

## NETWORK ENUMERATION WITH NMAP

### 1.1 Enumeration

Enumeration is about gathering much information as possible on a target, it's the most critical as its about finding ways we could attack a target. And it's not about the tools used but about the services, how it works making it easy in gathering information to use.

### 1.2 Host discovery

In host discovery Nmap can scan network range, single host scan, List of hosts scan and multiple host scan. And in each there is disabling of port scans with `-sn`, so as to discover live hosts. And using ICMP echo requests (`-PE`) in the scans it effective to get live hosts.

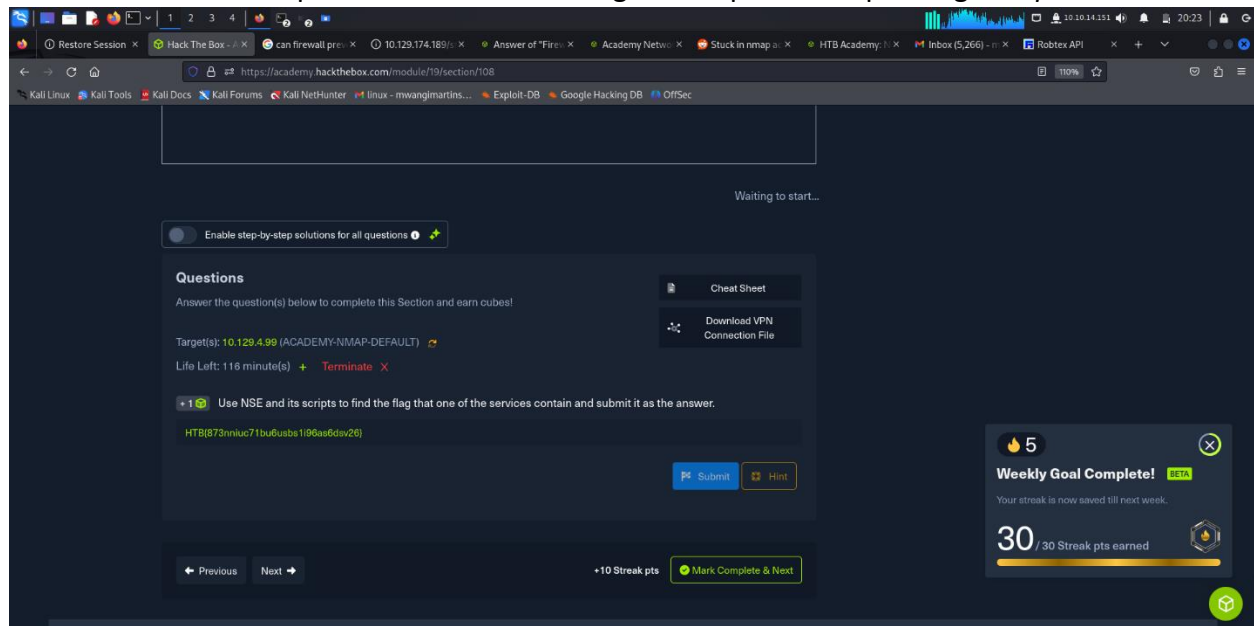
### 1.3 Service Enumeration

Using the option `-sV` we can find the version of the services. Nmap looks at the banners of the scanned ports and prints them out through identifying versions if it cannot find on versions, Nmap attempts to identify them through a signature-based matching system.

Some services do not immediately provide such information so using *Netcat* to listen on a port we can grab banners, and intercepting this traffic with *tcpdump* we can get more information on the service.

### 1.4 Scripting Engine

We can define the scripts either in default using `-sC` or specific script using `--script`



