HTB ID: HTB-394CC3AD1E

HACK THE BOX

NETWORK ENUMERATION WITH NMAP

Abbey Robinson

Time Management

Start Time: 9/9/25; 5:49 PM

End Time: 9/10/25; 3:05PM

Total Flags Captured: 9/9

Challenges/Roadblocks: I struggled with bypassing the firewall modules. I wasn't completely familiar with all the tacks to successfully get by the firewall. Up until the firewall modules I had no issues.

Flag 1:

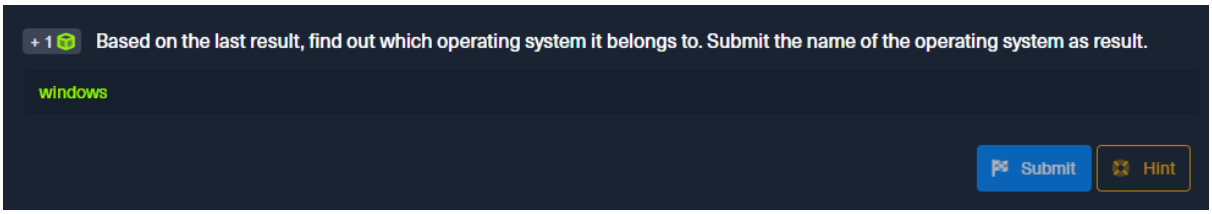
Flag Answer: Windows

Last Command Used: N/A

Steps:

1. To find out the operating system, I looked at the last screenshot HTB provided of the Nmap ICMP ping sweep. The output had some unfamiliar terms like ttl, and iplen.
2. I used the link provided in HTB called nmap.org. I read the definitions of what each of those meant. I learned that ttl means time to live and there are different numbers associated with the operating systems. 128 is windows, 68 is Linux, etc.

Image/Screenshot:



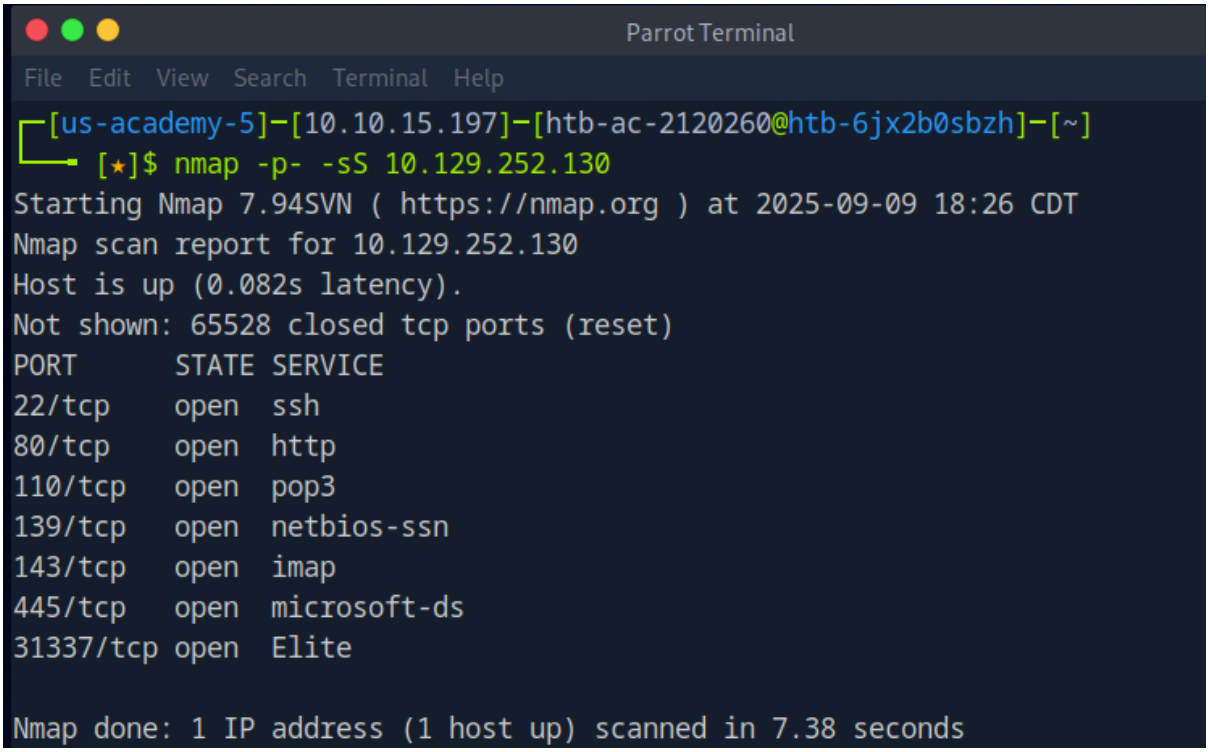
Flag 2:

