Ex0x5- Nmap

Jigar Patel

2023-10-17

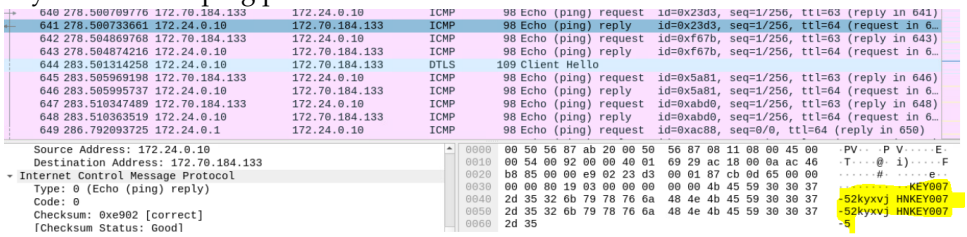
Contents

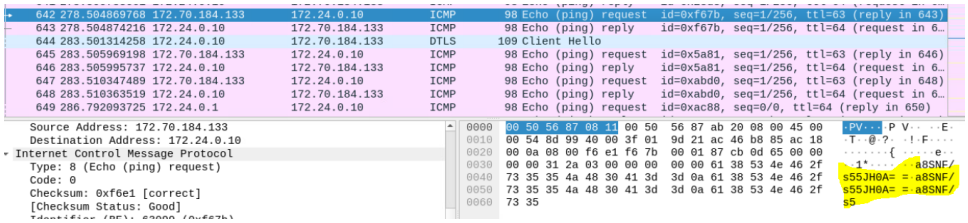
1 Attack Narrative

Nmap scan against **www.artstailor.com @ 172.70.184.133**.

1. Open up Wireshark using command *sudo wireshark* and select the active interface *eth0*.

2. We observe some ICMP activity going on. On closer look, we find the key in the ICMP ping probes.





   On concatenating, we find the key associated with this exercise as **KEY007-52kyxvjHNa8SNF/s55JH0A==**. We can remove this traffic clutter from the further exercise by filtering out ICMP packets of length 98.

