# File permissions in Linux

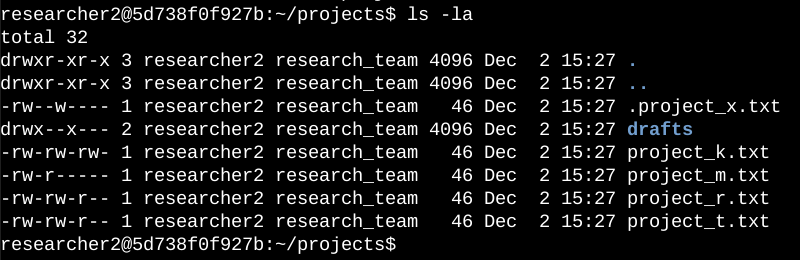
## Project description

In this project, I examined and managed file permissions within a Linux environment as part of my role as a security professional in a large organization. My primary responsibility was to ensure that users on the research team had appropriate access permissions to maintain system security. I utilized various Linux commands to check and modify file permissions, ensuring compliance with organizational policies.

## Check file and directory details

ls -la

* Explanation: This command lists all files and directories, including hidden ones, along with their permissions.



## Describe the permissions string

total 20

drwx- -x- - -2 researcher2 research\_team 4096 Oct 23 18:40 drafts

-rw-rw-rw - 1 researcher2 research\_team 46 Oct 23 18:40 project\_k.txt

-rw- - - - - - 1 researcher2 research\_team 46 Oct 23 18:40 project\_m.txt

-rw-rw -r -- 1 researcher2 research\_team 46 Oct 23 18:40 project\_r.txt

-rw-rw- r- - 1 researcher2 research\_team 46 Oct 23 18:40 project\_t.txt

## Change file permissions

chmod o-w project\_k.txt



## Change file permissions on a hidden file

chmod ug-w .project\_k.txt



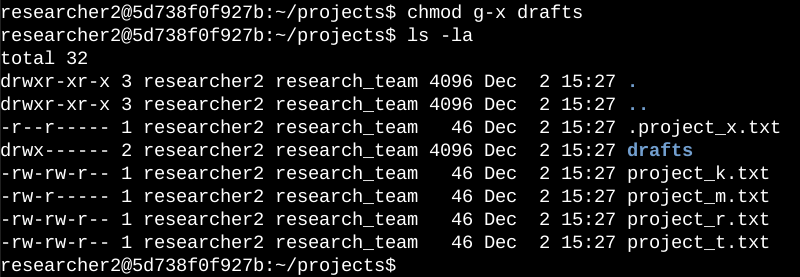
## 

## 

## 

## Change directory permissions

chmod g-rx project\_k.txt



## Summary

During the course of this activity, I employed a range of Linux commands to undertake effective file permissions management. By conducting a thorough review of current permissions through the utilization of the 'ls -la' command, I was able to pinpoint specific files necessitating modifications, such as 'project\_k.txt,' which required alterations to curtail unauthorized write access. Furthermore, I ensured that concealed files, such as '.project\_x.txt,' possessed suitable read permissions while simultaneously eliminating write access for all users. In conclusion, I adjusted the directory permissions associated with 'drafts' to limit access exclusively to the owner, thereby reinforcing our organization's established security protocols.