Flag Answer: 7

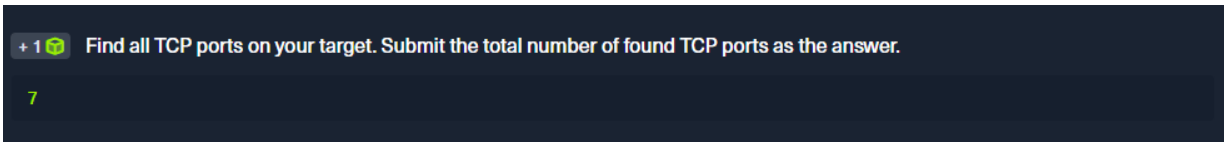
Last Command Used: nmap -p- -sS 10.129.252.130

Steps:

1. I used the command above to do an Nmap scan on my target. -p- tells Nmap to scan all ports and -sS is like a sneaky TCP SYN scan. The cheatsheet was useful on providing me the information on how to run different scans.
2. After it ran, I could successfully see 7 ports in the image below.



Image/Screenshot:



Flag 3:

Flag Answer: NIX-NMAP-DEFAULT

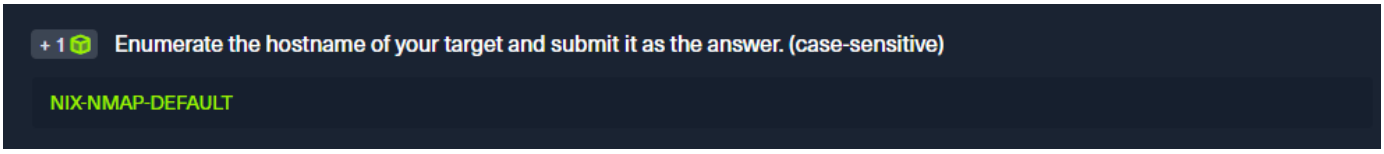
Last Command Used: nmap -sV -sC 10.129.252.130

Steps:

1. I used -sV and -sC to Nmap scan my target this time to enumerate the host name. From reading above and from previous modules, I know that -sV tells Nmap to try and figure out the exact software and its specific version number running on the open ports. -sC runs scripts that gather more information from the open ports, like potentially find a website name I was thinking.
2. By running this command I was able to enumerate the host name, NIX-NMAP-DEFAULT. Shown in the screenshot below I highlighted where I located the flag.

```
┌─[us-academy-5]─[10.10.15.197]─[htb-ac-2120260@htb-6jx2b0sbzh]─[~]
└──╼ [★]$ nmap -sV -sC 10.129.252.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-09 18:37 CDT
Nmap scan report for 10.129.252.130
Host is up (0.085s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 71:c1:89:90:7f:fd:4f:60:e0:54:f3:85:e6:35:6c:2b (RSA)
|   256 e1:8e:53:18:42:af:2a:de:c0:12:1e:2e:54:06:4f:70 (ECDSA)
|_  256 1a:cc:ac:d4:94:5c:d6:1d:71:e7:39:de:14:27:3c:3c (ED25519)
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
110/tcp   open  pop3        Dovecot pop3d
|_pop3-capabilities: UIDL TOP CAPA PIPELINING RESP-CODES SASL AUTH-RESP-CODE
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        Dovecot imapd (Ubuntu)
|_imap-capabilities: more Pre-login ID LOGINDISABLEDA0001 SASL-IR ENABLE post-login capabilities IMAP4rev1 have
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
31337/tcp open  Elite?
| fingerprint-strings:
|   GetRequest:
|_    220 HTB{pr0F7pDv3r510nb4nn3r}
1 service unrecognized despite returning data. If you know the service/version, please submit the following fing
SF-Port31337-TCP:V=7.94SVN%I=7%D=9/9%Time=68C0BA58%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,1F,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n");
Service Info: Host: NIX-NMAP-DEFAULT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Image/Screenshot:



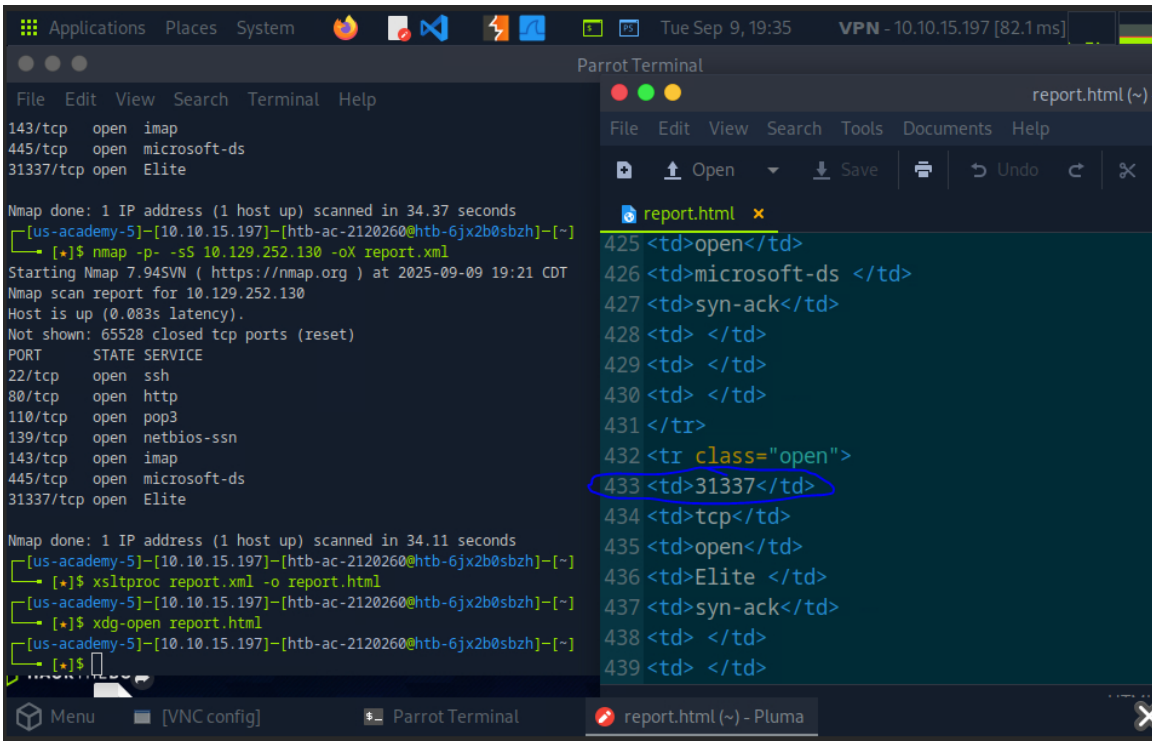
Flag 4:

Flag Answer: 31337

Last Command Used: xdg-open report.html

Steps:

1. I did **nmap -p- -sS 10.129.252.130**, again to start fresh because I took a break.
2. Then I ran **nmap -p- -sS 10.129.252.130 -oX report.xml**, to generate a report then did **xsltproc report.xml -o report.html**, to convert it to HTML like the flag asked for. I know from the HTB cheat sheet that -oX creates the file name and -o to convert.
3. After scrolling all the way down the HTML page, I found that the highest port number was 31337. Here is where I found it in the HTML:



Image/Screenshot:

+1 Perform a full TCP port scan on your target and create an HTML report. Submit the number of the highest port as the answer.

31337

Flag 5:

Flag Answer: HTB{pr0F7pDv3r510nb4nn3r}

Last Command Used: None, used scrolled up to my -sV -sC scan

Steps:

1. I went back to my original -sV -sC can to read through it again. From the previous flag I found that port number to be suspicious because I don't even know what that one means. After reading through the other ports I found no flags, so I knew it had to be located in port 31337. It was under the fingerprint-strings. Here is where I found it:

```
┌[us-academy-5]-[10.10.15.197]-[htb-ac-2120260@htb-6jx2b0sbzh]-[~]
└─• [★]$ nmap -sV -sC 10.129.252.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-09 18:37 CDT
Nmap scan report for 10.129.252.130
Host is up (0.085s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0
| ssh-hostkey:
|   2048 71:c1:89:90:7f:fd:4f:60:e0:54:f3:85:e6:35:6c:2b (RSA)
|   256 e1:8e:53:18:42:af:2a:de:c0:12:1e:2e:54:06:4f:70 (ECDSA)
|_  256 1a:cc:ac:d4:94:5c:d6:1d:71:e7:39:de:14:27:3c:3c (ED25519)
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
110/tcp   open  pop3        Dovecot pop3d
|_pop3-capabilities: UIDL TOP CAPA PIPELINING RESP-CODES SASL AUTH-RESP-CODE
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        Dovecot imapd (Ubuntu)
|_imap-capabilities: more Pre-login ID LOGINDISABLEDA0001 SASL-IR ENABLE post-login cap
 OK IDLE listed LOGIN-REFERRALS LITERAL+
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
31337/tcp open  Elite?
| fingerprint-strings:
|   GetRequest:
|_    220 HTB{pr0F7pDv3r510nb4nn3r}
1 service unrecognized despite returning data. If you know the service/version, please
gerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31337-TCP:V=7.94SVN%I=7%D=9/9%Time=68C0BA58%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,1F,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n");
Service Info: Host: NIX-NMAP-DEFAULT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Image/Screenshot:

+ 1 Enumerate all ports and their services. One of the services contains the flag you have to submit as the answer.

HTB{pr0F7pDv3r510nb4nn3r}

Flag 6:

Flag Answer: HTB{873nniuc71bu6usbs1i96as6dsv26}

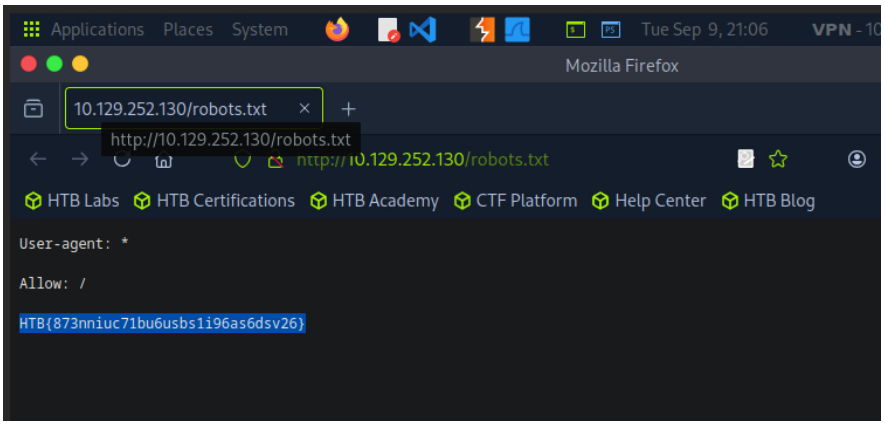
Last Command Used: sudo nmap 10.129.252.130 -p80 --script vuln -Pn

