Network Enumeration with Nmap:

Link to challenge: https://academy.hackthebox.com/module/19

(log in required)

Class: Tier I | Easy | Offensive

Host Enumeration

Host Discovery:

Question: Based on the last result, find out which operating system it belongs to. Submit the name of the operating system as result.

Answer: Windows

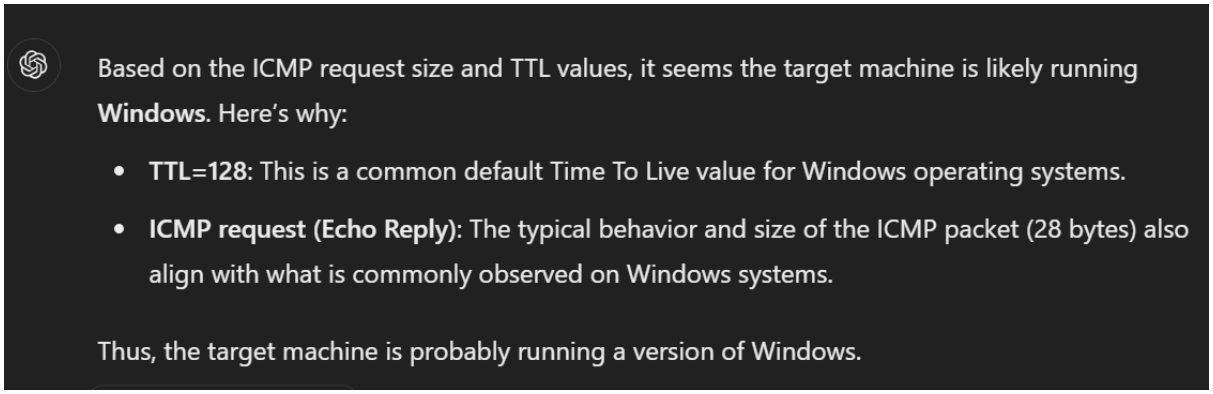
Method: lets take a look at the nmap scan:

```
amit9676@htb[/htb]$ sudo nmap 10.129.2.18 -sn -oA host -PE --packet-trace --disable-arp-ping

Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-15 00:12 CEST
SENT (0.0107s) ICMP [10.10.14.2 > 10.129.2.18 Echo request (type=8/code=0) id=13607 seq=0] IP [ttl=255 id=23541 iplen=28 ]
RCVD (0.0152s) ICMP [10.129.2.18 > 10.10.14.2 Echo reply (type=0/code=0) id=13607 seq=0] IP [ttl=128 id=40622 iplen=28 ]
Nmap scan report for 10.129.2.18
Host is up (0.086s latency).
MAC Address: DE:AD:00:00:BE:EF
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

The TTL (time to live) value of the response packet is 128, mostly associated with windows. Also the packet size is 28 bytes.

*Source: ChatGPT:



Host and Port Scanning:

Question: Find all TCP ports on your target. Submit the total number of found TCP ports as the answer.

Answer: 7

Method: we will use the command:

```
nmap <target-IP> -p- | grep "open" | wc -l
```

```
┌[eu-academy-2]-[10.10.14.129]-[htb-ac-1099135@htb-k5zwn
└─[★]$ nmap 10.129.86.139 -p- | grep "open" | wc -l
7
```

(we count the amount of lines where the word 'open' is mentioned)

Question: Enumerate the hostname of your target and submit it as the answer. (case-sensitive)

Answer: NIX-NMAP-DEFAULT

Method: we will run the command:

```
nmap <target-IP> -sV -sC | grep host -i
```

```
┌[eu-academy-2]-[10.10.14.129]-[htb-ac-1099135@htb-k5zwnzhogy]-[~]
└─[★]$ nmap 10.129.86.139 -sV -sC | grep host -i
Host is up (0.0099s latency).
| ssh-hostkey:
Service Info: Host: NIX-NMAP-DEFAULT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
Nmap done: 1 IP address (1 host up) scanned in 178.22 seconds
```

Saving the Results:

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

Answer: 31337

Method: lets run the scan:

```
sudo nmap <target-IP> -p- -oA target
```

where '-oA' outputs the scan result to a file called 'target':

```
┌─[eu-academy-2]─[10.10.14.129]─[htb-ac-1099135@htb-k5zwnzhogy]─[~]
└──╼ [★]$ sudo nmap 10.129.86.139 -p- -oA target
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 14:24 CDT
Nmap scan report for 10.129.86.139
Host is up (0.0089s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
31337/tcp open  Elite
```

While we can determine the highest port already, lets get it to HTML report:

One of the output files from the scan is 'target.xml':

