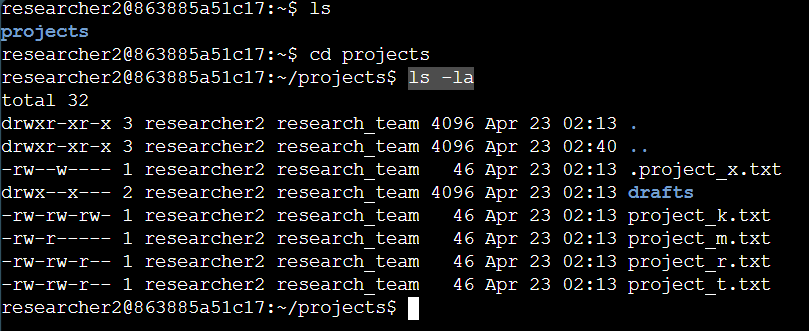
# File permissions in Linux

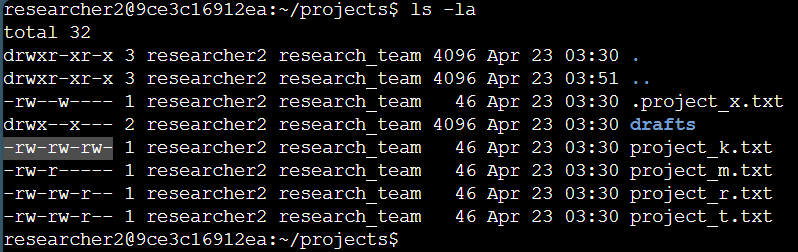
## Project description

Linux commands are what allow users to communicate and control the OS. As a security professional I have been tasked with examining existing file permissions on the file system, to ensure the appropriate users on the research team are authorized with the appropriate permissions. If permissions do not match the authorization of users, they will be modified to authorize appropriate users and remove any unauthorized access.

## Check file and directory details

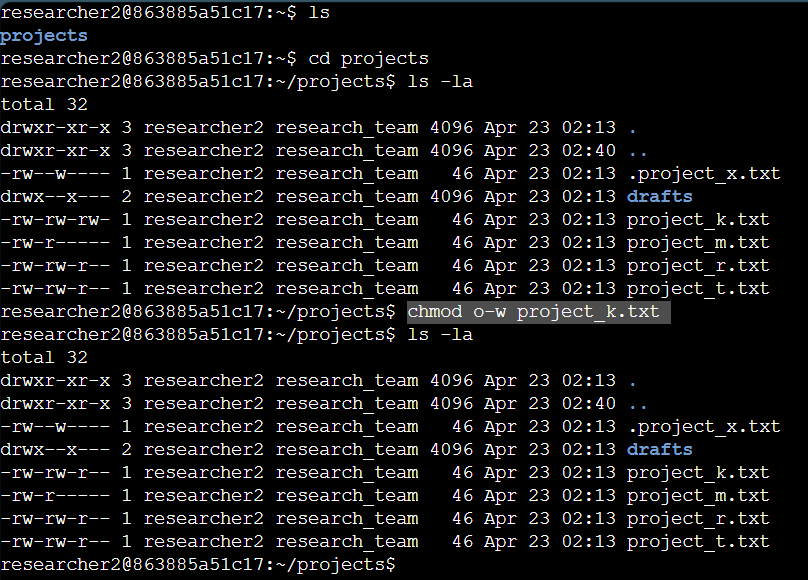
To check the file and directory details within the projects directory I used command “ls -la”. The command “ls” lists all contents within a directory or file. Adding the option “-l” will display a list of all permissions for files and sub-directories within a directory. Option “-a” will display any hidden files. Using command “ls -la” will display all file and directory permissions within the project's sub-directory including hidden files.

## Describe the permissions string

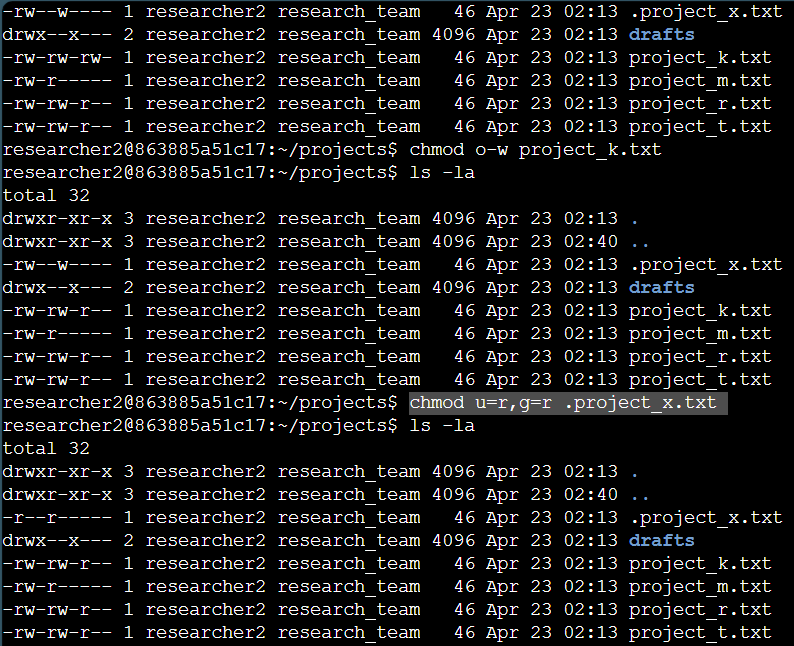
The output shows permissions granted for files and directories within the project’s directory. For example, the 10-character permission string for file” project\_k.txt” is read as follows: The 1st character “-” represents that the permissions are associated with a file, if it was a “d” the permissions would be associated with a directory. The 2nd through 4th character represents the permissions granted to the user, they have read permissions represented by “r” and write permissions represented by “w”, the “-” in this case indicates they lack execute permissions which would be represented by “x”. The 5th through 7th characters represents permissions granted to the group they have read and write permissions but lack execute permissions. The 8th- 10th characters represent permissions granted to others. They have read and write permissions but lack execute permissions.

