# File permissions in Linux

## Project description

As a security professional at a large organization, part of the job involves ensuring users on the team are authorized with the appropriate permissions, in order to keep the system secure.

## Check file and directory details

A screenshot of a computer

Description automatically generated

In order to check the current permissions in the projects directory, we first navigate to the projects directory through Linux command cd /home/researcher2/projects then to check the permissions of all files and directories including hidden ones in projects, we use

ls -la this command allows us to view permissions to files and directories including hidden files. It also displays additional information, including owner name, group file size, and time of last modification.

## Describe the permissions string



For example at the beginning of each file or directory, we have a 10-character string which conveys information about permissions in respect to the user, group, and other users on the system.   
In the output above, for instance, the first character is the file type, d for directory, otherwise - for a regular file. The second through fourth characters describe if the user has r for read, w for write, x for execute permissions, - if the user lacks the given permission. In this case, the user has all rwx, read, write, and execute permissions. The group only has execute permission, and other has no permissions.

## Change file permissions

The organization does not allow other to have write access to any files. After checking permissions, it is identified that project\_k.txt currently gives other read and write permissions.



In order to remove the write permission from other, we utilize the command

chmod o-w project\_k.txt

The chmod command changes permissions on files and directories. The argument o-w specifies that w (write) is being subtracted or removed from the o (other). The last argument specifies the file whose permissions we are modifying.

After executing the command, the file’s permissions look as follows:



## Change file permissions on a hidden file

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

  
  
In order to correct the permissions to this file we must execute the following command:  
chmod u-w,g-w,g+r .project\_x.txt

After executing the command, which removes write permissions from the user and group and adds read permissions to the group, the file’s permissions appear as follows:



## 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.  
  
Currently the permissions for the drafts directory are as follows:  


We must remove the execute permission from the group.

chmod g-x drafts

  
  
This effectively only gives researcher2 the user, permissions to modify and utilize the drafts directory.

## Summary

This task involved viewing and ensuring that the appropriate users, groups, and others, only have the necessary permissions to perform their jobs. This follows the principle of least privilege which is an information security concept that gives users the minimum levels of access to perform their job functions.