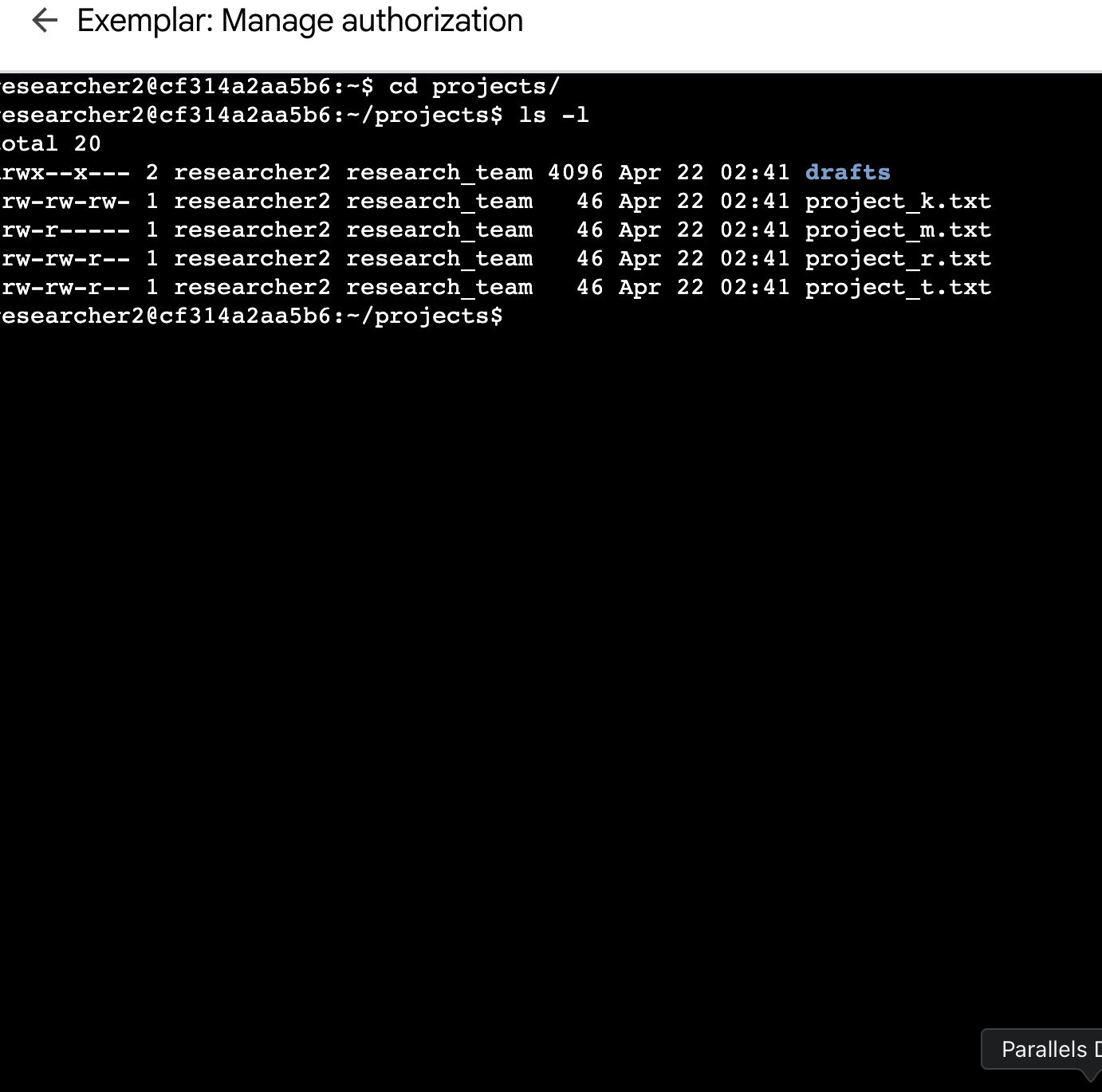
# File permissions in Linux

## Project description

In this activity called Manage Authorization, I was able to perform and examine the permissions on a directory and files within this project using Linux commands to configure authorization or granting access to specific resources. The purpose of this activity was to examine, change, add , update new permissions to each part of the type of owners in the Linux types either inside directories or files and in this activity I was working within the projects directory..

## Check file and directory details

To check files and directories permissions I was able to examine this activity by using the Linux command as “ls -l” which is a command that lists all the directories or files. Also, to examine if any file is hidden, a command that I used was “ls -a” that shows all the hidden files within a directory. A good combination of both commands can be useful in order to examine a full vision of the files and directories may have.



