

Laboratório – Autenticação, autorização e auditoria

Objetivos

- Em determinado cenário, selecione a devida autenticação, autorização ou auditoria de controle de acesso
- Instale e configure os controles de segurança ao gerenciar a auditoria com base nas melhores práticas

Parte 1: Como adicionar grupos, usuários e senhas em um sistema Linux

Parte 2: Verifique usuários, grupos e senhas

Parte 3: Uso de permissões simbólicas

Parte 4: Permissões absolutas

Histórico/Cenário

Você conduzirá as práticas de segurança de host com a linha de comando do Linux, executando as seguintes tarefas:

- Como adicionar grupos, usuários e senhas
- Verificação de grupos, usuários e senhas
- Configuração de permissões simbólicas
- Configuração de permissões absolutas

Recursos necessários

- Computador com Ubuntu 16.0.4 LTS instalado em uma máquina virtual VirtualBox ou VMware.

Parte 1: Como adicionar grupos, usuários e senhas em um sistema Linux

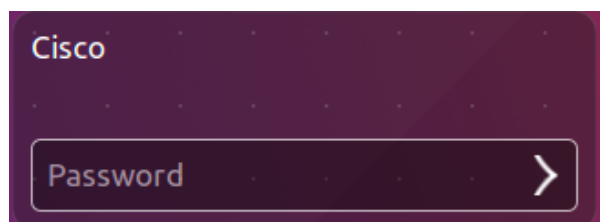
Nesta parte, você adicionará usuários, grupos e senhas à máquina de host local.

Passo 1: Abra uma janela de terminal no Ubuntu.

- Inicie uma sessão no Ubuntu usando as seguintes credenciais:

Usuário: **cisco**

Senha: **password**



- b. Clique no ícone de **terminal** para abrir um terminal.



Passo 2: Escale os privilégios para o nível do root, digitando o comando sudo su. Digite a senha password quando solicitado.

```
cisco@ubuntu:~$ sudo su
```

```
cisco@ubuntu:~$ sudo su  
[sudo] password for cisco:  
root@ubuntu:/home/cisco#
```

Passo 3: Adicione um novo grupo denominado HR, digitando o comando groupadd HR.

```
root@ubuntu:/home/cisco# groupadd HR
```

```
root@ubuntu:/home/cisco# groupadd HR  
root@ubuntu:/home/cisco#
```

Parte 2: Verifique os usuários, grupos e senhas

Passo 1: Verifique se o novo grupo foi adicionado à lista de arquivos de grupo, digitando cat /etc/group.

```
root@ubuntu:/home/cisco# cat /etc/group
```

```
root@ubuntu:/home/cisco# cat /etc/group  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:syslog,cisco  
Bob:x:1002:  
Eve:x:1003:  
Eric:x:1004:  
HR:x:1005:  
root@ubuntu:/home/cisco#
```

O novo grupo HR será adicionado na parte inferior do arquivo /etc/group com o ID de grupo 1005.

Passo 2: Adicione o novo usuário denominado jenny.

```
root@ubuntu:/home/cisco# adduser jenny
```

- Quando solicitada a nova senha, digite **lasocial**. Pressione **Enter**.
- Quando solicitada novamente, digite **lasocial**. Pressione **Enter**.
- Quando solicitado o nome completo, digite **jenny**. Pressione **Enter**.
- Para o restante das configurações, pressione **Enter** até quando a informação correta for solicitada.
- Digite **Y** para sim e pressione **Enter**.

```
root@ubuntu:/home/cisco# adduser jenny
Adding user `jenny' ...
Adding new group `jenny' (1006) ...
Adding new user `jenny' (1005) with group `jenny' ...
Creating home directory `/home/jenny' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for jenny
Enter the new value, or press ENTER for the default
  Full Name []: Jenny
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
```

Passo 3: Coloque o usuário jenny no grupo de HR.

```
root@ubuntu:/home/cisco# usermod -G HR jenny
```

```
root@ubuntu:/home/cisco# usermod -G HR jenny
root@ubuntu:/home/cisco#
```

Passo 4: Adicione outro novo usuário denominado joe.

```
root@ubuntu:/home/cisco# adduser joe
```

- Quando solicitada a nova senha, digite **tooth**. Pressione **Enter**.
- Quando solicitada novamente, digite **tooth**. Pressione **Enter**.
- Quando solicitado o nome completo, digite **joe**. Pressione **Enter**.
- Para o restante das configurações, pressione **Enter** até quando solicitado for a informação correta.

