file. According to the image above, the file project\_k.txt has write permissions to the other. I have changed the permissions of that file using the command line chmod o-w project\_k.txt to remove the write permissions on that file. 

After I have changed the permissions using the above command line , I double checked my work to make sure that the current file has the right permissions.



As you can see from the above image, the other user does not have write permissions anymore.

## Change file permissions on a hidden file

The .project\_x.txt hidden file should not have write permissions for anyone , so I had to use the following command line to remove the write permissions. 

As you can see the .project\_x.txt file now has only the read permissions.

## Change directory permissions

The group user has execute permissions on the /drafts directory. Only researcher2 users should be able to execute this directory. Using the command line below removed the execute permission from the group user.

## Summary

Using the command line makes it efficient for the cybersecurity professionals to grant or remove permissions from certain users and make sure all files and directories in a system are well maintained and kept safe.