## Describe the permissions string

A permission string describes who can read(r), write(w) and execute(x) a file for the three types of users as the user who is the creator of the file. Groups are referred to the users in the file group and others that refer to anyone else. Each type of string describes its own characteristics like read that it can only view the content of a file or directory. Write can modify content and execute that can run a file as a program.

The 10 character string can be determined by who has the authorization to access the file and also to determine and examine their specific permissions and they are represented by:.

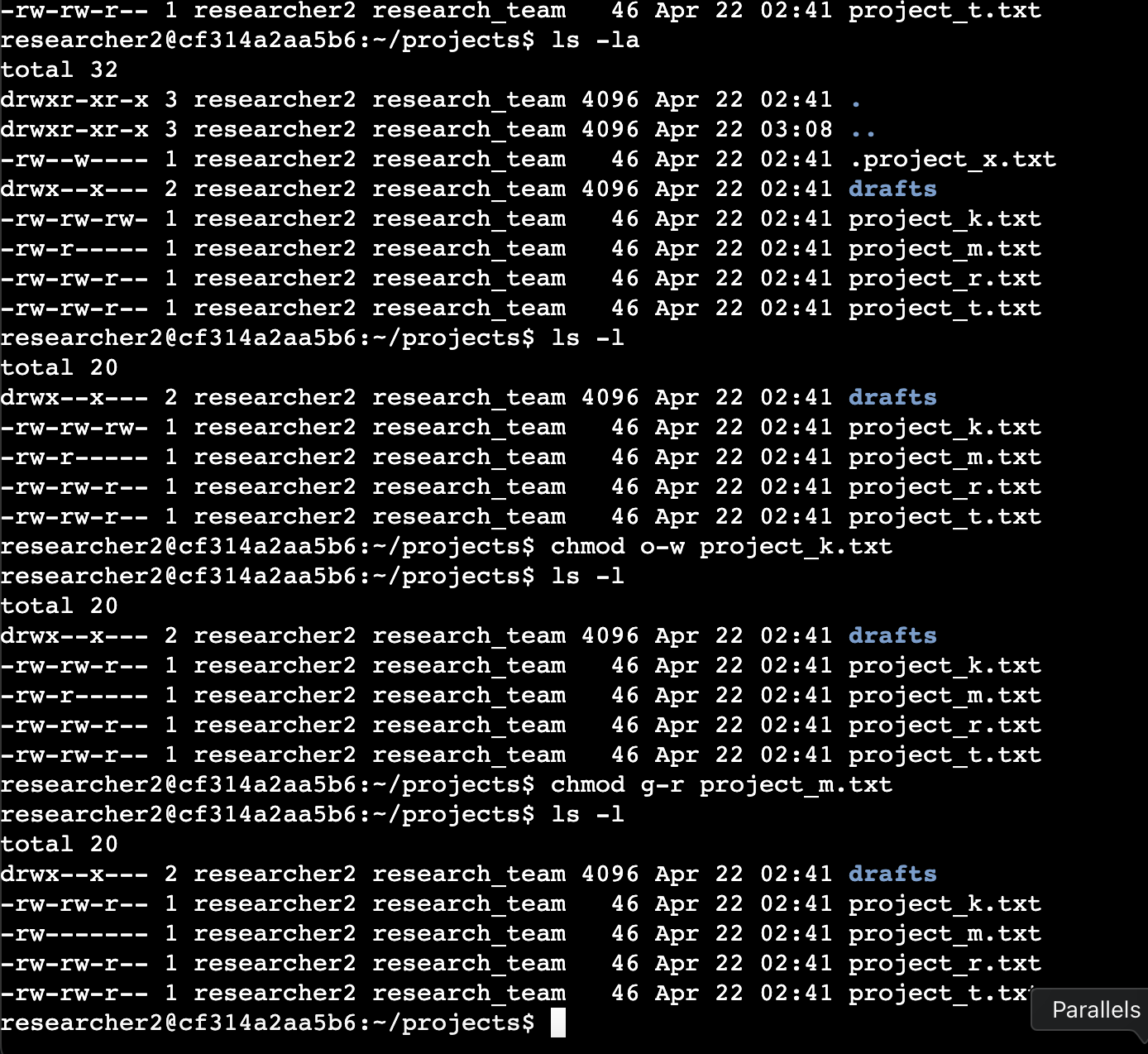
* 1st character: This character is either (-)file or (d)directory and these symbols indicate the family type.
* 2nd-4th character: These characters indicate the read(r), write(w), and execute(x) permission for the user.
* 5th-7th character: These characters indicate the read(r), write(w), and execute(x) permission for the group.
* 8th-10th character: These characters indicate the read(r), write(w), and execute(x) permission for other.

