# File permissions in Linux

## Project description

In the scenario presented by Google Cybersecurity Certificate, I was tasked with examining and managing the permissions on the files in the /home/researcher2/projects directory for the researcher2 user, who is a is part of the research\_team group.

So, in this project I check the permissions for all files in the directory, including any hidden files, to make sure that permissions align with the authorization that should be given. When it doesn't, I change the permissions using Linux commands.

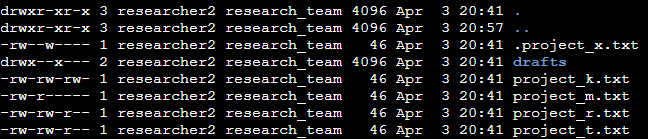
## Check file and directory details

To check file and directory permissions I used the following Linux command after navigating to the /projects directory:



This command is composed of a command (ls) and an option (-la) that modifies said command. The first of these, if no option were given, would just show the contents of the directory, excluding hidden files or directories which are identified with a ‘.’ or a ‘..’ at the start. If the option was just ‘-l’, the output would be the contents of the directory and the respective permission, but still excluding the hidden contents. So, to display both hidden and visible contents and their permissions the option ‘-la’ is used (if it was just ‘-a’ it would display all contents including hidden ones, but not their permissions).

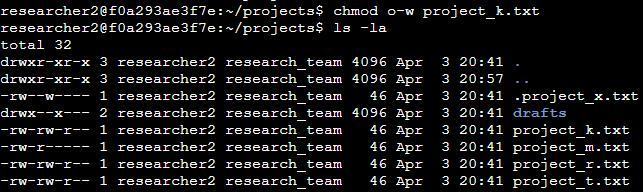
## Describe the permissions string

The output of said command was:  


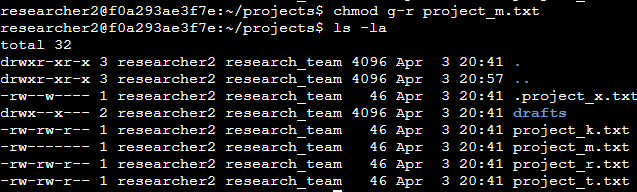
The first part of every line displays the type of content (file or directory) and respective permissions. This consists of a 10 digit string. The first digit specifies if it is a file with a ‘-’ or a directory with a ‘d’. The next three digits are the user permissions, the next three are the group permissions and the last three are the other permissions. The last part displays the name of the directory or file.

## Change file permissions

The ‘other’ users shouldn’t have any write permissions, so I used command ‘chmod’ (change mode) to remove said permission of the ‘project\_k.txt file’ for other users with the argument o-w, which means remove (-) the other users (o) writing permissions (w):



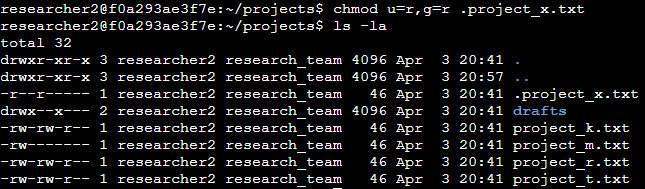
As the screenshot shows, I removed the permission successfully. The next permission to change is the group user read permission for the file project\_m.txt, since it should only be readable and writable by the user because it’s restricted. So I used the next command to remove said permission of the ‘project\_m.txt file’ for group users with the argument g-r, which means remove (-) the group users (g) reading permissions (r):



As the screenshot shows, I successfully changed the permissions for the file.

## Change file permissions on a hidden file

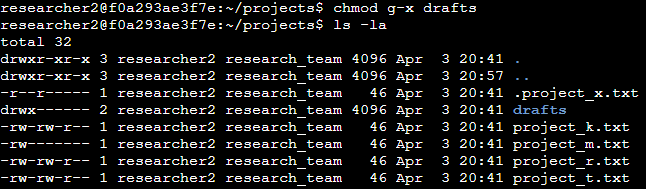
Next, the permissions for the hidden file ‘.project\_x.txt’ must be changed, since no user should be able to write on it, but the user and group should be able to read it. To accomplish this I used the next command to remove said permission of the ‘.project\_x.txt’ file for other and group users with the argument ‘u=r,g=r’, which means overwrite (=) the user (u) and group (g) users reading permissions (r):



As the screenshot shows, I changed the permissions successfully.

## Change directory permissions

Next, the ‘drafts’ directory permissions must be changed to restrict it’s access to the user, instead of also the group, so I used the next command to remove said permission of the ‘drafts’ directory for group users with the argument g-x, which means remove (-) the groupr users (g) executing permissions (x):



As the screenshot shows, I changed the permissions successfully.

## Summary

The first step I took was to check the user and group permissions for all files in the /projects directory. Next, I checked whether any files had incorrect permissions and changed the permissions as needed. Finally, I checked the permissions of the /home/researcher2/projects/drafts directory and modified them to remove any unauthorized access.