```
┌─[eu-academy-2]─[10.10.14.129]─[htb-ac
└──╼ [★]$ ls target.*
target.gnmap  target.nmap  target.xml
```

Lets get it to html document with the tool 'xsltproc':

```
xsltproc target.xml -o target.html
```

```
┌[eu-academy-2]-[10.10.14.129]-[htb-ac-10991
└─► [★]$ xsltproc target.xml -o target.html
┌[eu-academy-2]-[10.10.14.129]-[htb-ac-10991
└─► [★]$ ls target.html
target.html
```

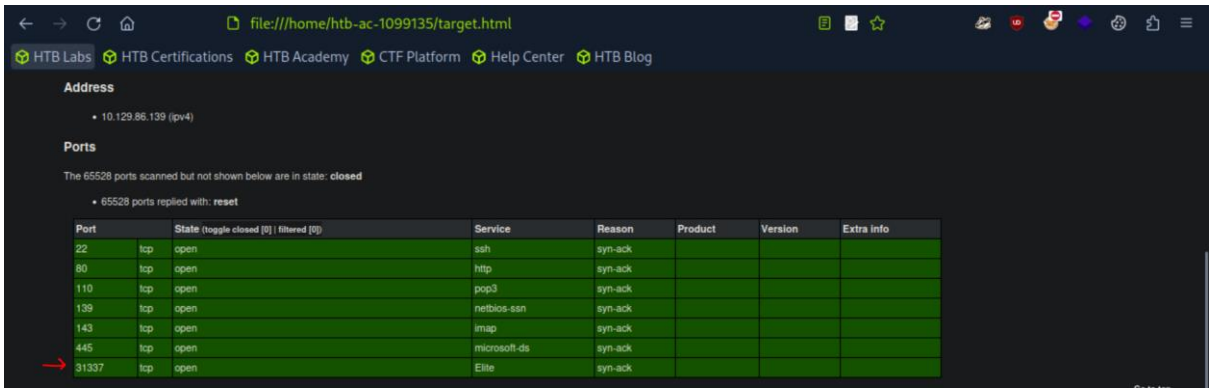
Now lets open the report on the browser. We will need the file's full path:

```
realpath target.html
```

```
┌[eu-academy-2]-[10.10.14.129]-[
└─► [★]$ realpath target.html
/home/htb-ac-1099135/target.html
```

Now lets enter in the browser URL:

```
/home/htb-ac-1099135/target.html
```



Service Enumeration:

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

Answer: HTB{pr0F7pDv3r510nb4nn3r}

Method: we will run the command:

```
nmap 10.129.86.139 -p- -sV -sC
```

where '-sV' and '-sC' performs extra investigation on the service, including among others: version detection, information obtaining and banner grabbing.

'-p-' assures the scan is performed on all ports.:

```
┌─[eu-academy-2]─[10.10.14.129]─[htb-ac-1099135@htb-k5zwnzhogy]─[~]
└──╼ [★]$ nmap 10.129.86.139 -p- -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 14:11 CDT
Nmap scan report for 10.129.86.139
```

*

*

```
31337/tcp open  Elite?
| fingerprint-strings:
|   GetRequest, SIPOptions:
|_    220 HTB{pr0F7pDv3r510nb4nn3r} <-
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?r
ew-service :
SF-Port31337-TCP:V=7.94SVN%I=7%D=9/16%Time=66E8830A%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,1F,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n")%r(SIPOptions,1F
SF:,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n");
Service Info: Host: NIX-NMAP-DEFAULT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The flag will appear on port 31337 'elite' service scan.

Nmap Scripting Engine:

Question: Use NSE and its scripts to find the flag that one of the services contain and submit it as the answer.

Answer: HTB{873nniuc71bu6usbs1i96as6dsv26}

Method: Lets run nmap vulnerability scan on the target machine port 80 (http):

```
sudo nmap <target-IP> -p 80 -sV --script vuln
```