## Change file permissions

To change file permissions, a command as chmod which is change mode and it is the way how to change permission in Linux. The way that it works is that it takes 2 or more arguments after the chmod command. For example:

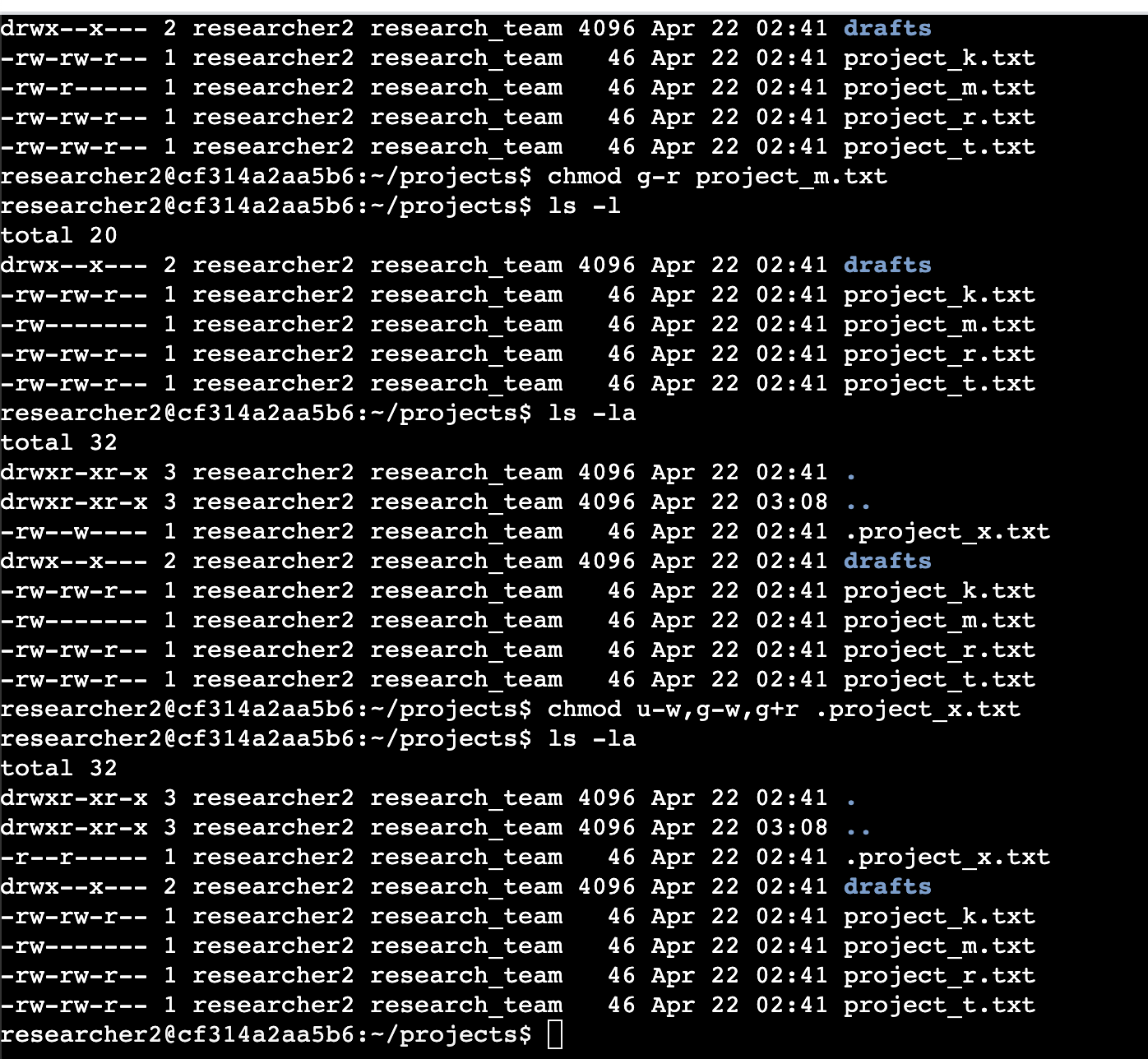
Chmod g+r access.txt

This command will grant access to the group but only for reading purposes. This action is managed by the chmod command that helps to change permission in Linux



## Change file permissions on a hidden file

To change permissions on a hidden file is also done by the command of chmod. Remember that chmod is a Linux command that helps to change permission for any type of user. A hidden file is a file that is hidden in any directory. To examine a hidden file the command is ls -a. This command will show all the hidden files.

