# File permissions in Linux

## Project description

The goal of this project is to represent the possible ways Linux commands can be used to secure the access to files and directory. Access and controls to files and folders should only be given to intended authorized persons but remain inaccessible to unauthorized person.

## Check file and directory details

## 

## Describe the permissions string

* In the **Projects** directory/folder, there are 5 files (including 1 hidden file [.project\_x.txt]) and 1 folder (drafts). The permission status for each are as follows:
* 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
* drafts are:
* User = read, write, execute
* Group = execute
* Other = none

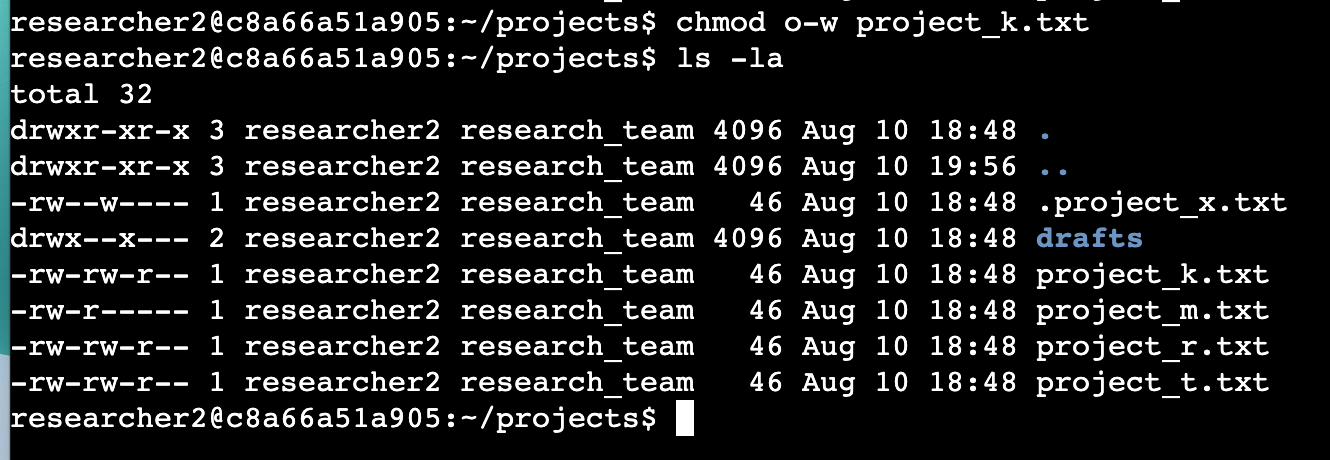
**--drwxrw-r-x**

* **The d represents that the content is a folder/directory.**
* **rwx (2nd – 4th letters) indicates that the User owner (u) has all read, write and execute permissions.**
* **rw- (5th -7th letters) indicates that the Group owners have read and write but not execute permissions.**
* **r-x (8th – 10th) indicates that the Other owner has only read and execute permissions but not write**

## Change file permissions

*The organization does not allow other to have write access to any files. Based on the permissions established in Step 3, identify which file needs to have its permissions modified. Use a Linux command to modify these permissions.*

