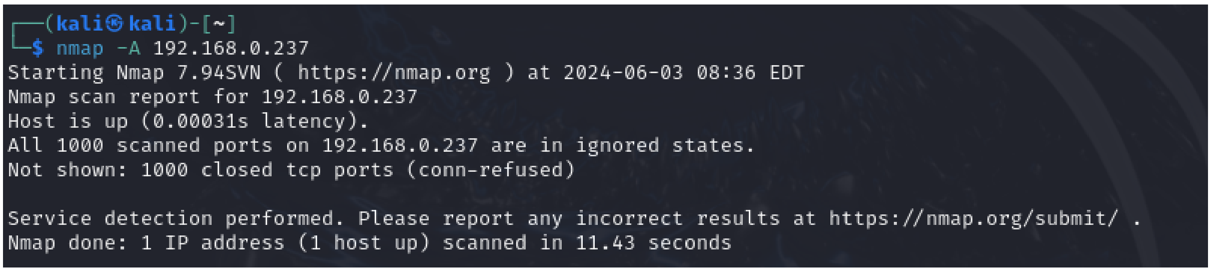
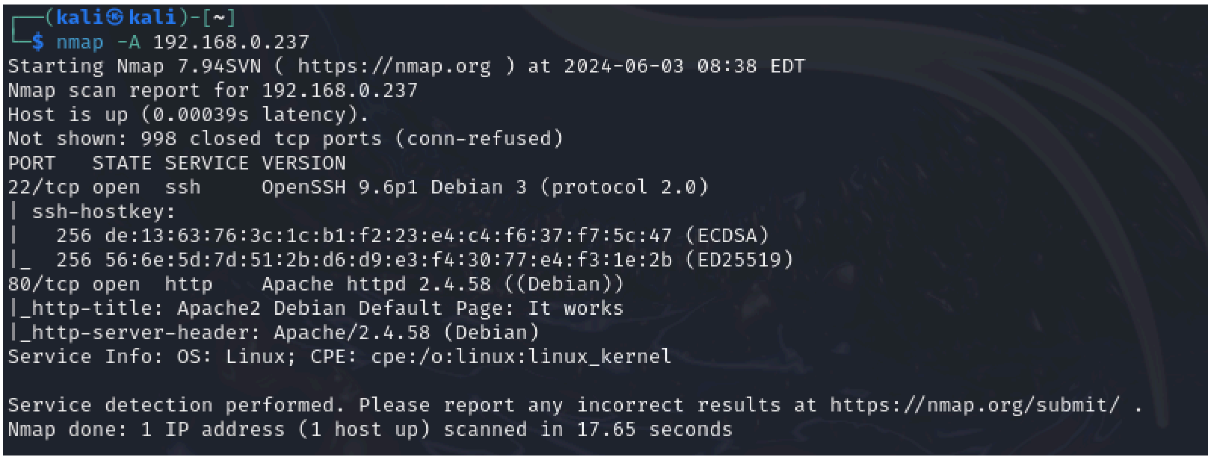
- Scan the Target Machine with Nmap.



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.0.237
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:36 EDT
Nmap scan report for 192.168.0.237
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.0.237 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds
```

- Open a terminal on your attacker machine. Use Nmap to scan the target machine's IP address for open ports.



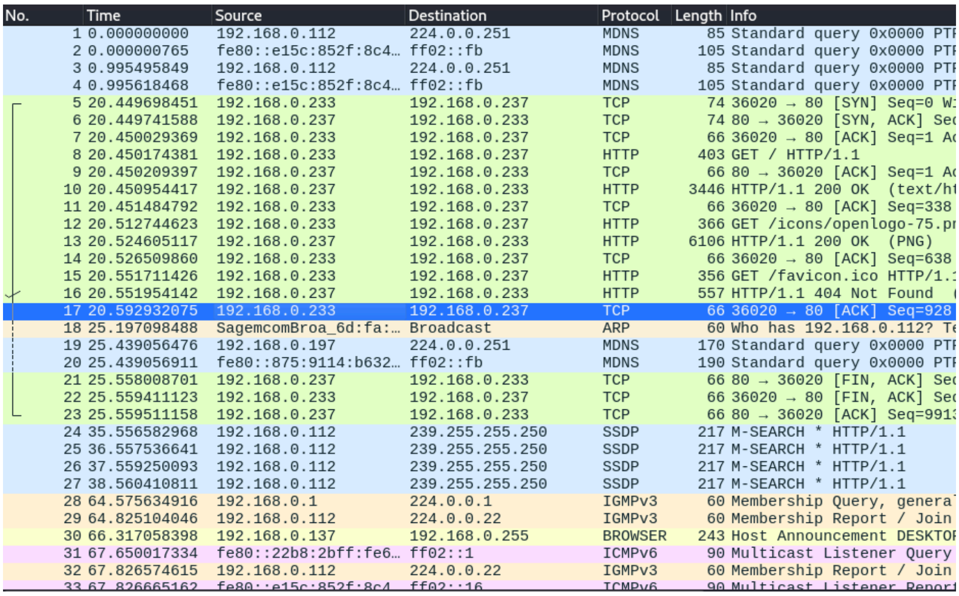
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.0.237
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:38 EDT
Nmap scan report for 192.168.0.237
Host is up (0.00039s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Debian 3 (protocol 2.0)
| ssh-hostkey:
|   256 de:13:63:76:3c:1c:b1:f2:23:e4:c4:f6:37:f7:5c:47 (ECDSA)
|_  256 56:6e:5d:7d:51:2b:d6:d9:e3:f4:30:77:e4:f3:1e:2b (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.58 (Debian)
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 17.65 seconds
```