Steps:

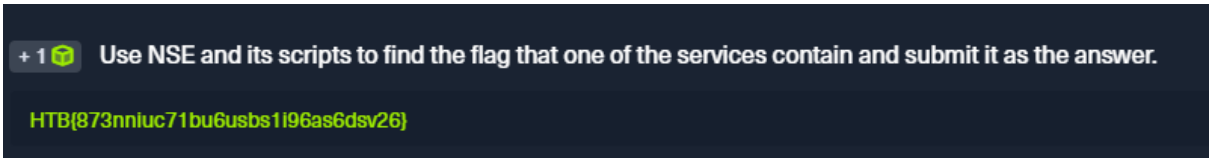
1. I first started by using the command **sudo nmap 10.129.252.130 -p22 --script vuln** to try to individually scan to see if there was something hidden, found nothing. This command uses Nmap with admin privileges to scan ports on the target IP for common vulnerabilities using a suite of built-in scripts.
2. I used **sudo nmap 10.129.252.130 -p80 --script vuln to scan port 80**, it told me to add -Pn because the host seemed to be down. I found that strange so now I did the command **sudo nmap 10.129.252.130 -p80 --script vuln -Pn**, then I noticed the robots.txt file. I will show that here:

```
┌─[us-academy-5]─[10.10.15.197]─[htb-ac-2120260@htb-6jx2b0sbzh]─[~]
└──╼ [★]$ sudo nmap 10.129.252.130 -p80 --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-09 20:55 CDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 13.19 seconds
┌─[us-academy-5]─[10.10.15.197]─[htb-ac-2120260@htb-6jx2b0sbzh]─[~]
└──╼ [★]$ sudo nmap 10.129.252.130 -p80 --script vuln -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-09 20:56 CDT
Nmap scan report for 10.129.252.130
Host is up (0.082s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /robots.txt: Robots file
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 32.13 seconds
```

3. I know that .txt files usually contain a flag from previous CTF's. Therefore, I opened Firefox looked up **10.129.252.130/robots.txt** enter. A page popped up with the flag. Here is what I saw:



Image/Screenshot:



Flag 7:

Flag Answer: ubuntu

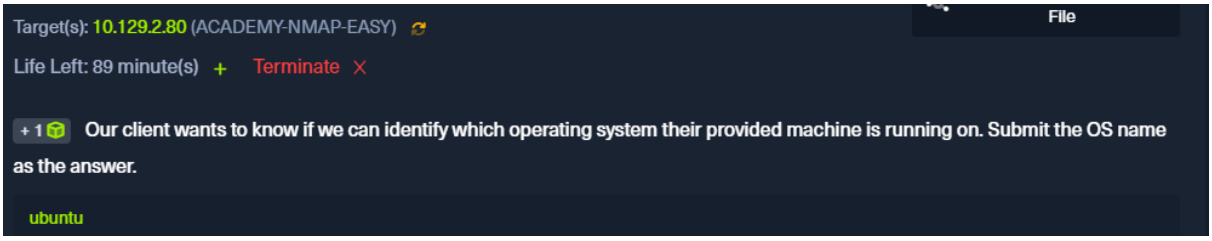
Last Command Used: nmap -p 80 --script=http-title,http-headers 10.129.2.80

Steps:

1. I started off with the command provided in a HTB example, **sudo nmap 10.129.2.80 -n -Pn -p 445 -O -S 10.129.2.200 -e tun0**. The output failed to route the target path. I knew trying different variations of this would not work as well.
2. I then went back into the HTB notes under the nmap scripting module and forgot about the script command. I realized if I use this command to scan titles/headers, I will most likely come across the OS system in the output with the firewall in place.
3. I then used the command with the script, **nmap -p 80 --script=http-title,http-headers 10.129.2.80** , and got the output I needed shown below.

```
┌─[us-academy-5]─[10.10.15.197]─[htb-ac-2120260@htb-1bnd5yzypt]─[~]
└──╼ [★]$ nmap -p 80 --script=http-title,http-headers 10.129.2.80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-10 10:21 CDT
Nmap scan report for 10.129.2.80
Host is up (0.077s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-headers:
|   Date: Wed, 10 Sep 2025 15:21:39 GMT
|   Server: Apache/2.4.29 (Ubuntu)
|   Last-Modified: Thu, 10 Sep 2020 02:14:12 GMT
|   ETag: "2c39-5aeec1fc9d59d"
|   Accept-Ranges: bytes
|   Content-Length: 11321
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
```

