# File permissions in Linux

## Project description

I needed to verify that users had the appropriate permissions to help keep the system secure. I will need to examine permissions using Linux commands and modify these permissions to authorize the appropriate users and remove any unauthorized access.

## Check file and directory details

I used the cd projects command to move to the projects directory. I then use the ls command with the -la option to look at all the permissions set for the files and subdirectories in the projects directory as well as see the hidden files.

## A screen shot of a computer program Description automatically generatedDescribe the permissions string

The 10 character string shows who has authorization to access a file and their permissions. The first character is a d or (-) and indicates the file type. A d for directory and a (-) if it’s a regular file. Characters 2-4 indicate read (r), write (w), and execute (x) permissions for the user. If one of these is a (-) then it indicates that permissions is not granted. Characters 5-7 indicate permissions for the group and characters 8-10 indication permissions for

One example is the .project\_k.txt file which has a string of -rw-rw-rw-. In this particular file you can see the first character is a hyphen indicating it’s a regular file. The next characters show that the user, group and other have the permissions of read and write, but do not have the execute permission.

## Change file permissions

I needed to change file permissions to not allow the other group to have write permission. Therefore, I used chmod o-w command to change permissions on the project\_k.txt file and remove the write permission from this file. I then checked permissions using ls -la command to verify the permission was removed.

## A screenshot of a computer program Description automatically generated

## Change file permissions on a hidden file

The hidden file needed to have permissions of only read for the user and the group. The first two lines show the commands I entered, I used the chmod u=r, g=r command on the .project\_x.txt file the = was a way to overwrite existing permissions as well as set up the new permissions of only read for the user and group. Then verified permissions using ls -la which is the output shown below. A screenshot of a computer program

Description automatically generated

## Change directory permissions

Next only researcher2 should be allowed to access the drafts directory. The research\_team still had execute permissions. The first two lines show me using the chmod g-x command to remove the execute permission from the research\_team in the drafts directory. Then reviewed permissions using ls -la. The following lines are the output of the second command.

## A screenshot of a computer Description automatically generatedSummary

After verifying the permissions in the projects directory. I needed to change permissions to match what my organization wanted for the files and directories in the projects directory. I first verified permissions in the directory using ls -la then I used the chmod command multiple times to change the permissions on the files and directories .