

Ex0x5- Nmap

Jigar Patel

2023-10-17

Contents

1	Attack Narrative	2
1.1	MITRE ATT&CK Framework TTPs	8

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.

640	278.508709770	172.70.184.133	172.24.0.10	ICMP	98 Echo (ping) request	id=0x23d3, seq=1/256, ttl=63 (reply in 641)
641	278.508733661	172.24.0.10	172.70.184.133	ICMP	98 Echo (ping) reply	id=0x23d3, seq=1/256, ttl=64 (request in 640)
642	278.504869768	172.70.184.133	172.24.0.10	ICMP	98 Echo (ping) request	id=0xf67b, seq=1/256, ttl=63 (reply in 643)
643	278.504874216	172.24.0.10	172.70.184.133	ICMP	98 Echo (ping) reply	id=0xf67b, seq=1/256, ttl=64 (request in 642)
644	283.581314258	172.24.0.10	172.70.184.133	DTLS	109 Client Hello	
645	283.585969198	172.70.184.133	172.24.0.10	ICMP	98 Echo (ping) request	id=0x5a81, seq=1/256, ttl=63 (reply in 646)
646	283.585995737	172.24.0.10	172.70.184.133	ICMP	98 Echo (ping) reply	id=0x5a81, seq=1/256, ttl=64 (request in 645)
647	283.510347489	172.70.184.133	172.24.0.10	ICMP	98 Echo (ping) request	id=0xabd9, seq=1/256, ttl=63 (reply in 648)
648	283.510363519	172.24.0.10	172.70.184.133	ICMP	98 Echo (ping) reply	id=0xabd9, seq=1/256, ttl=64 (request in 647)
649	286.792893725	172.24.0.1	172.24.0.10	ICMP	98 Echo (ping) request	id=0xac88, seq=0/0, ttl=64 (reply in 650)

Source Address: 172.24.0.10	0000	00 50 56 87 ab 20 00 50	56 87 08 11 08 00 45 00	PV... P V... E
Destination Address: 172.70.184.133	0010	00 54 00 92 00 00 40 01	69 29 ac 18 00 0a ac 46	T...@: i)....F
Internet Control Message Protocol	0020	b8 85 00 00 e9 02 23 d3	00 01 87 cb 0d 65 00 00#.....e
Type: 8 (Echo (ping) request)	0030	00 00 00 19 03 00 00 00	00 00 4b 45 59 30 30 37e
Code: 0	0040	2d 35 32 6b 79 78 76 6a	48 4e 4b 45 59 30 30 37	-52kxyvj HNKEY007
Checksum: 0xe902 [correct]	0050	2d 35 32 6b 79 78 76 6a	48 4e 4b 45 59 30 30 37	-52kxyvj HNKEY007
[Checksum Status: Good]	0060	2d 35		-5

642	278.504869768	172.70.184.133	172.24.0.10	ICMP	98 Echo (ping) request	id=0xf67b, seq=1/256, ttl=63 (reply in 643)
643	278.504874216	172.24.0.10	172.70.184.133	ICMP	98 Echo (ping) reply	id=0xf67b, seq=1/256, ttl=64 (request in 642)
644	283.581314258	172.24.0.10	172.70.184.133	DTLS	109 Client Hello	
645	283.585969198	172.70.184.133	172.24.0.10	ICMP	98 Echo (ping) request	id=0x5a81, seq=1/256, ttl=63 (reply in 646)
646	283.585995737	172.24.0.10	172.70.184.133	ICMP	98 Echo (ping) reply	id=0x5a81, seq=1/256, ttl=64 (request in 645)
647	283.510347489	172.70.184.133	172.24.0.10	ICMP	98 Echo (ping) request	id=0xabd9, seq=1/256, ttl=63 (reply in 648)
648	283.510363519	172.24.0.10	172.70.184.133	ICMP	98 Echo (ping) reply	id=0xabd9, seq=1/256, ttl=64 (request in 647)
649	286.792893725	172.24.0.1	172.24.0.10	ICMP	98 Echo (ping) request	id=0xac88, seq=0/0, ttl=64 (reply in 650)