Image/Screenshot:



Flag 8:

Flag Answer: HTB{GoTtgUnyze9Psw4vGjcuMpHRp})

Last Command Used: sudo nmap 10.129.2.48 -T4 -p53 -sU -sV -Pn -D RND:5 -stats-every=5s -vv -n

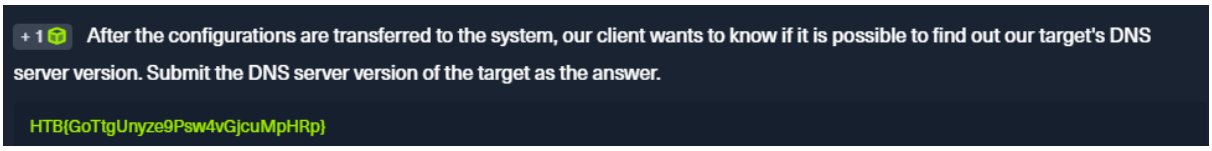
Steps:

1. I cannot lie this one stumped me. I started off with a simple non aggressive scan by using **sudo nmap -sV -p 53 10.129.2.48**. It performed the service version scan on port 53 which is DNS but, I did not get info in the output.
2. I then tried some of the HTB example prompts like **nmap -Pn -T4 -A -v -sV 10.129.2.48 -p 53 -D RND:5 --stats-every=5s**. This was more of an aggressive scan to try and find the DNS version, but again nothing related in the output.

3. I though that maybe the script command would work again like it did for me with the last one. I tried **nmap -sV --version-intensity 9 -p 53 --script dns-service-discovery 10.129.2.48**, which again was an aggressive scan. The version was still coming up blank.
4. I knew I was closer in step 2, so I went back to that command and adjusted it to now be **sudo nmap 10.129.2.48 -T4 -p53 -sU -sV -Pn -D RND:5 -stats-every=5s -vv -n**. This one worked I realized I did a TCP scan which was being blocked from the firewall, so instead I ued -sU in replace of -sV to do a UDP scan. This worked and the version was actually a flag. Here were my results:

```
─[us-academy-5]─[10.10.15.197]─[htb-ac-2120260@htb-1bnd5yzypt]─[~]
└──╼ [★]$ sudo nmap 10.129.2.48 -T4 -p53 -sU -sV -Pn -D RND:5 -stats-every=5s -vv -n

tarting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-10 10:55 CDT
SE: Loaded 46 scripts for scanning.
nitiating UDP Scan at 10:55
canning 10.129.2.48 [1 port]
iscovered open port 53/udp on 10.129.2.48
ompleted UDP Scan at 10:55, 0.16s elapsed (1 total ports)
nitiating Service scan at 10:55
canning 1 service on 10.129.2.48
tats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
ervice scan Timing: About 0.00% done
tats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
ervice scan Timing: About 0.00% done
tats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
ervice scan Timing: About 100.00% done; ETC: 10:55 (0:00:00 remaining)
ompleted Service scan at 10:55, 15.02s elapsed (1 service on 1 host)
SE: Script scanning 10.129.2.48.
SE: Starting runlevel 1 (of 2) scan.
nitiating NSE at 10:55
ompleted NSE at 10:55, 0.00s elapsed
SE: Starting runlevel 2 (of 2) scan.
nitiating NSE at 10:55
ompleted NSE at 10:55, 0.00s elapsed
map scan report for 10.129.2.48
ost is up, received user-set (0.078s latency).
canned at 2025-09-10 10:55:44 CDT for 15s

ORT   STATE SERVICE REASON              VERSION
3/udp open  domain  udp-response ttl 63 (unknown banner: HTB{GoTtgUnyze9Psw4vGicuMpHRp})
 service unrecognized despite returning data. If you know the service/version, please submi
g/cgi-bin/submit.cgi?new-service :
F-Port53-UDP:V=7.94SVN%I=7%D=9/10%Time=68C19F85%P=x86_64-pc-linux-gnu%r(D
```