3. Next, we perform a Nmap scan over TCP with options set to run version scan (-sV) and default scripts (-sC).

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV www.artstailor.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 13:03 EDT
Nmap scan report for www.artstailor.com (172.70.184.133)
Host is up (0.00070s latency).
rDNS record for 172.70.184.133: ns.artstailor.com
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 3c:d8:88:1f:86:cf:44:c8:d5:68:33:13:1c:de:2d:dd (ECDSA)
|_  256 db:47:2d:75:19:14:fd:5c:6c:cf:2e:95:9e:13:30:b7 (ED25519)
53/tcp open  domain  ISC BIND 9.18.16-1~deb12u1 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.18.16-1~deb12u1-Debian
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Art's Tailor Shop
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 21.30 seconds
```

We observe the following:

(a) We have **3 TCP open ports** on the web server www.artstailor.com.

(b) **Port 22** has SSH running with version *OpenSSH 9.21p1 Debian 2 (protocol 2.0)*.

(c) **Port 53** is running DNS service using *ISC BIND 9.18.16.1-1 deb12u1*.

(d) **Port 80** is running Apache httpd 2.4.57 (*Debian*).

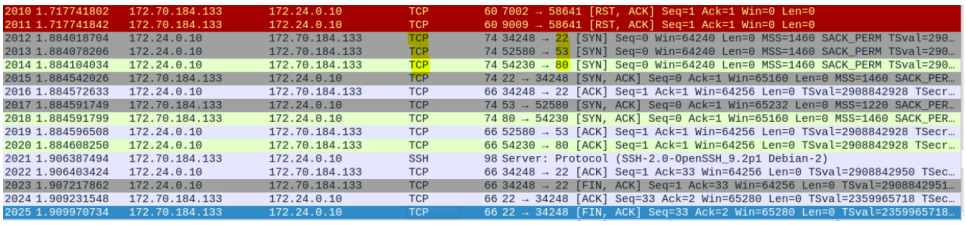
(e) We also observe the OS has been detected as a **Debian distro**.

4. Now, we look at the activity in Wireshark.

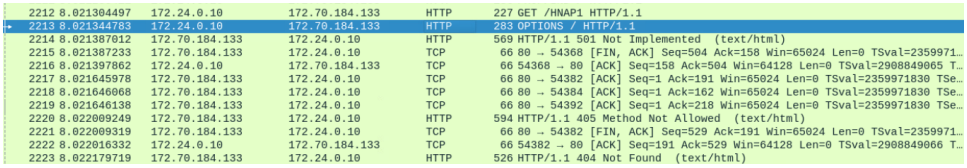
8	1.672879257	172.70.184.133	172.24.0.10	DNS	118 Standard query response 0x1607 PTR 133.184.70.172.in-addr.arpa PTR …
9	1.688426765	172.24.0.10	172.70.184.133	TCP	58 58641 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	1.688446522	172.24.0.10	172.70.184.133	TCP	58 58641 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	1.688453916	172.24.0.10	172.70.184.133	TCP	58 58641 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	1.688460428	172.24.0.10	172.70.184.133	TCP	58 58641 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	1.688468884	172.24.0.10	172.70.184.133	TCP	58 58641 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	1.688479965	172.24.0.10	172.70.184.133	TCP	58 58641 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	1.688486557	172.24.0.10	172.70.184.133	TCP	58 58641 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	1.688493320	172.24.0.10	172.70.184.133	TCP	58 58641 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	1.688499151	172.24.0.10	172.70.184.133	TCP	58 58641 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	1.688512686	172.24.0.10	172.70.184.133	TCP	58 58641 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	1.689064892	172.70.184.133	172.24.0.10	TCP	60 80 → 58641 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
