# Changing File Permissions in Linux

## Project description

The team needs to update file permissions for specific files and directories within the projects directory. The current permissions do not show the proper level of authorization that should be given. Updating the permissions will keep the system secure. To finish the project, I did the following tasks:

## Check file and directory details

The code here shows how I used Linux commands to find the current permissions set for the projects directory within the file system.

A screenshot of a computer

Description automatically generated

The second line shows the command to display the contents of the projects directory, displaying the contents in the following lines. I used the ls command with the -la option in order to display a detailed listing of the contents and any hidden files within the projects directory. The output of this command showed that there is one directory named drafts, a hidden file named .project\_x.txt, and five other project files. The 10-character string in the first column shows the current permissions set for each file and directory.

## Describe the permissions string

The 10-character string can be broken down to show what user is authorized to access the file and their specific permissions for that file. The characters and what they represents are:

* 1st Character: This character can be a d or a hyphen (-) and indicates the file type. If it is a d, it’s a directory. A hyphen (-) is a regular file.
* 2nd-4th Characters: These characters show the read (r), write (w), and execute (x) permissions for the user. Whenever these characters are a hyphen (-), the permission is not given for that user.
* 5th-7th Characters: These characters show the read (r), write (w), and execute (x) permissions for the group. Whenever these characters are a hyphen (-), the permission is not given for that group.
* 8th-10th Characters: These characters show the read (r), write (w), and execute (x) permissions for other kinds of users. This owner type is all other users that are on the system and not within the user and the group. Whenever these characters are a hyphen (-), the permission is not given for other.

For example, the file permissions for project\_k.txt are -rw-rw-rw-. The first character is a hyphen (-), so we know that project\_k.txt is a file. The second, fifth, and eighth characters are all (r), meaning the user, group, and other all have read permissions for this file. The second, sixth, and ninth characters are all (w), meaning the user, group, and other all have write permissions for this file. The third, seventh, and tenth characters are all (-), meaning no one has execute permissions for project\_k.txt.

## Change file permissions

The organization decided that other should not have write permissions for any files. To update this, I determined that project\_k.txt needs to have write permissions removed from other. The following code shows how I used Linux commands to do this.

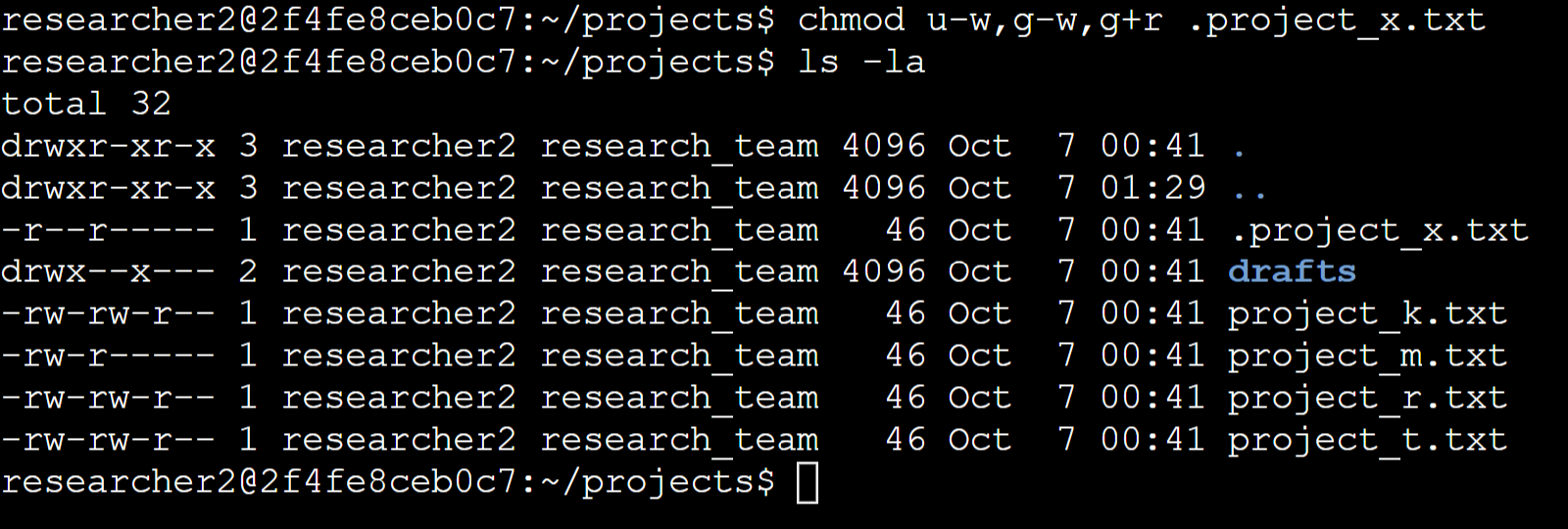
A screen shot of a computer

Description automatically generated

The first two lines show the commands I entered, the subsequent lines show the output of the second command. The chmod command changes file and directory permissions. Within the command, the first argument shows what permissions should be changed, and the second argument specifies the file or directory needed to be changed. In this instance, I removed write permissions from other (o-w) for the project\_k.txt file. I used ls -la to review the updates made.

## Change file permissions on a hidden file

The team archived .project\_x.txt recently; they do not want anyone to have write access to this file and want user and group to only have read access. The following code shows the Linux commands used to change these permissions.



The first line shows the command I used to update the permissions to this hidden file, and the second line shows the command used to display the output. I know that .project\_x.txt is a hidden file since it starts with a period (.). I removed write permissions from the user and group with u-w and g-w respectively. I then added read permissions to the group with g+r.

## Change directory permissions

The organization only wants the researcher2 user to have access to the drafts directory and the content within. No other user should have execute permissions. The following screenshot shows how I took execute permissions away from group.

A screenshot of a computer program

Description automatically generated

The first line shows the command I entered to perform this task, and the second line shows the command used to display the output. To remove execute permissions from the drafts directory, I used the chmod g-x command to remove them. The researcher2 user has execute permissions already, so nothing more needs to be added.

## Summary

This project allowed me to change multiple permissions to match the authorization level the organization wanted for files and directories within the projects directory. The first step was utilizing the ls -la command to check the current permissions, which allowed me to take the steps above to perform this task. I used the chmod command multiple times to change permissions on both files and directories.