# File permissions in Linux

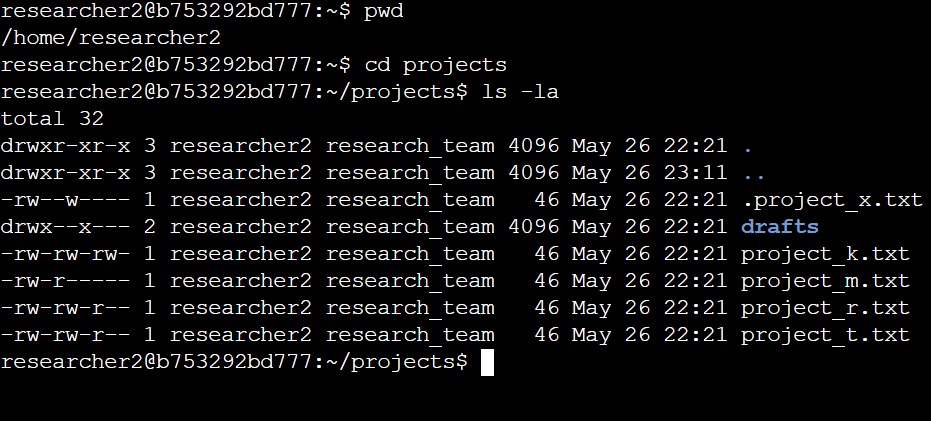
## Project description

In this project, I used Linux commands to check and manage file and directory permissions. I verified current permissions of files, including hidden files, and modified them to ensure proper security by restricting or granting read, write, or execute permissions to users, groups, and others.

## Check file and directory details

The command used to check file and directory details, including hidden files

ls -la



## Describe the permissions string

A cadeia de 10 caracteres mostra o **tipo do arquivo** e as **permissões de acesso** que ele tem para três tipos de usuários: **dono (user), grupo (group) e outros (others)**.

Por exemplo, na cadeia:  
 **-r--r-----**

* O **primeiro caractere** indica o **tipo do arquivo**:
  + Se for um arquivo comum, aparece **-**.
  + Se for um diretório, aparece **d**.
  + Se for um link, aparece **l**.
* Os **três próximos caracteres (2º ao 4º)** são as permissões do **dono do arquivo (user)**:
  + **r--** significa que o dono **pode ler**, mas **não pode escrever nem executar**.
* Os **três seguintes (5º ao 7º)** são as permissões do **grupo (group)**:
  + **r--** significa que o grupo também **pode ler**, mas **não pode escrever nem executar**.
* Os **três últimos (8º ao 10º)** são as permissões de **outros (others)**, que são todos os outros usuários do sistema:
  + **---** significa que **não têm nenhuma permissão** (não podem ler, escrever ou executar).

Essa cadeia serve para definir exatamente **quem pode acessar, alterar ou executar o arquivo**, garantindo controle e segurança no Linux.

## Change file permissions

O arquivo **project\_k.txt** estava com permissões incorretas (**rw-rw-rw-**), permitindo que tanto o grupo quanto outros usuários pudessem escrever no arquivo. Isso não é permitido pela política de segurança da organização, que não permite acesso de gravação para ninguém além do proprietário do arquivo.

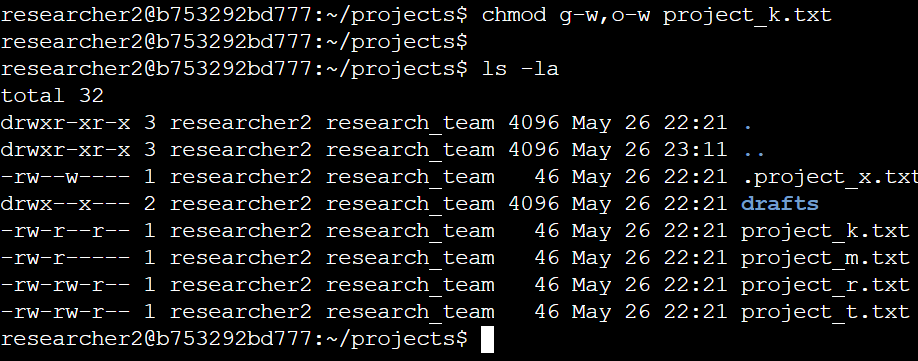
Para corrigir, utilizei o seguinte comando no terminal do Linux:

chmod g-w,o-w project\_k.txt

Este comando remove a permissão de **escrita (w)** do **grupo (g)** e de **outros (o)**, mantendo apenas a permissão de **leitura** para eles.

