Gerenciamento de Permissões de Arquivos no Linux

Introdução

Como profissional de segurança da informação, uma das tarefas fundamentais é garantir que os arquivos e diretórios do sistema estejam protegidos contra acessos não autorizados. Para isso, é necessário entender e controlar as permissões atribuídas a cada arquivo, assegurando que apenas os usuários apropriados possam ler, modificar ou executar esses arquivos. Neste relatório, descrevo o processo de verificação e ajuste das permissões em um diretório de projetos, garantindo conformidade com as políticas de segurança da organização.

Desenvolvimento

1. Navegando até o diretório alvo

Para começar, utilizei o comando `cd` para acessar o diretório onde os arquivos estão armazenados:

cd /home/researcher2/projects

2. Listando arquivos e suas permissões

Em seguida, listei todos os arquivos e diretórios, incluindo os ocultos, com detalhes das permissões usando:

ls -la

A saída mostrou uma lista detalhada, incluindo uma coluna com a cadeia de 10 caracteres que representa as permissões, o proprietário e o grupo de cada arquivo.

3. Interpretando a cadeia de permissões

Cada linha apresenta uma cadeia de 10 caracteres, onde:

- O primeiro caractere indica o tipo (diretório ou arquivo).

- Os três caracteres seguintes indicam permissões do proprietário (leitura, escrita, execução).
- Os próximos três caracteres indicam permissões do grupo.
- Os últimos três caracteres indicam permissões dos outros usuários.

Por exemplo, a permissão `-rw-rw-r--` para o arquivo `project_t.txt` indica que o usuário e o grupo têm permissão para leitura e escrita, enquanto outros usuários têm somente permissão de leitura.

4. Ajustando permissões incorretas

Foi identificado que alguns arquivos permitiam escrita para usuários não autorizados (outros), o que viola a política de segurança. Para remover essa permissão, utilizei o comando:

chmod o-w project_k.txt

Além disso, para o arquivo oculto `.project_x.txt`, que deve ser somente leitura para usuário e grupo e sem permissões para outros, executei:

chmod 440 .project_x.txt

No caso do diretório `drafts`, apenas o usuário proprietário deve ter permissão de execução para acesso, então ajustei:

chmod 700 drafts

5. Verificando as alterações

Após cada ajuste, utilizei novamente:

ls -la

para confirmar que as permissões haviam sido atualizadas corretamente, garantindo que os acessos indevidos foram removidos.

Conclusão

O processo de gerenciamento de permissões foi fundamental para reforçar a segurança no sistema de arquivos da equipe de pesquisa. Compreender e aplicar corretamente as permissões utilizando comandos como `ls` e `chmod` permite controlar o acesso aos arquivos, prevenindo modificações ou acessos não autorizados. Esta prática contribui para manter a integridade e confidencialidade dos dados críticos da organização.