- e. Digite **Y** para sim e pressione **Enter**.

```
root@ubuntu:/home/cisco# adduser joe
Adding user `joe' ...
Adding new group `joe' (1007) ...
Adding new user `joe' (1006) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
    Full Name []: Joe
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
```

- f. Coloque o usuário joe no grupo de HR.

```
root@ubuntu:/home/cisco# usermod -G HR joe
```

```
root@ubuntu:/home/cisco# usermod -G HR joe
root@ubuntu:/home/cisco#
```

Passo 5: Verifique os usuários recém-criados no arquivo passwd.

```
root@ubuntu:/home/cisco# cat /etc/passwd
```

```
root@ubuntu:/home/cisco# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
eve:x:1003:1003::/home/eve:
Eric:x:1004:1004::/home/Eric:
jenny:x:1005:1006:Jenny,,,:/home/jenny:/bin/bash
joe:x:1006:1007:Joe,,,:/home/joe:/bin/bash
```

Passo 6: Visualize os usuários criados no arquivo shadow.

```
root@ubuntu:/home/cisco# cat /etc/shadow
```

Parte 3: Uso de permissões simbólicas

- Passo 1: No sistema Ubuntu, aperte e mantenha pressionadas as teclas **CTRL+ALT+F1** até que a tela mude para o Terminal **tty1**.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login:
```

Observação: se não for possível usar o terminal tty1, retorne à interface gráfica do usuário (GUI) do host, usando as teclas **CTRL+ALT+F7** e abra uma janela de terminal na GUI Ubuntu OS. No prompt, digite **su -l jenny** e a senha **lasocial**. Continue na etapa 4.

```
cisco@ubuntu:~$ su -l jenny
```

```
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```

Nota: Se as teclas CTRL+ALT+F7 não funcionarem, tente CTRL+ALT+F8.

Passo 2: Quando estiver na tela de login do Terminal, digite **jenny** e pressione Enter.

Passo 3: Quando solicitada a senha, digite **lasocial** e pressione Enter.

Passo 4: Após fazer um login com sucesso, você verá o prompt **jenny@ubuntu:~\$**.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: jenny
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jenny@ubuntu:~$
```

Como não iniciamos a sessão como o root (superusuário), o cifrão (\$) será exibido em vez do # se tivéssemos entrado como o usuário root.

Passo 5: Visualize o diretório atual.

```
jenny@ubuntu:~$ pwd
```

```
jenny@ubuntu:~$ pwd
/home/jenny
```

Passo 6: Volte um nível de diretório para o diretório /home.

```
jenny@ubuntu:~$ cd ..
```

```
jenny@ubuntu:~$ cd ..
jenny@ubuntu:/home$
```

Passo 7: Liste todos os diretórios e suas permissões.

```
jenny@ubuntu:/home$ ls -l
```

```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:28 jenny
drwxr-xr-x  2 joe  joe   4096 Jun 28 19:18 joe
jenny@ubuntu:/home$
```

O sistema operacional Linux tem um total de 10 letras ou traços nos campos de permissões:

- O primeiro campo é um traço para um arquivo e um d para um diretório
- Os campos do 2º ao 4º são para o usuário
- Os campos do 5º ao 7º são para o grupo
- Os campos do 8º ao 10º são para outros (contas diferentes do grupo)



```
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
|         |         |         |         |         |
1st field 2nd - 4th fields (user) 5th - 7th fields (group) 8th - 10th fields (other)
```

Passo 8: Entre na pasta do Joe como Jenny, digitando o comando cd joe.

```
jenny@ubuntu:/home$ cd joe
```

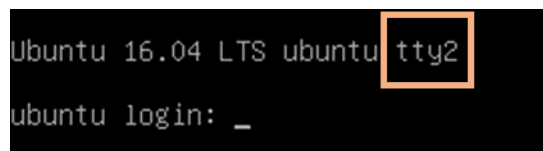
```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$
```

Observe que é possível acessar a *Joe's home folder*.