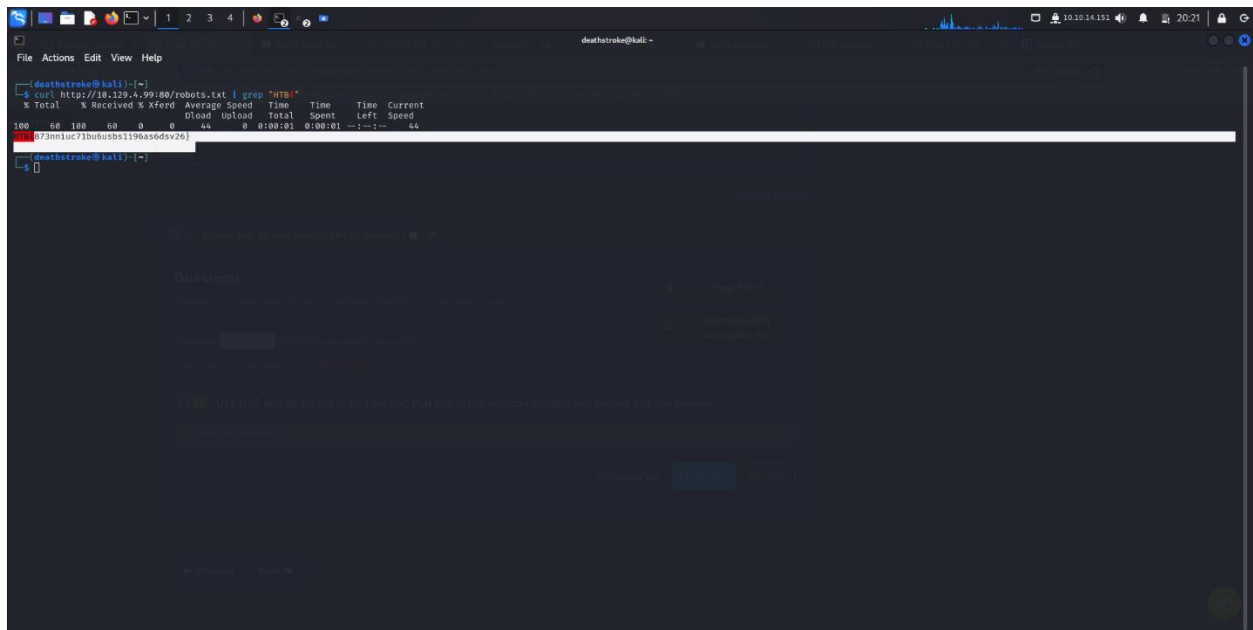
Used the NSE scripts in Nmap, that is script vuln to check for vulnerabilities,

```
File Actions Edit View Help
[deathstroke@kali:~]$ sudo nmap 10.129.2.49 -sV --script vuln --p- -sS -T4
[sudo] password for deathstroke:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 19:42 EAT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.80% done
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.80% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.80% done
Warning: 10.129.2.49 giving up on port because retransmission cap hit (6).
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.09% done; ETC: 20:01 (0:09:16 remaining)
Nmap scan report for 10.129.2.49
Host is up (0.19s latency).
Not shown: 65485 closed tcp ports (reset), 43 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu7.7 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/o:openbsd:openssh:7.6p1
| 9549236-C9FE-5A6A-9D7D-E943A248633A 10.0 https://vulners.com/githubexploit/9549236-C9FE-5A6A-9D7D-E943A248633A *EXPLOIT*
| 2C19FFA-EC0B-5E1A-AA4A-35A42C38071A 10.0 https://vulners.com/githubexploit/2C19FFA-EC0B-5E1A-AA4A-35A42C38071A *EXPLOIT*
| CVE-2023-28408 9.8 https://vulners.com/cve/CVE-2023-28408
| B0190C0B-1E9F-5631-9828-B06A15758223 9.8 https://vulners.com/githubexploit/B0190C0B-1E9F-5631-9828-B06A15758223 *EXPLOIT*
| 8F0C5A8B-3968-5F3C-823E-ED085379A623 9.8 https://vulners.com/githubexploit/8F0C5A8B-3968-5F3C-823E-ED085379A623 *EXPLOIT*
| 80A01159-548E-4A87-2DE69F922EC 9.8 https://vulners.com/githubexploit/80A01159-548E-4A8E-4A87-2DE69F922EC *EXPLOIT*
| 5E69688A-0806-57FA-BF6E-D09221D0827A 9.8 https://vulners.com/githubexploit/5E69688A-0806-57FA-BF6E-D09221D0827A *EXPLOIT*
| CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
| 55V92378 7.5 https://vulners.com/semhub/55V92378 *EXPLOIT*
| PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
| F0979183-AE88-5384-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-5384-86CF-3AF0523F3807 *EXPLOIT*
| 1337DAY-ID-26376 7.5 https://vulners.com/zdt/1337DAY-ID-26376 *EXPLOIT*
| CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617
| EDB-ID:46516 6.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
| EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
| CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
| CVE-2019-5189 6.8 https://vulners.com/cve/CVE-2019-5189
| C9A132FD-1F45-5342-86EF-B0AFA5EEFF63 6.8 https://vulners.com/githubexploit/C9A132FD-1F45-5342-86EF-B0AFA5EEFF63 *EXPLOIT*
| 1021308E-F683-3531-73626207 6.8 https://vulners.com/githubexploit/1021308E-F683-3531-73626207 *EXPLOIT*
| CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
| CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145
| CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111
| EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 *EXPLOIT*
| 1337DAY-ID-23228 5.8 https://vulners.com/zdt/1337DAY-ID-23228
| 1337DAY-ID-32089 5.8 https://vulners.com/zdt/1337DAY-ID-32089 *EXPLOIT*
| EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 *EXPLOIT*
| PACKETSTORM:181223 5.3 https://vulners.com/packetstorm/PACKETSTORM:181223 *EXPLOIT*
| MSF-AUXILIARY-SCANNER-SSH-SM_ENUMUSERS- 5.3 https://vulners.com/metasploit/MSF-AUXILIARY-SCANNER-SSH-SM_ENUMUSERS- *EXPLOIT*
| EDB-ID:45939 5.3 https://vulners.com/exploitdb/EDB-ID:45939 *EXPLOIT*
| EDB-ID:45233 5.3 https://vulners.com/exploitdb/EDB-ID:45233 *EXPLOIT*
| CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685
```