Image/Screenshot:



Flag 9:

Flag Answer: HTB{kjnsdf2n982n1827eh76238s98di1w6}

Last Command Used: sudo netcat -p 53 10.129.27.142 50000

Steps:

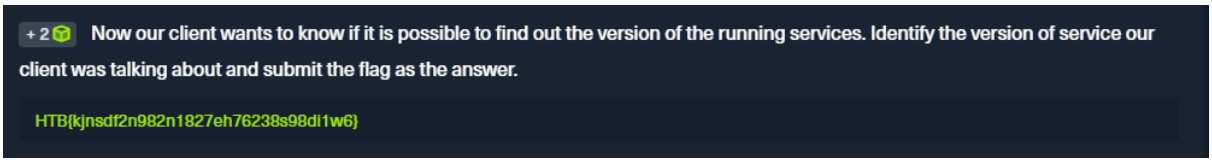
1. I started with doing a scan for both TCP And UDP by doing **nmap -sV -sC -p- 10.129.27.142**. This scanned all of the ports, the only result I got was port 22 and port 80.
2. I tried to scan these individually why doing commands like **nmap -sS -sV -p- --source-port 80 10.129.27.142**. I even tried different variations of this on both 22 and 80. Still got nothing useful. I fell down a bit of a rabbit hole here thinking that the flag was in one of these ports. I was wrong.
3. After about an hour of trying different scans, I asked for help from fellow classmate Alessio because I knew that these two ports are too obvious. It had to be a higher one that was suspicious. I couldn't find the right combination of tacks to get there. He hinted that port 53 was important again here because it's the standard port for DNS.
4. I then after troubleshooting a lot finally came up with this command **sudo nmap -sS -sV -Pn -n --source-port 53 -p- 10.129.27.142**. I ended up adding -n to reverse DNS search and it gave me a new port to discover, port 50000. Here is what the output looked like:

```
┌─[us-academy-5]─[10.10.15.197]─[htb-ac-2120260@htb-ps0srbun7d]─[~]
└──╼ [★]$ sudo nmap -sS -sV -Pn -n --source-port 53 -p- 10.129.27.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-10 13:30 CDT
Nmap scan report for 10.129.27.142
Host is up (0.078s latency).
Not shown: 64562 closed tcp ports (reset), 970 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protoc
ol 2.0)
80/tcp    open  http       Apache httpd 2.4.29 ((Ubuntu))
50000/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

5. **After I found port 50000 which was TCP, I knew I had to use a new tool to scan it. I searched up different tools I could use and Netcat was the first to work. I did sudo netcat -p 53 10.129.27.142 50000. Netcat let me create a connection and try to bypass a firewall that's blocking automated scans. Therefore, I then got the flag as shown below:**

```
┌─[us-academy-5]─[10.10.15.197]─[htb-ac-2120260@htb-ps0srbun7d]─[~]
└──╼ [★]$ sudo netcat -p 53 10.129.27.142 50000
220 HTB{kjnsdf2n982n1827eh76238s98di1w6}
421 Login timeout (300 seconds): closing control connection
```

Image/Screenshot:



Summary

Overall, I think that if I had more notes on using Nmap commands, I would have breezed through this a bit faster than I wanted to. This HTB taught me that I definitely need to spend more time doing Nmap scans, especially when you have to bypass things like firewalls. Some parts were easy, and some that really got me thinking. I was always on the right track, but was always missing a small piece to get the command to find what I needed.