NETWORK ENUMERATION WITH NMAP

1.1Enumeration

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.

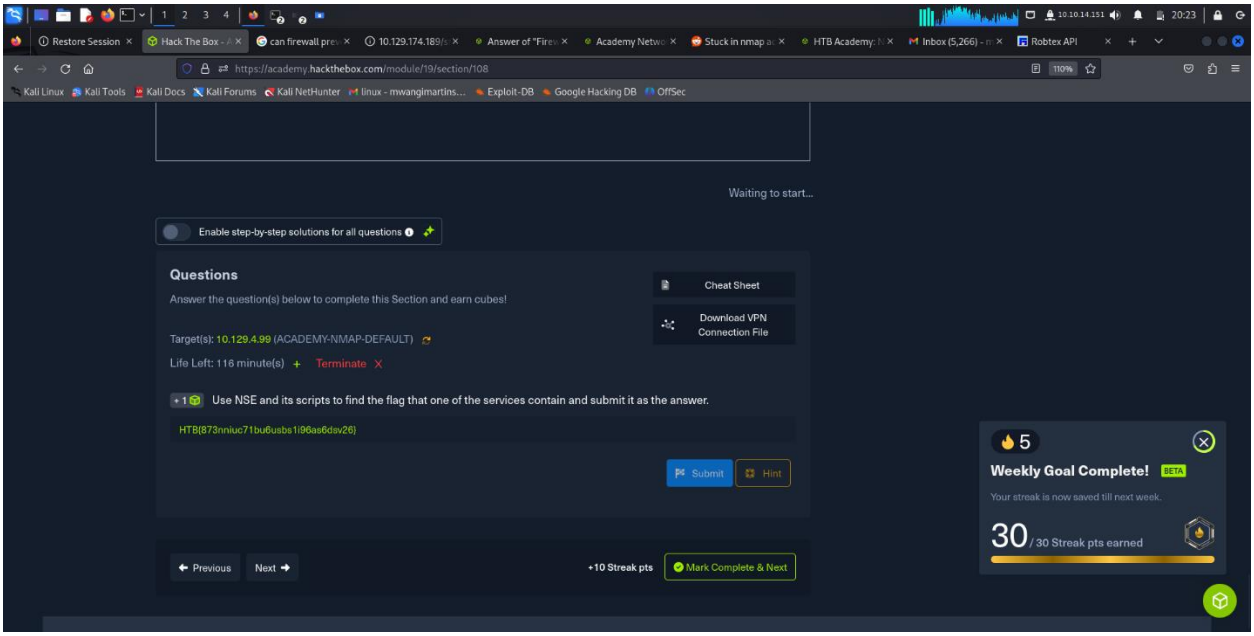
1.3 Service Enumeration

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.

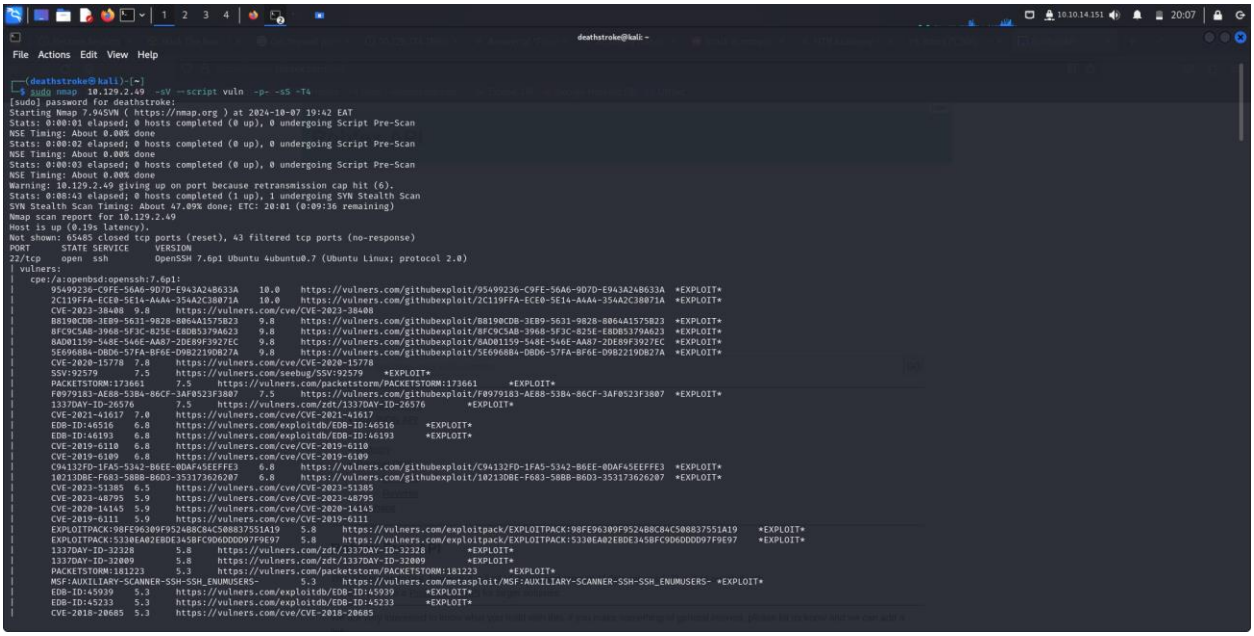
Some services do not immediately provide such information so using *Netcat* to listen on a port we can grab banners, and intercepting this traffic with *tcpdump* we can get more information on the service.

