Práctica de laboratorio: autenticación, autorización y auditoría

Objetivos

- Ante una situación, seleccione la autenticación, autorización o el control de acceso adecuado
- Instale y configure los controles de seguridad al realizar la administración de la cuenta, según las mejores prácticas

Parte 1: agregar grupos, usuarios y contraseñas en un sistema Linux

Parte 2: comprobar usuarios, grupos y contraseñas

Parte 3: utilizar permisos simbólicos

Parte 4: permisos absolutos

Aspectos básicos/situación

Usted realizará las prácticas de seguridad del host usando la línea de comandos de Linux por medio de las siguientes tareas:

- Cómo agregar grupos, usuarios y contraseñas
- Cómo comprobar grupos, usuarios y contraseñas
- Cómo establecer permisos simbólicos
- Cómo establecer permisos absolutos

Recursos necesarios

- Computadora con sistema Ubuntu 16.0.4 LTS instalado en una máquina virtual de VirtualBox o VMware.

Parte 1: Agregar grupos, usuarios y contraseñas en un sistema Linux

En esta parte, agregará los usuarios, los grupos y las contraseñas a la computadora de host local.

Paso 1: Abra una ventana del terminal en Ubuntu.

a. Inicie sesión en Ubuntu con las siguientes credenciales:

Usuario: **cisco**

Contraseña: **password**

b. Haga clic en el icono de **terminal** para abrir una terminal.

Paso 1: Aumente los privilegios al nivel de raíz introduciendo el comando de sudo su. Introduzca la contraseña «password» cuando se le solicite.

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

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

Paso 2: Agregue un nuevo grupo denominado HR al introducir el groupadd del comando HR.

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

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

Parte 2: Verificar usuarios, grupos y contraseñas

Paso 1: Verifique que se haya agregado el nuevo grupo a la lista de archivos de grupo 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#
```

El nuevo grupo HR se agregará a la parte inferior del archivo /etc/group con una ID de grupo de 1005.

Paso 2: Agregue un nuevo usuario llamado Jenny.

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

a. Cuando se le solicite una contraseña nueva, escriba **lasocial**. Presione **Intro**.

b. Cuando se le pregunte nuevamente, escriba **lasocial**. Presione **Intro**.

c. Cuando se le solicite un nombre completo, escriba **Jenny**. Presione **Intro**.

d. Para el resto de las configuraciones, presione **Ingresar** hasta que se le pregunte si la información es correcta.

e. Escriba **S** por sí y presione **Intro**.

```
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
```

Paso 3: Coloque el usuario Jenny en el grupo de RR. HH.

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

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

Paso 4: Agregar otro usuario nuevo llamado Joe.

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

a. Cuando se le solicite una contraseña nueva, escriba **tooth**. Presione **Intro**.

b. Cuando se le pregunte nuevamente, escriba **tooth**. Presione **Intro**.

c. Cuando se le solicite un nombre completo, escriba **Joe**. Presione **Intro**.

d. Para el resto de las configuraciones, presione **Ingresar** hasta que se le pregunte si la información es correcta.

e. Escriba **S** por sí y presione **Intro**.

```
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 el usuario Joe en el grupo de HR.

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

Paso 5: Verifique los usuarios creados recientemente en el archivo 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
jenny:x:1005:1006:Jenny,,,:/home/jenny:/bin/bash
joe:x:1006:1007:Joe,,,:/home/joe:/bin/bash
```

Paso 6: Vea los usuarios creados en el archivo oculto.

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

Parte 3: Utilizar permisos simbólicos

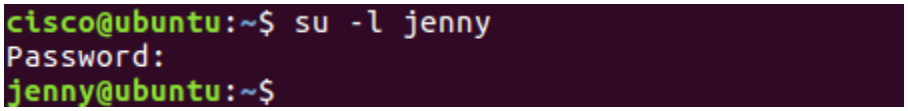
Paso 1: En el sistema Ubuntu, presione y mantenga presionadas las teclas CTRL+ALT+F1 hasta que la pantalla cambie a la terminal tty1.

```
Ubuntu 16.04 LTS ubuntu tty1

ubuntu login:
```

Nota: si no puede usar la terminal tty1, regrese a la interfaz gráfica de usuario (GUI) del host con las teclas **CTRL+ALT+F7** y abra una ventana del terminal en la GUI del sistema operativo Ubuntu. En la petición, ingrese **su –l jenny** e introduzca la contraseña **lasocial**. Proceda con el Paso 4.

