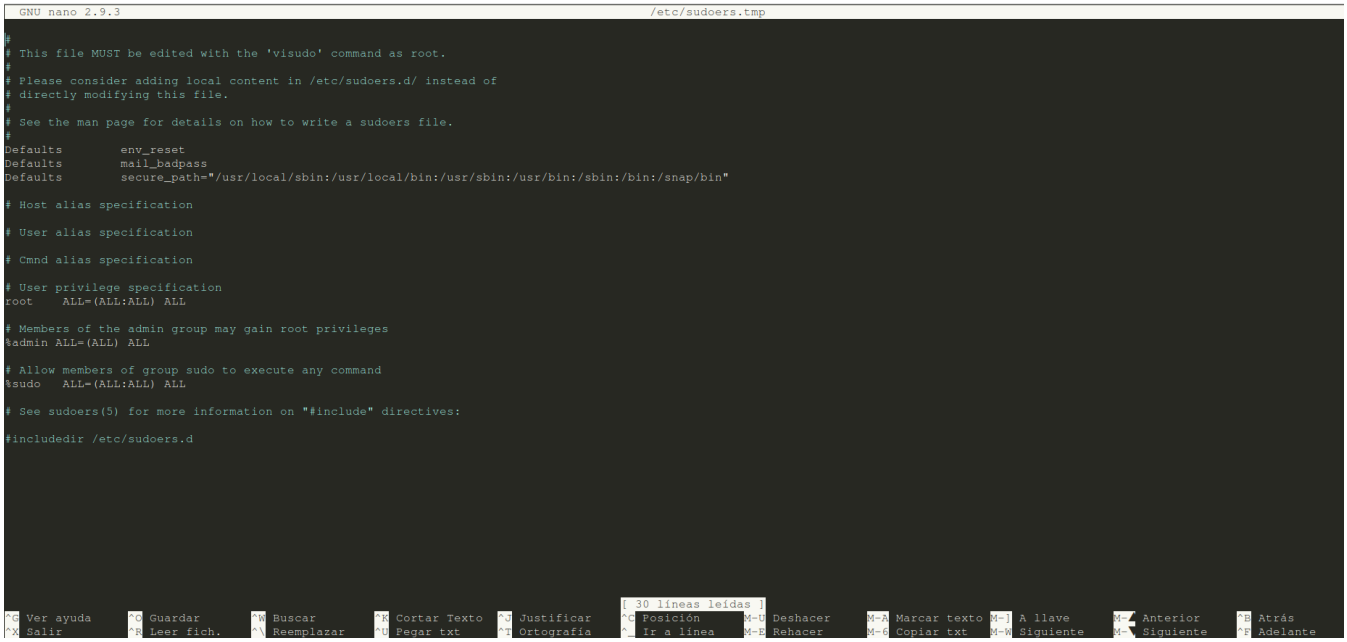
Fichero_Sudoers

07/11/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

Contenido

Comando Visudo



Se utiliza en sistemas basados en Linux, como Ubuntu, para editar el archivo de configuración /etc/sudoers, que controla el acceso y los permisos de los usuarios para ejecutar comandos con privilegios de superusuario (root) a través del comando sudo.

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Comando visudo -c

```
root@ubuntu:~# visudo -c
/etc/sudoers análisis OK
/etc/sudoers.d/README análisis OK
root@ubuntu:~#
```

Este comando verificará la sintaxis del archivo de configuración /etc/sudoers en busca de errores sin abrirlo para su edición.

Comando tail -4 /etc/passwd

```
root@ubuntu:~# tail -4 /etc/passwd
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
pavel:x:1001:1001:Pavel,,,,:/home/pavel:/bin/bash
telnetd:x:113:123::/nonexistent:/usr/sbin/nologin
root@ubuntu:~#
```

Se utiliza para mostrar las últimas cuatro líneas del archivo /etc/passwd en un sistema Linux.