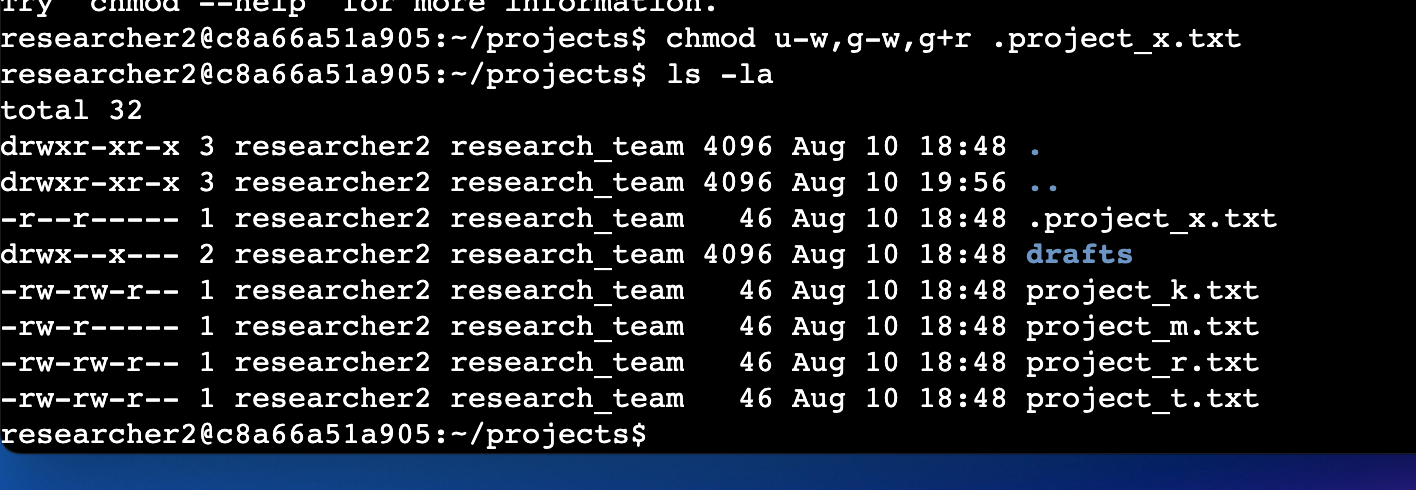
Presently, Other has write (w) permission on project\_k.txt. To change this, the file must the modified to remove the ‘w’ on position 9th using **Chmod** command.



## Change file permissions on a hidden file

The research team has archived .project\_x.txt, which is why it’s a hidden file. This file should not have write permissions for anyone, but the user and group should be able to read the file. Use a Linux command to assign .project\_x.txt the appropriate authorization.

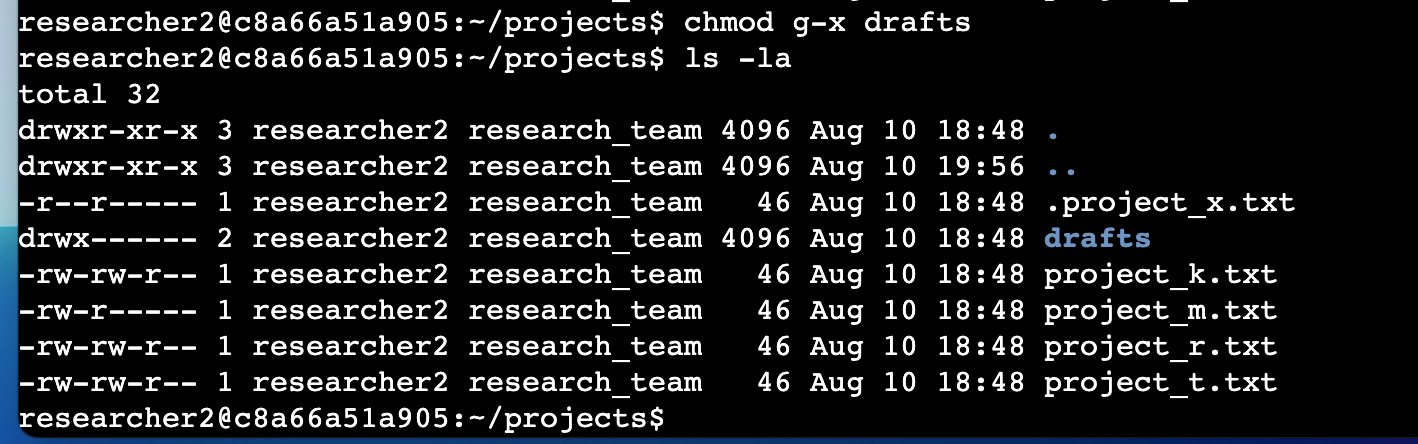
* Presently both User and Group can write on Project\_x.txt. The ‘w’ in both 3rd and 6th positions will have to be removed while we give the Group read permission.



## Change directory permissions

*The files and directories in the projects directory belong to the* **researcher2** *user. Only* **researcher2** *should be allowed to access the* **drafts** *directory and its contents. Use a Linux command to modify the permissions accordingly.*

* Presently, Group owners have execute permision on the draft folder. To achieve exclusive use to User owner, the ‘x’ persmision must be removed.



## Summary

With different combinations of read, write, and execute, different classes of file/directory owners can receive assorted user permissions, access, and control to resources needed to just efficiently do their jobs. Similarly, security analysts can effectively maintain a posture of least privilege in the permission given out to all users.