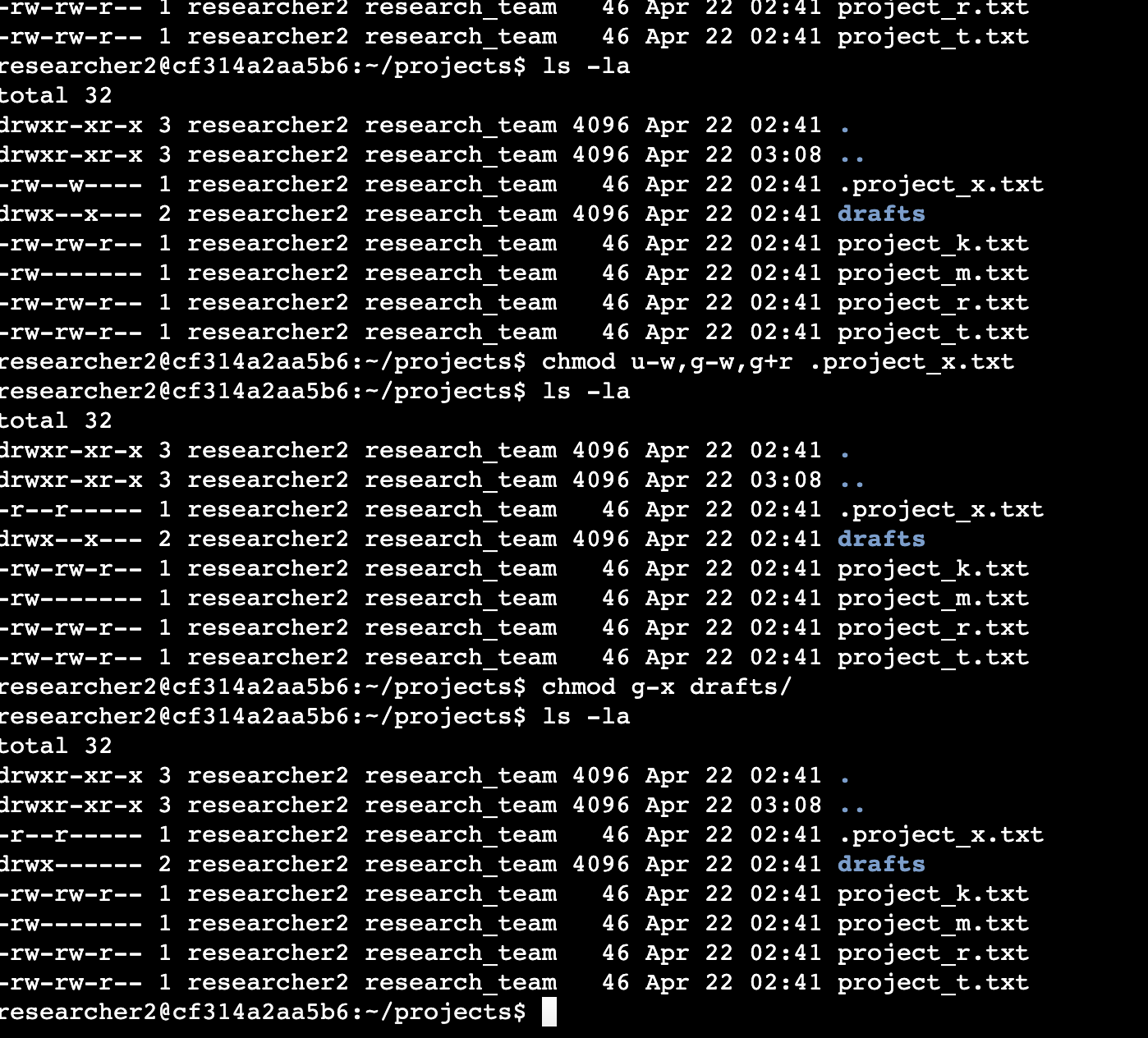


## Change directory permissions

To change directory permissions, a command as chmod which is change mode and it is the way how to change permission in Linux. The way that it works is that it takes 2 or more arguments after the chmod command.   
  
For example:

Chmod g+r kelvindocs

This command will give access to the group to only read kelvindocs



## Summary

To understand these commands it is important to understand what type of users we have in Linux in order to grant or deny access to a specific file or directory. This activity helps to understand the Linux commands in the area of managing permissions. It is also understandable that we need to understand the 10th line character to recognize when we try to change permissions.