1.4 Scripting Engine

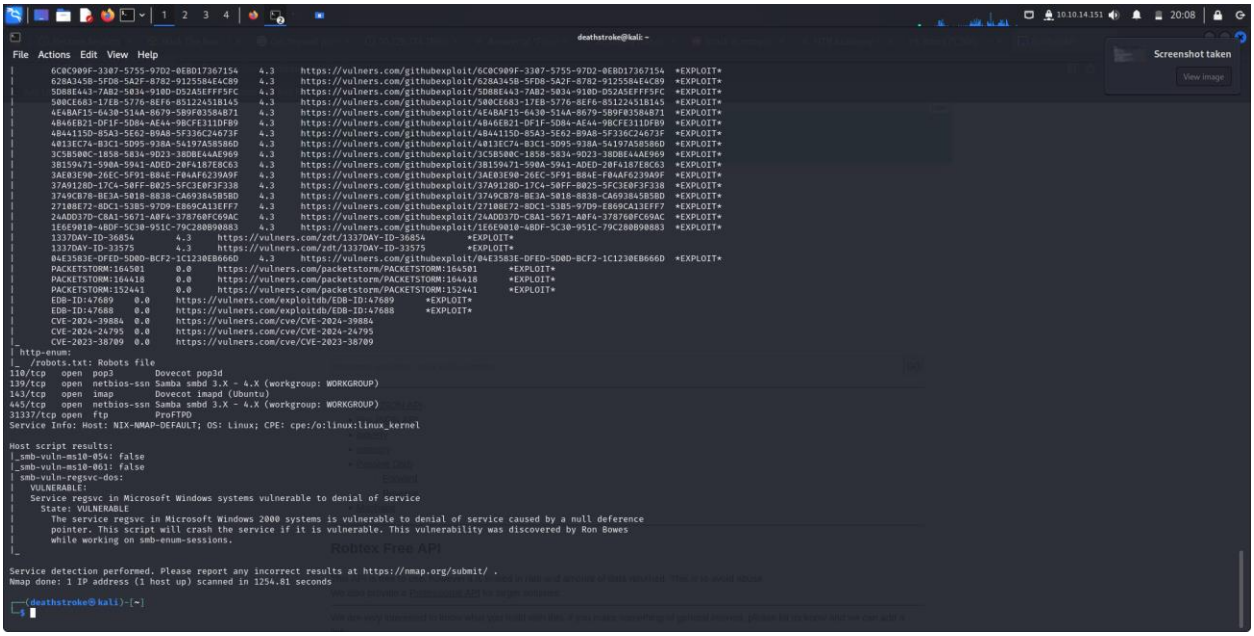
We can define the scripts either in default using *-sC* or specific script using *–script*



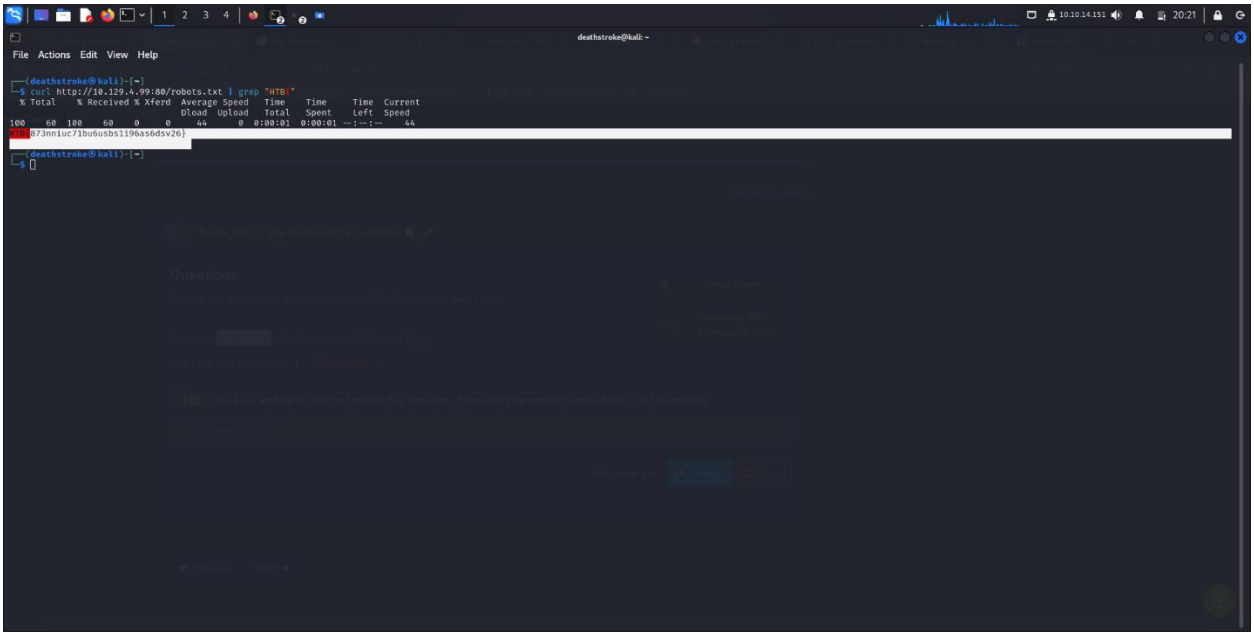
Used the NSE scripts in Nmap, that is script vuln to check for vulnerabilities,