From the output found various vulnerabilities, among them were vulnerabilities of services running port 80,

```
File Actions Edit View Help
[deathstroke@kali:~]$ sudo nmap 10.129.2.49 -sV --script vuln --p- -sS -T4
[sudo] password for deathstroke:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 19:42 EAT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.80% done
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.80% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.80% done
Warning: 10.129.2.49 giving up on port because retransmission cap hit (6).
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.09% done; ETC: 20:01 (0:09:16 remaining)
Nmap scan report for 10.129.2.49
Host is up (0.19s latency).
Not shown: 65485 closed tcp ports (reset), 43 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu7.7 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/o:openbsd:openssh:7.6p1
| 9549236-C9FE-5A6A-9D7D-E943A248633A 10.0 https://vulners.com/githubexploit/9549236-C9FE-5A6A-9D7D-E943A248633A *EXPLOIT*
| 2C19FFA-EC0B-5E1A-AA4A-35A42C38071A 10.0 https://vulners.com/githubexploit/2C19FFA-EC0B-5E1A-AA4A-35A42C38071A *EXPLOIT*
| CVE-2023-28408 9.8 https://vulners.com/cve/CVE-2023-28408
| B0190C0B-1E9F-5631-9828-B06A15758223 9.8 https://vulners.com/githubexploit/B0190C0B-1E9F-5631-9828-B06A15758223 *EXPLOIT*
| 8F0C5A8B-3968-5F3C-823E-ED085379A623 9.8 https://vulners.com/githubexploit/8F0C5A8B-3968-5F3C-823E-ED085379A623 *EXPLOIT*
| 80A01159-548E-4A87-2DE69F922EC 9.8 https://vulners.com/githubexploit/80A01159-548E-4A8E-4A87-2DE69F922EC *EXPLOIT*
| 5E69688A-0806-57FA-BF6E-D09221D0827A 9.8 https://vulners.com/githubexploit/5E69688A-0806-57FA-BF6E-D09221D0827A *EXPLOIT*
| CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
| 55V92378 7.5 https://vulners.com/semhub/55V92378 *EXPLOIT*
| PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
| F0979183-AE88-5384-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-5384-86CF-3AF0523F3807 *EXPLOIT*
| 1337DAY-ID-26376 7.5 https://vulners.com/zdt/1337DAY-ID-26376 *EXPLOIT*
| CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617
| EDB-ID:46516 6.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
| EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
| CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
| CVE-2019-5189 6.8 https://vulners.com/cve/CVE-2019-5189
| C9A132FD-1F45-5342-86EF-B0AFA5EEFF63 6.8 https://vulners.com/githubexploit/C9A132FD-1F45-5342-86EF-B0AFA5EEFF63 *EXPLOIT*
| 1021308E-F683-3531-73626207 6.8 https://vulners.com/githubexploit/1021308E-F683-3531-73626207 *EXPLOIT*
| CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
| CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145
| CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111
| EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 *EXPLOIT*
| 1337DAY-ID-23228 5.8 https://vulners.com/zdt/1337DAY-ID-23228
| 1337DAY-ID-32089 5.8 https://vulners.com/zdt/1337DAY-ID-32089 *EXPLOIT*
| EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5338EA02E0BE458FC90600097F9E97 *EXPLOIT*
| PACKETSTORM:181223 5.3 https://vulners.com/packetstorm/PACKETSTORM:181223 *EXPLOIT*
| MSF-AUXILIARY-SCANNER-SSH-SM_ENUMUSERS- 5.3 https://vulners.com/metasploit/MSF-AUXILIARY-SCANNER-SSH-SM_ENUMUSERS- *EXPLOIT*
| EDB-ID:45939 5.3 https://vulners.com/exploitdb/EDB-ID:45939 *EXPLOIT*
| EDB-ID:45233 5.3 https://vulners.com/exploitdb/EDB-ID:45233 *EXPLOIT*
| CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685
| http-nmap:
| /robots.txt: Robots file
| 130/tcp  open  pop3     Dovecot pop3d
| 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| 143/tcp  open  imap     Dovecot imapd (Ubuntu)
| 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| 31337/tcp open  ftp      ProFTPD
Service Info: Host: NIX-NMAP-DEFAULT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-051: false
|_ smb-vuln-regsvc-dos:
|   VULNERABLE!
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|   State: VULNERABLE
|   The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowers while working on smb-enum-sessions.
|   Roblox Free API
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1254.81 seconds
```

Using curl with target IP and port 80, grepping the part of the flag, I got the flag,



```
deathstroke@kali:~$ curl http://10.129.4.99:80/robots.txt | grep "HTB"
100  60  100  60  0  0  44  0  0:00:01  0:00:01  --:--:--  44
[73m1uCF2buus0s1190as0dsV20]
```

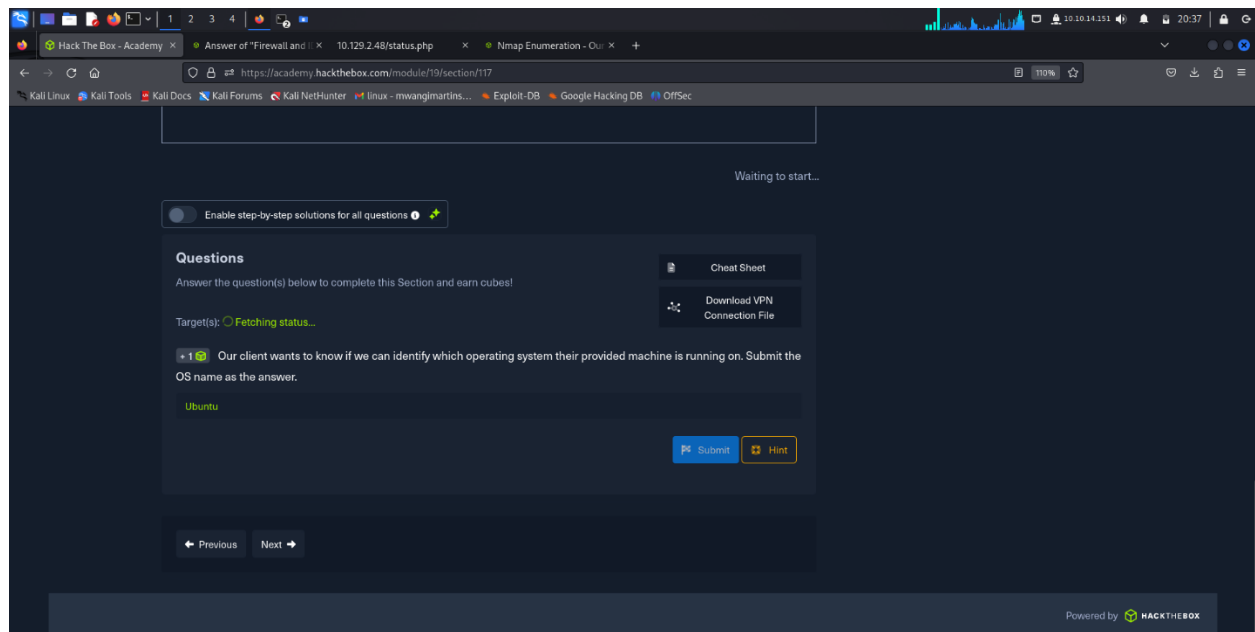
## 1.5 Firewall and IPS/IDS Evasion Easy Lab