Source Address: 172.70.184.133	0000	30 50 56 87 08 11 00 50	56 87 ab 20 08 00 45 00	PV... P V... E
Destination Address: 172.24.0.10	0010	00 54 00 92 00 00 3f 01	9d 21 ac 40 b8 85 ac 18	T...@? :!F...
Internet Control Message Protocol	0020	00 0a 08 00 f6 e1 f6 7b	00 01 87 cb 0d 65 00 00{.....e
Type: 8 (Echo (ping) request)	0030	00 00 31 2a 03 00 00 00	00 00 61 38 53 4e 46 2f	1*.....a8SNF/
Code: 0	0040	73 35 35 4a 48 30 41 3d	3d 0a 61 38 53 4e 46 2f	s55JH0A= a8SNF/
Checksum: 0xf6e1 [correct]	0050	73 35 35 4a 48 30 41 3d	3d 0a 61 38 53 4e 46 2f	s55JH0A= a8SNF/
[Checksum Status: Good]	0060	73 35		s5

On concatenating, we find the key associated with this exercise as **KEY007-52kxyvjHN a8SNF/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 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 → 130 [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	130 → 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	1.717741892	172.70.184.133	172.24.0.10	TCP	60 7892 → 58841 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2011	1.717741842	172.70.184.133	172.24.0.10	TCP	60 9892 → 58841 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2012	1.884818784	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	1.884878296	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	1.8848184034	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	1.884542826	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	1.884596598	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	1.906493424	172.24.0.10	172.70.184.133	TCP	66 34248 → 22 [ACK] Seq=1 Ack=33 Win=64256 Len=0 TSval=2908842950 TSecr...
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 TSecr...
2025	1.909978734	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)