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



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



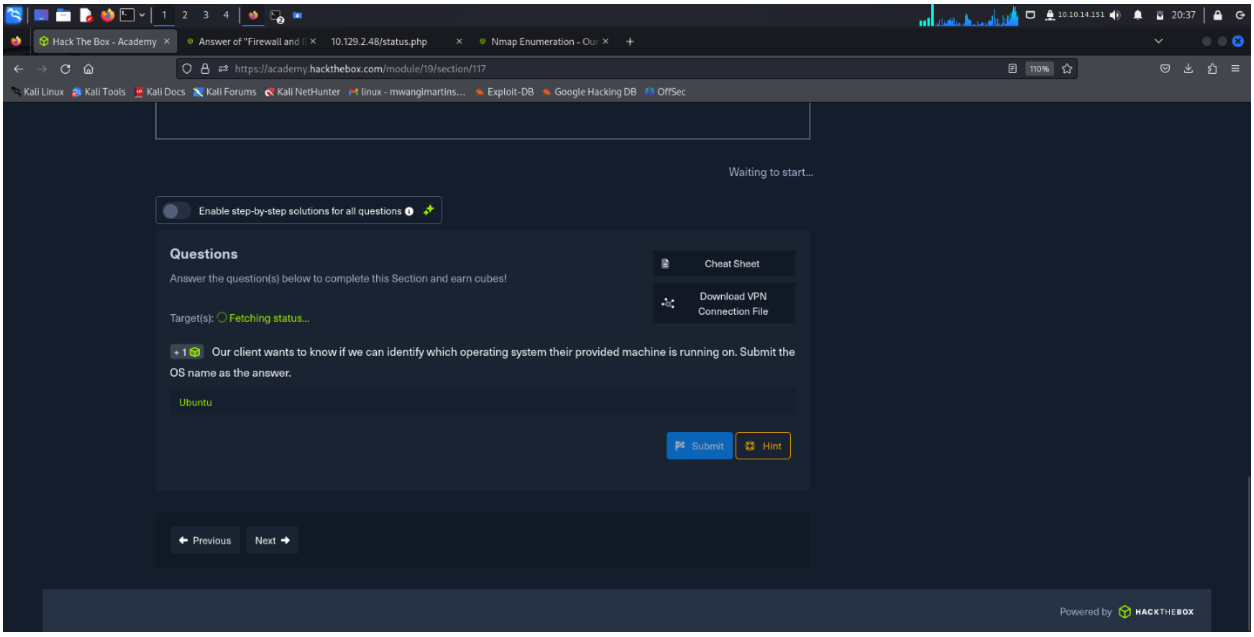
1.5 **Firewall and IPS/IDS Evasion Easy Lab**

Scenario

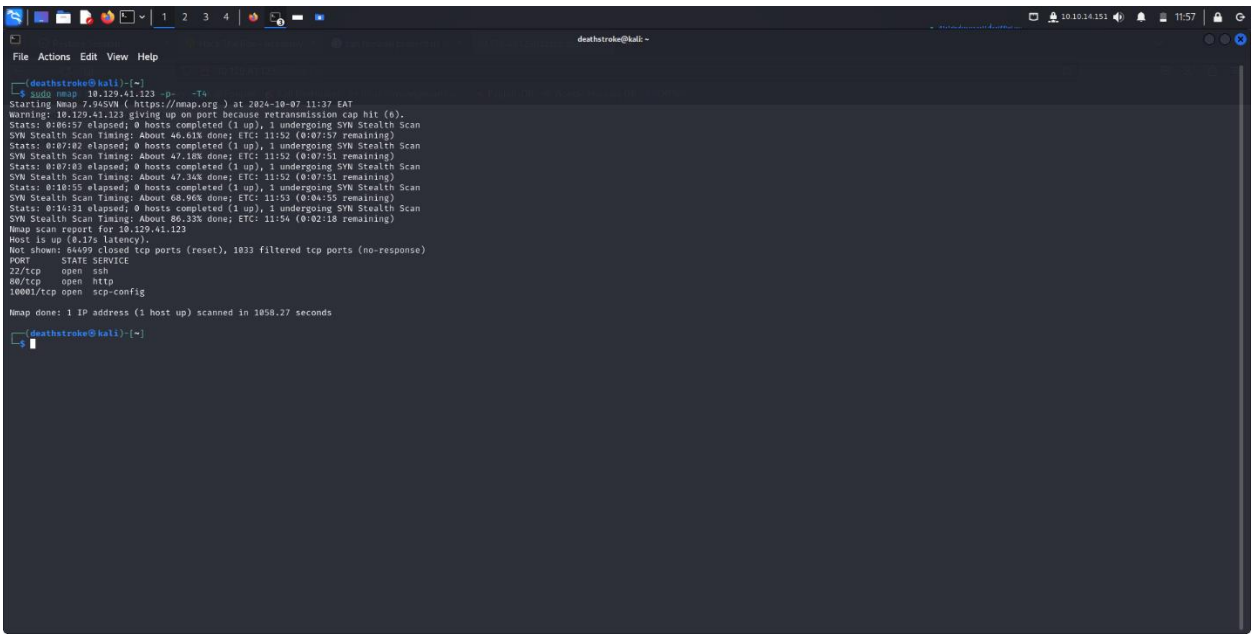
A company hired us to test their IT security defenses, including their IDS and IPS systems. Our client wants to increase their IT security and will, therefore, make specific improvements to their IDS/IPS systems after each successful test. We do not know, however, according to which guidelines these 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.

