# File permissions in Linux

## Project description

[Describe what you accomplish through Linux commands.]

As a security professional at a large organization working with their research team and part of the job is to ensure users on this team are authorized with the appropriate permissions. And it is done by examining existing permissions on the file system and determining if the permissions match the authorization that should be given. If they do not match, the permissions would need to be modified to authorize the appropriate users and remove any unauthorized access.

## Check file and directory details

After using the command cd projects which takes you to the project’s directory, executing the command ls -l returns all the file and directory permissions.

A screenshot of a computer

Description automatically generated with low confidence

## Describe the permissions string



The 10-character string in front shows what permissions the different items in the directory have. The “d” in the beginning means that this item is a directory, and if there was a “-“ then that means that it is a file. Then there are 3 sets of permissions which are given to different types of owners (format: (d *or* -)rwx1rwx2rwx3), the first set of permissions is for the “user”, and in this case it’s the user “researcher2” and the user is the owner. The second set of permissions is for the “group”, which is a large group the owner is part of (ex. *Marketing\_dept, Human\_Resources, Payroll\_dept*). And the third set of permissions is for “other”, this is for all other users on the system. The permission “r” stands for read and this means it gives the ability to read file contents and for directories it means it can read all the contents in the directory including files and subdirectories. The permission “w” stands for write, which means this is the ability to make modifications to file contents; for directories, this is the ability to create new files in the directory (ex. using the touch command). The permission “x” means this gives the ability to execute the file if it’s a program; for directories, this is the ability to enter the directory and access its files. If a “-“ in place of a permission, then it means that permission is not enabled for that file or directory.

## Change file permissions

The organization does not allow the permission set “other” to have any write privileges. First I used the command ls -l to list out the permissions for the files and directories in the project directory. Then after identifying that the file project\_k.txt has write permissions for the other category, I used the command chmod o-w project\_k.txt to remove the write permission from other.

A screenshot of a computer program

Description automatically generated with low confidence

## Change file permissions on a hidden file

First to change the file permissions of a hidden file you need to list them out, and to do this I used the command ls -la, alternatively if you just wanted to list the hidden files you would use ls -a. This file should not have write permissions for anyone, but the user and group should be able to read the file and the hidden file is .project\_x.txt, the “.” Indicates it’s a hidden file. So use the command chmod u-w,g-w .project\_x.txt which gets rid of the write permission for user and group as they were the ones who had write permissions, but then group now needs read permission and you add that by using the command chmod g+r .project\_x.txt

A screenshot of a computer program

Description automatically generated with medium confidence

## 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. In order to accomplish this you would first list out the items in the projects directory using the command ls -l, since your already in the projects directory and if your not you would use the cd projects command to first get there. Then you would use the command **chmod g-x drafts** to remove the remaining permission for group.

A screenshot of a computer screen

Description automatically generated with medium confidence

## Summary

Permissions on files and directories were examined and managed in the **/home/researcher2/projects** directory for the researcher2 user. First, the user and group permissions for all files in the project’s directory were checked. Then, I checked whether any files have incorrect permissions and changed the permissions as needed. And lastly, I checked the permissions of the **/home/researcher2/drafts** directory and modified these permissions to remove any unauthorized access. Using Linux commands teaches the concept of authorization, which is the notion of granting access to specific resources in a system. In Linux, file and directory permissions are used to specify who has access to specific files and directories. As a security analyst, setting appropriate access permissions is critical to protecting sensitive information and maintaining the overall security of a system.