Curitiba, 04, maio de 2023.

**Disciplina**: Segurança de Serviços e Servidores

**Professor:** Jhonatan Geremias

**Estudante:**

**Atividade**

**Permissões Especiais Linux**

# **Descrição da Atividade:**

Nesta atividade iremos explorar o mecanismo de controle de acesso em arquivos no Linux, vamos apresentar as permissões básicas e as permissões especiais. Como pré-requisito para esta atividade, o estudante deve ter acesso a uma máquina com o sistema operacional Linux, sugiro que utilize uma máquina virtual.

**Especificação:**

Esta atividade consiste na leitura do material de apoio e na realização da atividade prática. A atividade está estruturada em duas etapas, a primeira etapa aborda as permissões básicas no Linux, na sequência o estudo é direcionado as permissões especiais. O aluno deve ler o material de apoio para fornecer suporte a realização do exercício prático que será realizado no ambiente Linux. Ao final da realização de cada uma das etapas o aluno deve coletar um *printscreen* contendo todos os comandos solicitados. Para auxiliar o estudante no desenvolvimento da atividade está sendo disponibilizado dois links abaixo que poderão ser úteis.

[Guia Foca - Linux](https://www.guiafoca.org/#download)

[Documentação Ubuntu](https://help.ubuntu.com/)

**Material de Apoio – Permissões Básicas Linux**

As permissões básicas no Linux são: leitura, escrita e execução. Tais permissões são concedidas aos usuários considerando três blocos, proprietário, grupo e outros. As permissões são definidas na figura abaixo:



Para alterar as permissões básicas no Linux utilizamos o comando chmod, este comando pode ser utilizado de forma nominal ou por representação binária. A proposta desta atividade consiste em demostrar como definir as permissões no Linux de forma nominal. Na forma nominal, modificamos a permissão atual utilizando uma máscara que permite alterar a permissão do objeto. Segue a sintaxe do comando chmod:

chmod <máscara> <objeto>

Para alterar as permissões de um objeto (arquivo ou diretório) é necessário ter privilégios sobre ele. Assim, para obter os privilégios de superusuário podemos utilizar o comando “sudo” antecedendo o comando que queremos executar, este comando vai fornecer os privilégios necessários, será solicitado que você forneça a senha do usuário para elevar os privilégios.

sudo chmod <máscara> <objeto>

A máscara na representação nominal é sempre estruturada em três partes, respeitando sua ordem:

**1. Bloco de destino:** usuário (u), grupo (g), outros (o) e todos (a);

**2. Operação:** incluir (+) ou remover permissão (-);

**3. Permissão:** leitura (r), escrita (w) e execução (x).

Por exemplo para adicionar a permissão de execução para o usuário você deve combinar o bloco de destino, neste caso o usuário (u), operação (+) e permissão é execução (x), assim teremos a seguinte máscara u+x. Esta máscara deve ser utilizada com o comando chmod na sequência o objeto a ser alterado. O objeto corresponde ao arquivo ou diretório. Por exemplo, podemos alterar a permissão do arquivo arquivo1.txt, a permissão seria:

chmod u+x arquivo1.txt

Em contrapartida para remover a permissão de execução do usuário você realiza o mesmo procedimento, a única diferença é que será necessário utilizar o sinal de subtração (-) para remover a permissão, assim devemos executar o seguinte comando:

chmod u-x arquivo1.txt

Para adicionar a permissão de execução para o grupo o processo é mesmo, devemos alterar apenas o bloco de destino, neste caso o grupo corresponde a letra “g”.

chmod g+x arquivo1.txt

Para adicionar a permissão de execução para o outros, devemos alterar apenas o bloco de destino, neste caso outros corresponde a letra “o”.

chmod o+x arquivo1.txt

Para definir a permissão de leitura (r) e escrita (w) devemos seguir a mesma lógica. Por exemplo definir a permissão de leitura para o usuário:

chmod u+r arquivo1.txt

Ainda é possível atribuir a permissão para todos os blocos utilizando a letra “a” (all), neste sentido a permissão será aplicada para o usuário, grupo e outros. Por exemplo adicionar a permissão de execução para todos.

chmod a+x arquivo1.txt

Adicionalmente podemos combinar mais de um bloco de destino, ou mais de um tipo de permissão. Alternativamente ao invés de utilizar a letra “a” poderíamos combinar as três letras. Por exemplo adicionar a permissão de execução para o usuário, grupo e outros.

chmod ugo+x arquivo1.txt

Poderíamos definir a permissão apenas sobre o usuário (u) e o grupo (g).

chmod ug+x arquivo1.txt

Ainda definir mais de um tipo de permissão simultaneamente, por exemplo o usuário com a permissão de leitura (r) e escrita (w).