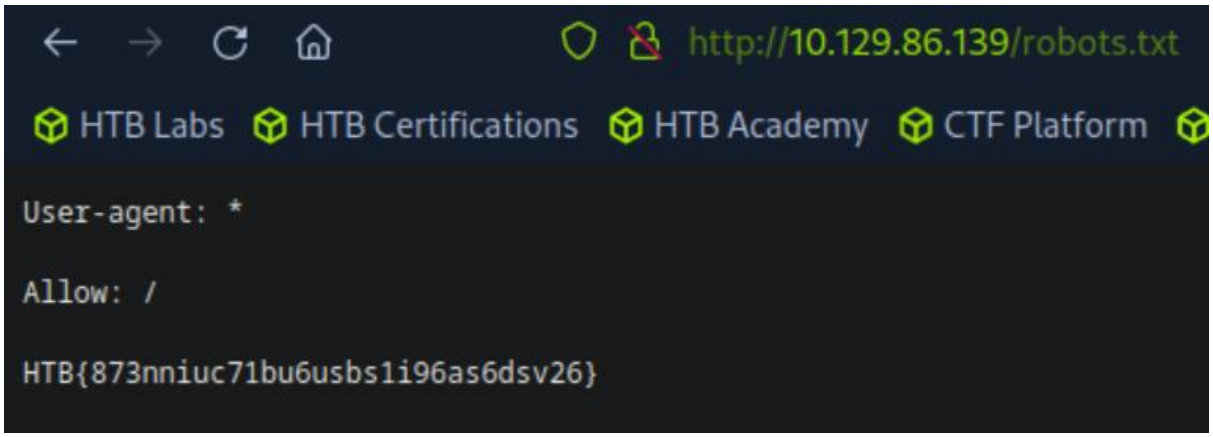
```
┌[eu-academy-2]-[10.10.14.129]-[htb-ac-1099135@htb-k5zwnzhogy]-[~]
└──╼ [★]$ sudo nmap 10.129.86.139 -p 80 -sV --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 15:03 CDT
Nmap scan report for 10.129.86.139
Host is up (0.26s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-enum:
|_  /robots.txt: Robots file ←
| http-csrf: Couldn't find any CSRF vulnerabilities
```

We see the existence of 'robots.txt' file (instructions page for web-crawlers).

Lets take a look in it:

```
http://<target-IP>/robots.txt
```



Bypass Security Measures

Firewall and IDS/IPS Evasion - Easy Lab:

Question: Our client wants to know if we can identify which operating system their provided machine is running on. Submit the OS name as the answer.

Answer: Ubuntu

Method: in principal, the command:

```
nmap <target-IP> -sV
```

will get the results:

```
┌─[eu-academy-2]─[10.10.14.125]─[htb-ac-1099135@htb-ak8oa2nvpp]─[~]
└──╼ [★]$ nmap 10.129.236.28 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 11:34 CDT
Nmap scan report for 10.129.236.28
Host is up (0.0084s latency).
Not shown: 869 closed tcp ports (reset), 128 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol
2.0)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
10001/tcp open  ftp     ProFTPD
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 68.39 seconds
```

However we wish to perform stealthy scan to raise a little alert as possible, we will use the command:

```
sudo nmap <target-IP> -p 22 -sV -D RND:5 --disable-arp-ping
-Pn -e tun0
```

```
┌──[eu-academy-2]─[10.10.14.125]─[htb-ac-1099135@htb-ak8oa2nvpp]─[~]
└──╼ [★]$ sudo nmap 10.129.236.28 -p 22 -sV -D RND:5 --disable-arp-ping -Pn -e tun0
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 11:53 CDT
Nmap scan report for 10.129.236.28
Host is up (0.0085s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
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 13.24 seconds
```

Where we run stealth scan againt ssh port 22, with the following features:

Command Breakdown:

- `sudo nmap 10.129.236.28`: The target IP address (requires `sudo` for certain privileges).
- `-p 22`: Specifies that only port 22 (typically used for SSH) will be scanned.
- `-sV`: Enables service version detection on the specified port (to determine what service and version are running on port 22).
- `-D RND:5`: This is decoy scanning. Nmap will spoof 5 random IP addresses as decoys, making it harder for the target to know your real IP.
- `--disable-arp-ping`: Disables ARP ping for host discovery (useful on networks where ARP might trigger detection).
- `-Pn`: Tells Nmap to skip the host discovery step (Nmap will assume the host is up and proceed with scanning, avoiding ping requests).
- `-e tun0`: Specifies to use the `tun0` interface (typically used in VPNs or for tunneling).

Basically we employ decoy tactics to make the real scan less suspicious.