Nos metemos con otro usuario

```
root@ubuntu:~# login pavel
Contraseña:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Infrastructure está desactivado

Se puede aplicar 1 actualización de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

116 actualizaciones de seguridad adicionales se pueden aplicar con ESM Infra.
Aprenda más sobre cómo activar el servicio ESM Infra for Ubuntu 18.04 at
https://ubuntu.com/18-04

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


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.

pavel@ubuntu:~$
```

Comando cd /mnt

```
pavel@ubuntu:/$ cd /mnt/
pavel@ubuntu:/mnt$ ls -lh
total 0
pavel@ubuntu:/mnt$
```

El comando cd /mnt se utiliza para cambiar el directorio de trabajo actual a la ruta /mnt en un sistema Linux.

Creamos una carpeta llamada folder_01

```
pavel@ubuntu:/mnt$ sudo mkdir folder_01
[sudo] contraseña para pavel:
pavel no está en el archivo sudoers. Se informará de este incidente.
pavel@ubuntu:/mnt$
```

Al crear la carpeta nos lo rechaza porque el usuario Pavel no esta dentro del archivo sudoers

Accedemos otra vez a la configuración de visudo

```
root@ubuntu:~# visudo
```

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Agregamos el usuario Pavel

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

pavel ALL=(ALL:ALL) /usr/bin/mkdir
```

Comando which mkdir

```
root@ubuntu:~# which mkdir
/bin/mkdir
root@ubuntu:~#
```

El comando which mkdir se utiliza para determinar la ubicación del ejecutable de mkdir en el sistema. mkdir es un comando en sistemas Unix y Linux que se utiliza para crear directorios

Hacemos el comanco visudo -c

```
root@ubuntu:~# visudo -c
/etc/sudoers análisis OK
/etc/sudoers.d/README análisis OK
root@ubuntu:~#
```

Nos metemos con el usuario Pavel

```
root@ubuntu:~# login pavel
Contraseña:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Infrastructure está desactivado

Se puede aplicar 1 actualización de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

116 actualizaciones de seguridad adicionales se pueden aplicar con ESM Infra.
Aprenda más sobre cómo activar el servicio ESM Infra for Ubuntu 18.04 at
https://ubuntu.com/18-04

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


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.

pavel@ubuntu:~$
```

```
pavel@ubuntu:~$ cd /mnt/
pavel@ubuntu:/mnt$ ls
pavel@ubuntu:/mnt$
```

Creamos la carpeta folder01

```
pavel@ubuntu:~$ sudo mkdir folder01
[sudo] contraseña para pavel:
pavel@ubuntu:~$ ls
Descargas  Documentos  Escritorio  folder01  Imágenes  Música  Plantillas  Público  Vídeos
pavel@ubuntu:~$ ls -lh
total 36K
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Descargas
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Documentos
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Escritorio
drwxr-xr-x 2 root  root  4,0K nov  7 18:59 folder01
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Imágenes
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Música
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Plantillas
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Público
drwxr-xr-x 2 pavel pavel 4,0K nov  7 18:51 Vídeos
pavel@ubuntu:~$
```

Ahora borramos la carpeta folder01

```
pavel@ubuntu:/mnt$ sudo rm -rf folder01/
Disculpe, el usuario pavel no está autorizado para ejecutar «/bin/rm -rf folder01/» como root
en ubuntu
pavel@ubuntu:/mnt$
```

El usuario no puede borrar el fichero

Editamos el fichero visudo para que el usuario Pavel pueda borrar

```
# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

%sudo ALL=NOPASSWD:ALL

pavel ALL=(ALL:ALL) /bin/mkdir,/bin/rm
```

Verificamos que ahora podamos borrar

```
pavel@ubuntu:~$ cd /mnt/
pavel@ubuntu:/mnt$ sudo rm -rf folder01/
pavel@ubuntu:/mnt$ ls -lh
total 0
pavel@ubuntu:/mnt$
```

Configuramos el fichero visudo para que el usuario Pavel no ponga contraseña