chmod u+rw arquivo1.txt

As permissões nominais podem ser atribuídas de única vez, devem ser separadas por virgula. Por exemplo adicionar a permissão de execução (x) para o usuário (u) e remover (-) a permissão de escrita (w) do grupo (g).

chmod u+x,g-w arquivo1.txt

As permissões podem ser aplicadas sobre os diretórios, você precisa adicionar a opção de recursividade (-R). Por exemplo, adicionar a permissão de escrita para o usuário no diretório “tsi\_pasta1”.

chmod -R u+w tsi\_pasta1

**Atividade Etapa 1 – Permissões Linux Básicas**

1. Verifique qual o seu diretório corrente (pwd).
2. Acesse o diretório home do usuário. (cd ~)
3. Crie um diretório com o seu "nome".
4. Acesse o diretório criado anteriormente “nome”. Ex.: cd jhonatan
5. Crie dois arquivos “arquivo1.txt” e “arquivo2.txt”.
6. Liste os arquivos no diretório e verifique as permissões padrões.
7. Adicione a permissão de execução para o usuário e outros no arquivo arquivo1.txt.
8. Remova a permissão de escrita do grupo no arquivo arquivo1.txt.
9. Adicione a permissão de execução para o grupo no arquivo arquivo2.txt e remova a permissão de escrita do usuário utilizando uma única linha de comando (separar por virgula).
10. Crie o diretório tsi\_pasta1.
11. Remova a permissão de execução de todos no diretório tsi\_pasta1. (utilizar o “a” - todos).
12. Adicione a permissão de escrita do usuário, grupo e outros no diretório tsi\_pasta1. (utilizar a permissão “ugo” – usuário, grupo e outros).
13. Liste os arquivos e diretórios e verifique as permissões concedidas.
14. Efetue um *printscreen* contendo todos os comandos anteriores para compor seu relatório.

**Atenção**: No item 4, você deve criar a pasta como o seu nome pois será utilizado para correção. No item 14 é necessário que no *printscreen* os comandos estejam legíveis.

**Material de Apoio – Permissões Especiais Linux**

Podemos definir permissões adicionais para os arquivos e diretórios. Os três modelos especiais para controle de acesso são denominados Set User ID (SUID), *Set Group ID* (SGID) e *Sticky Bit* (*Sticky*).



As permissões especiais alteram o comportamento padrão do sistema operacional na manipulação dos arquivos e diretórios que possuem tais permissões.

A propriedade SUID permite ajustar o ID do usuário (*SetUID*), é aplicada apenas para arquivos executáveis não tendo qualquer efeito sob diretórios. Esta permissão de acesso só pode ser definida no campo de execução do proprietário do arquivo, atribuição realizada com a letra “s”. Tal funcionalidade proporciona a criação e utilização de programas privilegiados que podem usar arquivos que são normalmente inacessíveis a outros usuários.

chmod u+s arquivo2.txt

Alternativamente, a propriedade SGID é utilizada para ajustar o ID do grupo. Esta propriedade tem uma função bastante semelhante a propriedade SUID para arquivos executáveis, contudo esta propriedade tem um efeito especial quando aplicado sob diretórios. Esta permissão de acesso especial só pode ser definida no campo que habilita a execução para o grupo, atribuição realizada com a letra “s”.

chmod g+s tsi\_pasta

Adicionalmente, a propriedade *Sticky,* quando habilitada em arquivos executáveis faz com que o sistema mantenha uma imagem do programa em memória depois que o programa finalizar. Esta permissão de acesso especial é definida no campo que habilita a execução para outros usuários, atribuição realizada com a letra “t”.

chmod o+t arquivo2.txt

**Atividade Etapa 2 – Permissões Linux Especiais**

1. Verifique qual o seu diretório corrente (pwd).
2. Acesse o diretório home do usuário. (cd ~)
3. Acesse o diretório com o seu nome. Ex.: cd jhonatan
4. Crie o novamente o arquivo “arquivo3.txt”.
5. Crie o novamente o arquivo “arquivo4.txt”.
6. Crie o diretório “tsi\_pasta2”.
7. Liste os arquivos no diretório e verifique as permissões padrões.
8. Adicione a permissão *Set User ID* sobre o arquivo “arquivo3.txt”.
9. Adicione a permissão *Set Group ID* sobre o diretório “tsi\_pasta2”.
10. Adicione a permissão *Sticky Bit* sobre o arquivo “arquivo4.txt”.
11. Liste os arquivos e diretórios e verifique as permissões concedidas.
12. Efetue um *printscreen* contendo todos os comandos anteriores para compor seu relatório.

**Atenção:** No item 3, você deve acessar a pasta como o seu nome pois será utilizado para correção. No item 12 é necessário que no *printscreen* os comandos estejam legíveis.