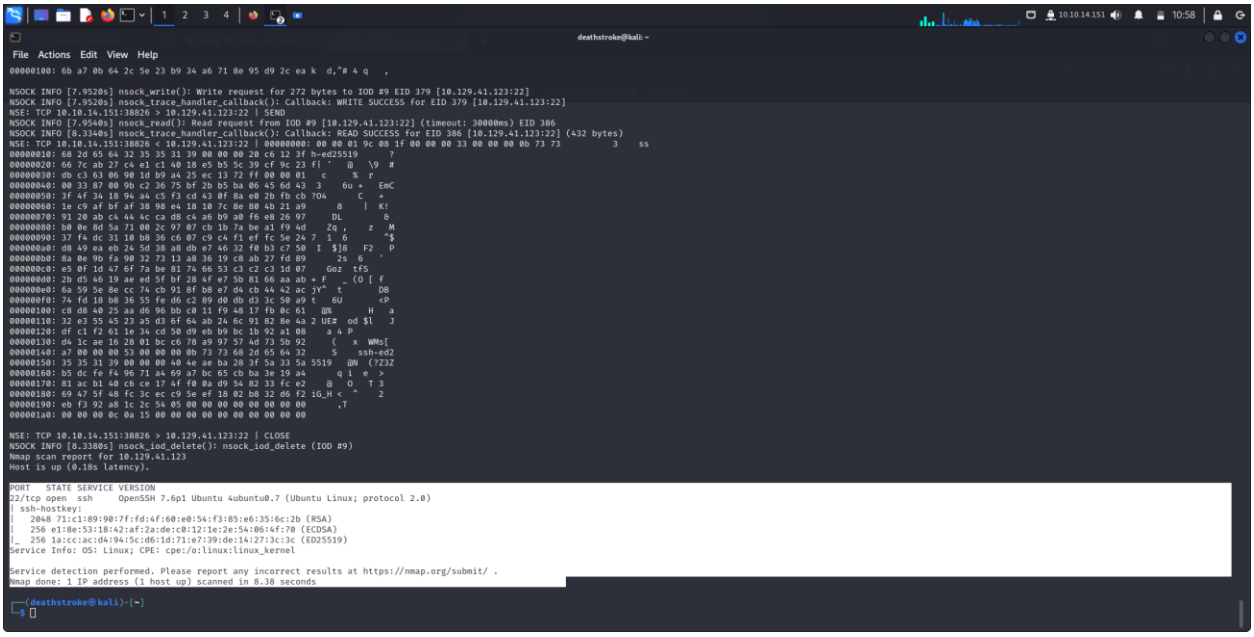
Viewing the Nmap output there was a SYN packet sent to port 22, ssh and target responded with a SA which is SYN-ACK packet, as it was trying to establish a TCP connection,

```
File  Actions  Edit  View  Help
NSE: TCP 10.10.14.151:52484 > 10.129.41.123:22 | CLOSE
NSOCK INFO [3.2150s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSE: UDP 10.10.14.151:54851 > 10.129.41.123:1434 | CLOSE
NSOCK INFO [3.2150s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [3.2210s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [3.2390s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOD #3) EID 56
NSOCK INFO [3.2390s] mksock_bind_addr(): Binding to 0.0.0.0:1022 (IOD #3)
NSOCK INFO [3.4020s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 56 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1022 > 10.129.41.123:22 | CONNECT
NSOCK INFO [3.4080s] nsock_sendto(): Sendto request for 44 bytes to IOD #3 EID 67 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1022 > 10.129.41.123:22 | 00000000: 80 00 00 28 49 5f d4 47 00 00 00 00 00 00 00 02    (I_ G
00000010: 00 01 86 a0 00 00 00 02 00 00 00 00 00 00 00 00
00000020: 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 10.10.14.151:1022 > 10.129.41.123:22 | SEND
NSOCK INFO [3.4180s] nsock_read(): Read request from IOD #3 [10.129.41.123:22] (timeout: 1853ms) EID 74
NSOCK INFO [3.5800s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 74 [10.129.41.123:22] (41 bytes): SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7..
NSE: TCP 10.10.14.151:1022 < 10.129.41.123:22 | SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7

NSOCK INFO [3.5840s] nsock_read(): Read request from IOD #3 [10.129.41.123:22] (timeout: 1853ms) EID 82
NSOCK INFO [5.4370s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 82 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1022 > 10.129.41.123:22 | CLOSE
NSOCK INFO [5.4410s] nsock_iod_delete(): nsock_iod_delete (IOD #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 -Pn -n --packet-trace --disable-arp-ping -sC -sV
Starting Nmap 7.945VN ( 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=1164092419 win=1024 <mss 1460>
RCVD (0.5099s) TCP 10.129.41.123:22 > 10.10.14.151:55824 SA ttl=63 id=0 iplen=44  seq=3459208696 win=64240 <mss 1340>
NSOCK INFO [0.7220s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.7230s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOD #1) EID 8
NSOCK INFO [0.9000s] 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 IOD #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-4ubuntu0.7..
Service scan hard match (Probe NULL matched with NULL line 3524): 10.129.41.123:22 is ssh.  Version: |OpenSSH|7.6p1 Ubuntu 4ubuntu0.7|Ubuntu Linux; protocol 2.0|
NSOCK INFO [1.0710s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [1.1100s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [1.1310s] nsock_connect_udp(): UDP connection requested to 10.129.41.123:1434 (IOD #1) EID 8
NSOCK INFO [1.1310s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [1.1320s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOD #2) EID 16
NSOCK INFO [1.1320s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [1.1360s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOD #3) EID 24
NSOCK INFO [1.1360s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [10.129.41.123:1434]
```