20	1.689065112	172.70.184.133	172.24.0.10	TCP	60 143 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	1.689065182	172.70.184.133	172.24.0.10	TCP	60 1723 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	1.689065252	172.70.184.133	172.24.0.10	TCP	60 3306 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	1.689065322	172.70.184.133	172.24.0.10	TCP	60 995 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	1.689065392	172.70.184.133	172.24.0.10	TCP	60 8080 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	1.689065463	172.70.184.133	172.24.0.10	TCP	60 113 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	1.689065533	172.70.184.133	172.24.0.10	TCP	60 22 → 58641 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
27	1.689146985	172.24.0.10	172.70.184.133	TCP	54 58641 → 80 [RST] Seq=1 Win=0 Len=0
28	1.689165240	172.24.0.10	172.70.184.133	TCP	54 58641 → 22 [RST] Seq=1 Win=0 Len=0
29	1.689172864	172.70.184.133	172.24.0.10	TCP	60 139 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

We observe that Nmap sends **TCP SYN** on **various TCP port numbers** including 80, 143, 22, etc. For **closed ports**, it receives packets with flags **RST & ACK** set while for **open ports** it receives packets with **SYN & ACK**. In the figure, we get SYN-ACK responses on ports 80 and 22, while other ports can be seen giving RST-ACK.

After identifying the open ports Nmap sends various packets with different protocols to grab HTTP, SSH, or other service banners from them.



2010	1.717741802	172.70.184.133	172.24.0.10	TCP	60 7002 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2011	1.717741842	172.70.184.133	172.24.0.10	TCP	60 9009 → 58641 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2012	1.884018704	172.24.0.10	172.70.184.133	TCP	74 34248 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=290…
2013	1.884078206	172.24.0.10	172.70.184.133	TCP	74 52580 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=290…
2014	1.884104034	172.24.0.10	172.70.184.133	TCP	74 54230 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=290…
2015	1.884542026	172.70.184.133	172.24.0.10	TCP	74 22 → 34248 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PER…
2016	1.884572633	172.24.0.10	172.70.184.133	TCP	66 34248 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2908842928 TSecr…
2017	1.884591749	172.70.184.133	172.24.0.10	TCP	74 53 → 52580 [SYN, ACK] Seq=0 Ack=1 Win=65232 Len=0 MSS=1220 SACK_PER…
2018	1.884591799	172.70.184.133	172.24.0.10	TCP	74 80 → 54230 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PER…
