



su, sudo

Identidad

Para más seguridad, aunque tenga privilegios de *root* para un sistema, tiene sentido utilizarlos solo temporalmente para prevenir daños accidentales. *su* y *sudo* le permiten cambiar la identidad rápidamente desde la línea de ordenes.

POR HEIKE JURZIK

Los privilegios de *root* son necesarios para tareas administrativas, pero no tiene sentido ser el superusuario todo el tiempo. Es preferible convertirse en *root* para una tarea administrativa y luego volver a ser un usuario "normal". Dos ordenes, *su* y *sudo*, le permiten cambiar de identidad.

su

La orden *su* ("substitute user") le permite cambiar su ID en la línea de ordenes. La orden lanza un nuevo intérprete de ordenes en segundo plano usando nuevos IDs de usuario (UID) y de grupo (GID). Cuando teclee *su* para convertirse en superusuario, u otro usuario con privilegios, deberá conocer la contraseña para la cuenta de ese usuario.

La sintaxis básica del comando es *su [-] [nombredeusuario]*; pero hay una sutil diferencia, dependiendo de si teclea el signo menos o no. El signo menos (o alternativamente el parámetro

-l o su forma larga *--login*) se asegura de que realmente entra en el sistema, fijando así las variables de entorno apropiadas y el intérprete de ordenes y cambiando al directorio de trabajo de ese usuario (su directorio 'home'). Las variables de entorno no cambian si omite el signo menos y esto podría significar que el nuevo usuario no tiene ningún privilegio para el directorio actual (Véase la Figura 1).

Si no suministra un nombre, se supondrá *root*, la cuenta del superusuario. Esto también es lo que conduce a la falsa idea que *su* es realmente una abreviatura de "superuser". Por omisión la orden *su* no permite al nuevo usuario lanzar aplicaciones X. Los usuarios externos primero deben tener permiso para utilizar el servidor de X para salida y esto significa editar el archivo *.Xauthority* en el directorio de trabajo adecuado (véase también *man xauth*). Para permitir al usuario *root* lanzar un programa X en un





Xterm que pertenezca al usuario *petronella*, necesita extraer una clave desde *.Xauthority*, añadirla al *.Xauthority* del administrador y entonces redefinir la variable *DISPLAY* (véase el Listado 1).

su también le permite usar otra cuenta para lanzar una sola orden. Para hacer esto, indique la opción *-c* (*--command*):

```
huhn@asteroid:~$ su -c "less /var/log/messages"
Password:
```

El uso de la orden *su* se anota en la bitácora (*log*). En función de la distribución que use, esas entradas de bitácora se localizarán en */var/log/auth.log* (p. e. en Debian) o en */var/log/messages* (p. e. en Suse Linux). Los intentos inválidos son fácilmente localizados, permitiendo al usuario *admin* ver rápidamente quien ha intentado apropiarse indebidamente de los privilegios de *root*

```
Dec 22 14:50:50 asteroid: PAM_unix[2108]: authentication failure; (uid=500) -> root for su service
Dec 22 14:50:52 asteroid: su[2108]: pam_authenticate: Authentication failure
Dec 22 14:50:52 asteroid: su[2108]: - pts/8 huhn-root
```

Si es el usuario *admin*, no necesita introducir una contraseña después de teclear la orden *su*. Usted puede asumir cualquier identidad para probar rápidamente una modificación desde la perspectiva de otro usuario.

sudo

La orden *sudo* le permite evitar dar a conocer la contraseña de *root* de una máquina, lo cual es comprensible por motivos de seguridad. La orden realiza lo

```
petronella@asteroid:~$ su huhn
Password:
huhn@asteroid:/home/petronella$ ls
ls: .: Permission denied
huhn@asteroid:/home/petronella$ cd
huhn@asteroid:~$ cd -
bash: cd: /home/petronella: Permission denied
huhn@asteroid:~$
```

Figura 1: Sin el apropiado ingreso en el sistema, no tiene ningún privilegio.

que el nombre sugiere: “sudo” es la abreviatura de “substitute user, do” (sustituye el usuario, haz) y facilita a usuarios individuales o grupos los privilegios administrativos por un período limitado y limitándose a una tarea específica. Un usuario puede entonces simplemente teclear su propia contraseña para lanzar una orden privilegiada.