```
jenny@ubuntu:/home/joe$ cd ..
```

```
jenny@ubuntu:/home/joe$ cd ..
jenny@ubuntu:/home$
```

Passo 9: Aperte e mantenha pressionadas as teclas CTRL+ALT+F2 para mudar para outra sessão do Terminal (tty2).



```
Ubuntu 16.04 LTS ubuntu tty2
ubuntu login: _
```

Passo 10: Inicie uma sessão como o usuário root com a senha secretpassword.

```
Ubuntu 16.04 LTS ubuntu tty2
ubuntu login: root
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.
```

Observação: se não for possível usar o terminal tty2, retorne à interface gráfica do usuário (GUI) do host, usando as teclas **CTRL+ALT+F7** e abra uma janela de terminal na GUI Ubuntu OS. No prompt, digite **sudo -i** e a senha **password**.

```
cisco@ubuntu:~$ sudo -i
[sudo] password for cisco:
root@ubuntu:~#
```

Passo 11: Mude para o diretório /home.

```
root@ubuntu:~# cd /home
```

```
root@ubuntu:~# cd /home
root@ubuntu:/home#
```

Passo 12: Mude a permissão de “others” na pasta do joe, tornando-a não executável.

```
root@ubuntu:/home# chmod o-x joe
```

```
root@ubuntu:/home# chmod o-x joe
root@ubuntu:/home#
```

Passo 13: Liste os diretórios novamente com as respectivas permissões.

```
root@ubuntu:/home# ls -l
```

```
root@ubuntu:/home# ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwxr-xr--  2 joe   joe   4096 Jun 28 19:18 joe
root@ubuntu:/home#
```

Observe que agora existem dois traços no campo “others” para a pasta do joe.

Passo 14: Aperte e mantenha pressionadas as teclas CTRL+ALT+F1 para retornar à outra sessão do Terminal (tty1). Verifique se está visualizando o seguinte prompt de comando: jenny@ubuntu:/home\$.

Passo 15: Tente acessar a pasta do Joe novamente.

```
jenny@ubuntu:/home$ cd joe
```

```
jenny@ubuntu:/home$ cd joe
-bash: cd: joe: Permission denied
jenny@ubuntu:/home$
```

Observe que não temos as permissões para essa ação.

O gráfico abaixo mostra exemplos de outras maneiras de usar o comando **chmod**:

chmod command	Resultados.
chmod u+rwx	Adiciona permissões de leitura, edição e execução para o usuário
chmod u+rw	Adiciona permissões de leitura e edição para o usuário
chmod o+r	Adiciona permissão de leitura para outros
chmod g-rwx	Remove permissões de leitura, edição e execução para o grupo

Passo 16: Digite exit e pressione Enter para encerrar a sessão do Terminal.**Parte 4: Permissões absolutas****Passo 1: Inicie uma sessão como o usuário joe com a senha tooth no terminal tty1.**

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: joe
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

* Documentation:  https://help.ubuntu.com/
```

Observação: se não for possível usar o terminal tty1, retorne à interface gráfica do usuário (GUI) do host, usando as teclas **CTRL+ALT+F7**, e abra uma janela de terminal na GUI Ubuntu OS. No prompt, digite **sudo -l joe** e a senha **tooth**.

```
jenny@ubuntu:/home$ exit
logout
cisco@ubuntu:~$ su -l joe
Password:
joe@ubuntu:~$
```

Passo 2: Imprima o diretório de trabalho atual.

```
joe@ubuntu:~$ pwd
```

```
joe@ubuntu:~$ pwd
/home/joe
joe@ubuntu:~$
```


Passo 3: Volte um nível de diretório para o diretório /home.

```
joe@ubuntu:~$ cd ..
```

```
joe@ubuntu:~$ cd ..  
joe@ubuntu:/home$
```

Passo 4: Liste todos os diretórios e suas permissões no diretório de trabalho atual.

```
joe@ubuntu:/home~$ ls -l
```

```
joe@ubuntu:/home$ ls -l  
total 12  
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco  
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny  
drwxr-xr--  3 joe   joe   4096 Jun 29 00:12 joe  
joe@ubuntu:/home$
```

Observe que a pasta do Joe está configurada para que “others” não possam acessar a pasta.

