Atividade Prática : CHMOD - Gerenciamento de Permissões e Ambiente de Servidor

Objetivo

Aplicar o comando **chmod** em diferentes cenários de um ambiente de servidor (configuração, log e scripts) para garantir a segurança e a funcionalidade do sistema, a notação numérica.

Materiais por Dupla

- 1 Computador com **Linux Mint/Ubuntu** instalado.
- Acesso ao terminal (Ctrl + Alt + T).

Fase 1: Preparação do Ambiente (Simulação de Servidor)

Criar a estrutura básica de um servidor no diretório **/tmp** para simular um ambiente limpo.

1. **Criar a Estrutura:** Crie o diretório principal e subdiretórios essenciais.

```
cd /tmp

mkdir Servidor_Web

cd Servidor_Web

mkdir logs scripts publico
```

2. **Criar Arquivos Chave:** Crie os arquivos dentro dos diretórios.

```
# Arquivo no diretório principal

touch configuracao.conf

# Arquivos nos subdiretórios

touch logs/acesso.log

touch publico/index.html

touch scripts/rotina_diaria.sh
```

3. **Adicionar Conteúdo ao Script:** Use o nano para inserir o seguinte código no arquivo scripts/rotina_diaria.sh.

Exemplo de Script (Cria um log simples):

```
#!/bin/bash

# Script de Backup
```

echo "----------" >> /tmp/Servidor_Web/logs/rotina.log

echo "Rotina executada em: $(date)" >> /tmp/Servidor_Web/logs/rotina.log

echo "Verificando o estado do serviço..." >> /tmp/Servidor_Web/logs/rotina.log

 # Simulando a execução de um comando que requer permissão

/bin/hostname >> /tmp/Servidor_Web/logs/rotina.log 2>&1

echo "----------" >> /tmp/Servidor_Web/logs/rotina.log

Dica: Salve (Ctrl+O) e Saia (Ctrl+X) do nano.

Fase 2: Aplicação e Teste do CHMOD (Notação Numérica)

. Utilize o chmod para aplicar as permissões necessárias e use o comando ls -l após cada passo para verificar a alteração. **Lembre-se de sempre executar o comando a partir do diretório Servidor_Web**.

Cenário 1: Arquivos de Configuração (Máxima Segurança)

O arquivo *configuracao.conf* contém senhas de acesso ao banco de dados e **não** deve ser lido por ninguém além do administrador (dono)

1. **Defina a Permissão 600 (Somente Dono):**
    - Dono (U): Ler, Escrever.
    - Grupo (G): Nenhuma.
    - Outros (O): Nenhuma.

chmod 600 configuracao.conf

Verifique: ls -l configuracao.conf

Cenário 2: Logs de Acesso (Apenas Leitura)

O arquivo *logs/acesso.log* deve ser **legível** para todos (para análise), mas **apenas** o sistema (e o Dono) podem escrever novos registros

Defina a Permissão 644 (Leitura Comum):

- Dono (U): Ler, Escrever.
- Grupo (G): Apenas Ler.
- Outros (O): Apenas Ler.

chmod 644 logs/acesso.log

Verifique: ls -l logs/acesso.log

Cenário 3: O Script Executável (Teste de x - Execução)

O script *scripts/rotina_diaria.sh* é um programa de rotina e **precisa** de permissão de execução para rodar.

1. **Defina a Permissão 744 (Execução e Leitura para Todos):**
   - Dono (U): Ler, Escrever, **Executar**.
   - Grupo (G): Ler.
   - Outros (O): Ler.

chmod 744 scripts/rotina_diaria.sh

Verifique: ls -l scripts/rotina_diaria.sh ((O arquivo deve ter o **x** na permissão e, dependendo do terminal, mudar de cor).).

2. **Teste de Execução:** Tente rodar o script no terminal:

scripts/rotina_diaria.sh

Verifique se o arquivo logs/rotina.log foi criado e contém o log de execução.

Cenário 4: Diretório Público (Conteúdo Web)

O diretório público deve permitir que o servidor Web acesse e leia os arquivos, mas deve proibir que usuários comuns alterem a estrutura.

1. **Defina a Permissão 755 (Padrão de Diretório Web):**
   - Dono (U): Ler, Escrever, Executar.
   - Grupo (G): Ler, Executar.
   - Outros (O): Ler, Executar.

chmod 755 publico

Verifique: ls -ld público (Use a opção -d para ver a permissão do diretório, e não do conteúdo).

Fase 3: Relatório e Conclusão

A dupla deve documentar os comandos e a lógica.

1. **Tabela de Permissões:** Crie uma tabela com os comandos **chmod** utilizados e o resultado da verificação (ls -l).

Arquivo	**Permissão Numérica**	**Permissão Letras (rwx)**	**Justificativa de Segurança**
configuracao.conf	600	-rw-------	Máxima restrição: só o dono pode ler/escrever.
logs/acesso.log	644	_	_
scripts/rotina_diaria.sh	744	_	_
publico/	755	_	_

2. **Reflexão final :** Explique qual permissão faltaria no scripts/rotina_diaria.sh se a permissão fosse 644 e por que o script falharia.