El usuario *admin* necesita crear una lista de usuario autorizados a ejecutar ordenes específicas privilegiadas en el archivo */etc/sudoers*. Mientras trabaja como *root*, edite el archivo con la orden *visudo*. este programa ofrece las características habituales del editor *vi* con algunas funciones adicionales. *visudo* “bloquea” el fichero */etc/sudoers* para evitar que sea editado por múltiples usuarios a la vez. Además *visudo* comprueba la sintaxis del fichero al terminar y le informa de cualquier error si lo encuentra:

```
>>> sudoers file: syntax error, line 20 <<<
What now?
```

Dispone de tres alternativas: pulsar *e* para editar el fichero de nuevo, *x* para cancelar los cambios y salir del editor o *Q* para salvar los cambios a pesar del error.

Hay una entrada predeterminada para *root ALL=(ALL) ALL* en */etc/sudoers*. Esto permite hacer todo al usuario *root*,

pero por supuesto *root* también puede hacerlo sin *sudo*. Si necesita conceder a otro usuario privilegios de *root* sin restricciones en una máquina, simplemente copie esta línea y sustituya *root* por el nombre de ese usuario. Después de salvar el archivo, este usuario podrá ejecutar órdenes de administración mediante *sudo*, por ejemplo:

```
huhn@asteroid:~$ sudo /sbin/shutdown
Password:
```

Si no se permite al usuario usar *sudo*, aparecerá un mensaje como este: “*sudo: huhn is not in the sudoers file. This incident will be reported.*” (*sudo: huhn no está en el archivo sudoers. Se informará de este suceso*). La medida predeterminada, que puede ser cambiada en */etc/sudoers*, es enviar un correo alertando al administrador con los detalles del usuario que ha intentado lanzar *sudo* (véase la Figura 2). Para estar seguros, los usuarios sin privilegios pueden teclear *sudo -l* para mostrar una lista de las ordenes permitidas.

Control Minucioso

La sección *Host alias specification* de */etc/sudoers* le permite especificar las máquinas donde las ordenes específicas de *sudo* deben aplicarse. Podemos utilizar el *Host Alias* para crear un grupo de ordenadores mediante la especificación de sus nombre o definiendo un rango de direcciones IP. Esta característica solamente tiene sentido si aplicamos una configuración centralizada de *sudo* en múltiples ordenadores.

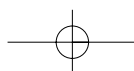
La sección *User Alias* le permite crear grupos que necesiten los mismos privilegios. Primero definimos el tipo de alias (p. e. *User Alias*), después un nombre de alias (que puede contener mayúsculas, subrayados y números), un mapeo indicado por el signo “=” y finalmente los nombres de usuario separados por comas. Vamos agregar los usuarios *huhn* y *petronella* a un grupo que se le permite parar la máquina:

```
# User alias specification
User_Alias SHUTTERSDOWN=huhn,petronella
```

GLOSARIO

UID: Cada usuario se identifica mediante un UID (“User IDentification number”), que lo mapea de manera única a la cuenta del usuario. Puede encontrar fácilmente su propio ID tecleando “echo \$UID”

GID: Además del UID, los usuarios tienen un GID (“Group IDentification number”) que indica su pertenencia a un grupo. Los miembros de un grupo pueden compartir privilegios. La orden “id” indica su UID y su GID actual.



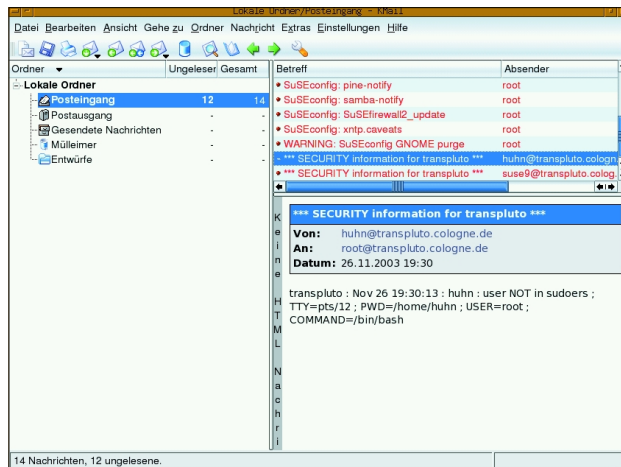


Figura 2: La seguridad es muy valiosa; sudo informa de los accesos ilegítimos.