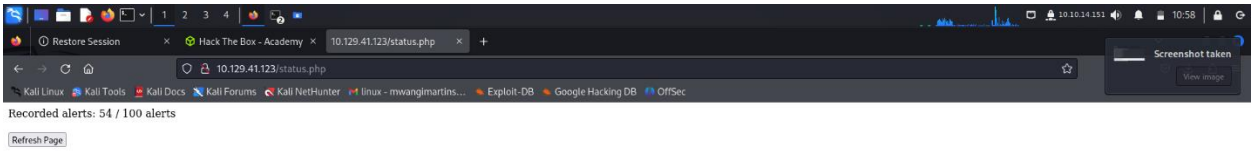
Nmap looks at the banners of the scanned ports and prints them out, in this scan it was to grab a banner that gave more information about the service, that is its version and the OS it was running on.

```
File  Actions  Edit  View  Help
00000020: 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 10.10.14.151:1022 > 10.129.41.123:22 | SEND
NSOCK INFO [3.4180s] nsock_read(): Read request from IOD #3 [10.129.41.123:22] (timeout: 1853ms) EID 74
NSOCK INFO [3.5800s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 74 [10.129.41.123:22] (41 bytes): SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7..
NSE: TCP 10.10.14.151:1022 < 10.129.41.123:22 | SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7

NSOCK INFO [3.5840s] nsock_read(): Read request from IOD #3 [10.129.41.123:22] (timeout: 1853ms) EID 82
NSOCK INFO [5.4370s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 82 [10.129.41.123:22]
NSE: TCP 10.10.14.151:1022 > 10.129.41.123:22 | CLOSE
NSOCK INFO [5.4410s] nsock_iod_delete(): nsock_iod_delete (IOD #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 -Pn -n --packet-trace --disable-arp-ping -sC -sV
Starting Nmap 7.945VN ( 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=1164092419 win=1024 <mss 1460>
RCVD (0.5099s) TCP 10.129.41.123:22 > 10.10.14.151:55824 SA ttl=63 id=0 iplen=44  seq=3459208696 win=64240 <mss 1340>
NSOCK INFO [0.7220s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.7230s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOD #1) EID 8
NSOCK INFO [0.9000s] 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 IOD #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-4ubuntu0.7..
