**Uso responsable de sudo**

Anteriormente, exploraste la autorización, la autenticación y los comandos de Linux con **sudo**, **useradd** y **userdel**. El comando **sudo** es importante para las/los analistas de seguridad porque permite a los/las usuarios/as tener permisos elevados sin arriesgar el sistema ejecutando comandos como usuario root. En esta lectura, continuarás explorando la autorización, la autenticación y los comandos de Linux y aprenderás dos comandos más que se pueden usar con **sudo**: **usermod** y **chown**.

**Uso responsable de sudo**

Para administrar la autorización y la autenticación, tienes que ser un **usuario root** o un usuario con privilegios elevados para modificar el sistema. El usuario root (raíz) también puede llamarse “superusuario”. Para convertirte en usuario root, debes iniciar sesión como tal. Sin embargo, no se recomienda ejecutar comandos como usuario root en Linux, ya que pueden surgir riesgos de seguridad si un agente de amenaza compromete esa cuenta. También es fácil cometer errores irreversibles, y el sistema no puede rastrear quién ejecutó un comando. Por estas razones, en lugar de iniciar sesión como usuario root, se recomienda usar **sudo** en Linux cuando necesites privilegios elevados.

El comando **sudo** otorga temporalmente permisos elevados a usuarios específicos. El nombre de este comando proviene de “super user do” (“superusuario” y “hacer”). Para que puedan usar **sudo**, se les debe otorgar acceso a los usuarios a través de un archivo de configuración, que se llama “sudoers file”. Si bien es preferible usar **sudo** a iniciar sesión como usuario root, es importante tener en cuenta que los usuarios con permisos elevados para usar **sudo** podrían estar en mayor riesgo en caso de un ataque.

Esta situación puede compararse con la de un hotel que tiene una llave maestra. La llave maestra se puede usar para acceder a cualquier habitación del hotel. Algunos/as trabajadores necesitan esta llave para realizar su trabajo. Por ejemplo, para limpiar todas las habitaciones, la persona a cargo debería escanear la tarjeta de identificación y, luego, usar esta llave maestra. Sin embargo, si una persona ajena a la red del hotel obtuviera acceso a la tarjeta de identificación y la llave maestra de la persona a cargo de la limpieza, podría acceder a cualquier habitación del hotel. En este ejemplo, la persona a cargo de la limpieza con la llave maestra representa a un/a usuario/a que usa **sudo** para obtener privilegios elevados. Debido a los peligros que **sudo** supone, solo quienes estrictamente necesitan usarlo deben tener estos permisos.

Además, incluso si necesitas acceso a **sudo**, debes tener cuidado y usarlo solo con los comandos que necesitas. La ejecución de comandos con **sudo** permite a los/las usuarios/as eludir los controles de seguridad típicos que existen para evitar que un/a atacante obtenga acceso elevado.

**Nota**: Ten cuidado de no usar **sudo** si estás copiando comandos de una fuente en línea. Es importante que no uses **sudo** por accidente.

**Autenticación y autorización con sudo**

Puedes usar **sudo** para muchas tareas de gestión de autenticación y autorización. Como recordatorio, la **autenticación** es el proceso de verificar quién es una persona, mientras que la **autorización** es el concepto de otorgar acceso a recursos específicos en un sistema. Estos son algunos de los comandos clave que se utilizan para estas tareas:

**useradd**

El comando **useradd** agrega un usuario al sistema. Para agregar un usuario con el nombre de usuario **fgarcia** con **sudo**, ingresa **sudo useradd fgarcia**. Existen otras opciones que puedes usar con **useradd**:

* **-g**: Establece el grupo predeterminado del usuario, también conocido como su grupo principal.
* **-G**: Agrega al usuario a grupos adicionales, también llamados grupos complementarios o secundarios.

Para usar la opción **-g**, debe especificarse el grupo principal después de **-g**. Por ejemplo, al ingresar **sudo useradd -g security fgarcia**, se agrega a **fgarcia** como un nuevo usuario y se le asigna **security** como grupo principal.

