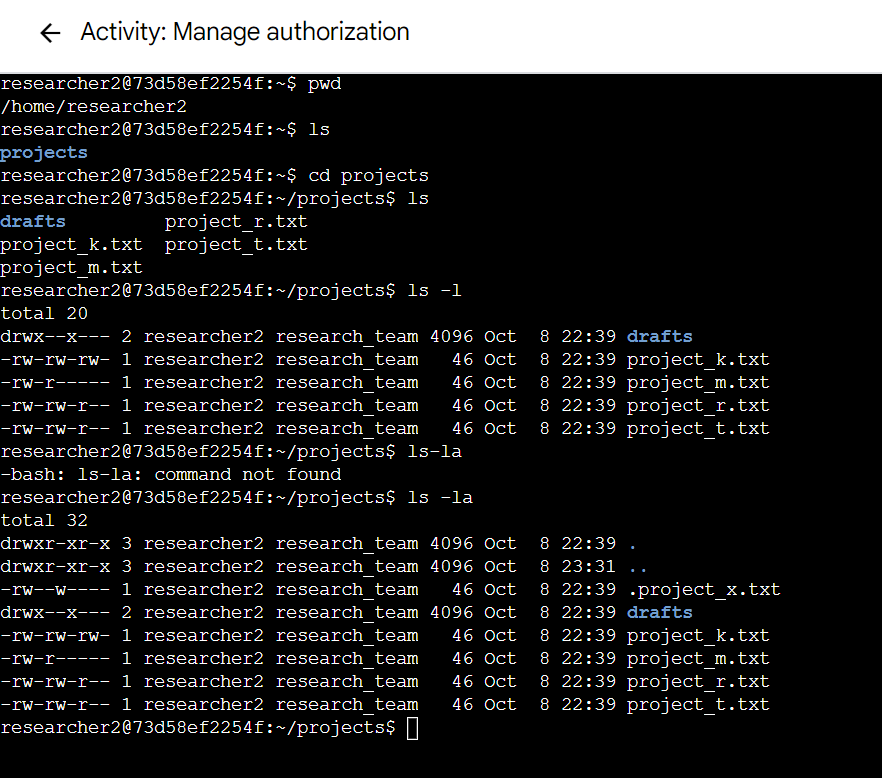
# File permissions in Linux

## Project description

This project entails managing and securing file permissions on a Linux system to ensure only authorized users have appropriate access. Including examining and modifying permissions to prevent unauthorized access and ensure that users can only interact with files and directories as permitted by their role within the organization.

## Check file and directory details

To review and document the details of files within the /home/researcher2/projects directory, begin by navigating to this directory using the command cd /home/researcher2/projects. Once positioned within the directory, execute the command ls -la to list all contents, including hidden files, along with their detailed attributes. This output will display the permissions, link count, owner, group, size, modification date, and names of each file and directory. This comprehensive listing helps in verifying the current state of file permissions and ownership, ensuring that they align with organizational security policies.