## Change file permissions

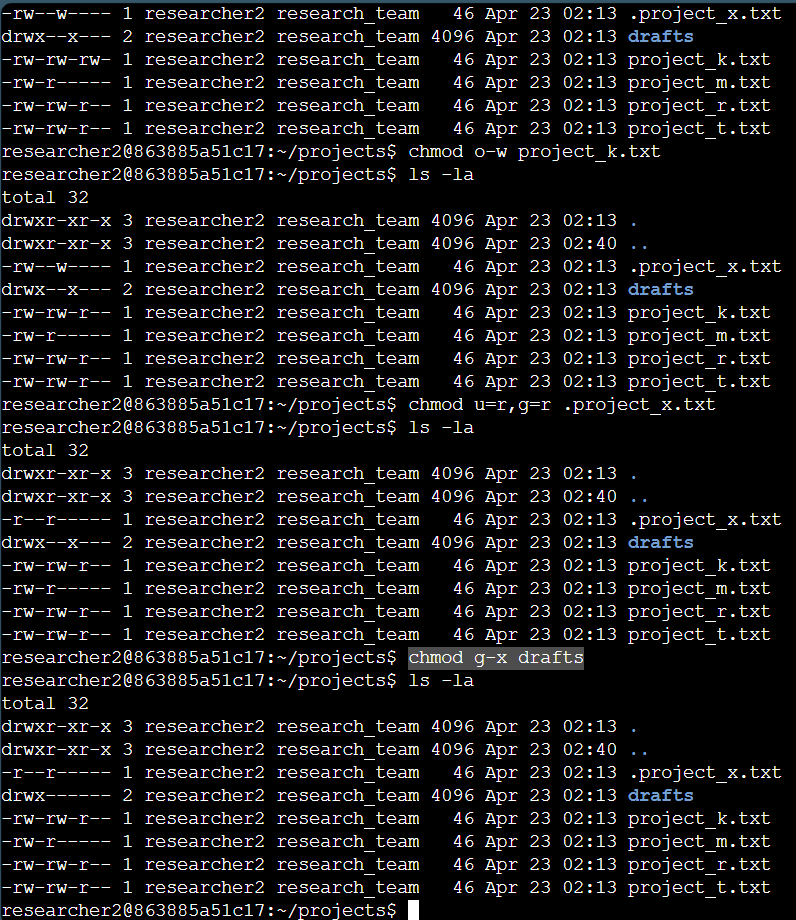
Our company doesn't allow the other owner type to have write permissions to any files so we must change the permission of file projects\_k.txt as it is the only file that grants the other owner type write permissions. We do this using the command “chmod o-w projects\_k.txt.”



## Change file permissions on a hidden file

The research team archived “. project\_x.txt” which is why it appears as a hidden file, hidden files appear with a “.” before the file name. This file should not grant any owner type write permissions. However, the user and group owner type should have read permissions for this file. To assign the correct permissions to this file the command “chmod u=r,g=r .project\_x.txt” should be used. The chmod command indicates we are changing permissions, the “u=r” represents changes to the user owner type “u” the “=” indicates that previous permissions should be overwritten by the permission in the command “r”, the “g=r” represents changes to the group owner type “g” the “=” indicates that previous permissions should be overwritten by the permission in the command “r”. The .projects\_x.txt is the file in which permissions will be modified. Alternatively, the command “chmod u-w,g–w+r .project\_x.txt” can be used, in this command the “+” means to add a permission, while “-” means to remove a permission.

## Change directory permissions

In the projects directory the files and directories belong to Researcher 2, so they alone should have access to the draft’s directory and its contents. As the owner, the user owner type should be the only one with execute access, represented by an “x”. To do this we use the command “chmod g-x drafts”. The chmod command indicates we are changing permissions, the “g-x” argument states we want to remove execute permissions from the group owner type, and the “drafts” argument indicates we want to remove the group owner types execute permissions from the draft directory.

## Summary

The commands used here have allowed me to ensure that this system is secure by adding permissions to authorized owner types and removing permissions from unauthorized owner types.