- 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 -p1-256 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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.44 seconds

```

We observe the following:

- UDP Port 40 Filtered/Open with an unknown service. When a UDP port does not respond, Nmap says it is filtered.
- UDP Port 53 Open with DNS running using ISC BIND 9.18.16-1 deb12u1.

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

Time	Source	Destination	Protocol	Length	Info
61.62	040941693	172.24.0.10	UDP	42	40347 → 81 Len=0
62.62	040948080	172.24.0.10	UDP	42	40347 → 30 Len=0
63.62	040953896	172.24.0.10	UDP	42	40347 → 120 Len=0
64.62	040959857	172.24.0.10	UDP	42	40347 → 117 Len=0
65.62	040965598	172.24.0.10	UDP	42	40347 → 14 Len=0
66.62	040971559	172.24.0.10	UDP	42	40347 → 1 Len=0
67.62	040977280	172.24.0.10	UDP	42	40347 → 36 Len=0
68.62	040983311	172.24.0.10	UDP	42	40347 → 25 Len=0
69.62	040989372	172.24.0.10	UDP	56	40347 → 80 Len=14
70.62	040995083	172.24.0.10	UDP	42	40347 → 76 Len=0
71.62	041003890	172.24.0.10	UDP	42	40347 → 20 Len=0
72.63	137722596	172.24.0.10	UDP	42	40349 → 29 Len=0
73.63	137818110	172.24.0.10	UDP	42	40349 → 70 Len=0
74.63	137819117	172.24.0.10	UDP	56	40349 → 80 Len=14
75.63	137826290	172.24.0.10	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.

66	86.170207945	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
67	86.170208346	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
68	86.170208416	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
69	86.170208476	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
70	86.170208547	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
71	86.170208607	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
72	86.172368808	172.24.0.10	172.70.184.133	UDP	42 57298 → 49 Len=0
73	86.172384878	172.24.0.10	172.70.184.133	UDP	42 57298 → 38 Len=0
74	86.172392603	172.24.0.10	172.70.184.133	Portmap	82 V104316 proc=0 Call
75	86.172398964	172.24.0.10	172.70.184.133	RPC	82 Continuation
76	86.172406088	172.24.0.10	172.70.184.133	UDP	42 57298 → 93 Len=0

Time to Live: 57	0000	00 50 56 87 08 11 00 50 56 87 ab 20 08 00 45 c0	→	00 50 56 87 08 11 00 50 56 87 ab 20 08 00 45 c0
Protocol: UDP (17)	0010	00 38 2e c3 00 00 3f 01 3b 54 ac 46 b8 85 ac 18	→	00 38 2e c3 00 00 3f 01 3b 54 ac 46 b8 85 ac 18
Header Checksum: 0x157e [validation disabled]	0020	00 0a 03 03 0e 05 00 00 00 00 45 00 00 1c 5b 65	→	00 0a 03 03 0e 05 00 00 00 00 45 00 00 1c 5b 65
[Header checksum status: Unverified]	0030	00 00 39 11 15 7e ac 18 00 0a ac 46 b8 85 df d2	→	00 00 39 11 15 7e ac 18 00 0a ac 46 b8 85 df d2
Source Address: 172.24.0.10	0040	00 34 00 08 0e e9	→	00 34 00 08 0e e9
Destination Address: 172.70.184.133				
IP Datagram Protocol, Src Port: 57298, Dst Port: 52				
Source Port: 57298				

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.

300	136.930146802	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
301	137.930561502	172.24.0.10	172.70.184.133	TFTP	72 Option Acknowledgement, \001=, \001=, =, \aversion\004bind=[Mal-
302	137.930641752	172.24.0.10	172.70.184.133	TFTP	54 Unknown (0x0000)
303	137.931629595	172.70.184.133	172.24.0.10	TFTP	109 Option Acknowledgement, 6=, \001=\001, =, =\aversion\004bind, =\020
304	137.931629976	172.70.184.133	172.24.0.10	TFTP	60 Unknown (0x0000)
305	137.931688470	172.24.0.10	172.70.184.133	ICMP	137 Destination unreachable (Port unreachable)
306	137.931690651	172.24.0.10	172.70.184.133	ICMP	82 Destination unreachable (Port unreachable)
307	138.931680031	172.24.0.10	172.70.184.133	UDP	42 57298 → 106 Len=0
308	138.932679225	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
309	139.932869992	172.24.0.10	172.70.184.133	UDP	42 57298 → 113 Len=0
310	139.933685025	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
311	140.933938500	172.24.0.10	172.70.184.133	UDP	42 57298 → 51 Len=0
312	140.934070045	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
317	141.934985525	172.24.0.10	172.70.184.133	UDP	42 57298 → 118 Len=0
318	141.935570302	172.70.184.133	172.24.0.10	ICMP	70 Destination unreachable (Port unreachable)
319	142.936045424	172.24.0.10	172.70.184.133	UDP	42 57298 → 79 Len=0

[Header checksum status: Unverified]	0000	00 50 56 87 08 11 00 50 56 87 ab 20 08 00 45 00	→	00 50 56 87 08 11 00 50 56 87 ab 20 08 00 45 00
Source Address: 172.70.184.133	0010	00 5f f4 89 00 00 3f 11 76 16 ac 46 b8 85 ac 18	→	00 5f f4 89 00 00 3f 11 76 16 ac 46 b8 85 ac 18