El próximo paso es definir un alias para la orden *shutdown* en la sección *Cmdnd alias specification*. Para hacer esto, introduzca la ruta absoluta al programa requerido:

```
# Cmdnd alias specification
Cmdnd_Alias DOWN = /sbin/shutdown
```

Para decirle a *sudo* que los *SHUTTERS-DOWN* están autorizados a ejecutar esta orden, necesitamos otra entrada debajo de *User privilege specification*:

```
SHUTTERS-DOWN ALL = DOWN
```

Los usuarios del grupo *SHUTTERS-DOWN* ahora pueden apagar la máquina tecleando *sudo /sbin/shutdown*. Pero hay una forma más fácil de otorgar a un solo usuario permiso para ejecutar una sola orden. Por ejemplo, la entrada:

```
huhn ALL = /usr/sbin/visudo
```

otorga al usuario *huhns* permiso para editar el archivo */etc/sudoers* usando la orden *sudo /usr/sbin/visudo*.

¿Libre o Restringido?

Una simple entrada en */etc/sudoers* le permite restar privilegios a un usuario individual. La sintaxis para hacer esto es como sigue:

```
SHUTTERS-DOWN ALL = DOWN
petronella ALL = !DOWN
```

Es importante especificar la excepción inmediatamente después de la regla, ya

que el archivo se analiza desde arriba hacia abajo. Esto le permitirá mantener el grupo *SHUTTERS-DOWN*, al cuál se le puede permitir ejecutar otras ordenes, mientras que al mismo tiempo se restringe a *petronella* el permiso para apagar la máquina. Si *petronella* intenta ejecutar la orden, simplemente le mostrará un mensaje como el siguiente: “Sorry, user *petronella* is not allowed to execute ‘*/usr/sbin/visudo*’ as root on *asteroid.linux-magazine.com*.” (Lo siento, el usuario *petronella* no tiene permiso para ejecutar ‘*/usr/sbin/visudo*’ como root en *asteroid.linux-magazine.com*).

Si quiere eliminar el indicador (prompt) de contraseña para una o varias ordenes, simplemente active el indicador *NOPASSWD*:

```
SHUTTERS-DOWN ALL=NOPASSWD:DOWN
```

En vez de reducir el nivel de la seguridad que *sudo* proporciona, puede incrementarlo, obligando al usuario que

Listado 1: Display

```
01 petronella@asteroid:~$ xauth
02 extract key $DISPLAY
03 huhn@asteroid:~$ su -
04 Password:
05 asteroid:~# xauth merge
06 home/huhn/key
07 asteroid:~# export
   DISPLAY=:0.0
```

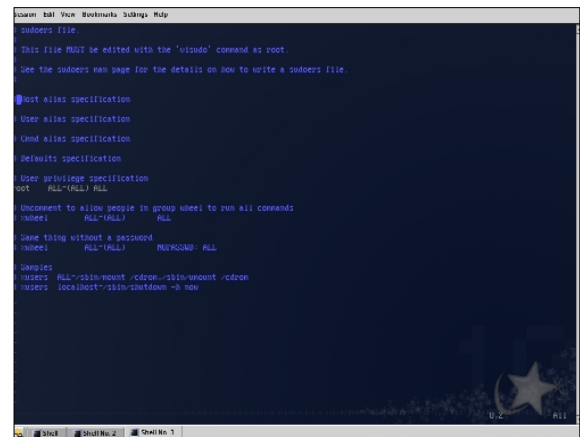


Figura 3: Se recomienda editar el fichero */etc/sudoers* solamente con el programa */usr/sbin/visudo*.

introduzca la contraseña cada vez que ejecute *sudo*. Por omisión *sudo* ejecuta una especie de sistema de boletos con un intervalo que asegura, por ejemplo, que no pueda abrirse en la máquina una consola del intérprete de ordenes con privilegios de *root* que pueda comprometer todo el sistema sin excepción. La validez predeterminada para el boleto para la mayoría de las distros es de 15 minutos. Pero se puede configurar a 0 minutos añadiendo la siguiente línea a */etc/sudoers*:

```
Defaults timestamp_timeout = 0
```

Opcional

sudo también tiene algunos parámetros de línea de ordenes. Probablemente el más importante de ellos sea *-s*, que le permite lanzar un intérprete de ordenes como *root*. No es necesario configurar accesos al servidor X, solamente teclear *sudo -s* será suficiente para que el administrador lance programas sobre el servidor gráfico.

El conmutador *-L* lista todas las opciones en el archivo */etc/sudoers*. Si quiere extender su boleto sin ejecutar una orden, solo tiene que introducir *sudo -v*. Si el intervalo se ha agotado, se le indicará que teclee la contraseña. También puede dar de baja un boleto tecleando *sudo -k*. El indicador *-b* le permite ejecutar una orden en segundo plano; sin embargo, no podrá moverlo de nuevo al primer plano con la orden normal de control de trabajos del intérprete de ordenes, *fg*.