```
#includedir /etc/sudoers.d

%sudo ALL=NOPASSWD:ALL

pavel ALL=NOPASSWD:/bin/mkdir,/bin/rm
```

Creando el usuario no nos pide contraseña

```
pavel@ubuntu:~$ cd /mnt/
pavel@ubuntu:/mnt$ sudo mkdir folder01
pavel@ubuntu:/mnt$ ls -lh
total 4,0K
drwxr-xr-x 2 root root 4,0K nov  7 19:22 folder01
pavel@ubuntu:/mnt$
```

Borramos el fichero de nuevo sin que nos pida contraseña

```
pavel@ubuntu:/mnt$ sudo rm -rf folder01/
pavel@ubuntu:/mnt$ ls -lh
total 0
pavel@ubuntu:/mnt$
```

Configuramos el fichero de visudo

```
This file MUST be edited with the 'visudo' command as root.

Please consider adding local content in /etc/sudoers.d/ instead of
directly modifying this file.

See the man page for details on how to write a sudoers file.

faults        env_reset
faults        mail_badpass
faults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/sn

Host alias specification

User alias specification

Cmnd alias specification

User privilege specification
ot    ALL=(ALL:ALL) ALL

Members of the admin group may gain root privileges
dmin ALL=(ALL) ALL

Allow members of group sudo to execute any command
udo   ALL=(ALL:ALL) ALL

See sudoers(5) for more information on "#include" directives:

ncludedir /etc/sudoers.d

udo ALL=NOPASSWD:ALL

vel ALL=NOPASSWD:/bin/mkdir,/bin/rm
```

```
pavel ALL=NOPASSWD:/bin/mkdir,/bin/rm

pavel ALL=(ALL:ALL)/bin/passwd, !/bin/passwd root
```

Verificamos que esta todo bien

```
root@ubuntu:~# visudo -c
/etc/sudoers análisis OK
/etc/sudoers.d/README análisis OK
root@ubuntu:~#
```

Nos metemos con la cuenta Pavel a la que hemos configurado

```
root@ubuntu:~# login pavel
Contraseña:
Último inicio de sesión: mar nov  7 19:22:13 CET 2023 en pts/0
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Infrastructure está desactivado

Se puede aplicar 1 actualización de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

116 actualizaciones de seguridad adicionales se pueden aplicar con ESM Infra.
Aprenda más sobre cómo activar el servicio ESM Infra for Ubuntu 18.04 at
https://ubuntu.com/18-04

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

pavel@ubuntu:~$
```

Probamos cambiar las contraseñas

```
pavel@ubuntu:~$ sudo passwd usuario
[sudo] contraseña para pavel:
Nueva contraseña:
CONTRASEÑA INCORRECTA: Es demasiado corta.
CONTRASEÑA INCORRECTA: es demasiado sencilla
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
pavel@ubuntu:~$
```

Para un usuario si nos deja cambiar la contraseña

```
pavel@ubuntu:~$ sudo passwd root
Disculpe, el usuario pavel no está autorizado para ejecutar «/usr/bin/passwd root» como root e
n ubuntu
pavel@ubuntu:~$
```

Pero para el usuario root no nos deja

Prohibimos que haga ping con sudo al usuario Pavel

```
pavel ALL=(ALL)!/bin/ping
```

```
pavel@ubuntu:~$ sudo ping 10.68.16.116
[sudo] contraseña para pavel:
Disculpe, el usuario pavel no está autorizado para ejecutar «/bin/ping 10.68.16.116» como root
 en ubuntu
pavel@ubuntu:~$
```

Prohibimos que haga pwd con sudo al usuario Pavel

```
pavel ALL=(ALL)!/bin/pwd
                                                [ 40 líneas
^G Ver ayuda    ^O Guardar      ^W Buscar       ^K
```

```
pavel@ubuntu:~$ sudo pwd
[sudo] contraseña para pavel:
Disculpe, el usuario pavel no está autorizado para ejecutar «/bin/pwd» como root en ubuntu
pavel@ubuntu:~$
```