### Scenario

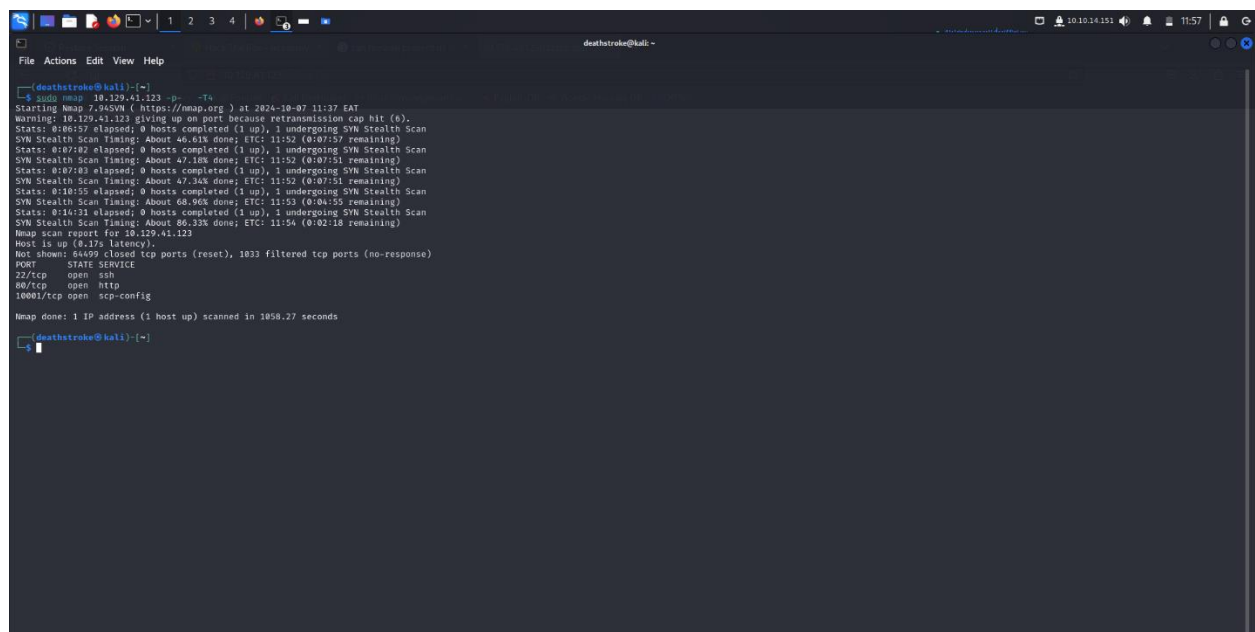
A company hired us to test their IT security defenses, including their IDS and IPS systems. Our client wants to increase their IT security and will, therefore, make specific improvements to their IDS/IPS systems after each successful test. We do not know, however, according to which guidelines these changes will be made. Our goal is to find out specific information from the given situations.

To evade firewall/IDS/IPS you can use either SYN scan (-sS) which is stealthy or TCP-ACK scan (-sA) which hard to filtered,

### Questions



Started off by checking the ports that I was working with



From this output port 22,80 could both give information of the Operating System they are running on choose to go with port 22 for ssh, and using SYN Scan(-sS),

Used -sS to send SYN packets to the target, and used --packet-trace to view the packets being sent and received.

Viewing the Nmap output there was a SYN packet sent to port 22, ssh and target responded with a SA which is SYN-ACK packet, as it was trying to establish a TCP connection,

```
File Actions Edit View Help
deathstroke@kali: ~
NSE: TCP 10.10.14.151:1822 > 10.129.41.123:22 | CLOSE
Nsock INFO [3.2150s] nsock_io_delete(): nsock_io_delete (IOO #2)
Nsock INFO [3.2150s] nsock_io_delete(): nsock_io_delete (IOO #1)
Nsock INFO [3.2150s] nsock_io_delete(): nsock_io_delete (IOO #3)
Nsock INFO [3.2390s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOO #3) EID 56
Nsock INFO [3.2390s] nsock_bind_addr(): binding to 0.0.0.0:81822 (IOO #3)
Nsock INFO [3.4020s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 56 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1822 > 10.129.41.123:22 | CONNECT
Nsock INFO [3.4080s] nsock_sendto(): Sendto request for 44 bytes to IOO #3 EID 67 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1822 > 10.129.41.123:22 | 00000000: 00 00 00 28 49 5f d4 47 00 00 00 00 00 00 02 (1_G
00000010: 00 01 86 00 00 00 00 00 00 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nsock INFO [3.4080s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 67 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1822 > 10.129.41.123:22 | SEND
Nsock INFO [3.4180s] nsock_read(): Read request from IOO #3 [10.129.41.123:22] (timeout: 1853ms) EID 74
Nsock INFO [3.5080s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 74 [10.129.41.123:22] (41 bytes): SSH-2.0-OpenSSH_7.6p1 Ubuntu-kubuntub.7..
NSE: TCP 10.10.14.151:1822 < 10.129.41.123:22 | SSH-2.0-OpenSSH_7.6p1 Ubuntu-kubuntub.7
Nsock INFO [3.5080s] nsock_read(): Read request from IOO #3 [10.129.41.123:22] (timeout: 1853ms) EID 82
Nsock INFO [3.4370s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 82 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1822 > 10.129.41.123:22 | CLOSE
Nsock INFO [5.4410s] nsock_io_delete(): nsock_io_delete (IOO #3)
Nmap scan report for 10.129.41.123
Host is up (0.16s latency).

PORT      STATE      SERVICE VERSION
22/tcp    unfiltered ssh

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds

deathstroke@kali:~$ sudo nmap -sS 10.129.41.123 -p 22 -n --packet-trace --disable-arp-ping -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 11:16 EAT
SENT (0.3338s) TCP 10.10.14.151:55824 > 10.129.41.123:22 S ttl=43 id=17839 iplen=44 seq=1164892419 win=1024 cwnd 1460>
RVD (0.5099s) TCP 10.129.41.123:22 > 10.10.14.151:55824 SA ttl=63 id=0 iplen=44 seq=3459286696 win=64240 cwnd 1340>
Nsock INFO [0.7220s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOO #1) EID 8
Nsock INFO [0.7230s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [10.129.41.123:22]
Service scan sending probe NULL to 10.129.41.123:22 (tcp)
Nsock INFO [0.9000s] nsock_read(): Read request from IOO #1 [10.129.41.123:22] (timeout: 6000ms) EID 18
Nsock INFO [1.0710s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [10.129.41.123:22] (41 bytes): SSH-2.0-OpenSSH_7.6p1 Ubuntu-kubuntub.7..
Service scan hard match (Probe NULL matched with NULL line 3524): 10.129.41.123:22 is ssh. Version: [OpenSSH]7.6p1 Ubuntu-kubuntub.7[Ubuntu Linux; protocol 2.0]
Nsock INFO [1.0710s] nsock_io_delete(): nsock_io_delete (IOO #1)
Nsock INFO [1.1180s] nsock_connect_tcp(): UDP connection requested to 10.129.41.123:1434 (IOO #1) EID 8
Nsock INFO [1.1310s] nsock_io_new2(): nsock_io_new (IOO #2)
Nsock INFO [1.1320s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOO #2) EID 16
Nsock INFO [1.1320s] nsock_io_new2(): nsock_io_new (IOO #3)
Nsock INFO [1.1360s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOO #3) EID 24
Nsock INFO [1.1360s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [10.129.41.123:1434]
```

