Identify Denial-of-Service (DoS) Attack with Wireshark

What is Wireshark?

Wireshark is a widely used open-source network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It provides deep insight into network communications, making it an essential tool for network administrators, security professionals, and developers.

Question: Identify SYN Floods.

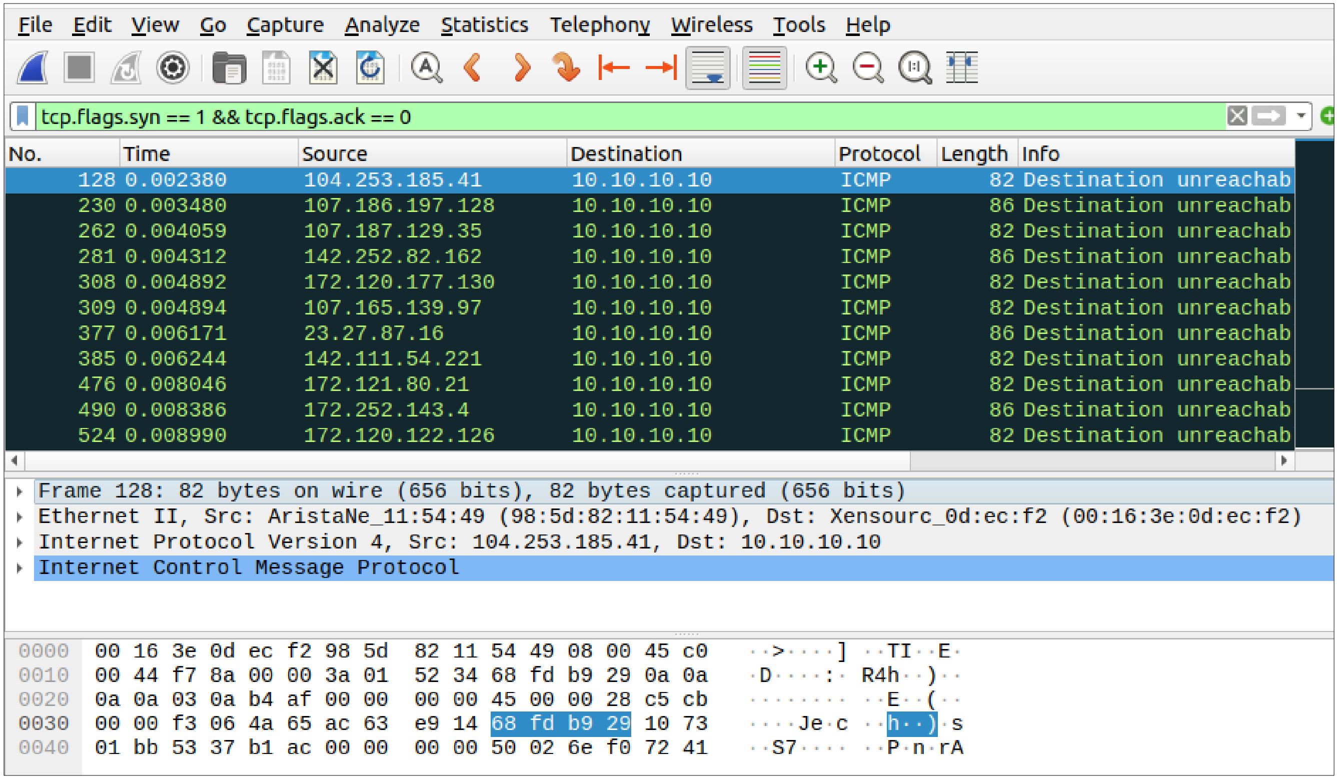
What are SYN floods?

A SYN flood is a type of Denial of Service (DoS) attack that targets the TCP handshake process to overwhelm a server or network resource, making it unavailable to legitimate users.

This process is characterized by a process where the attacker sends a large number of SYN packets to the target server, often with spoofed source IP addresses. The server responds to each SYN packet with a SYN-ACK, expecting an ACK in return. Since the source IP addresses are often fake, the server never receives the expected ACK, leaving the connection half-open. The server maintains these half-open connections in a queue, consuming resources. If the queue becomes full, the server can no longer accept new connections, effectively denying service to legitimate users.

Steps

- Import pcap.
- Query: the image below shows SYN Flood query example:



```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

```
No.      Time      Source            Destination    Protocol  Length Info
     128 0.002380  104.253.185.41    10.10.10.10    ICMP          82 Destination unreachab
     230 0.003480  107.186.197.128   10.10.10.10    ICMP          86 Destination unreachab
     262 0.004059  107.187.129.35    10.10.10.10    ICMP          82 Destination unreachab
     281 0.004312  142.252.82.162    10.10.10.10    ICMP          86 Destination unreachab
     308 0.004892  172.120.177.130   10.10.10.10    ICMP          82 Destination unreachab
     309 0.004894  107.165.139.97    10.10.10.10    ICMP          82 Destination unreachab
     377 0.006171  23.27.87.16       10.10.10.10    ICMP          86 Destination unreachab
     385 0.006244  142.111.54.221    10.10.10.10    ICMP          82 Destination unreachab
     476 0.008046  172.121.80.21     10.10.10.10    ICMP          82 Destination unreachab
     490 0.008386  172.252.143.4     10.10.10.10    ICMP          86 Destination unreachab
     524 0.008990  172.120.122.126   10.10.10.10    ICMP          82 Destination unreachab
```

```
▸ Frame 128: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
▸ Ethernet II, Src: AristaNe_11:54:49 (98:5d:82:11:54:49), Dst: Xensourc_0d:ec:f2 (00:16:3e:0d:ec:f2)
▸ Internet Protocol Version 4, Src: 104.253.185.41, Dst: 10.10.10.10
▸ Internet Control Message Protocol
```

```
0000  00 16 3e 0d ec f2 98 5d  82 11 54 49 08 00 45 c0   ··>····]  ··TI··E·
0010  00 44 f7 8a 00 00 3a 01  52 34 68 fd b9 29 0a 0a   ·D····:·  R4h··)··
0020  0a 0a 03 0a b4 af 00 00  00 00 45 00 00 28 c5 cb   ········  ··E··(··
0030  00 00 f3 06 4a 65 ac 63  e9 14 68 fd b9 29 10 73   ····Je·c  ··h··)·s
0040  01 bb 53 37 b1 ac 00 00  00 00 50 02 6e f0 72 41   ··S7····  ··P·n·rA
```

Findings: numerous SYN packets without corresponding ACK packets.