# File permissions in Linux

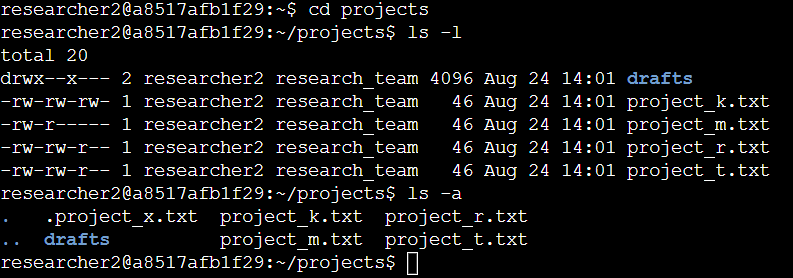
## Project description

I am a security professional at a large organization, primarily working with the research team. Part of my job is to ensure that users on this team have the appropriate permissions, which helps keep our system secure.

My task involves examining existing permissions on the file system to determine if they match the authorization that should be given. If they do not match, I need to modify the permissions to authorize the appropriate users and remove any unauthorized access.

## Check file and directory details

First, I listed the contents and permissions to the projects directory, which I used the ls -l command. I then listed the contents and permissions to any hidden files and subdirectories that exist, which I used the ls -a command. From the very beginning I could have used the ls -la command to show the contents and permissions for all available and hidden files and subdirectories.

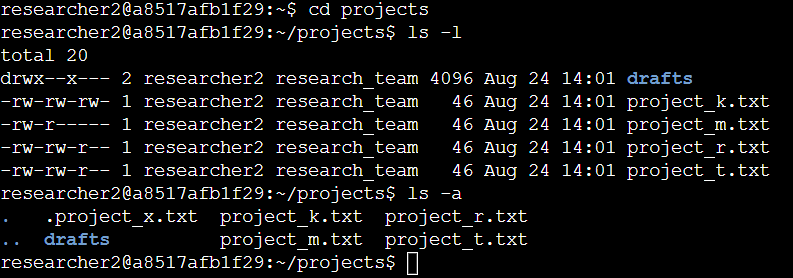




## Describe the permissions string

The permissions string is represented with a 10-character string. The first character defines whether the permission is for a (d) directory or a (-) for a file. The next 3 characters defines the permissions for the owner type user, which is represented by (r) read, (w) write, (x) execute or

(-) indicating that permission is not granted. This is the same for the next 3 characters and the last 3 characters, but for the owner type group and other.

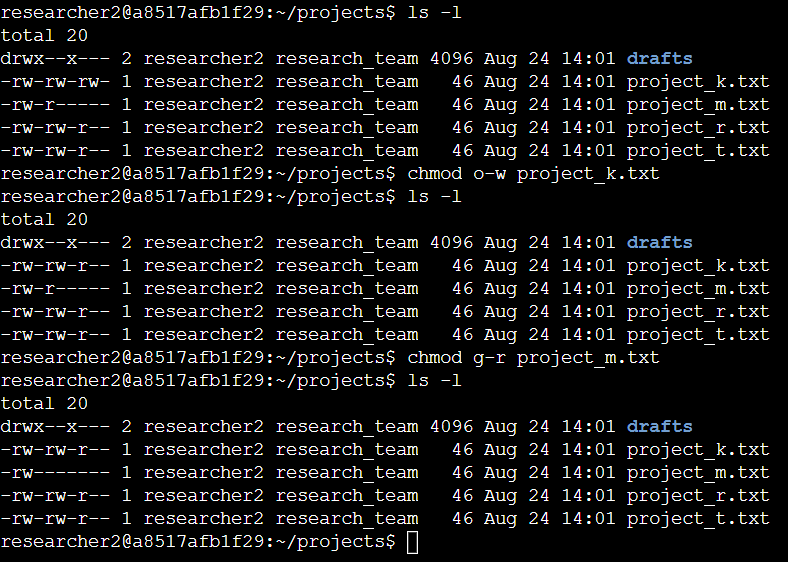




## Change file permissions

The organization does not allow for other to have writing permissions so I used the