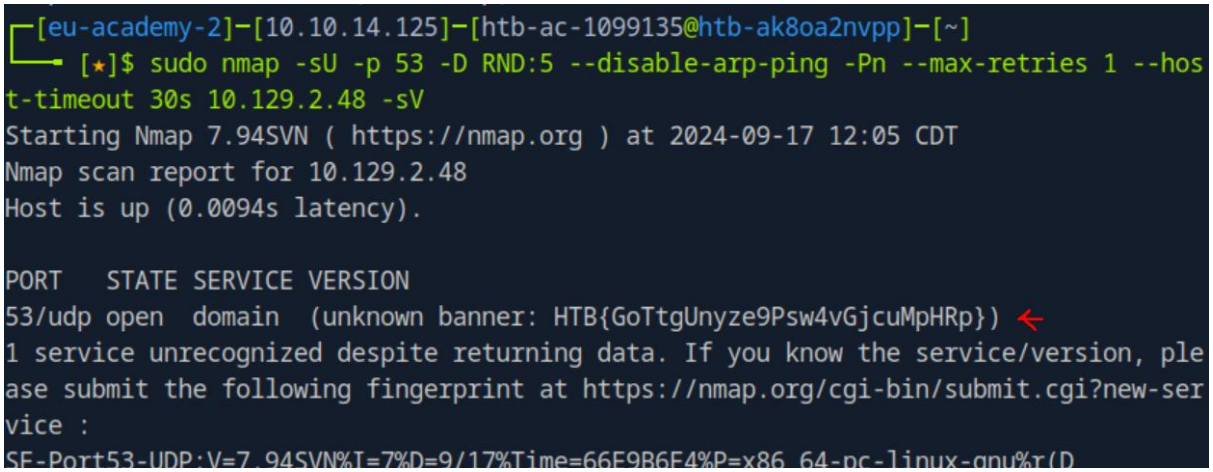
Firewall and IDS/IPS Evasion - Medium Lab:

Question: After the configurations are transferred to the system, our client wants to know if it is possible to find out our target's DNS server version. Submit the DNS server version of the target as the answer.

Answer: HTB{GoTtgUnyze9Psw4vGjcuMpHRp}

Method: we will run the following command:

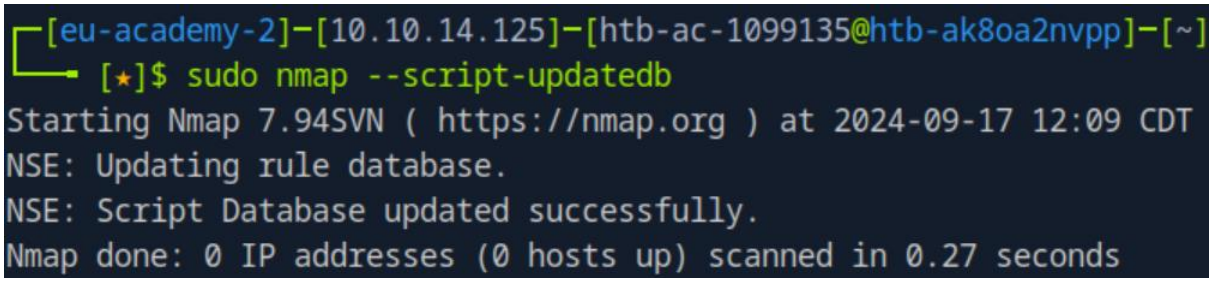
```
sudo nmap -sU -p 53 -D RND:5 --disable-arp-ping -Pn --max-retries 1 --host-timeout <target-IP> -sV
```



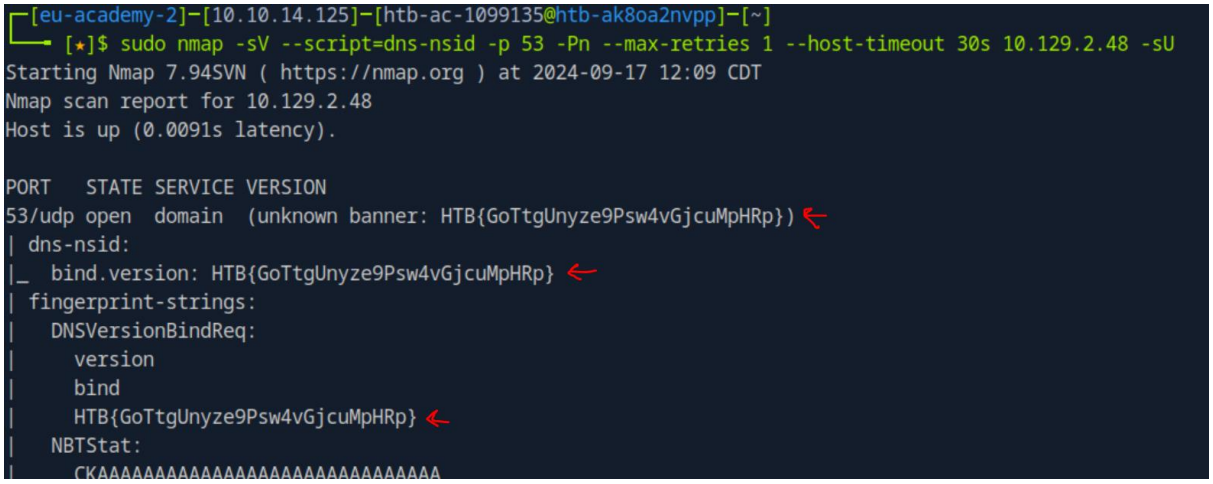
In addition to the stealth parameters, we will scan for UDP ('-sU'), and for versions ('-sV').