Nmap looks at the banners of the scanned ports and prints them out, in this scan it was to grab a banner that gave more information about the service, that is its version and the OS it was running on.

```
File Actions Edit View Help
deathstroke@kali: ~
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Nsock INFO [3.4080s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 67 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1822 > 10.129.41.123:22 | SEND
Nsock INFO [3.4180s] nsock_read(): Read request from IOO #3 [10.129.41.123:22] (timeout: 1853ms) EID 74
Nsock INFO [3.5080s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 74 [10.129.41.123:22] (41 bytes): SSH-2.0-OpenSSH_7.6p1 Ubuntu-kubuntub.7..
NSE: TCP 10.10.14.151:1822 < 10.129.41.123:22 | SSH-2.0-OpenSSH_7.6p1 Ubuntu-kubuntub.7
Nsock INFO [3.5080s] nsock_read(): Read request from IOO #3 [10.129.41.123:22] (timeout: 1853ms) EID 82
Nsock INFO [3.4370s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 82 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1822 > 10.129.41.123:22 | CLOSE
Nsock INFO [5.4410s] nsock_io_delete(): nsock_io_delete (IOO #3)
Nmap scan report for 10.129.41.123
Host is up (0.16s latency).

PORT      STATE      SERVICE VERSION
22/tcp    unfiltered ssh

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds

deathstroke@kali:~$ sudo nmap -sS 10.129.41.123 -p 22 -n --packet-trace --disable-arp-ping -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 11:16 EAT
SENT (0.3338s) TCP 10.10.14.151:55824 > 10.129.41.123:22 S ttl=43 id=17839 iplen=44 seq=1164892419 win=1024 cwnd 1460>
RVD (0.5099s) TCP 10.129.41.123:22 > 10.10.14.151:55824 SA ttl=63 id=0 iplen=44 seq=3459286696 win=64240 cwnd 1340>
Nsock INFO [0.7220s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOO #1) EID 8
Nsock INFO [0.7230s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [10.129.41.123:22]
Service scan sending probe NULL to 10.129.41.123:22 (tcp)
Nsock INFO [0.9000s] nsock_read(): Read request from IOO #1 [10.129.41.123:22] (timeout: 6000ms) EID 18
Nsock INFO [1.0710s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [10.129.41.123:22] (41 bytes): SSH-2.0-OpenSSH_7.6p1 Ubuntu-kubuntub.7..
Service scan hard match (Probe NULL matched with NULL line 3524): 10.129.41.123:22 is ssh. Version: [OpenSSH]7.6p1 Ubuntu-kubuntub.7[Ubuntu Linux; protocol 2.0]
Nsock INFO [1.0710s] nsock_io_delete(): nsock_io_delete (IOO #1)
Nsock INFO [1.1180s] nsock_connect_tcp(): UDP connection requested to 10.129.41.123:1434 (IOO #1) EID 8
Nsock INFO [1.1310s] nsock_io_new2(): nsock_io_new (IOO #2)
Nsock INFO [1.1320s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOO #2) EID 16
Nsock INFO [1.1320s] nsock_io_new2(): nsock_io_new (IOO #3)
Nsock INFO [1.1360s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOO #3) EID 24
Nsock INFO [1.1360s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [10.129.41.123:1434]
NSE: UDP 10.10.14.151:46322 > 10.129.41.123:1434 | CONNECT
NSE: UDP 10.10.14.151:46322 > 10.129.41.123:1434 | 00000000: 00
Nsock INFO [1.2050s] nsock_write(): Write request for 1 bytes to IOO #1 EID 35 [10.129.41.123:1434]
Nsock INFO [1.2050s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 35 [10.129.41.123:1434]
NSE: UDP 10.10.14.151:46322 > 10.129.41.123:1434 | SEND
Nsock INFO [1.2080s] nsock_read(): Read request from IOO #1 [10.129.41.123:1434] (timeout: 5000ms) EID 42
Nsock INFO [1.2940s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 16 [10.129.41.123:22]
NSE: TCP 10.10.14.151:36906 > 10.129.41.123:22 | CONNECT
Nsock INFO [1.3020s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [10.129.41.123:22]
NSE: TCP 10.10.14.151:36906 > 10.129.41.123:22 | CONNECT
Nsock INFO [1.3160s] nsock_readlines(): Read request for 1 lines from IOO #2 [10.129.41.123:22] EID 50
```