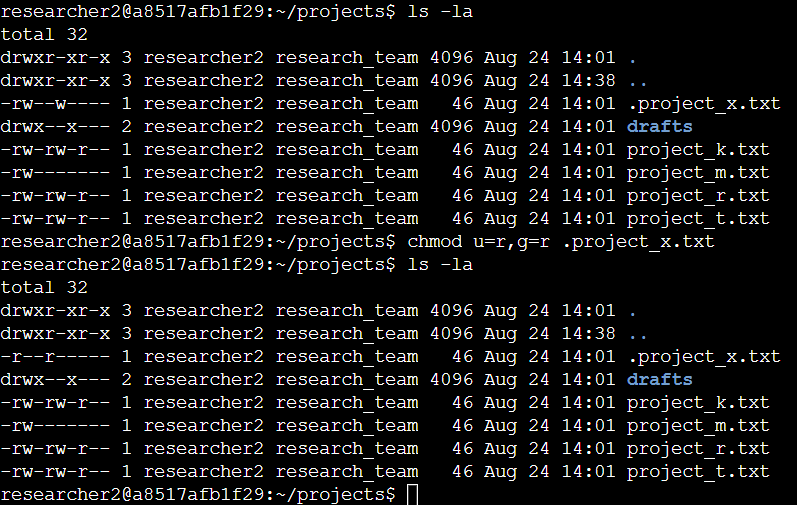
chmod o-w project\_k.txt command to take away the write permission for owner type other on the file project\_k.txt.





## Change file permissions on a hidden file

The research team has archived hidden file project\_x.txt and should not allow anyone to have write permissions for it, but to only allow the user and group to read it. To do so I input the command chmod u=r,g=r .project\_x.txt . By using (=) it will remove the write permission to both the user and group, and replace it with only the read permission for the user and group.

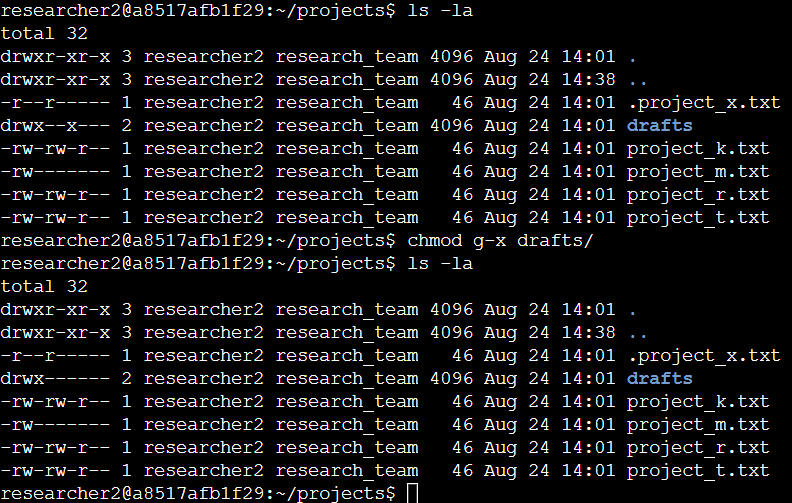




## Change directory permissions

The files and directory in the projects directory belong to researcher2 user and only researcher2 should be allowed to access the drafts directory and its contents. I used the command

chmod g-x drafts/ to take away the permission for owner type group to execute files in drafts directory. This makes it so reasercher2 is the only one able to access the directory drafts and access its contents.





## Summary

I identified several files and directories within the organization that had improper permissions. I meticulously reviewed and adjusted these permissions, ensuring that only authorized personnel have access. By implementing these changes, we have significantly reduced potential security risks, enhancing our overall data protection strategy.