# **FILE PERMISSIONS IN LINUX**

## 

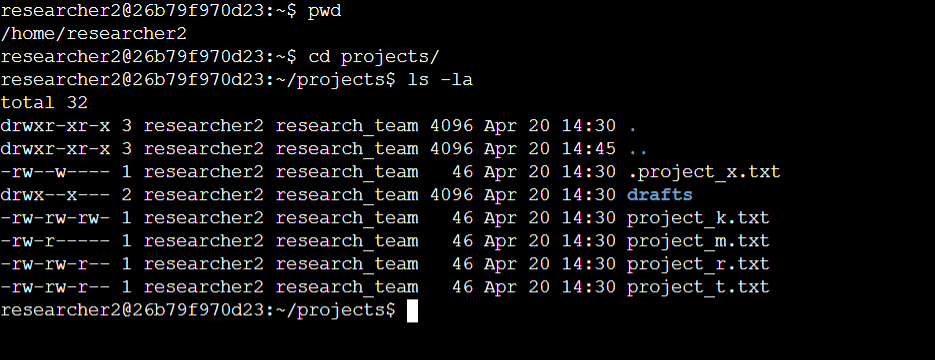
## **Project description**

This project includes examining and managing file permissions within the ***/home/researcher2/projects*** directory for the researcher2 user, who belongs to the research\_team group. The goal is to ensure that permissions align with the appropriate authorization levels and remove any unauthorized access.

## **Check file and directory details**

Here, we will perform the following tasks.

1. Navigate to the  ***projects***directory.
2. List contents and permissions.
3. Identify the group that owns the files.
4. Check for hidden files and identify any present.



In the ***/home/researcher2/projects*** directory, there are five files with the following names and permissions:

● ***project\_k.txt***

○ User = read, write

○ Group = read, write

○ Other = read, write

● ***project\_m.txt***

○ User = read, write

○ Group = read

○ Other = none

● ***project\_r.txt***

○ User= read, write

○ Group = read, write

○ Other = read

● ***project\_t.txt***

○ User = read, write

○ Group = read, write

○ Other = read

● ***.project\_x.txt***

○ User = read, write

○ Group = write

○ Other = none

There is also one subdirectory inside the projects directory named ***drafts***. The permissions on drafts are:

● User = read, write, execute

● Group = execute

● Other = none

## **Describe the permissions string**

The 10-character string in the permissions section of the output represents the file permissions in Linux. Each character signifies specific access rights for different user categories. Let's take an example from the above output.



* Here , d indicates that it is a directory.
* The next 2 to 4 characters indicate the type of permissions given to user / owner

The user has read, write and execute permissions.

* The next 5 to 7 characters indicate the type of permissions for the group.

The group has only execute permissions.

* The last 8 to 10 characters indicate the type of permissions for others.

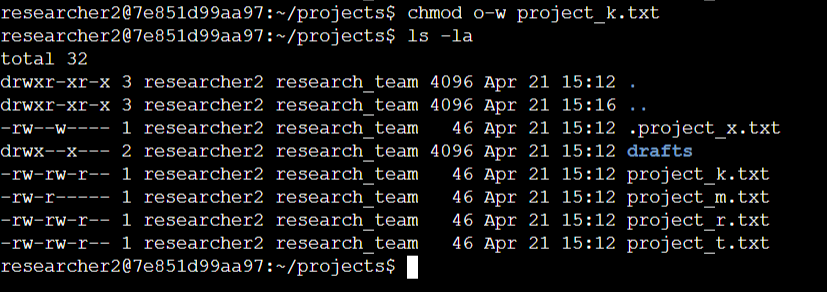
The others have no permissions.

## 

## **Change file permissions**

In this step we are going to check whether any file allows the other users to write files or not. In the above example we can see that there is only one file which allows other user to write i.e., ***project\_k.txt*** .

So we will change the permissions of ***project\_k.txt*** so that the owner type of other doesn’t have write permissions.



## 

## 

## 

## 

## Now file ***project\_m.txt*** is a restricted file and should not be readable or writable by the group or other. Only the user should have these permissions on this file. So we will change the permissions for group so that the group doesn’t have read or write permissions.

## 

## 

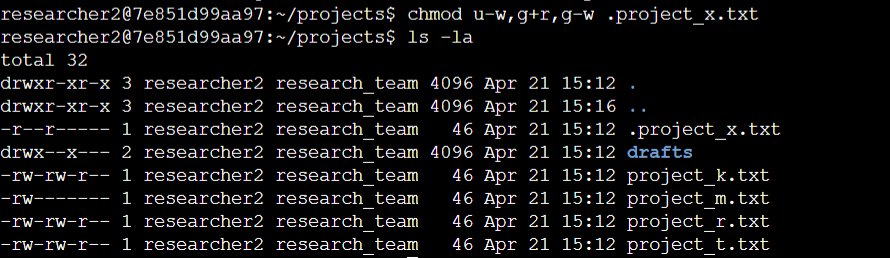
## 

## **Change file permissions on a hidden file**

In this task, you must determine if a hidden file has incorrect permissions and then change the permissions as needed. This action will further remove unauthorized access and strengthen security on the system.

The file ***.project\_x.txt*** is a hidden file that has been archived and should not be written to by anyone.

Here we will change the permission of this file so that the user and the group can read, but not write to, the file



## 

## 

## 

## 

## 

## 

## 

## 

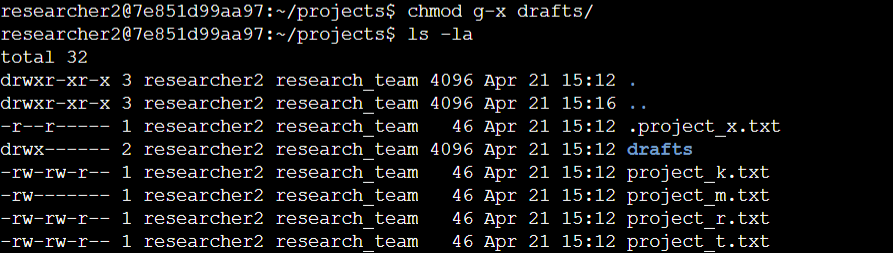
## 

## 

## **Change directory permissions**

In this task, we will change the permissions of a directory. First, we will check the group permissions of the ***/home/researcher2/projects/drafts*** directory and then modify the permissions as required.

Then we will remove the execute permission for the group from the ***drafts*** directory.



## 

## 

## 

## **Summary**

I began by conducting a comprehensive review of permissions within the projects directory using the ***`ls -la***` command. This provided crucial insights into the current authorization levels for files and directories. Armed with this information, I proceeded to adjust permissions to align with the organization's desired security standards. Utilizing the ***`chmod`*** command iteratively, I made targeted modifications to various files and directories within the projects directory, ensuring that each adjustment matched the specified level of authorization.