- Analyze the Nmap scan results. Identify open ports, services running on those ports, and any version information Nmap discovers.

  - Open ports: 22: SSH - 9.6p1 Debian 3

    80: Apache2 - Apache/2.4.58

- Capture Network Traffic with Wireshark

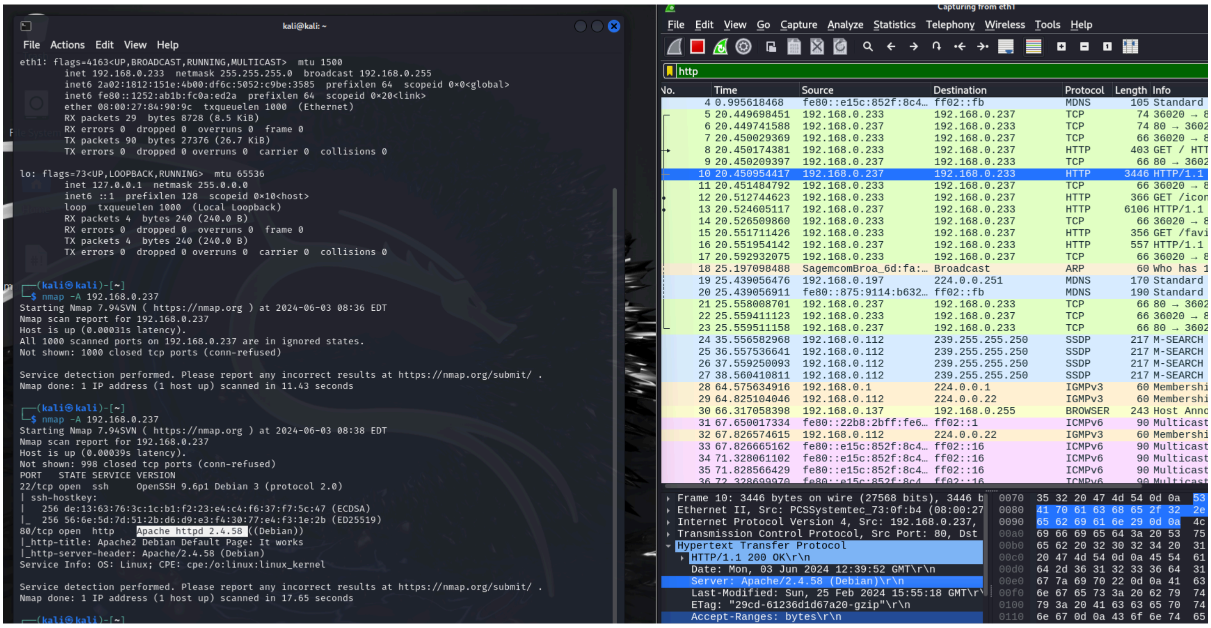


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.112	224.0.0.251	MDNS	85	Standard query 0x0000 PTR
2	0.000000765	fe80::e15c:852f:8c4…	ff02::fb	MDNS	105	Standard query 0x0000 PTR
3	0.995495849	192.168.0.112	224.0.0.251	MDNS	85	Standard query 0x0000 PTR
4	0.995618468	fe80::e15c:852f:8c4…	ff02::fb	MDNS	105	Standard query 0x0000 PTR
5	20.449698451	192.168.0.233	192.168.0.237	TCP	74	36020 → 80 [SYN] Seq=0 W
6	20.449741588	192.168.0.237	192.168.0.233	TCP	74	80 → 36020 [SYN, ACK] Sec
7	20.450029369	192.168.0.233	192.168.0.237	TCP	66	36020 → 80 [ACK] Seq=1 Ac
8	20.450174381	192.168.0.233	192.168.0.237	HTTP	403	GET / HTTP/1.1
9	20.450209397	192.168.0.237	192.168.0.233	TCP	66	80 → 36020 [ACK] Seq=1 Ac
10	20.450954417	192.168.0.237	192.168.0.233	HTTP	3446	HTTP/1.1 200 OK (text/ht
11	20.451484792	192.168.0.233	192.168.0.237	TCP	66	36020 → 80 [ACK] Seq=338
12	20.512744623	192.168.0.233	192.168.0.237	HTTP	366	GET /icons/openlogo-75.pr
13	20.524605117	192.168.0.237	192.168.0.233	HTTP	6106	HTTP/1.1 200 OK (PNG)
14	20.526509860	192.168.0.233	192.168.0.237	TCP	66	36020 → 80 [ACK] Seq=638
15	20.551711426	192.168.0.233	192.168.0.237	HTTP	356	GET /favicon.ico HTTP/1.:
16	20.551954142	192.168.0.237	192.168.0.233	HTTP	557	HTTP/1.1 404 Not Found (
17	20.592932075	192.168.0.233	192.168.0.237	TCP	66	36020 → 80 [ACK] Seq=928
18	25.197098488	SagemcomBroa_6d:fa:…	Broadcast	ARP	60	Who has 192.168.0.112? Te
19	25.439056476	192.168.0.197	224.0.0.251	MDNS	170	Standard query 0x0000 PTR
20	25.439056911	fe80::875:9114:b632…	ff02::fb	MDNS	190	Standard query 0x0000 PTR
21	25.558008701	192.168.0.237	192.168.0.233	TCP	66	80 → 36020 [FIN, ACK] Sec
22	25.559411123	192.168.0.233	192.168.0.237	TCP	66	36020 → 80 [FIN, ACK] Sec
23	25.559511158	192.168.0.237	192.168.0.233	TCP	66	80 → 36020 [ACK] Seq=991:
24	35.556582968	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