The sequence of command will also work:

```
sudo nmap --script-updatedb;
sudo nmap -sV --script=dns-nsid -p 53 -Pn --max-retries 1 --host-timeout 30s <target-IP> -sU;
```



update the nmap script database


[eu-academy-2]-[10.10.14.125]-[htb-ac-1099135@htb-ak8oa2nvpp]-[~]
[★]$ sudo nmap -sV --script=dns-nsid -p 53 -Pn --max-retries 1 --host-timeout 30s 10.129.2.48 -sU
Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-17 12:09 CDT
Nmap scan report for 10.129.2.48
Host is up (0.0091s latency).
PORT STATE SERVICE VERSION
53/udp open domain (unknown banner: HTB{GoTtgUnyze9Psw4vGjcuMpHRp})
| dns-nsid:
|_ bind.version: HTB{GoTtgUnyze9Psw4vGjcuMpHRp}
| fingerprint-strings:
| DNSVersionBindReq:
| version
| bind
| HTB{GoTtgUnyze9Psw4vGjcuMpHRp}
| NBTStat:

Firewall and IDS/IPS Evasion - Hard Lab:

Question: Now our client wants to know if it is possible to find out the version of the running services. Identify the version of service our client was talking about and submit the flag as the answer.

Answer: HTB{kjnsdf2n982n1827eh76238s98di1w6}

Method: we will adhere to the module section's 'Firewall and IDS/IPS Evasion' and the question's hint suggestion to scan target port 50000 from our source port 53:

```
sudo nmap <target-IP> -p 50000 -sS -Pn -n --disable-arp-ping
--packet-trace --source-port 53
```

```
┌[eu-academy-2]─[10.10.14.125]─[htb-ac-1099135@htb-ak8oa2nvpp]─[~]
└──╼ [★]$ sudo nmap 10.129.235.210 -p 50000 -sS -Pn -n --disable-arp-ping --packet-trace --source-port 53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:06 CDT
SENT (0.0305s) TCP 10.10.14.125:53 > 10.129.235.210:50000 S ttl=47 id=53773 iplen=44  seq=4088894309 win=1024 <mss 1460>
RCVD (0.0388s) TCP 10.129.235.210:50000 > 10.10.14.125:53 SA ttl=63 id=0 iplen=44  seq=103102736 win=64240 <mss 1362>
Nmap scan report for 10.129.235.210
Host is up (0.0085s latency).

PORT      STATE SERVICE
50000/tcp open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

*note – not including source port 53 will not work, due to the assumption the target port is expecting traffic from DNS service only. (due to firewall/IDS/IPS rule.

For forther reading from the 'Firewall and IDS/IPS Evasion' section:

DNS Proxying

By default, `Nmap` performs a reverse DNS resolution unless otherwise specified to find more important information about our target. These DNS queries are also passed in most cases because the given web server is supposed to be found and visited. The DNS queries are made over the `UDP port 53`. The `TCP port 53` was previously only used for the so-called "`Zone transfers`" between the DNS servers or data transfer larger than 512 bytes. More and more, this is changing due to IPv6 and DNSSEC expansions. These changes cause many DNS requests to be made via TCP port 53.

However, `Nmap` still gives us a way to specify DNS servers ourselves (`--dns-server <ns>,<ns>`). This method could be fundamental to us if we are in a demilitarized zone (`DMZ`). The company's DNS servers are usually more trusted than those from the Internet. So, for example, we could use them to interact with the hosts of the internal network. As another example, we can use `TCP port 53` as a source port (`--source-port`) for our scans. If the administrator uses the firewall to control this port and does not filter IDS/IPS properly, our TCP packets will be trusted and passed through.

*

Anyway as we established port 50000 is open – lets perform banner grabbing:

```
sudo ncat -nv --source-port 53 10.129.235.210 50000
```

*dont forget sudo as the source port is privileged one. *

```
┌─[eu-academy-2]─[10.10.14.125]─[htb-ac-1099135@htb-ak8oa2nvpp]─[~]
└──╼ [★]$ sudo ncat -nv --source-port 53 10.129.235.210 50000
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
Ncat: Connected to 10.129.235.210:50000.
220 HTB{kjnsdf2n982n1827eh76238s98di1w6}
```