Service scan hard match (Probe NULL matched with NULL line 3524): 10.129.41.123:22 is ssh.  Version: |OpenSSH|7.6p1 Ubuntu 4ubuntu0.7|Ubuntu Linux; protocol 2.0|
NSOCK INFO [1.0710s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [1.1100s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [1.1310s] nsock_connect_udp(): UDP connection requested to 10.129.41.123:1434 (IOD #1) EID 8
NSOCK INFO [1.1310s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [1.1320s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOD #2) EID 16
NSOCK INFO [1.1320s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [1.1360s] nsock_connect_tcp(): TCP connection requested to 10.129.41.123:22 (IOD #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: 03

NSOCK INFO [1.2050s] nsock_write(): Write request for 1 bytes to IOD #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 [1.2600s] nsock_read(): Read request from IOD #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 10.10.14.151:36904 > 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 IOD #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,



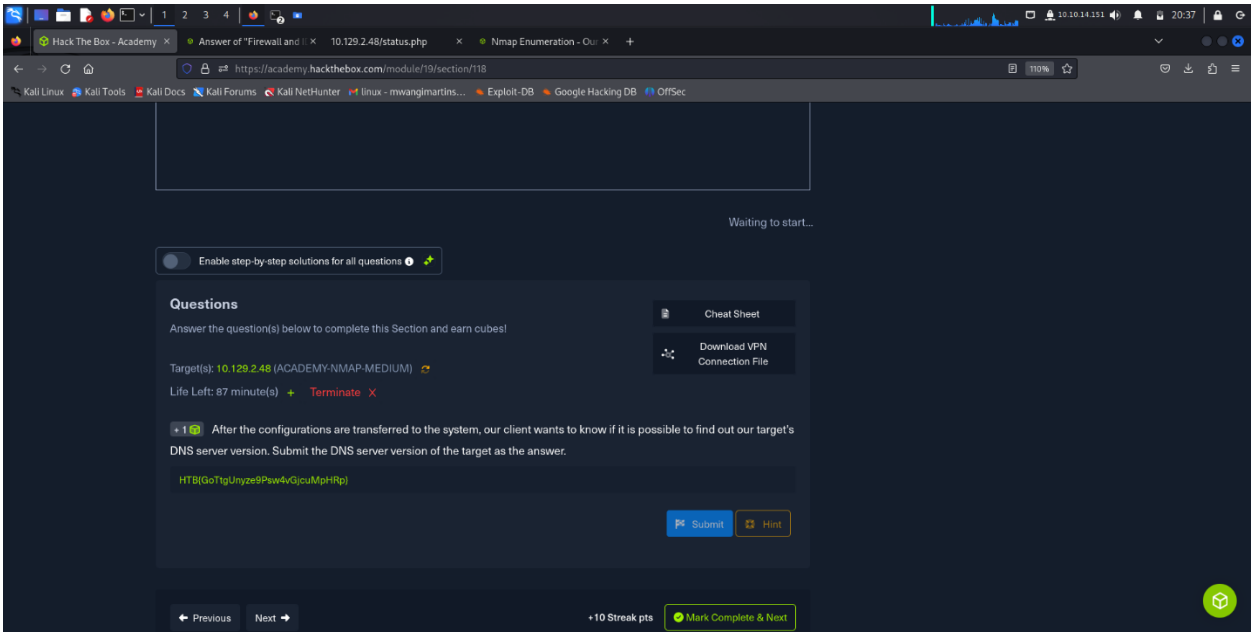
The task was about being quiet as possible not to detected by the firewall/IDS/IPS and get blocked,



1.6 Firewall and IPS/IDS Evasion Medium Lab

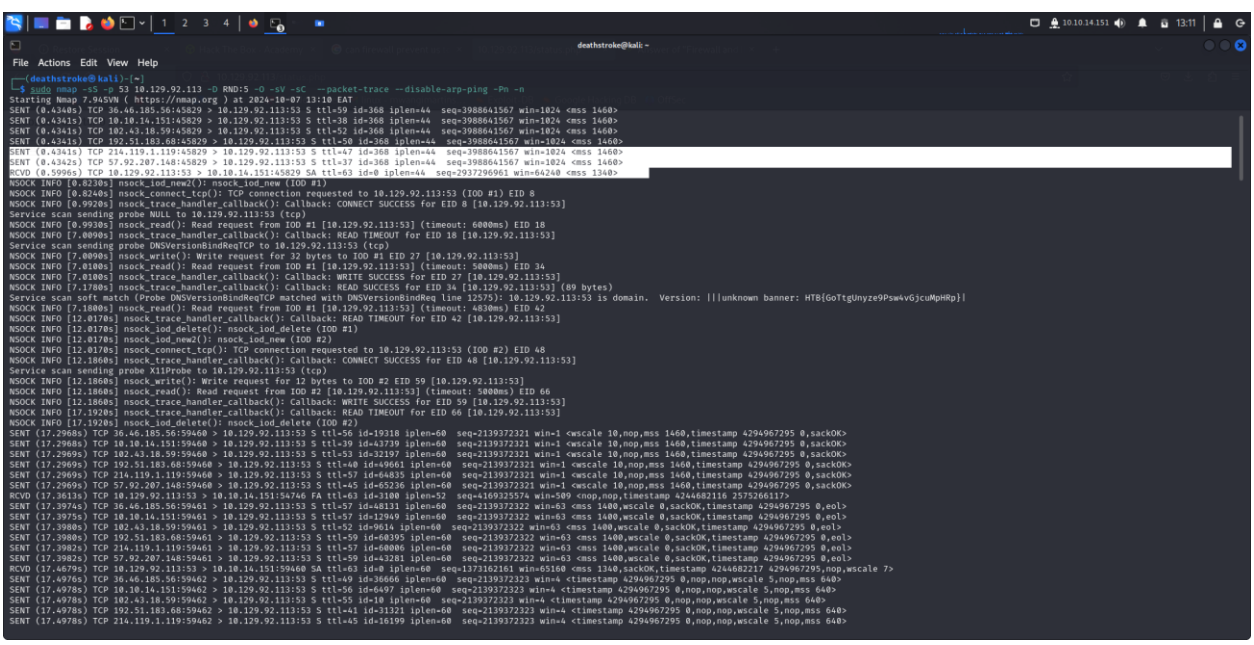
Scenario

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.



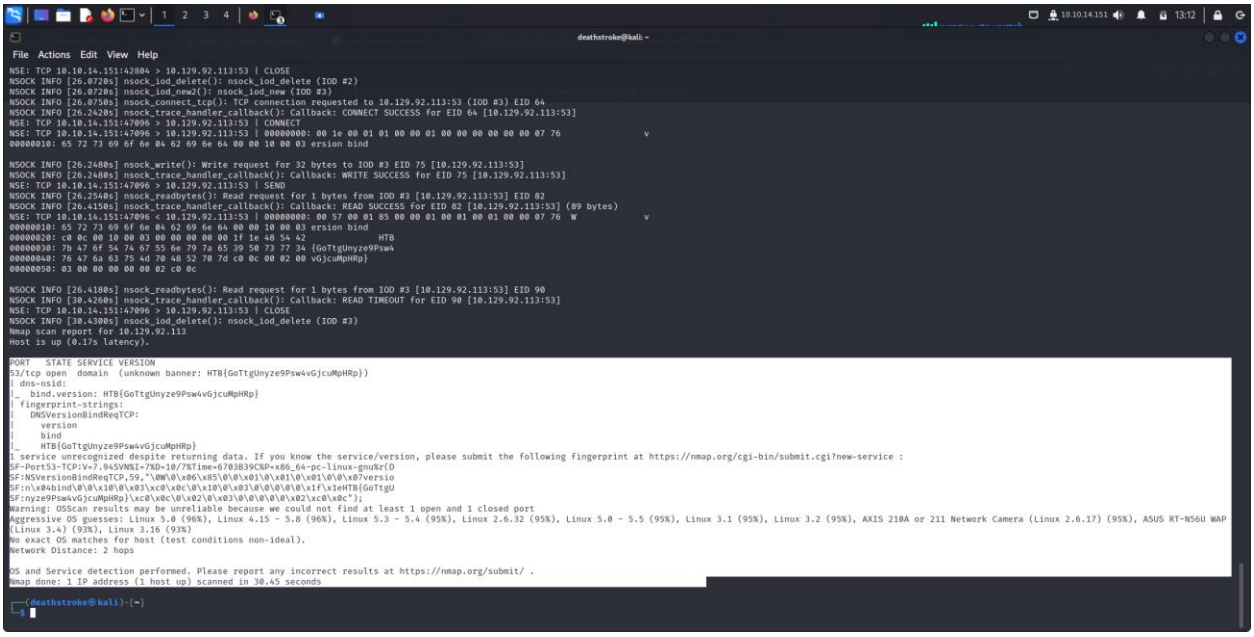
Using the information about DNS server and knowing it uses port 53 on TCP, used SYN scan, Decoys and version and script,

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.