If the Nmap didn't grab a banner then the -sV gave results of the services version and OS its running on,

```
File Actions Edit View Help
0000100: 6b a7 8b 64 2c 5e 23 b9 34 a6 71 8e 95 d9 2c ea k d,"8 + q ,
NSOCK INFO [7.9528s] nssock_write(): Write request for 272 bytes to 100.89.610.379 [10.129.41.123:22]
NSOCK INFO [7.9528s] nssock_trace_handler_callback(): callback: WRITE SUCCESS for EID 379 [10.129.41.123:22]
NSE: TCP 10.10.14.151:38826 > 10.129.41.123:22 | SEND
NSOCK INFO [7.9548s] nssock_read(): Read request from 100.89 [10.129.41.123:22] (timeout: 30000ms) EID 386
NSOCK INFO [8.2348s] nssock_trace_handler_callback(): callback: READ SUCCESS for EID 386 [10.129.41.123:22]
NSE: TCP 10.10.14.151:38826 < 10.129.41.123:22 | 00000000: 00 00 01 9c 00 1f 00 00 00 33 00 00 00 0b 73 73 3 ss
00000010: 68 2d 65 64 32 35 31 39 00 00 00 20 c6 12 3f h-ed25519 7
00000020: 68 7c ab 2f ca e1 c1 40 18 c5 b5 5c 39 cf 9c 23 f1 b v9 #
00000030: db c3 63 06 98 1d b9 aa 25 ec 13 72 ff 00 00 01 c % r'
00000040: 00 33 87 00 9b c2 36 75 bf 2b 05 ba 06 45 6d 43 3 Gu * EmC
00000050: 3f 4f 3a 18 9a aa c5 f2 cd 42 0f 8a e8 2b fb cb 704 C +
00000060: 1e c9 af bf af 38 98 e4 18 10 7c 8e 08 4b 21 a9 8 i K!
00000070: 91 28 ab c4 44 4c ca d0 c4 a6 b9 a8 f6 e8 26 97 DL E
00000080: b8 0e ad 5a 71 00 2c 97 87 cb 1b 7a be a1 f9 4d 2e , r H
00000090: 37 f4 dc 31 18 b8 36 c6 07 c9 c4 f1 ef fc 5e 24 7 1 6 "S
000000a0: d8 49 ea eb 24 5d 38 a8 db e7 46 32 f8 b3 c7 58 I $18 F2 P
000000b0: 8a 0e 9b fa 98 32 71 11 ab 36 19 c8 ab 27 fd 89 25 6 '
000000c0: e5 0f 1d 47 6f 7a be 81 74 66 53 c3 c2 c3 1d 07 GoZ tfs
000000d0: 2b d5 46 19 aa ed 5f d1 28 4f 07 56 81 66 aa ab * f _ (0 { f
000000e0: 6a 59 5e 8e cc 7a c9 91 0f b8 a7 d4 c8 44 42 ac 37* t DB
000000f0: 7a fd 18 b8 36 53 fe d6 c2 89 d0 db d3 3c 58 a9 t 6U cP
00000100: c8 08 48 25 aa 0f 96 d0 c8 1f 48 17 fb 0c 61 05 H a
00000110: 32 e3 55 45 23 a5 c3 6f 6a ab 24 6c 91 82 8e 4a 2 UEZ od $! J
00000120: df c1 f2 61 1e 3a cd 50 d9 eb b9 bc 15 92 a1 08 a A P
00000130: de 1c ee 15 28 81 bc c0 78 e9 97 46 73 50 92 ( x WMe[
00000140: a7 00 00 53 00 00 00 00 72 72 68 2d 65 64 32 S ssh-ed2
00000150: 35 35 31 39 00 00 00 40 4a aa ba 28 3f 5a 33 5a 5519 DM (723Z
00000160: b5 dc fe fa 98 71 aa 69 a7 bc 65 cb ba 3e 19 a4 q 1 e >
00000170: 81 ac b1 48 c6 ce 17 4f f0 0a d9 5a 82 33 fc e2 B O T 3
00000180: 69 47 5f 48 fc 3c ec c9 5e ef 18 02 b8 32 d6 f2 16_H < " 2
00000190: eb f2 92 ab 1c 2c 5a 05 00 00 00 00 00 00 00 00 rT
000001a0: 00 00 00 0c 0a 15 00 00 00 00 00 00 00 00 00 00

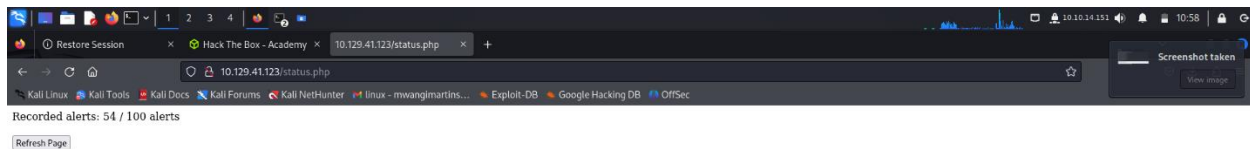
NSE: TCP 10.10.14.151:38826 > 10.129.41.123:22 | CLOSE
NSOCK INFO [8.3388s] nssock_io_delete(): nssock_io_delete (100.89)
Nmap scan report for 10.129.41.123
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 71:c1:89:98:7f:fd:4f:00:e0:54:f3:85:e6:35:6c:2b (RSA)
|_ 256 e1:8e:53:18:42:af:2a:dc:c8:12:1e:2e:54:86:4f:70 (ECDSA)
|_ 256 1a:ccc:ac:d4:94:15:c6:d6:1d:71:e7:39:de:14:27:3c:3c (ED25519)
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 8.36 seconds

(deathstroke@kali) ~$
```

The task was about being quiet as possible not to be detected by the firewall/IDS/IPS and get blocked,