25	36.557536641	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
26	37.559250093	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
27	38.560410811	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
28	64.575634916	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, genera
29	64.825104046	192.168.0.112	224.0.0.22	IGMPv3	60	Membership Report / Join
30	66.317058398	192.168.0.137	192.168.0.255	BROWSER	243	Host Announcement DESKTOF
31	67.650017334	fe80::22b8:2bff:fe6…	ff02::1	ICMPv6	90	Multicast Listener Query
32	67.826574615	192.168.0.112	224.0.0.22	IGMPv3	60	Membership Report / Join
33	67.826665162	fe80::e15c:852f:8c4…	ff02::16	ICMPv6	90	Multicast Listener Report

- Open Wireshark on your target machine. Start capturing traffic on the network interface connected to your attacker machine

- On your attacker machine, use a web browser to access a website you know is running on port 80. This will generate traffic between the two machines.

- Correlate Nmap and Wireshark Findings



```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.233  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2a02:1812:151e:4b00:df6c:5052:c9be:3585  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::1252:ab1b:fc0a:ed2a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:84:90:9c  txqueuelen 1000  (Ethernet)
        RX packets 29  bytes 8728 (8.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 90  bytes 27376 (26.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.0.237
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:36 EDT
Nmap scan report for 192.168.0.237
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.0.237 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.0.237
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 08:38 EDT
Nmap scan report for 192.168.0.237
Host is up (0.00039s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Debian 3 (protocol 2.0)
| ssh-hostkey:
|   256 de:13:63:76:3c:1c:b1:f2:23:e4:c4:f6:37:f7:5c:47 (ECDSA)
|_  256 56:6e:5d:7d:51:2b:d6:d9:e3:f4:30:77:e4:f3:1e:2b (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.58 (Debian)
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 17.65 seconds

┌──(kali㉿kali)-[~]
```

Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

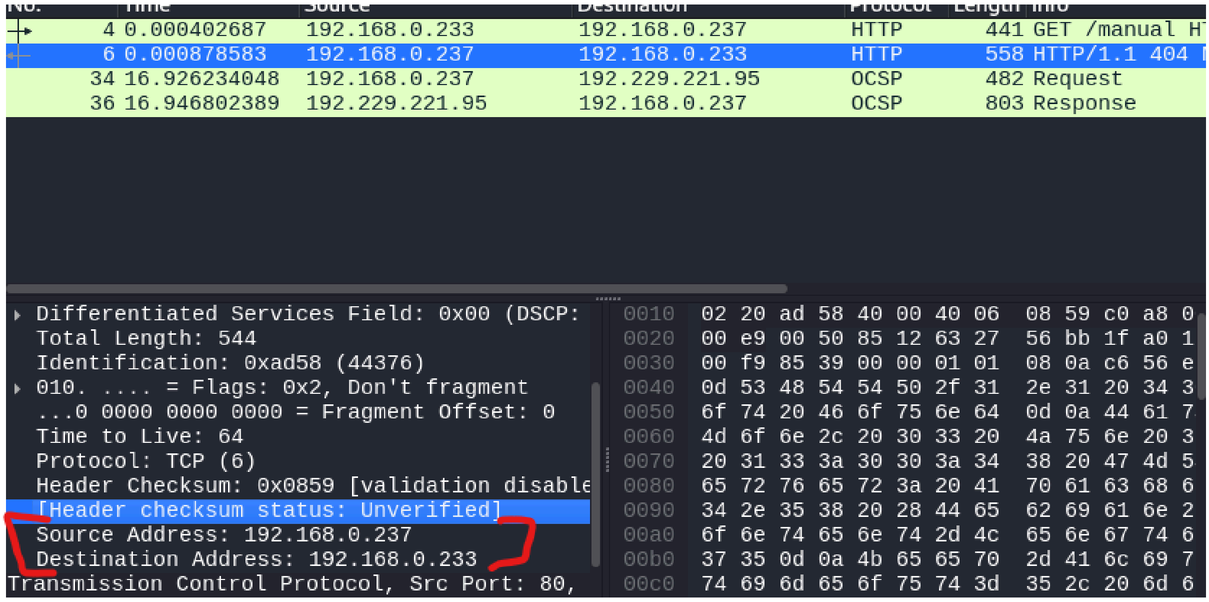
No.	Time	Source	Destination	Protocol	Length	Info
4	0.995618468	fe80::e15c:852f:8c4…	ff02::fb	MDNS	105	Standard
5	20.449698451	192.168.0.233	192.168.0.237	TCP	74	36020 → 8
6	20.449741588	192.168.0.237	192.168.0.233	TCP	74	80 → 3602
7	20.450029369	192.168.0.233	192.168.0.237	TCP	66	36020 → 8
8	20.450174381	192.168.0.233	192.168.0.237	HTTP	403	GET / HTT
9	20.450209397	192.168.0.237	192.168.0.233	TCP	66	80 → 3602
10	20.450954417	192.168.0.237	192.168.0.233	HTTP	3446	HTTP/1.1
11	20.451484792	192.168.0.233	192.168.0.237	TCP	66	36020 → 8
12	20.512744623	192.168.0.233	192.168.0.237	HTTP	366	GET /icon
13	20.524605117	192.168.0.237	192.168.0.233	HTTP	6106	HTTP/1.1
14	20.526509860	192.168.0.233	192.168.0.237	TCP	66	36020 → 8
15	20.551711426	192.168.0.233	192.168.0.237	HTTP	356	GET /favi
16	20.551954142	192.168.0.237	192.168.0.233	HTTP	557	HTTP/1.1
17	20.592932075	192.168.0.233	192.168.0.237	TCP	66	36020 → 8
18	25.197098488	SagemcomBroa_6d:fa:…	Broadcast	ARP	60	Who has 1
19	25.439056476	192.168.0.197	224.0.0.251	MDNS	170	Standard
20	25.439056911	fe80::875:9114:b632…	ff02::fb	MDNS	190	Standard
21	25.558008701	192.168.0.237	192.168.0.233	TCP	66	80 → 3602
22	25.559411123	192.168.0.233	192.168.0.237	TCP	66	36020 → 8
23	25.559511158	192.168.0.237	192.168.0.233	TCP	66	80 → 3602
24	35.556582968	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH
25	36.557536641	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH
26	37.559250093	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH
27	38.560410811	192.168.0.112	239.255.255.250	SSDP	217	M-SEARCH
28	64.575634916	192.168.0.1	224.0.0.1	IGMPv3	60	Membershi
29	64.825104046	192.168.0.112	224.0.0.22	IGMPv3	60	Membershi
30	66.317058398	192.168.0.137	192.168.0.255	BROWSER	243	Host Anno
31	67.650017334	fe80::22b8:2bff:fe6…	ff02::1	ICMPv6	90	Multicast
32	67.826574615	192.168.0.112	224.0.0.22	IGMPv3	60	Membershi
33	67.826665162	fe80::e15c:852f:8c4…	ff02::16	ICMPv6	90	Multicast
34	71.328061102	fe80::e15c:852f:8c4…	ff02::16	ICMPv6	90	Multicast
35	71.828566429	fe80::e15c:852f:8c4…	ff02::16	ICMPv6	90	Multicast
36	72.328699970	fe80::e15c:852f:8c4…	ff02::16	ICMPv6	90	Multicast

```
› Frame 10: 3446 bytes on wire (27568 bits), 3446 b    0070  35 32 20 47 4d 54 0d 0a  53
› Ethernet II, Src: PCSSystemtec_73:0f:b4 (08:00:27    0080  41 70 61 63 68 65 2f 32  2e
› Internet Protocol Version 4, Src: 192.168.0.237,     0090  65 62 69 61 6e 29 0d 0a  4c
› Transmission Control Protocol, Src Port: 80, Dst     00a0  69 66 69 65 64 3a 20 53  75
⌄ Hypertext Transfer Protocol                          00b0  65 62 20 32 30 32 34 20  31
  › HTTP/1.1 200 OK\r\n                                00c0  20 47 4d 54 0d 0a 45 54  61
    Date: Mon, 03 Jun 2024 12:39:52 GMT\r\n            00d0  64 2d 36 31 32 33 36 64  31
    Server: Apache/2.4.58 (Debian)\r\n                 00e0  67 7a 69 70 22 0d 0a 41  63
    Last-Modified: Sun, 25 Feb 2024 15:55:18 GMT\r\    00f0  6e 67 65 73 3a 20 62 79  74
    ETag: "29cd-61236d1d67a20-gzip"\r\n                0100  79 3a 20 41 63 63 65 70  74
    Accept-Ranges: bytes\r\n                           0110  6e 67 0d 0a 43 6f 6e 74  65
```