```
(deathstroke@kali)-[~]
$ sudo nmap -sS -p 53 10.129.92.113 -D RND:5 -O -sV -sC --packet-trace --disable-arp-ping -Pn -n
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:10 EAT
SENT (0.4340s) TCP 36.46.185.56:45829 > 10.129.92.113:53 S ttl=59 id=368 iplen=44  seq=3988641567 win=1024 <mss 1460>
SENT (0.4341s) TCP 10.10.14.151:45829 > 10.129.92.113:53 S ttl=38 id=368 iplen=44  seq=3988641567 win=1024 <mss 1460>
SENT (0.4341s) TCP 102.43.18.59:45829 > 10.129.92.113:53 S ttl=52 id=368 iplen=44  seq=3988641567 win=1024 <mss 1460>
SENT (0.4341s) TCP 192.51.183.68:45829 > 10.129.92.113:53 S ttl=50 id=368 iplen=44  seq=3988641567 win=1024 <mss 1460>
SENT (0.4341s) TCP 214.119.1.119:45829 > 10.129.92.113:53 S ttl=47 id=368 iplen=44  seq=3988641567 win=1024 <mss 1460>
SENT (0.4342s) TCP 57.92.207.148:45829 > 10.129.92.113:53 S ttl=37 id=368 iplen=44  seq=3988641567 win=1024 <mss 1460>
RCVD (0.5996s) TCP 10.129.92.113:53 > 10.10.14.151:45829 SA ttl=63 id=0 iplen=44  seq=2937296961 win=64240 <mss 1340>
NSOCK INFO [0.8230s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.8240s] nsock_connect_tcp(): TCP connection requested to 10.129.92.113:53 (IOD #1) EID 8
NSOCK INFO [0.9920s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [10.129.92.113:53]
Service scan sending probe NULL to 10.129.92.113:53 (tcp)
NSOCK INFO [0.9930s] nsock_read(): Read request from IOD #1 [10.129.92.113:53] (timeout: 6000ms) EID 18
NSOCK INFO [7.0090s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 18 [10.129.92.113:53]
Service scan sending probe DNSVersionBindReqTCP to 10.129.92.113:53 (tcp)
NSOCK INFO [7.0090s] nsock_write(): Write request for 32 bytes to IOD #1 EID 27 [10.129.92.113:53]
NSOCK INFO [7.0100s] nsock_read(): Read request from IOD #1 [10.129.92.113:53] (timeout: 5000ms) EID 34
NSOCK INFO [7.0100s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [10.129.92.113:53]
NSOCK INFO [7.1780s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 34 [10.129.92.113:53] (89 bytes)
Service scan soft match (Probe DNSVersionBindReqTCP matched with DNSVersionBindReq line 12575): 10.129.92.113:53 is domain.  Version: |||unknown banner: HTB{GoTtgUnyze9Psw4vGjcuMpHRp}|
NSOCK INFO [7.1800s] nsock_read(): Read request from IOD #1 [10.129.92.113:53] (timeout: 4830ms) EID 42
NSOCK INFO [12.0170s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 42 [10.129.92.113:53]
NSOCK INFO [12.0170s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [12.0170s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [12.0170s] nsock_connect_tcp(): TCP connection requested to 10.129.92.113:53 (IOD #2) EID 48
NSOCK INFO [12.1860s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 48 [10.129.92.113:53]
Service scan sending probe X11Probe to 10.129.92.113:53 (tcp)
NSOCK INFO [12.1860s] nsock_write(): Write request for 12 bytes to IOD #2 EID 59 [10.129.92.113:53]
NSOCK INFO [12.1860s] nsock_read(): Read request from IOD #2 [10.129.92.113:53] (timeout: 5000ms) EID 66
NSOCK INFO [12.1860s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [10.129.92.113:53]
NSOCK INFO [17.1920s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 66 [10.129.92.113:53]
NSOCK INFO [17.1920s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
SENT (17.2968s) TCP 36.46.185.56:59460 > 10.129.92.113:53 S ttl=56 id=19318 iplen=60  seq=2139372321 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
SENT (17.2968s) TCP 10.10.14.151:59460 > 10.129.92.113:53 S ttl=39 id=43739 iplen=60  seq=2139372321 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