2019	1.884596508	172.24.0.10	172.70.184.133	TCP	66 52580 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2908842928 TSecr…
2020	1.884608250	172.24.0.10	172.70.184.133	TCP	66 54230 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2908842928 TSecr…
2021	1.906387494	172.70.184.133	172.24.0.10	SSH	98 Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2)
2022	1.906403424	172.24.0.10	172.70.184.133	TCP	66 34248 → 22 [ACK] Seq=1 Ack=33 Win=64256 Len=0 TSval=2908842950 TSec…
2023	1.907217862	172.24.0.10	172.70.184.133	TCP	66 34248 → 22 [FIN, ACK] Seq=1 Ack=33 Win=64256 Len=0 TSval=2908842951…
2024	1.909231548	172.70.184.133	172.24.0.10	TCP	66 22 → 34248 [ACK] Seq=33 Ack=2 Win=65280 Len=0 TSval=2359965718 TSec…
2025	1.909970734	172.70.184.133	172.24.0.10	TCP	66 22 → 34248 [FIN, ACK] Seq=33 Ack=2 Win=65280 Len=0 TSval=2359965718…



2212	8.021304497	172.24.0.10	172.70.184.133	HTTP	227 GET /HNAP1 HTTP/1.1
2213	8.021344783	172.24.0.10	172.70.184.133	HTTP	283 OPTIONS / HTTP/1.1
2214	8.021387012	172.70.184.133	172.24.0.10	HTTP	569 HTTP/1.1 501 Not Implemented (text/html)
2215	8.021387233	172.70.184.133	172.24.0.10	TCP	66 80 → 54368 [FIN, ACK] Seq=504 Ack=158 Win=65024 Len=0 TSval=2359971…
2216	8.021397862	172.24.0.10	172.70.184.133	TCP	66 54368 → 80 [ACK] Seq=158 Ack=504 Win=64128 Len=0 TSval=2908849065 T…
2217	8.021645978	172.70.184.133	172.24.0.10	TCP	66 80 → 54382 [ACK] Seq=1 Ack=191 Win=65024 Len=0 TSval=2359971830 TSe…
2218	8.021646068	172.70.184.133	172.24.0.10	TCP	66 80 → 54384 [ACK] Seq=1 Ack=162 Win=65024 Len=0 TSval=2359971830 TSe…
2219	8.021646138	172.70.184.133	172.24.0.10	TCP	66 80 → 54392 [ACK] Seq=1 Ack=218 Win=65024 Len=0 TSval=2359971830 TSe…
2220	8.022009249	172.70.184.133	172.24.0.10	HTTP	594 HTTP/1.1 405 Method Not Allowed (text/html)
2221	8.022009319	172.70.184.133	172.24.0.10	TCP	66 80 → 54382 [FIN, ACK] Seq=529 Ack=191 Win=65024 Len=0 TSval=2359971…
2222	8.022016332	172.24.0.10	172.70.184.133	TCP	66 54382 → 80 [ACK] Seq=191 Ack=529 Win=64128 Len=0 TSval=2908849066 T…
2223	8.022179719	172.70.184.133	172.24.0.10	HTTP	526 HTTP/1.1 404 Not Found (text/html)

5. Next, we scan the UDP ports using the options to perform UDP scan (-sU) within the port limit 1-256 (-p1-256).

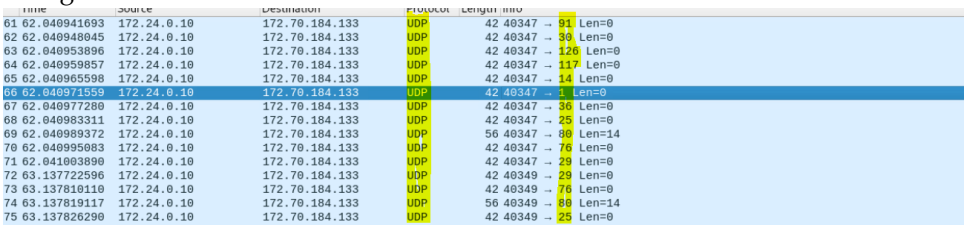
```
└─$ sudo nmap -sU -sV -p1-126 www.artstailor.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 13:11 EDT
Nmap scan report for www.artstailor.com (172.70.184.133)
Host is up (0.00081s latency).
rDNS record for 172.70.184.133: ns.artstailor.com
Not shown: 124 closed udp ports (port-unreach)
PORT   STATE         SERVICE VERSION
40/udp open|filtered unknown