- Stop the capture on your target machine's Wireshark.

- Open the captured traffic file in Wireshark on your attacker machine.

- Analyze the captured packets. Can you identify the communication between your attacker machine and the target machine? Do the details in the captured packets match what you discovered with Nmap?



```
No.   Time          Source          Destination     Protocol  Length Info
    4 0.000402687   192.168.0.233   192.168.0.237   HTTP         441 GET /manual H
    6 0.000878583   192.168.0.237   192.168.0.233   HTTP         558 HTTP/1.1 404 
   34 16.926234048  192.168.0.237   192.229.221.95  OCSP         482 Request
   36 16.946802389  192.229.221.95  192.168.0.237   OCSP         803 Response
```

```
  Differentiated Services Field: 0x00 (DSCP:
  Total Length: 544
  Identification: 0xad58 (44376)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x0859 [validation disable
  [Header checksum status: Unverified]
  Source Address: 192.168.0.237
  Destination Address: 192.168.0.233
Transmission Control Protocol, Src Port: 80,
```

```
0010  02 20 ad 58 40 00 40 06  08 59 c0 a8 0
0020  00 e9 00 50 85 12 63 27  56 bb 1f a0 1
0030  00 f9 85 39 00 00 01 01  08 0a c6 56 e
0040  0d 53 48 54 54 50 2f 31  2e 31 20 34 3
0050  6f 74 20 46 6f 75 6e 64  0d 0a 44 61 7
0060  4d 6f 6e 2c 20 30 33 20  4a 75 6e 20 3
0070  20 31 33 3a 30 30 3a 34  38 20 47 4d 5
0080  65 72 76 65 72 3a 20 41  70 61 63 68 6
0090  34 2e 35 38 20 28 44 65  62 69 61 6e 2
00a0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 6
00b0  37 35 0d 0a 4b 65 65 70  2d 41 6c 69 7
00c0  74 69 6d 65 6f 75 74 3d  35 2c 20 6d 6
```

- Repeat step 1 but use a different Nmap scan type that scans for fewer ports (e.g., nmap -sS <target_IP> for a SYN scan). Try capturing traffic for a different service running on a different port (e.g., SSH on port 22).