SENT (17.2969s) TCP 102.43.18.59:59460 > 10.129.92.113:53 S ttl=53 id=32197 iplen=60  seq=2139372321 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
SENT (17.2969s) TCP 192.51.183.68:59460 > 10.129.92.113:53 S ttl=40 id=49661 iplen=60  seq=2139372321 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
SENT (17.2969s) TCP 214.119.1.119:59460 > 10.129.92.113:53 S ttl=57 id=64835 iplen=60  seq=2139372321 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
SENT (17.2969s) TCP 57.92.207.148:59460 > 10.129.92.113:53 S ttl=45 id=65236 iplen=60  seq=2139372321 win=1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
RCVD (17.3613s) TCP 10.129.92.113:53 > 10.10.14.151:54746 FA ttl=63 id=3100 iplen=52  seq=4169325574 win=509 <nop,nop,timestamp 4244682116 2573266117>
SENT (17.3974s) TCP 36.46.185.56:59461 > 10.129.92.113:53 S ttl=57 id=48131 iplen=60  seq=2139372322 win=63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
SENT (17.3975s) TCP 10.10.14.151:59461 > 10.129.92.113:53 S ttl=57 id=12949 iplen=60  seq=2139372322 win=63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
SENT (17.3980s) TCP 102.43.18.59:59461 > 10.129.92.113:53 S ttl=52 id=9614 iplen=60  seq=2139372322 win=63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
SENT (17.3980s) TCP 192.51.183.68:59461 > 10.129.92.113:53 S ttl=59 id=60395 iplen=60  seq=2139372322 win=63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
SENT (17.3982s) TCP 214.119.1.119:59461 > 10.129.92.113:53 S ttl=57 id=60006 iplen=60  seq=2139372322 win=63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
SENT (17.3982s) TCP 57.92.207.148:59461 > 10.129.92.113:53 S ttl=59 id=43281 iplen=60  seq=2139372322 win=63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
RCVD (17.4679s) TCP 10.129.92.113:53 > 10.10.14.151:59460 SA ttl=63 id=0 iplen=60  seq=1373162161 win=65160 <mss 1340,sackOK,timestamp 4244682217 4294967295,nop,wscale 7>
SENT (17.4976s) TCP 36.46.185.56:59462 > 10.129.92.113:53 S ttl=49 id=36666 iplen=60  seq=2139372323 win=4 <timestamp 4294967295 0,nop,nop,wscale 5,nop,mss 640>
SENT (17.4978s) TCP 10.10.14.151:59462 > 10.129.92.113:53 S ttl=56 id=6497 iplen=60  seq=2139372323 win=4 <timestamp 4294967295 0,nop,nop,wscale 5,nop,mss 640>
SENT (17.4978s) TCP 102.43.18.59:59462 > 10.129.92.113:53 S ttl=55 id=10 iplen=60  seq=2139372323 win=4 <timestamp 4294967295 0,nop,nop,wscale 5,nop,mss 640>
SENT (17.4978s) TCP 192.51.183.68:59462 > 10.129.92.113:53 S ttl=41 id=31321 iplen=60  seq=2139372323 win=4 <timestamp 4294967295 0,nop,nop,wscale 5,nop,mss 640>
SENT (17.4978s) TCP 214.119.1.119:59462 > 10.129.92.113:53 S ttl=45 id=16199 iplen=60  seq=2139372323 win=4 <timestamp 4294967295 0,nop,nop,wscale 5,nop,mss 640>
```

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

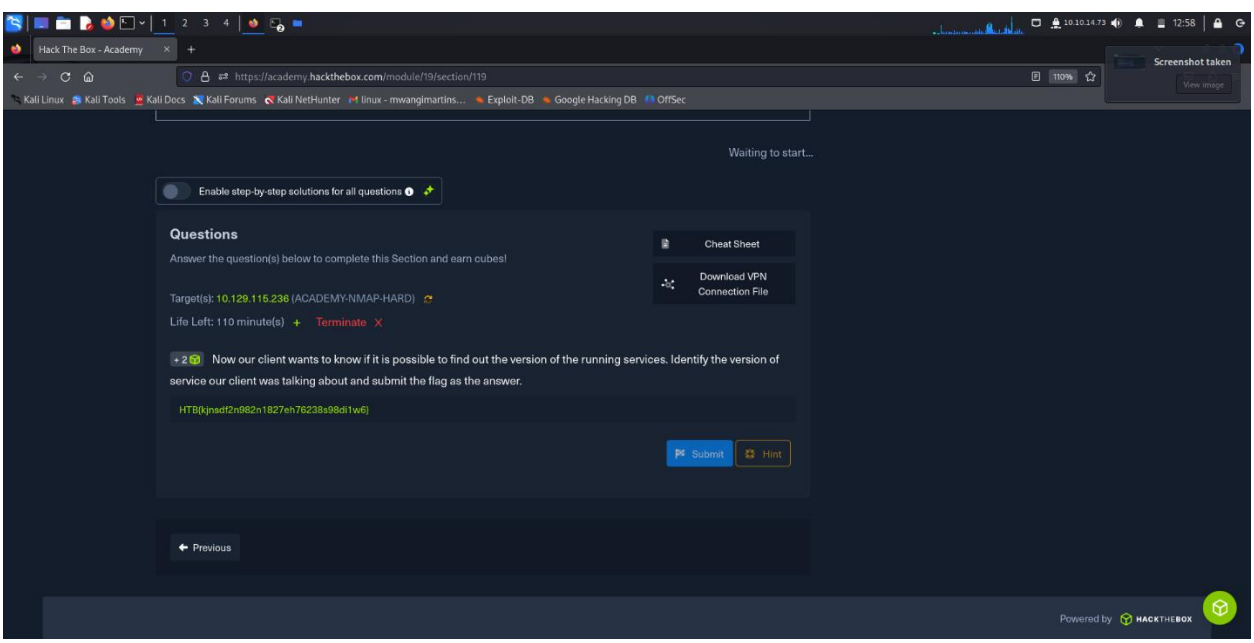


1.7 Firewall and IPS/IDS Evasion Hard Lab

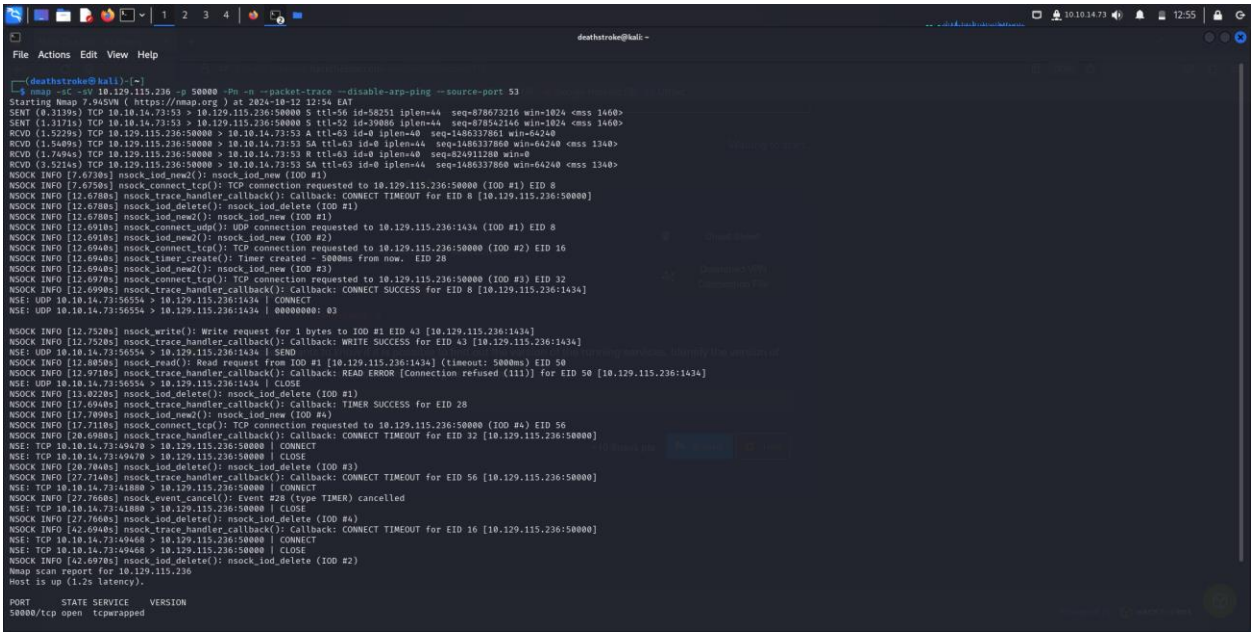
Scenario

With our second test's help, our client was able to gain new insights and sent one of its administrators to a training course for IDS/IPS systems. As our client told us, the training would last one week. Now the administrator has taken all the necessary precautions and wants us to test this again because specific services must be changed, and the communication for the provided software had to be modified.

Question



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.



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