Para usar la opción **-G**, debe incluirse el grupo complementario en el comando después de **-G**. Con la opción **-G**, puedes agregar más de un grupo complementario a la vez. Al ingresar **sudo useradd -G finance,admin** **fgarcia,** se agrega a **fgarcia** como usuario nuevo y se lo añade a los grupos existentes **finance** y **admin**.

**usermod**

El comando **usermod** modifica las cuentas de usuario existentes. Las mismas opciones *-***g** y **-G** del comando **useradd** pueden utilizarse con **usermod** si el usuario ya existe.

Para cambiar el grupo principal de un usuario existente, debes usar la opción **-g**. Por ejemplo, al ingresar **sudo usermod -g executive fgarcia**, se cambiaría el grupo principal de **fgarcia** a **executive**.

Para agregar un grupo complementario para un usuario existente, debes usar la opción **-G**. También necesitas una opción **-a**, que agrega al usuario a un grupo existente y solo se usa con la opción **-G**. Por ejemplo, al ingresar **sudo usermod -a -G marketing fgarcia**, se agregaría el usuario existente **fgarcia** al grupo complementario **marketing**.

**Nota:** Al cambiar el grupo complementario de un usuario existente, si no incluyes la opción **-a**, **-G** reemplazará a cualquier grupo complementario existente con aquellos  que se especifiquen después de **usermod**. El uso de **-a** con **-G** asegura que se agreguen los nuevos grupos, pero no se reemplaza a los grupos existentes.

Hay otras opciones que puedes usar con **usermod** para especificar cómo quieres modificar el usuario, entre ellas, las siguientes:

* **-d**: Cambia el directorio de inicio del usuario.
* **-l**: Cambia el nombre de inicio de sesión del usuario.
* **-L**: Bloquea la cuenta para que el usuario no pueda iniciar sesión.

La opción siempre va después del comando **usermod**. Por ejemplo, para cambiar el directorio de inicio de **fgarcia** a **/home/garcia\_f**, ingresa **sudo usermod -d /home/garcia\_f fgarcia**. La opción **-d** va justo después del comando **usermod** y antes de los otros dos argumentos necesarios.

**userdel**

El comando **userdel** elimina a un usuario del sistema. Por ejemplo, al ingresar **sudo userdel fgarcia**, se elimina a **fgarcia** como usuario. Ten cuidado antes de eliminar a un usuario con este comando.

El comando **userdel** no elimina los archivos en el directorio de inicio del usuario, a menos que se use la opción **-r**. Al ingresar **sudo userdel -r fgarcia**, se eliminaría a **fgarcia** como usuario y se eliminarían todos los archivos en su directorio de inicio. Antes de eliminar cualquier archivo de usuario, debes asegurarte de tener copias de seguridad en caso de que las necesites más adelante.

**Nota**: En lugar de eliminar al usuario, podrías considerar desactivar su cuenta con **usermod -L**. Esto le impide al usuario iniciar sesión y te otorga acceso a su cuenta y sus permisos asociados. Por ejemplo, si un usuario abandona una organización, esta opción te permitiría identificar los archivos sobre los que tiene propiedad, por lo que podrías transferir esta propiedad a otros usuarios.

**chown**

El comando **chown** cambia la propiedad de un archivo o un directorio. Puedes usar **chown** para cambiar la propiedad del usuario o del grupo. Para cambiar el usuario propietario del archivo **access.txt a fgarcia**, ingresa **sudo** **chown fgarcia access.txt**. Para cambiar el grupo propietario del archivo *access.txt* a *security*, ingresa **sudo** **chown :security access.txt**. Tienes que ingresar dos puntos (**:**) antes de **security** para designarlo como un nombre de grupo.

Al igual que con **useradd**, **usermod** y **userdel**, existen otras opciones que puedes usar con **chown**.

**Conclusiones clave**

La autenticación es el proceso mediante el cual un/a usuario/a verifica su identidad, mientras que la autorización es el proceso mediante el cual se determina a qué tiene acceso. Puedes usar el comando **sudo** para ejecutar temporalmente comandos con privilegios elevados y completar las tareas de gestión de autenticación y autorización. Específicamente, **useradd**, **userdel**, **usermod** y **chown** se pueden utilizar para administrar usuarios y propiedad de archivos.