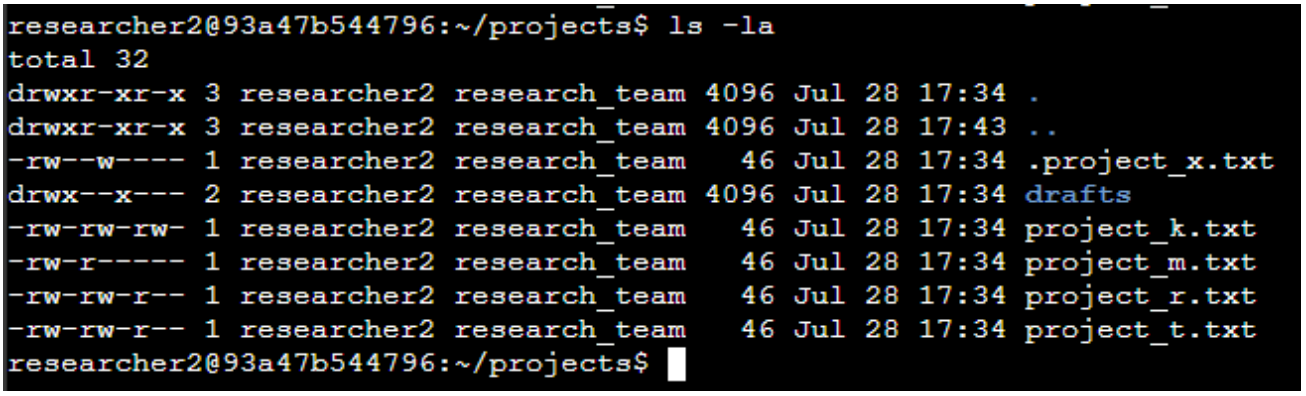
Permissões de Arquivo no Linux

Descrição do projeto

Como parte de uma iniciativa de segurança para uma equipe de pesquisa, foi necessário auditar e atualizar as permissões de arquivos e diretórios no diretório `projects`. As permissões existentes não refletiam o nível de autorização adequado, representando um risco de segurança. Para mitigar esse risco, realizei uma análise e reconfiguração das permissões para garantir que apenas usuários autorizados tivessem o acesso apropriado, fortalecendo a segurança do sistema.

Verificando os detalhes do arquivo e do diretório

O primeiro passo foi inspecionar as permissões atuais no diretório *projects*. Utilizei o comando *ls -la* para listar todos os arquivos, incluindo os ocultos, e exibir seus detalhes de permissão.



A saída revelou um diretório(`drafts`), um arquivo oculto (`.project_x.txt`) e cinco outros arquivos de projeto. A primeira coluna em cada linha representa a cadeia de 10 caracteres que define as permissões para cada item.

Descrição da sequência de permissões

A cadeia de 10 caracteres de permissões é fundamental para o controle de acesso no Linux. Por exemplo, a permissão `drwxr-xr-x` pode ser decomposta da seguinte forma:

> **1º caractere (`d`):** Indica o tipo de arquivo. `d` para diretório, `-` para um arquivo regular.
> **2º ao 4º caracteres (`rwx`):** Permissões do **usuário** (dono). `r` (leitura), `w`

(escrita) e `x` (execução).

5º ao 7º caracteres (`r-x`): Permissões do **grupo**. O grupo tem permissão de leitura (`r`) e execução (`x`), mas não de escrita (`-`).

8º ao 10º caracteres (`r-x`): Permissões para **outros** (todos os demais usuários). Assim como o grupo, outros usuários podem ler e executar, mas não escrever.

Alteração das permissões de arquivo

A política da organização determina que a permissão de escrita (`w`) deve ser removida para a categoria "outros" em todos os arquivos, para evitar modificações não autorizadas. O arquivo `project_k.txt` violava essa regra. O comando `chmod` foi usado para corrigir isso.

```
-rw-rw-rw- 1 researcher2 research_team   46 Jul 28 17:34 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 28 17:34 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_t.txt
researcher2@93a47b544796:~/projects$ chmod o-w project_k.txt
researcher2@93a47b544796:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Jul 28 17:34 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 28 17:34 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_t.txt
researcher2@93a47b544796:~/projects$
```

O comando `chmod o-w` remove (`-`) a permissão de escrita (`w`) para outros (`o`) no arquivo `project_k.txt` , alinhando-o com a política de segurança.

Alteração de permissões de arquivo em um arquivo oculto

O arquivo `.project_x.txt` é um arquivo de projeto arquivado e oculto. A política exige que ninguém tenha permissão de escrita, e que tanto o usuário quanto o grupo tenha apenas permissão de leitura. As permissões foram ajustadas com o seguinte comando:

```
drwxr-xr-x 3 researcher2 research team 4096 Jul 28 17:43 ..
-rw--w---- 1 researcher2 research team   46 Jul 28 17:34 .project x.txt
drwx--x--- 2 researcher2 research_team 4096 Jul 28 17:34 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 28 17:34 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_t.txt
researcher2@93a47b544796:~/projects$ chmod u=r,g=r .project_x.txt
researcher2@93a47b544796:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jul 28 17:34 .
drwxr-xr-x 3 researcher2 research team 4096 Jul 28 17:43 ..
-r--r----- 1 researcher2 research_team   46 Jul 28 17:34 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jul 28 17:34 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 28 17:34 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_t.txt
researcher2@93a47b544796:~/projects$
```

O comando `chmod u=r,g=r` define explicitamente as permissões: o usuário (`u`) pode apenas ler (`=r`), e o grupo (`g`) também pode apenas ler (`=r`). As permissões para outros já estavam ausentes, o que atende ao requisito.

Alterar permissões de diretório

O diretório `drafts` deve ser acessível apenas pelo usuário `researcher2` . Nenhuma outra pessoa, incluindo membros do `research_team` , deve ter permissão para listar seu conteúdo. Para isso, a permissão de execução (`x`) foi removida do grupo.

```
researcher2@93a47b544796:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research team 4096 Jul 28 17:34 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 28 17:34 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_t.txt
researcher2@93a47b544796:~/projects$ chmod g-x drafts/
researcher2@93a47b544796:~/projects$ ls -l
total 20
drwx------ 2 researcher2 research_team 4096 Jul 28 17:34 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 28 17:34 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 28 17:34 project_t.txt
researcher2@93a47b544796:~/projects$
```

O comando `chmod g-x` remove (`-`) a permissão de execução (`x`) para o grupo (`g`) no diretório `drafts` . Sem a permissão de execução, os membros do grupo não podem acessar o diretório.

Resumo

Neste projeto, realizei uma auditoria de segurança das permissões de arquivos no diretório `projects`. Utilizando os comandos `ls` para inspeção e `chmod` para modificação, ajustei sistematicamente as permissões em arquivos regulares, arquivos ocultos e diretórios para alinhá-los com as políticas de segurança da organização. Essas ações reforçaram a integridade e a confidencialidade dos dados da equipe de pesquisa, demonstrando a aplicação prática do controle de acesso no Linux para proteger informações sensíveis.