# File permissions in Linux

## Project description

The process outlined for this project is to manage the authorization and directory permissions for multiple levels of files and directories within a Linux Command Line Interface.

## Check file and directory details

## 

First, moving the current directory to the instructed directory by using the “cd” command to change the directory.   
  
Once this is completed, the next request is to determine the files and directory details. To do this, we run a “ls -la” command. The “ls” command lists the files and directories within the current area, and the “-la” modifier is to list the files and hidden files of the directory along with their permissions listed.

## Describe the permissions string

The Permission strings in front of each group is listed as the following:  
  
drwxrwxrwx, this can be broken up into the following: the first RWX is the read, write and execute of the user, the 2nd is for the group, and the 3rd is for others. If there is a letter listed in the permissions then it is active. So for example in “project\_k.txt”, we see the following: -rw-rw-rw- which means that the user, group and others have read and write access to this file, but no executable access for the file.

## Change file permissions

## 

The next statement here is to change the file permissions of the project\_k.txt so that the others group does not have write access. This can be done with the “chmod” command. This modifies the permissions of the specific group listed.

In this case we did the following: “chmod o-w project\_K.txt”  
  
There are 3 parts, the first is the “chmod” which is the command, the 2nd part is the specific permissions, “o-w” means that we are removing write access from the others group, and the last part is the specific file being adjusted. In this case it is “project\_k.txt”  
  
when we ran the “ls -la” command again, w see that within project\_k.txt that within the other users, it does NOT have a “w” for write permissions in the last 3 markings for the others group.

## Change file permissions on a hidden file

## 

In the case of hidden files, they are prefixed with a “.” Before it, so for example in this case the hidden file is “.project\_x.txt”  
  
The instructions for the course has asked us to remove any write permissions and ensure that both the user and group have read permission only.  
  
In this case we had to issue 3 separate commands. The first two removed write permissions from both the User and the Group. The last command added the Read permission for the group to be added within this authorization. Once we checked again via “ls -la” we are able to see that “.project\_x.txt” is read only to both the User and Group, and all write abilities has been removed at this time.

## Change directory permissions

## 

For this, we have been asked to check for the drafts directory to ensure that only the user has access to the directory.  
  
In the first “ls -la” we see that the drafts directory listed in blue has RWX access for the user AND that the Group has Executable (X) access. With the “chmod” command where we removed the X access from the group for the drafts directory, and then checked again using the “ls -la” command it seemed to have executed perfectly.

## Summary

Overall within the course, we have not only identified and modified files both overt and hidden, but also have modified access to directories as well.