```
cisco@ubuntu:~$ su –l jenny
```

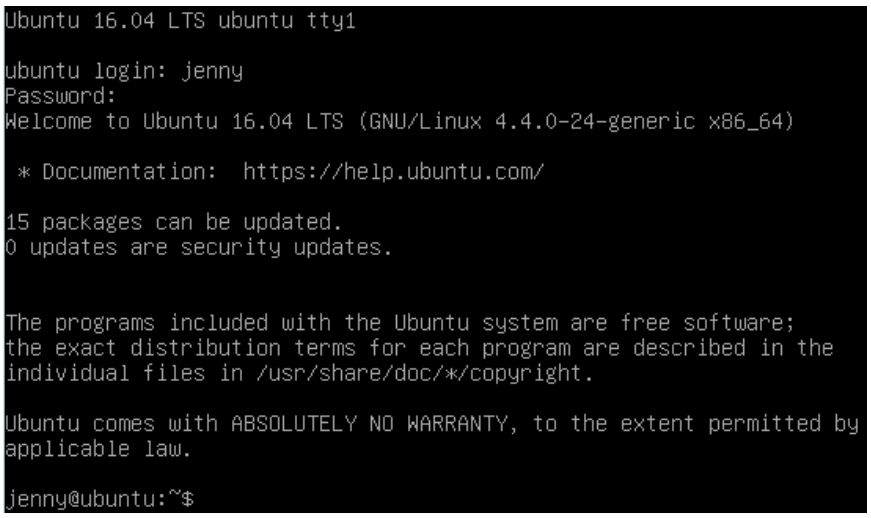


Nota: si las teclas CTRL+ALT+F7 no funcionaron, intente con las teclas CTRL+ALT+F8.

Paso 2: Una vez en la pantalla de inicio de sesión de la terminal, escriba jenny y presione Intro.

Paso 3: Cuando se le solicite la contraseña, escriba «lasocial» y presione Intro.

Paso 4: Si inicia sesión correctamente, verá el indicador *jenny@ubuntu:~$* .



Debido a que no iniciamos sesión como la *raíz* (superusuario), recibimos un símbolo del dólar en lugar de # si iniciáramos sesión como el usuario raíz.

Paso 5: Vea su directorio actual.

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

Paso 6: Retroceda un nivel de directorio en el directorio /home.

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

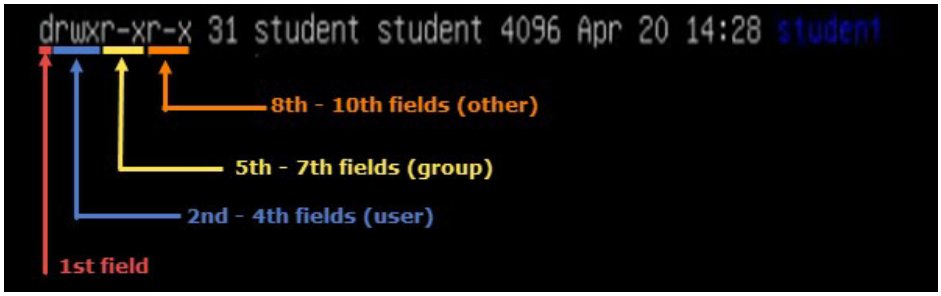
Paso 7: Enumere todos los directorios y sus permisos.

```
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$
```

El sistema operativo Linux tiene un total de 10 letras o guiones en los campos de permiso:

- El primer campo es un guión de un archivo an a d de un directorio
- Los campos segundo a cuarto son para el usuario
- Los campos quinto a séptimo son para el grupo
- Los campos octavo a décimo son para otros (cuentas diferentes de las del grupo)



Paso 8: Ingrese la carpeta de Joe como Jenny al escribir el comando cd joe.

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

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

Observe que podemos ingresar a la *carpeta doméstica de Joe*.

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

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

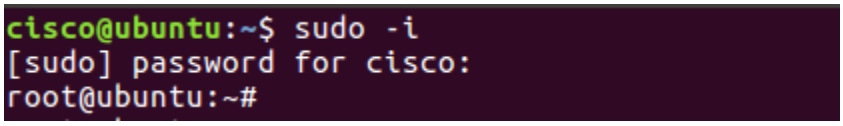
Paso 9: Mantenga presionadas las teclas CTRL+ALT+F2 para cambiar a otra sesión de terminal (tty2).