Após executar o comando, usei o comando ls -la para verificar, e as permissões ficaram assim:

-rw-r--r--

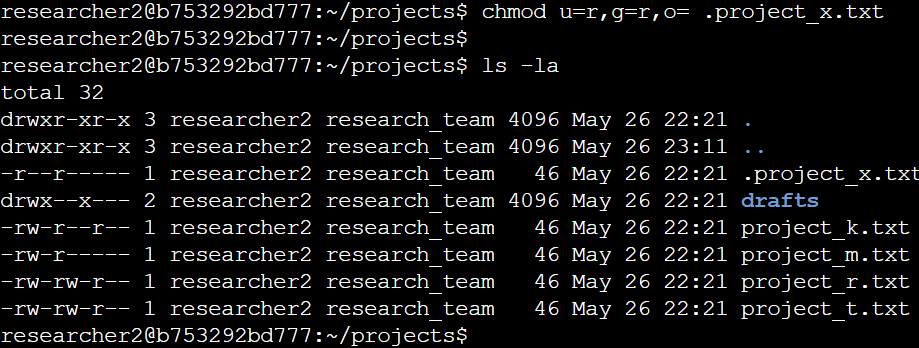
Agora, apenas o **proprietário** pode **ler e escrever** no arquivo. O **grupo** e os **outros usuários** possuem apenas **permissão de leitura**, o que atende aos requisitos da organização. 

## Change file permissions on a hidden file

O arquivo **.project\_x.txt** é um arquivo oculto, utilizado pela equipe de pesquisa como um arquivo arquivado. De acordo com a política de segurança da organização, **nenhum usuário deve ter permissão de gravação nesse arquivo**, mas o **usuário (owner)** e o **grupo (group)** devem ter permissão de **leitura**.

Para configurar corretamente essas permissões, utilizei o seguinte comando no terminal do Linux:

chmod u=r,g=r,o= .project\_x.txt

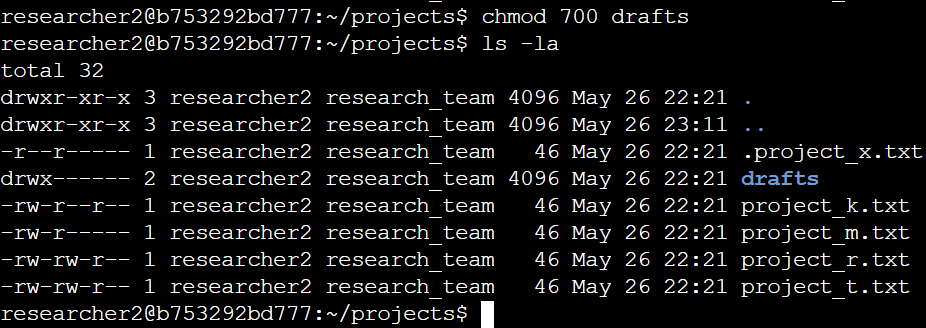


## Change directory permissions

O diretório **drafts** deve ser acessível **apenas pelo usuário researcher2**, e nenhum outro usuário (nem do grupo, nem others) deve ter acesso ao conteúdo desse diretório.

Para aplicar essa configuração de segurança, utilizei o seguinte comando no terminal do Linux:

chmod 700 drafts



## Summary

Durante o projeto, analisei as permissões de diversos arquivos e diretórios no sistema, identifiquei permissões incorretas e corrigi todas as que não estavam de acordo com a política de segurança. Configurei arquivos sensíveis, como .project\_x.txt, para que não tivessem permissão de gravação, mantendo acesso restrito apenas para leitura do usuário e do grupo. Além disso, apliquei restrições no diretório drafts para que somente o usuário proprietário tivesse acesso. Este processo garantiu que os dados da equipe de pesquisa fossem devidamente protegidos, seguindo boas práticas de segurança no Linux.