A outra forma de atribuir permissões, além de usar permissões simbólicas, é o uso de permissões absolutas. As permissões absolutas usam um número octal de três dígitos para representar as permissões para o responsável, grupo e outros.

A tabela abaixo define cada valor absoluto e as permissões correspondentes:

Número	Permissões
7	Leitura, edição e execução
6	Leitura e Escrita
5	Ler e Executar
4	Leitura
3	Edição e execução
2	Gravação
1	Execução
0	None

Ao digitar o comando **chmod 764 examplefile**, o examplefile será atribuído às seguintes permissões:

- O usuário obterá permissões de leitura, edição e execução
- O grupo obterá permissões de leitura e edição
- Outros obterão acesso de leitura

Detalhamento de como 764 representa essas permissões:

Dígito	Equivalente Binário	Permissão
7 (user)	111	1-Read 1-Write 1-Execute
6 (group)	110	1-Read 1-Write 0-No Execute
4 (others)	100	1-Read 0-No Write 0-No Execute

Passo 5: Modifique o campo “others” na pasta do Joe de modo que outros possam ler e executar, mas não possam editar e, ao mesmo tempo, mantenha o campo “user” para leitura, edição e execução.

```
joe@ubuntu:/home$ chmod 705 joe
```

```
joe@ubuntu:/home$ chmod 705 joe
joe@ubuntu:/home$
```

Passo 6: Liste as permissões de arquivo do diretório atual, para ver se as mudanças absolutas foram efetuadas.

```
joe@ubuntu:/home$ ls -l
```

```
joe@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 iennu iennu 4096 Jun 28 23:52 iennu
drwx--r-x  3 joe   joe   4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

Passo 7: Mude para o diretório /home/joe.

```
joe@ubuntu:/home$ cd joe
```

```
joe@ubuntu:/home$ cd joe
joe@ubuntu:~$
```

Passo 8: Crie um arquivo de texto simples denominado test.txt usando touch.

```
joe@ubuntu:~$ touch test.txt
```

```
joe@ubuntu:~$ touch test.txt
joe@ubuntu:~$
```

a. Digite **exit** e pressione **Enter** para encerrar a sessão do Joe.

- b. No Terminal tty1, inicie outra sessão como **jenny** e digite a senha **lasocial**. Pressione **Enter**.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: jenny
Password:
```

Observação: se não for possível usar o terminal tty1, retorne à interface gráfica do usuário (GUI) do host, usando as teclas **CTRL+ALT+F7** e abra uma janela de terminal na GUI Ubuntu OS. No prompt, digite **su -l jenny** e a senha **lasocial**.

```
cisco@ubuntu:~$ su -l jenny
```

```
joe@ubuntu:~$ exit
logout
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```

Passo 9: Mude para o diretório /home.

```
jenny@ubuntu:~$ cd /home
```

```
jenny@ubuntu:~$ cd /home
jenny@ubuntu:/home$
```

Passo 10: Liste todos os diretórios com as respectivas permissões.

```
jenny@ubuntu:/home$ ls -l
```

```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x  3 jenny jenny 4096 Jun 28 23:52 jenny
drwx---r-x  3 joe  joe   4096 Jun 29 00:32 joe
jenny@ubuntu:/home$
```

Passo 11: Mude para o diretório /home/joe e indique o conteúdo do diretório.

```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$ ls -l
```

```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$ ls -l
total 12
-rw-r--r-- 1 joe joe 8980 Jun 28 19:18 examples.desktop
-rw-rw-r-- 1 joe joe    0 Jun 29 00:22 test.txt
jenny@ubuntu:/home/joe$
```

Observe que é possível entrar na pasta do Joe e ler os arquivos no diretório. É possível ver o arquivo *test.txt*.

Passo 12: Tente criar um arquivo.

```
jenny@ubuntu:/home/joe$ touch jenny.txt
```

```
jenny@ubuntu:/home/joe$ touch jenny.txt  
touch: cannot touch 'jenny.txt': Permission denied  
jenny@ubuntu:/home/joe$
```

Observe que não temos permissão para criar o arquivo.

Passo 13: Feche todas as janelas remanescentes.