53/udp open          domain  ISC BIND 9.18.16-1~deb12u1 (Debian Linux)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.44 seconds
```

We observe the following:

(a) UDP Port 40 Filtered/Open with an unknown service. When a UDP port does not respond, Nmap says it is filtered.

(b) UDP Port 53 Open with DNS running using ISC BIND 9.18.16.1-1 deb12u1.

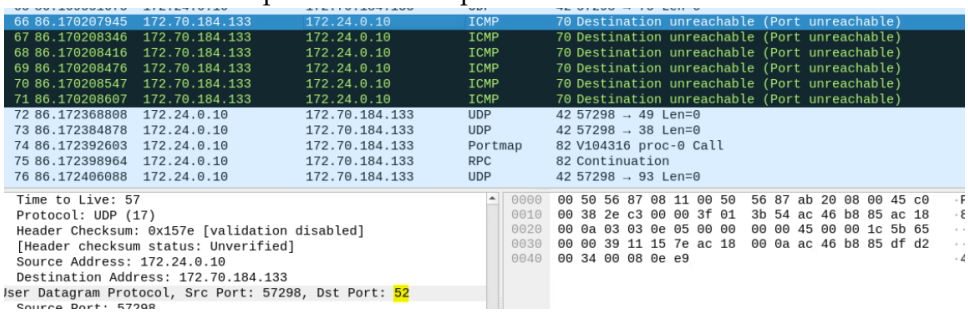
6. We again look at Wireshark to look at the UDP scan.



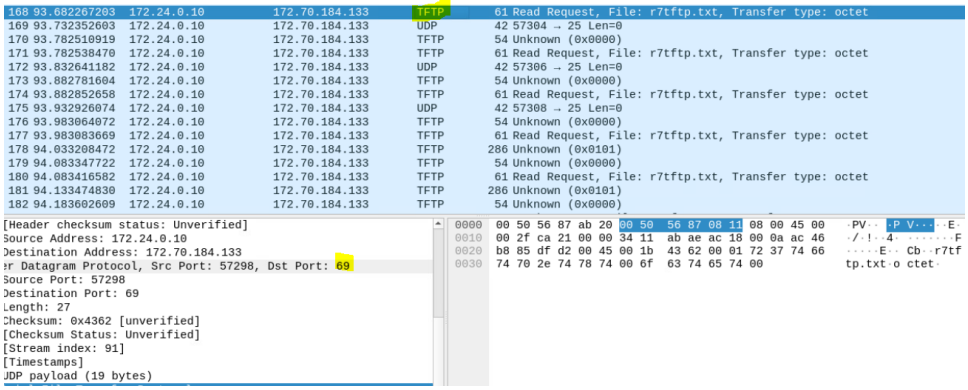
	Time	Source	Destination	Protocol	Length Info
61	62.040941693	172.24.0.10	172.70.184.133	UDP	42 40347 → 91 Len=0
62	62.040948045	172.24.0.10	172.70.184.133	UDP	42 40347 → 30 Len=0
63	62.040953896	172.24.0.10	172.70.184.133	UDP	42 40347 → 126 Len=0
64	62.040959857	172.24.0.10	172.70.184.133	UDP	42 40347 → 117 Len=0
65	62.040965598	172.24.0.10	172.70.184.133	UDP	42 40347 → 14 Len=0
66	62.040971559	172.24.0.10	172.70.184.133	UDP	42 40347 → 1 Len=0
67	62.040977280	172.24.0.10	172.70.184.133	UDP	42 40347 → 36 Len=0
68	62.040983311	172.24.0.10	172.70.184.133	UDP	42 40347 → 25 Len=0
69	62.040989372	172.24.0.10	172.70.184.133	UDP	56 40347 → 80 Len=14
70	62.040995083	172.24.0.10	172.70.184.133	UDP	42 40347 → 76 Len=0
71	62.041003890	172.24.0.10	172.70.184.133	UDP	42 40347 → 29 Len=0
72	63.137722596	172.24.0.10	172.70.184.133	UDP	42 40349 → 29 Len=0
73	63.137810110	172.24.0.10	172.70.184.133	UDP	42 40349 → 76 Len=0
74	63.137819117	172.24.0.10	172.70.184.133	UDP	56 40349 → 80 Len=14
75	63.137826290	172.24.0.10	172.70.184.133	UDP	42 40349 → 25 Len=0

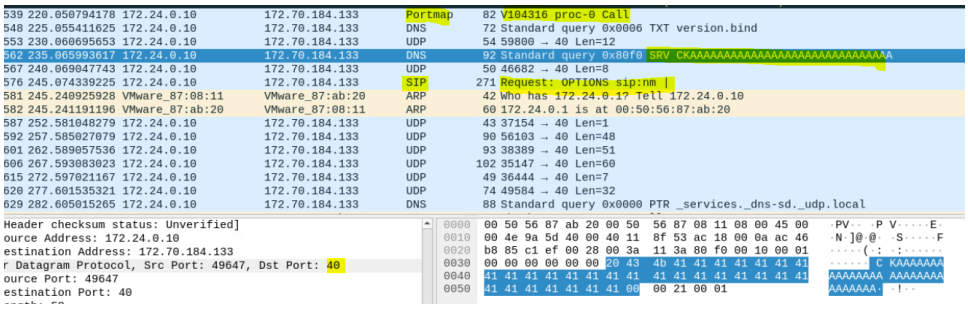
We observe Nmap is sending UDP packets on various port numbers, with almost empty data.

Next, we observe replies from the victim machine. We get ICMP Destination Unreachable replies for various ports.



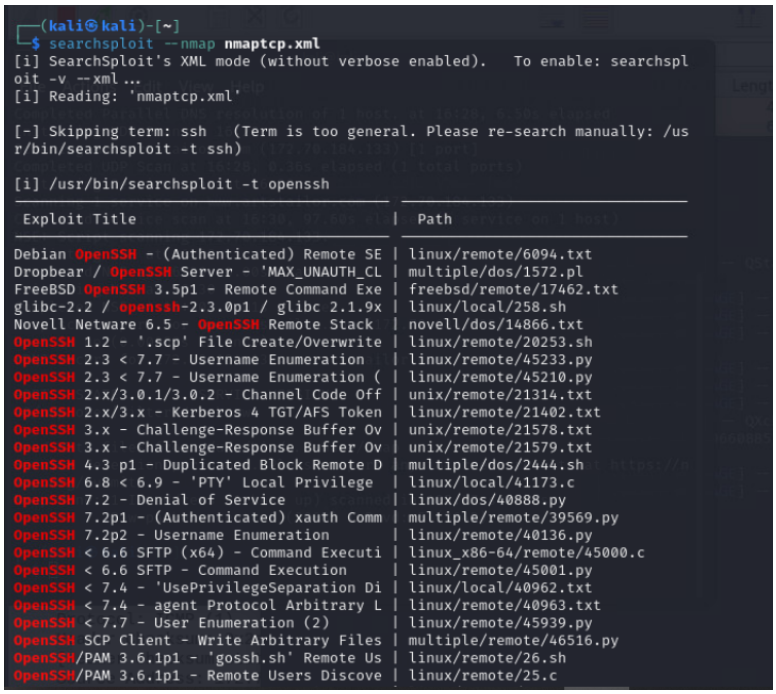
For ports for which it does not immediately get Destination Unreachable, Nmap sends probing packets using various known protocols. We see Nmap trying protocols such as TFTP (Trivial FTP), Portmap, and SIP (Session Initiation Protocol) to gather version information.



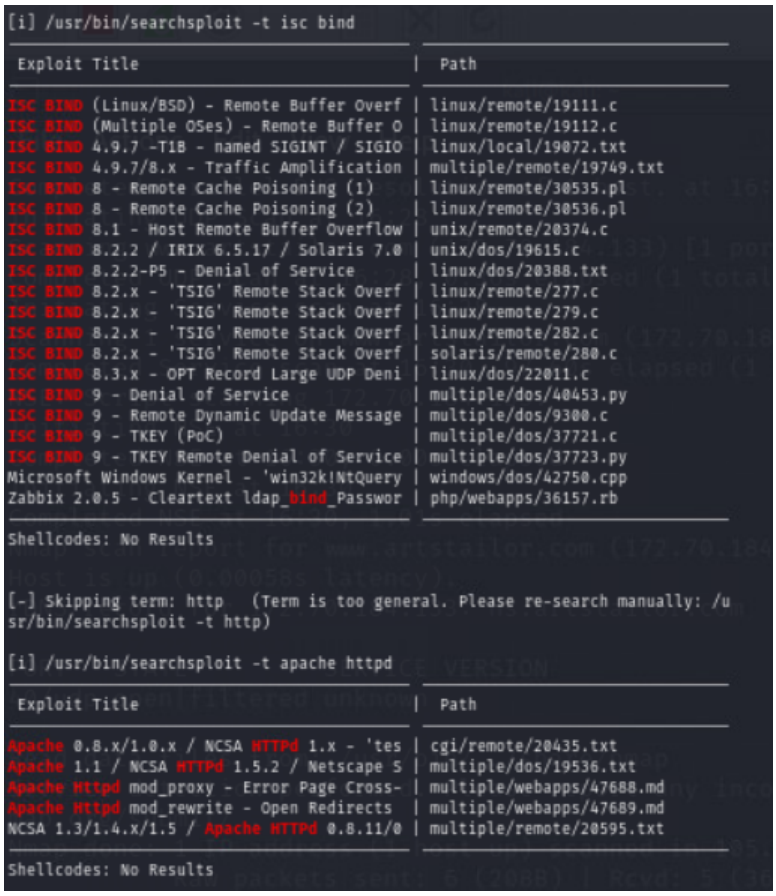


7. On a side note, we observe that the **UDP scan** took **239.44 seconds** while the **TCP scan** took only **21.30 seconds**. This is because of two reasons. Machines are not obliged to respond to closed UDP ports. And, the second is services running on UDP are also not obliged to respond to malformed UDP packets. This forces Nmap to use long waiting times for responses and also forces it to do more enumeration to collect accurate data.