Destination Address: 172.24.0.10	0020	00 0a 00 35 df d2 00 4b d6 49 00 06 85 00 00 01	→	00 0a 00 35 df d2 00 4b d6 49 00 06 85 00 00 01
IP Datagram Protocol, Src Port: 53, Dst Port: 57298	0030	00 01 00 00 00 00 07 76 65 72 73 69 6f 6e 04 62	→	00 01 00 00 00 00 07 76 65 72 73 69 6f 6e 04 62
Source Port: 53	0040	69 6e 64 00 00 10 00 03 c0 0c 00 10 00 03 00 00	→	69 6e 64 00 00 10 00 03 c0 0c 00 10 00 03 00 00
Destination Port: 57298	0050	00 00 00 19 18 39 2e 31 38 2e 31 36 2d 31 7e 64	→	00 00 00 19 18 39 2e 31 38 2e 31 36 2d 31 7e 64
Length: 75	0060	65 62 31 32 75 31 2d 44 65 62 69 61 6e	→	65 62 31 32 75 31 2d 44 65 62 69 61 6e

168	93.682267203	172.24.0.10	172.70.184.133	TFTP	61 Read Request, File: r7tftp.txt, Transfer type: octet
169	93.732352003	172.24.0.10	172.70.184.133	UDP	42 57304 → 25 Len=0
170	93.782518919	172.24.0.10	172.70.184.133	TFTP	54 Unknown (0x0000)
171	93.782538470	172.24.0.10	172.70.184.133	TFTP	61 Read Request, File: r7tftp.txt, Transfer type: octet
172	93.832641182	172.24.0.10	172.70.184.133	UDP	42 57306 → 25 Len=0
173	93.882781004	172.24.0.10	172.70.184.133	TFTP	54 Unknown (0x0000)
174	93.882852058	172.24.0.10	172.70.184.133	TFTP	61 Read Request, File: r7tftp.txt, Transfer type: octet
175	93.932926074	172.24.0.10	172.70.184.133	UDP	42 57308 → 25 Len=0
176	93.983064072	172.24.0.10	172.70.184.133	TFTP	54 Unknown (0x0000)
177	93.983083669	172.24.0.10	172.70.184.133	TFTP	61 Read Request, File: r7tftp.txt, Transfer type: octet
178	94.033208472	172.24.0.10	172.70.184.133	TFTP	286 Unknown (0x0101)
179	94.083347722	172.24.0.10	172.70.184.133	TFTP	54 Unknown (0x0000)
180	94.083416582	172.24.0.10	172.70.184.133	TFTP	61 Read Request, File: r7tftp.txt, Transfer type: octet
181	94.133474830	172.24.0.10	172.70.184.133	TFTP	286 Unknown (0x0101)
182	94.183602009	172.24.0.10	172.70.184.133	TFTP	54 Unknown (0x0000)

[Header checksum status: Unverified]	0000	00 50 56 87 ab 20 00 50 56 87 08 11 08 00 45 00	→	00 50 56 87 ab 20 00 50 56 87 08 11 08 00 45 00
Source Address: 172.24.0.10	0010	00 2f ca 21 00 00 34 11 ab ae ac 18 00 0a ac 46	→	00 2f ca 21 00 00 34 11 ab ae ac 18 00 0a ac 46
Destination Address: 172.70.184.133	0020	b8 85 df d2 00 45 00 1b 43 62 00 01 72 37 74 66	→	b8 85 df d2 00 45 00 1b 43 62 00 01 72 37 74 66
IP Datagram Protocol, Src Port: 57298, Dst Port: 69	0030	74 70 2e 74 78 74 00 6f 63 74 65 74 00	→	74 70 2e 74 78 74 00 6f 63 74 65 74 00
Source Port: 57298				
Destination Port: 69				
Length: 27				
Checksum: 0x4362 [unverified]				
[Checksum Status: Unverified]				
[Stream Index: 91]				
[Timestamps]				
UDP payload (19 bytes)				

539	220.050794178	172.24.0.10	172.70.184.133	Portmap	82	V104316 proc-0 Call
548	225.055411625	172.24.0.10	172.70.184.133	DNS	72	Standard query 0x0006 TXT version.bind
553	230.060095053	172.24.0.10	172.70.184.133	UDP	54	59000 → 40 Len=12
562	235.065993617	172.24.0.10	172.70.184.133	DNS	92	Standard query 0x80f0 SRV CKAAAAAAAAAAAAAAAAAAAAAAAAAAAA
567	240.069047743	172.24.0.10	172.70.184.133	UDP	50	46682 → 40 Len=8
576	245.074339225	172.24.0.10	172.70.184.133	SIP	271	Request: OPTIONS sip:nm
581	245.240925928	VMware_87:08:11	VMware_87:ab:20	ARP	42	who has 172.24.0.1? Tell 172.24.0.10
582	245.241191196	VMware_87:ab:20	VMware_87:08:11	ARP	60	172.24.0.1 is at 00:50:56:87:ab:20
587	252.581948279	172.24.0.10	172.70.184.133	UDP	43	37154 → 40 Len=1
592	257.585027079	172.24.0.10	172.70.184.133	UDP	90	56103 → 40 Len=48
601	262.589057536	172.24.0.10	172.70.184.133	UDP	93	38389 → 40 Len=51
606	267.593083023	172.24.0.10	172.70.184.133	UDP	102	35147 → 40 Len=60
615	272.597021167	172.24.0.10	172.70.184.133	UDP	49	36444 → 40 Len=7
620	277.601535321	172.24.0.10	172.70.184.133	UDP	74	49584 → 40 Len=32
629	282.605015265	172.24.0.10	172.70.184.133	DNS	88	Standard query 0x0000 PTR _services._dns-sd._udp.local

Header checksum status: Unverified]		0000	00 50 56 87 ab 20 00 50	56 87 00 11 00 00 45 00	PV...P V....E
Source Address: 172.24.0.10		0010	00 4e 9a 5d 40 00 40 11	8f 53 ac 18 00 0a ac 46	N]@ @. .S....F
Destination Address: 172.70.184.133		0020	b8 85 c1 ef 00 28 00 3a	11 3a 80 f0 00 10 00 01(: :.....
Datagram Protocol, Src Port: 49647, Dst Port: 40		0030	00 00 00 00 00 00 20 43	40 41 41 41 41 41 41 41C KAAAAAA
Source Port: 49647		0040	41 41 41 41 41 41 41 41	41 41 41 41 41 41 41 41	AAAAAAA AAAAAAA
Destination Port: 40		0050	41 41 41 41 41 41 41 00	00 21 00 01	AAAAAAA ! !...

- 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.
- 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
```



```
[i] /usr/bin/searchsploit -t isc bind
```