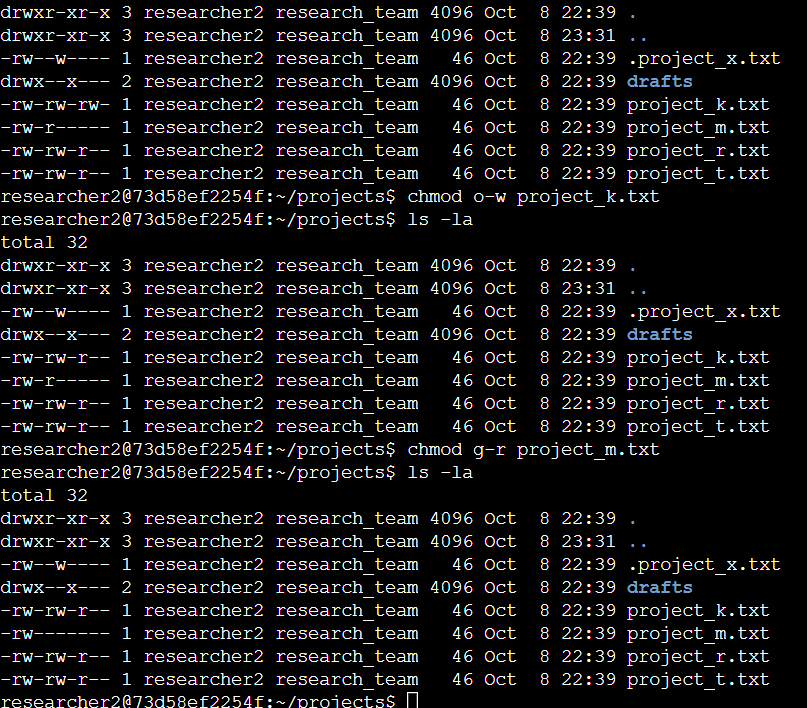
## Describe the permissions string

In Linux, the permissions string is represented by 10 characters. The first character denotes the type of file (e.g., - for a regular file, d for directory). The next nine characters are grouped in threes, representing the permissions for the owner, group, and others respectively (rwxr-xr-- where r stands for read, w for write, and x for execute).

## Change file permissions

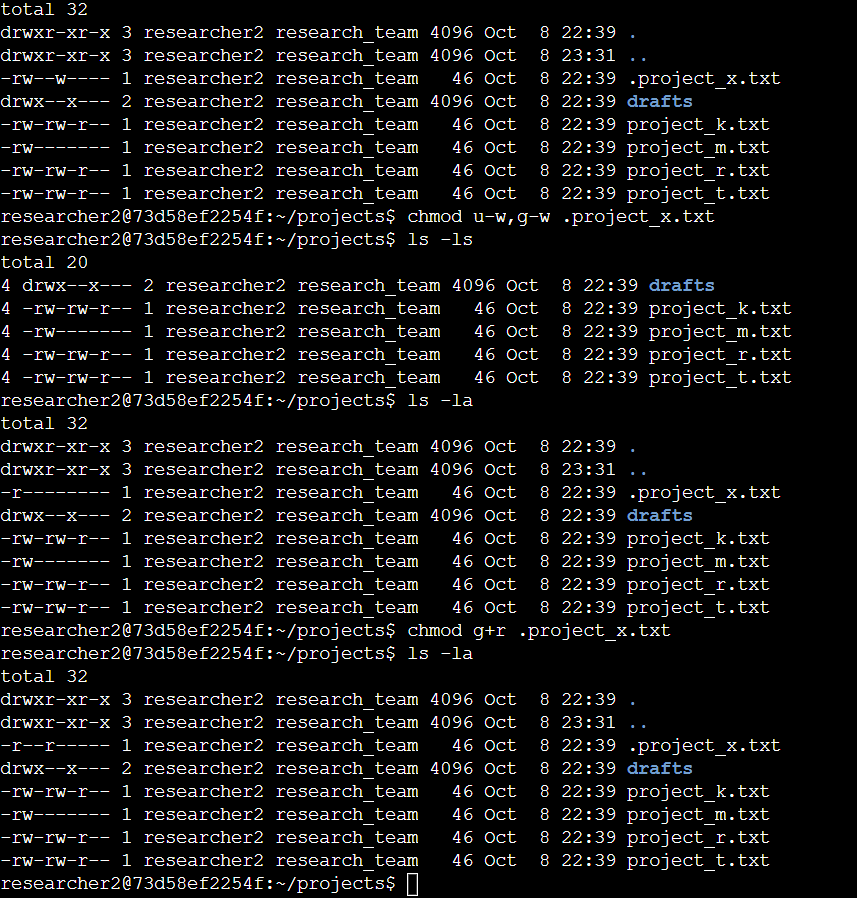
It was determined that the file project\_k.txt incorrectly allowed write permissions for 'other' users, which posed a security risk. To address this issue and ensure tighter security controls, the command chmod o-w project\_k.txt was executed. This command modifies the file permissions of project\_k.txt, specifically removing the write permission for users other than the owner and group, effectively restricting unauthorized modifications.

