Finding flags from open port redis

First I always ping to the machine IP address (**10.129.203.95)** to see if the connection is working

And then I use nmap to scan for opening port by using

Nmap –top-ports 10000 **10.129.203.95**

Using –top-ports will allow nmap to scan over 10000 ports and see if any of them is open

A screen shot of a computer

AI-generated content may be incorrect.

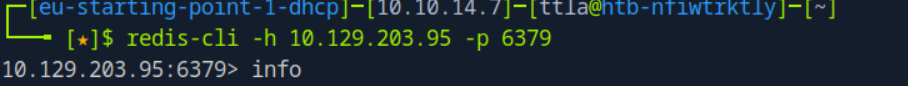
Once I know the port open is redis

I used

redis-cli -h 10.129.203.95 -p 6379

to access the redis server from port 6379

-h is the hostname and -p is port where it is sit



And then I search from google the command for finding information and statistics about this server redis

Then I found and used info to get information

It will shows out how many keys are there

Then I use keys\* to show all the keys\*

So basically keys are like storages that contain values inside and that value can be exploited and used by hacker

A screenshot of a computer program

AI-generated content may be incorrect.

And the infor that we need it flag that contain the value we looking for

Then use

Get flag

Just like dictionary in python , in redis they have key-pair value

So by get flag we actually get key and return value

A close up of numbers

AI-generated content may be incorrect.