### **Permissões de arquivo no Linux**

#### **Descrição do projeto**

Neste projeto, demonstro como usar comandos do Linux para verificar, interpretar e modificar permissões de arquivos e diretórios. Isso é fundamental para garantir a segurança do sistema, permitindo apenas o acesso apropriado por usuários e grupos autorizados.

#### **Verificar detalhes de arquivos e diretórios**

Para verificar os detalhes e permissões dos arquivos e diretórios (inclusive arquivos ocultos), utilizei o seguinte comando:

ls -la /home/researcher2/projects

Este comando lista todos os arquivos e subdiretórios, mostrando detalhes como permissões, dono, grupo e nome do arquivo.

#### **Descrever a cadeia de permissões**

Exemplo de cadeia de permissões:

-rw-rw-r--

Significado:

* O primeiro caractere indica o tipo ( - = arquivo comum, d = diretório, l = link simbólico).
* Os próximos três (rw-) indicam as permissões do **usuário** (read, write).
* Os próximos três (rw-) indicam as permissões do **grupo**.
* Os últimos três (r--) indicam as permissões de **outros usuários**.

Neste exemplo, o **usuário** e o **grupo** têm permissões de leitura e escrita, enquanto **outros** podem apenas ler.

#### **Alterar permissões de arquivo**

Arquivo com permissões indevidas:  
 project\_k.txt permite escrita para outros usuários.

Para remover a permissão de escrita de "others", usei o seguinte comando:

chmod o-w /home/researcher2/projects/project\_k.txt

Esse comando garante que apenas usuários autorizados possam modificar o arquivo.

#### **Alterar permissões de um arquivo oculto**

O arquivo oculto .project\_x.txt precisa ser restrito. O objetivo é permitir apenas **leitura** para o **usuário** e o **grupo**, e **nenhum acesso** para outros.

Comando utilizado:

chmod 440 /home/researcher2/projects/.project\_x.txt

A cadeia de permissões resultante será:

-r--r-----

#### **Alterar permissões de diretório**

Para restringir completamente o acesso ao diretório drafts somente ao usuário researcher2, executei o comando:

chmod 700 /home/researcher2/projects/drafts

Isso garante que **somente o proprietário** pode ler, escrever e executar (acessar) o diretório.

#### **Resumo**

Neste exercício, usei comandos do Linux para examinar e modificar permissões de arquivos e diretórios. Verifiquei permissões com ls -la, interpretei as cadeias de 10 caracteres, corrigi permissões indevidas com chmod, incluindo arquivos ocultos, e apliquei as configurações necessárias para proteger um diretório sensível. Esse processo é essencial para manter a segurança e o controle de acesso em sistemas baseados em Linux.