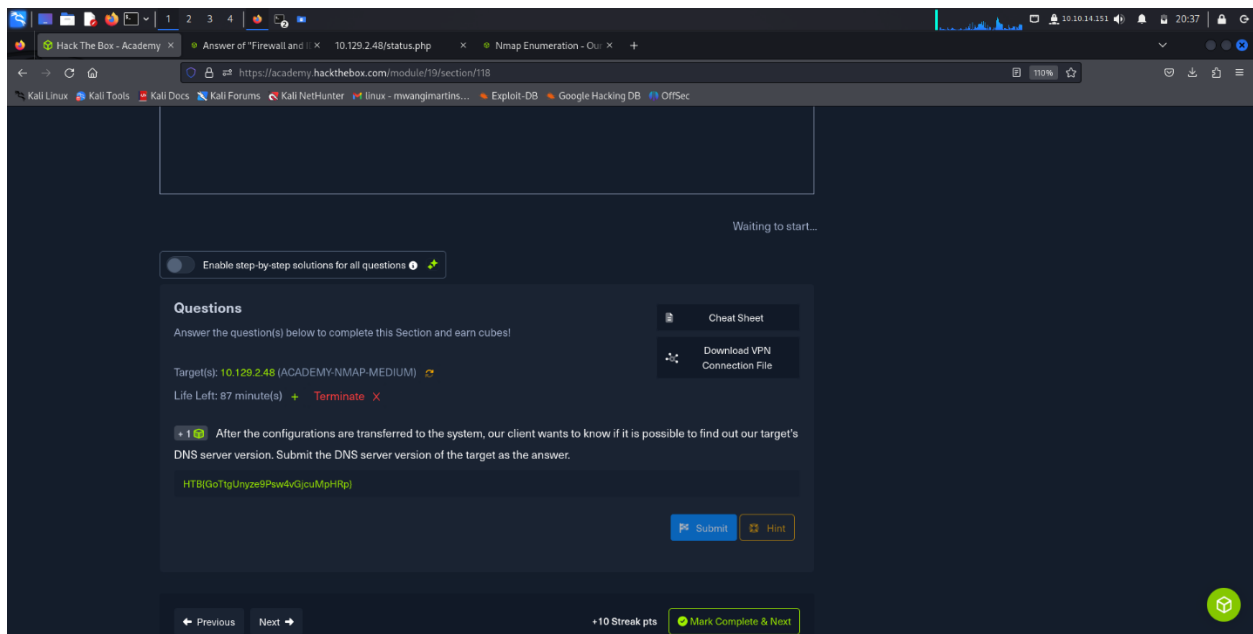


## 1.6 Firewall and IPS/IDS Evasion Medium Lab

### Scenario

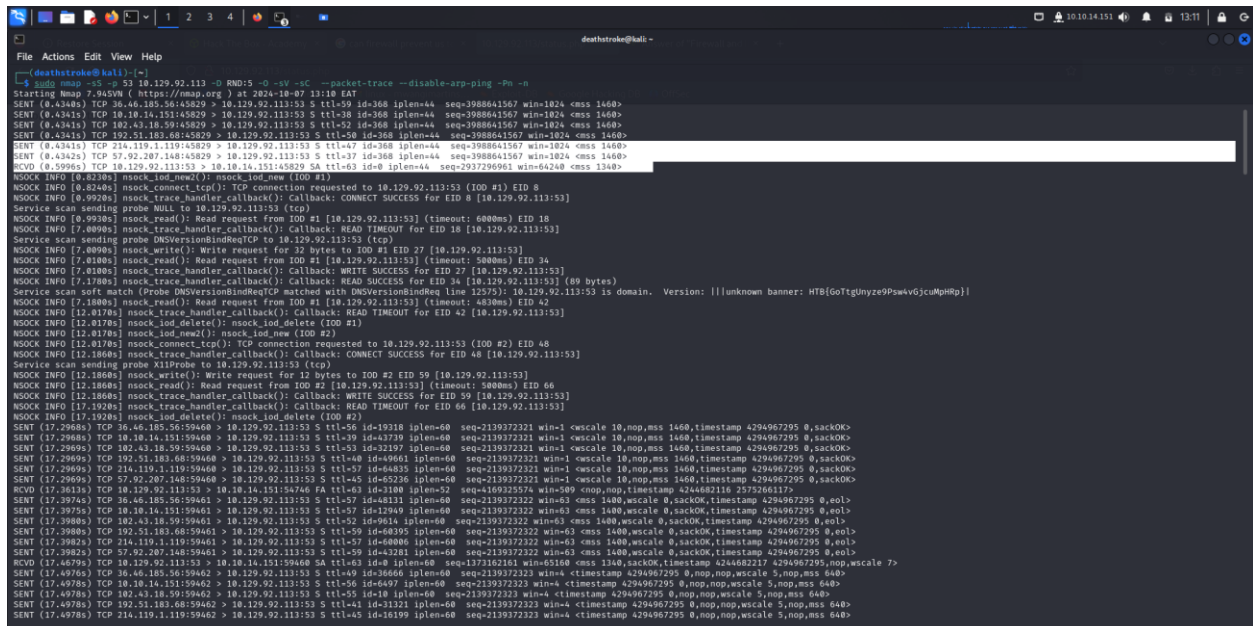
After we conducted the first test and submitted our results to our client, the administrators made some changes and improvements to the IDS/IPS and firewall. We could hear that the administrators were not satisfied with their previous configurations during the meeting, and they could see that the network traffic could be filtered more strictly.





Using the information about DNS server and knowing it uses port 53 on TCP, used SYN scan, Decoys and version and script,

On investigating the Nmap output, there was 5 randomly generated IPs and My own IP sent SYN packet and the decoys IPs got dropped as there was response on them and the My IP got a response target that is SYN-ACK packet.