Furthermore, it was found that project\_m.txt, a file meant to be highly restricted, had overly permissive group permissions. To correct this and secure the file against unauthorized group access, the command chmod g-rw project\_m.txt was used to remove both read and write permissions for the group, ensuring that only the owner retains the ability to manipulate the file. This action aligns the file’s permissions with the stringent security requirements necessary for sensitive files in the organization.



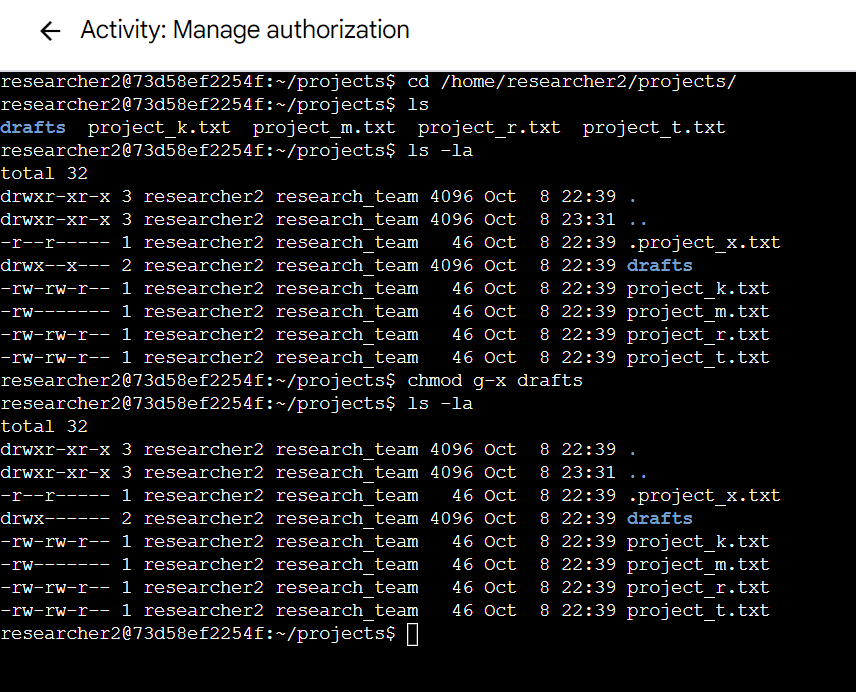
## Change file permissions on a hidden file

In addressing the security requirements for the hidden file .project\_x.txt, the first step involves verifying its current permissions to ensure that the file is protected against unauthorized writing while maintaining readability for the user and group. This check can be performed by executing the command ls -l .project\_x.txt within the appropriate directory. Based on the outcome that requires adjustment, the next action is to modify the file permissions so that both the user and the group can read but not modify the file. This can be achieved by running the command chmod 440 .project\_x.txt. This sets the permissions so that the owner and the group have read-only access, while all others have no permissions, thereby aligning the file’s security settings with the organizational policies on sensitive, archived information.



## Change directory permissions

For the task of securing the /home/researcher2/projects/drafts directory, it is necessary to first inspect the current group permissions and then modify them to restrict access exclusively to the researcher2 user. Starting within the projects directory, the command ls -ld drafts can be used to display the existing permissions for the drafts subdirectory. To ensure that only researcher2 can access this directory, the next step involves revoking the execute permission for the group, making the directory inaccessible to other group members. This is accomplished by executing the command chmod g-x drafts, which alters the permissions such that only the owner, researcher2, retains the execute permission, effectively securing the directory from unauthorized group access. This method ensures that sensitive draft materials are protected by limiting directory traversal privileges to the designated user only.



## Summary

To adjust the permissions of the /home/researcher2/projects/drafts directory to ensure exclusive access for the researcher2 user, begin by inspecting the current group permissions with the command ls -ld drafts while situated in the projects directory. After evaluating the permissions, execute chmod g-x drafts to remove execute permissions for the group. This change restricts access to the drafts directory, preventing group members from entering or listing its contents, thereby securing sensitive data to be accessible solely by the user researcher2. This approach effectively safeguards the directory against unauthorized group access.