Exploit Title	Path
ISC BIND (Linux/BSD) - Remote Buffer Overf	linux/remote/19111.c
ISC BIND (Multiple OSes) - Remote Buffer O	linux/remote/19112.c
ISC BIND 4.9.7 -T1B - named SIGINT / SIGIO	linux/local/19072.txt
ISC BIND 4.9.7/8.x - Traffic Amplification	multiple/remote/19749.txt
ISC BIND 8 - Remote Cache Poisoning (1)	linux/remote/30535.pl
ISC BIND 8 - Remote Cache Poisoning (2)	linux/remote/30536.pl
ISC BIND 8.1 - Host Remote Buffer Overflow	unix/remote/20374.c
ISC BIND 8.2.2 / IRIX 6.5.17 / Solaris 7.0	unix/dos/19615.c
ISC BIND 8.2.2-P5 - Denial of Service	linux/dos/20388.txt
ISC BIND 8.2.x - 'TSIG' Remote Stack Overf	linux/remote/277.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overf	linux/remote/279.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overf	linux/remote/282.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overf	solaris/remote/280.c
ISC BIND 8.3.x - OPT Record Large UDP Deni	linux/dos/22011.c
ISC BIND 9 - Denial of Service	multiple/dos/40453.py
ISC BIND 9 - Remote Dynamic Update Message	multiple/dos/9300.c
ISC BIND 9 - TKEY (PoC)	multiple/dos/37721.c
ISC BIND 9 - TKEY Remote Denial of Service	multiple/dos/37723.py
Microsoft Windows Kernel - 'win32k!NtQuery	windows/dos/42750.cxx
Zabbix 2.0.5 - Cleartext ldap_bind_Passwor	php/webapps/36157.rb

```
Shellcodes: No Results

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

[i] /usr/bin/searchsploit -t apache httpd
```

Exploit Title	Path
Apache 0.8.x/1.0.x / NCSA HTTPd 1.x - 'tes	cgi/remote/20435.txt
Apache 1.1 / NCSA HTTPd 1.5.2 / Netscape S	multiple/dos/19536.txt
Apache httpd mod_proxy - Error Page Cross-	multiple/webapps/47688.md
Apache httpd mod_rewrite - Open Redirects	multiple/webapps/47689.md
NCSA 1.3/1.4.x/1.5 / Apache HTTPd 0.8.11/0	multiple/remote/20595.txt

```
Shellcodes: No Results
```

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