From viewing the banner grabbed one can find the flag, but the output of the service version gave clear picture,





nowing they were required to add another port for users, and it being port 50000, sent packets using source port 53 to check if the firewall will accept port 53, and it did, meaning it was weakly configured thus even the IPS/IDS might be so.

```
File Actions Edit View Help
[deathstroke@kali:~]$ nmap -sV 10.129.115.236 -p 50000 -Pn -n --packet-trace --disable-arp-ping --source-port 53
Starting Nmap 7.95SVN ( https://nmap.org ) at 2024-10-12 12:54 EAT
SENT (8.3139s) TCP 10.10.14.73:53 > 10.129.115.236:50000 S ttl=66 id=58231 iplen=64 seq=878673216 win=1024 cmsg=1460<
SENT (1.3171s) TCP 10.10.14.73:53 > 10.129.115.236:50000 S ttl=52 id=39080 iplen=64 seq=878542146 win=1024 cmsg=1460<
RCVD (1.5229s) TCP 10.129.115.236:50000 > 10.10.14.73:53 A ttl=53 id=0 iplen=40 seq=1486337860 win=64240 cmsg=1340<
RCVD (1.5409s) TCP 10.129.115.236:50000 > 10.10.14.73:53 SA ttl=43 id=0 iplen=44 seq=1486337860 win=64240 cmsg=1340<
RCVD (1.7494s) TCP 10.129.115.236:50000 > 10.10.14.73:53 R ttl=63 id=0 iplen=40 seq=824911208 win=0
RCVD (3.5214s) TCP 10.129.115.236:50000 > 10.10.14.73:53 SA ttl=63 id=0 iplen=44 seq=1486337860 win=64240 cmsg=1340<
NSOCK INFO [7.6758s] nssock_io_new(): nssock_io_new (IOO #1)
NSOCK INFO [7.6758s] nssock_connect_tcp(): TCP connection requested to 10.129.115.236:50000 (IOO #1) EID 8
NSOCK INFO [12.6788s] nssock_trace_handler_callback(): Callback: CONNECT TIMEOUT for EID 8 [10.129.115.236:50000]
NSOCK INFO [12.6788s] nssock_io_delete(): nssock_io_delete (IOO #1)
NSOCK INFO [12.6788s] nssock_io_new(): nssock_io_new (IOO #1)
NSOCK INFO [12.6918s] nssock_connect_udp(): UDP connection requested to 10.129.115.236:1434 (IOO #2) EID 8
NSOCK INFO [12.6918s] nssock_io_new(): nssock_io_new (IOO #2)
NSOCK INFO [12.6948s] nssock_connect_tcp(): TCP connection requested to 10.129.115.236:50000 (IOO #2) EID 16
NSOCK INFO [12.6948s] nssock_timer_create(): Timer created - 5000ms from now. EID 28
NSOCK INFO [12.6948s] nssock_io_new(): nssock_io_new (IOO #3)
NSOCK INFO [12.6978s] nssock_connect_tcp(): TCP connection requested to 10.129.115.236:50000 (IOO #3) EID 32
NSOCK INFO [12.6998s] nssock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [10.129.115.236:1434]
NSE: UDP 10.10.14.73:56554 > 10.129.115.236:1434 | CONNECT
NSE: UDP 10.10.14.73:56554 > 10.129.115.236:1434 | 00000000: 03
NSOCK INFO [12.7520s] nssock_write(): Write request for 1 bytes to IOO #1 EID 43 [10.129.115.236:1434]
NSOCK INFO [12.7520s] nssock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [10.129.115.236:1434]
NSE: UDP 10.10.14.73:56554 > 10.129.115.236:1434 | SEND
NSOCK INFO [12.8050s] nssock_read(): Read request from IOO #1 [10.129.115.236:1434] (timeout: 5000ms) EID 50
NSOCK INFO [12.9718s] nssock_trace_handler_callback(): Callback: READ ERROR [Connection refused (111)] for EID 50 [10.129.115.236:1434]
NSE: UDP 10.10.14.73:56554 > 10.129.115.236:1434 | CLOSE
NSOCK INFO [13.0220s] nssock_io_delete(): nssock_io_delete (IOO #1)
NSOCK INFO [17.6948s] nssock_trace_handler_callback(): Callback: TIMER SUCCESS for EID 28
NSOCK INFO [17.7008s] nssock_io_new(): nssock_io_new (IOO #4)
NSOCK INFO [17.7118s] nssock_connect_tcp(): TCP connection requested to 10.129.115.236:50000 (IOO #4) EID 56
NSOCK INFO [20.6908s] nssock_trace_handler_callback(): Callback: CONNECT TIMEOUT for EID 32 [10.129.115.236:50000]
NSE: TCP 10.10.14.73:49478 > 10.129.115.236:50000 | CONNECT
NSE: TCP 10.10.14.73:49478 > 10.129.115.236:50000 | CLOSE
NSOCK INFO [20.7848s] nssock_io_delete(): nssock_io_delete (IOO #3)
NSOCK INFO [27.7148s] nssock_trace_handler_callback(): Callback: CONNECT TIMEOUT for EID 56 [10.129.115.236:50000]
NSE: TCP 10.10.14.73:41800 > 10.129.115.236:50000 | CONNECT
NSOCK INFO [27.7668s] nssock_event_cancel(): Event #28 (type TIMER) cancelled
NSE: TCP 10.10.14.73:41800 > 10.129.115.236:50000 | CLOSE
NSOCK INFO [27.7668s] nssock_io_delete(): nssock_io_delete (IOO #4)
NSOCK INFO [42.6948s] nssock_trace_handler_callback(): Callback: CONNECT TIMEOUT for EID 16 [10.129.115.236:50000]
NSE: TCP 10.10.14.73:49468 > 10.129.115.236:50000 | CONNECT
NSE: TCP 10.10.14.73:49468 > 10.129.115.236:50000 | CLOSE
NSOCK INFO [42.6978s] nssock_io_delete(): nssock_io_delete (IOO #2)
Nmap scan report for 10.129.115.236
Host is up (1.2s latency).
PORT      STATE SERVICE
50000/tcp open  tcpwrapped

PORT      STATE SERVICE
50000/tcp open  tcpwrapped
```

Running the netcat on source-port 53 and listening on port 50000, it revealed the flag,

```
File Actions Edit View Help
[deathstroke@kali:~]$ nc -l -p 50000 --source-port 53
connection to 10.129.115.236 50000 port (tcp/*) succeeded!
220 HTB[kjnsdF2u82n1827eh7623898d1w6]
```