```
Ubuntu 16.04 LTS ubuntu tty2

ubuntu login: _
```

Paso 10: Inicie sesión como usuario raíz con la contraseña «secretpassword».

Nota: Si no puede usar terminal tty2, vuelva a la interfaz gráfica de usuario (GUI) del host con las teclas **CTRL+ALT+F7** y abra una ventana de terminal en la GUI del SO Ubuntu. En la petición, ingrese **sudo -i** e introduzca la contraseña **password**.

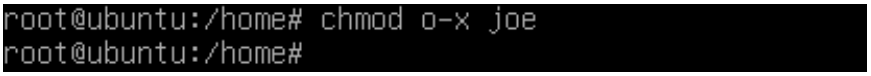


Paso 11: Cambie al directorio /home.

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

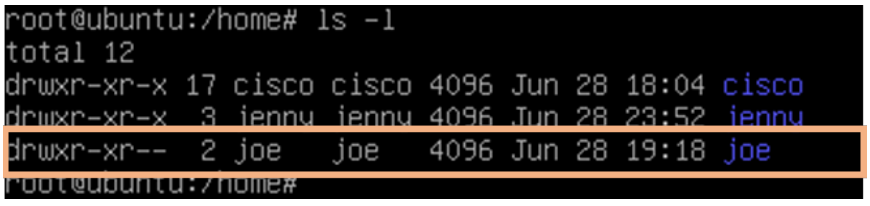
Paso 12: Cambie el permiso de «otros» en la carpeta de Joe al no permitir que pueda ejecutarse.

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



Paso 13: Enumere los directorios una vez más con sus permisos respectivos.

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



Observe que ahora aparecen dos guiones en el campo “otros” para la carpeta de Joe.

Paso 14: Mantenga presionadas las teclas CTRL+ALT+F1 para volver a la otra sesión de terminal (tty1). Asegúrese de estar viendo el siguiente indicador de comando: jenny@ubuntu:/home$.

Paso 15: Intente volver a ingresar a la carpeta de Joe.

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

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

Observe que no tenemos los permisos para hacerlo.

La siguiente tabla muestra ejemplos de otras maneras en que se puede utilizar el comando **chmod**:

comando chmod	Resultados
chmod u+rwx	Agrega permisos de lectura, escritura y ejecución para el usuario
chmod u+rw	Agrega permisos de lectura y escritura para el usuario
chmod o+r	Agrega permisos de lectura para otros
chmod g-rwx	Elimina permisos de lectura, escritura y de ejecución para el grupo

Paso 16: Escriba «salir» y luego presione Intro para salir de la sesión de terminal.

Parte 4: Permisos absolutos

Paso 1: Inicie sesión como usuario Joe con la contraseña tooth mientras se encuentra en la 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/
```

Nota: si no puede usar la terminal tty1, regrese a la interfaz gráfica de usuario (GUI) del host con las teclas **CTRL+ALT+F7** y abra una ventana de terminal en la GUI del sistema operativo Ubuntu. En la petición, introduzca **sudo –l joe** y luego introduzca la contraseña **tooth**.

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

Paso 2: Imprima su directorio de trabajo actual.

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

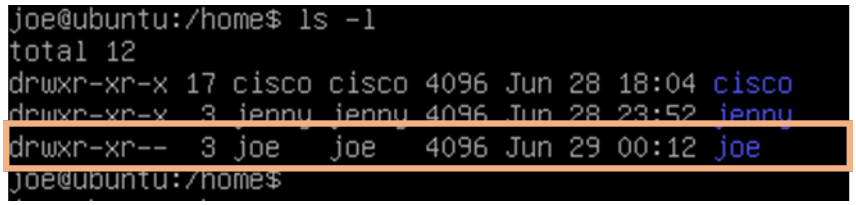
```
joe@ubuntu:~$ pwd
/home/joe
joe@ubuntu:~$
```

Paso 3: Retroceda un nivel de directorio al directorio /home.

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

Paso 4: Enumere todos los directorios y sus permisos en el directorio de trabajo actual.

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



Observe que la carpeta de Joe está configurada para que “otros” no puedan acceder a la carpeta.

Otra manera de asignar permisos además de utilizar permisos simbólicos es utilizar permisos absolutos. Los permisos absolutos usan un número de tres dígitos octal para representar los permisos para el propietario, el grupo y otro.