8. Now using this information, we will perform searches using **searchsploit**. We can manually search or use an **automated option** with searchsploit to use the output from Nmap. We will use the latter. By running Nmap with option *-oA output-file-name*, it will write its output to disk in different formats including XML. We can then use this generated XML file as an input to searchsploit with option *–nmap*.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit --nmap nmaptcp.xml
[i] SearchSploit's XML mode (without verbose enabled).   To enable: searchsploit -v --xml ...
[i] Reading: 'nmaptcp.xml'

[-] Skipping term: ssh   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ssh)

[i] /usr/bin/searchsploit -t openssh
------------------------------------------------------ ---------------------------------
 Exploit Title                                        |  Path
------------------------------------------------------ ---------------------------------
Debian OpenSSH - (Authenticated) Remote SE | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CL | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Exe | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack  | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration   | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration ( | linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Ov | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Ov | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote D | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege  | linux/local/41173.c
OpenSSH 7.2 - Denial of Service            | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Comm | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration       | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Executi | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution     | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Di | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary L | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)       | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Us | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discove | linux/remote/25.c
```



We have the following observations for the machine's services:

(a) **OpenSSH** has **no exploit available**.

(b) **ISC BIND** on first look looks vulnerable to *ISC BIND 9 - DOS. TKEY, etc.* However on further inspection using **exploitdb.com** we find that those are not applicable for 9.18.16. Therefore **no exploit is available**.

(c) **Apache HTTP** has **no exploit available**.

1.1 MITRE ATT&CK Framework TTPs

TA0043: Reconnaissance

T1595: Active Scanning

.002: Vulnerability Scanning