La siguiente tabla describe cada valor absoluto y los permisos correspondientes:

Número	Permisos
7	Lectura, escritura y ejecución
6	Lectura y escritura
5	Lectura y ejecución
4	Lectura
3	Escritura y ejecución
2	Escritura
1	Ejecución
0	Ninguna

Al escribir el comando **chmod 764 *examplefile***, se asignarán los siguientes permisos al archivo de ejemplo:

- El usuario recibirá permisos de lectura, escritura y ejecución
- El grupo tendrá permisos de lectura y escritura
- Otros obtendrán acceso de lectura

Explicación sobre cómo 764 representa estos permisos:

Dígito	Equivalente binario	Permiso
7 (usuario)	111	1-Lectura 1-Escritura 1-Ejecución
6 (grupo)	110	1-Lectura 1-Escritura 0-Sin ejecución
4 (otros)	100	1-Lectura 0-Sin escritura 0-Sin ejecución

Paso 5: Modifique el campo «otros» de la carpeta de Joe para que otros puedan leer y ejecutar, pero no escribir mientras aún mantienen el campo «usuario» para leer, escribir y ejecutar.

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

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

Paso 6: Enumere los permisos de archivo del directorio actual para ver que los cambios absolutos se hayan realizado.

```
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
drwx---r-x  3 joe   joe   4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

Paso 7: Cambie al directorio */home/joe*.

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

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

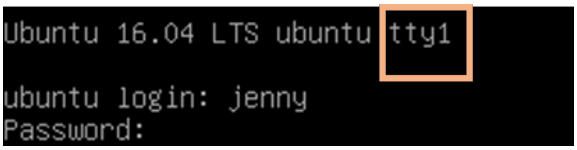
Paso 8: Cree un archivo de texto simple denominado test.txt usando *touch*.

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

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

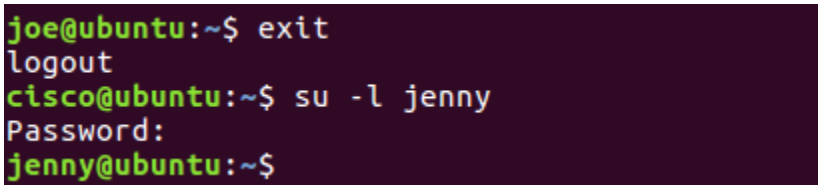
a. Escriba **exit** y luego presione **Intro** para salir de la sesión de Joe.

b. En la terminal tty1, vuelva a iniciar sesión como **jenny** e ingrese la contraseña **lasocial**. Presione **Intro**.



Nota: si no puede usar la terminal tty1, regrese a la interfaz gráfica de usuario (GUI) del host con las teclas **CTRL+ALT+F7** y abra una ventana del terminal en la GUI del sistema operativo Ubuntu. En la petición, ingrese **su –l jenny** e introduzca la contraseña **lasocial**.

```
cisco@ubuntu:~$ su –l jenny
```

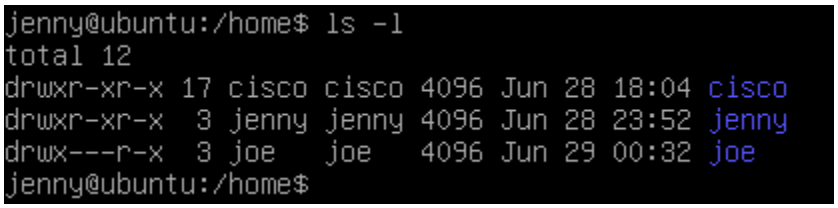


Paso 9: Cambie al directorio /home.

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

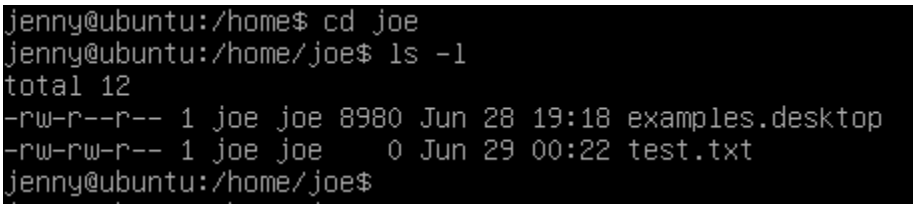
Paso 10: Enumere todos los directorios con sus permisos respectivos.

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



Paso 11: Cambie al directorio /home/joe e indique el contenido del directorio.

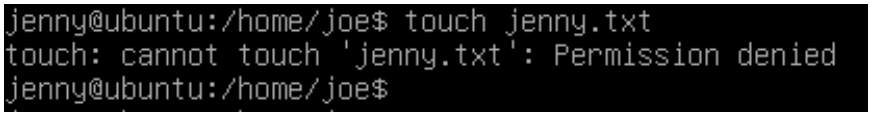
```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$ cd ..
```



Observe que podemos ingresar a la carpeta de Joe y leer los archivos dentro del directorio. Podemos ver el archivo *test.txt*.

Paso 12: Intente crear un archivo.

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



Observe que no tenemos permiso para crear el archivo.

Paso 13: Cierre todas las ventanas restantes.