

Assignment No 2- SYN Attack Simulation

Net-ID: sdh140430

Swapnil Hasabe

Problem statement: As posted on e-learning, Simulate and observe SYN Attack using VMs.

Tools Learned: **Wireshark, SCAPY, python**

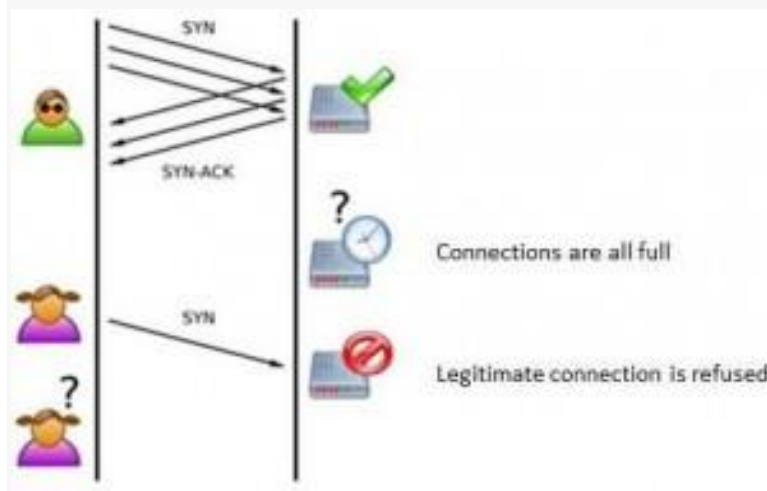
Need of Three way handshake: Machines cannot see each other. So, there should be connection between those machines.

A SYN flood is a type of denial-of-service attack in which an attacker sends a succession of SYN requests to a victim's system in order to consume enough server resources. In result, server becomes unresponsive when any legitimate client sends request to server.

Three way handshake:

```
Client                                Server
-----                                -----
SYN----->
<-----SYN-ACK
ACK----->
Client and server can send server specific data now
```

How To Detect TCP Syn Flood Attack



IP spoofing is the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.

I used command to start HTTP server on VM machine at port no.8000

python -m SimpleHTTPServer

Step1: Attacker machine IP.addr="192.168.0.8" sends SYN Packets To Victim Machine (192.168.0.20)

The image shows a Wireshark packet capture from interface wlan0. The filter is set to `ip.dst==192.168.0.20`. The capture shows a series of SYN packets from 192.168.0.8 to 192.168.0.20. The first packet is a [FIN, ACK] from 8000-52624. Subsequent packets are [SYN] from 22000-8000 and [RST] from 54 22000-8000. The rest of the packets are [TCP Retransmission] of the [SYN] packet. The packet details pane shows the selected packet as a Transmission Control Protocol, Src Port: 8000 (8000), Dst Port: 52624 (52624), Seq: 1, Ack: 2, Len: 0. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
855	570.16244106	192.168.0.8	192.168.0.20	TCP	66	8000-52624 [FIN, ACK] Seq=1 Ack=2 Win=227 Len=0 TSval=817947 TSecr=570237898
1505	847.28357506	192.168.0.8	192.168.0.20	TCP	61	22000-8000 [SYN] Seq=0 Win=8192 Len=7
1507	847.29110306	192.168.0.8	192.168.0.20	TCP	54	22000-8000 [RST] Seq=1 Win=0 Len=0
2261	1339.0714586	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2263	1339.1076696	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2264	1339.1354606	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2265	1339.1635546	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2266	1339.1994586	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2267	1339.2315336	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2268	1339.2835866	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2269	1339.3275186	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2270	1339.3755076	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2271	1339.4155086	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2272	1339.4555116	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2273	1339.4994326	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2274	1339.5395936	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2275	1339.5835156	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2276	1339.6234776	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2277	1339.6635186	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2278	1339.6954866	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2279	1339.7275166	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2280	1339.7633326	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2281	1339.8075136	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2282	1339.8474896	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2283	1339.8915146	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2284	1339.9315486	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7
2285	1339.9715546	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 22000-8000 [SYN] Seq=0 Win=8192 Len=7

Transmission Control Protocol, Src Port: 8000 (8000), Dst Port: 52624 (52624), Seq: 1, Ack: 2, Len: 0

0000 c0 ce cd e7 a0 f1 4c bb 58 cf c5 95 08 00 45 00L. X.....E.
0010 00 34 7c fd 40 00 40 06 3c 5a c0 a8 00 08 c0 a8 .4|. @. @. <Z.....
0020 00 14 1f 40 cd 90 be 4f 44 60 73 68 28 67 80 11 ... @...0 D'sh(g...
0030 e0 e3 a8 2d 00 00 01 01 08 0a 00 0c 7b 1b 21 fd{.l.
0040

wlan0: <live capture in progres... Packets: 3818 · Displayed: 426 (11.2%) Profile: Default

Step2 : Victim machine receives SYN Packets and it sends back “SYN+ACK” packets Flag(SYN) Syn:Set

Wireshark capture showing a SYN flood attack. The packet list shows multiple SYN packets from 192.168.0.8 to 192.168.0.20. Packet 9725 is the first SYN+ACK response from 192.168.0.20 to 192.168.0.8.

No.	Time	Source	Destination	Protocol	Length	Info
9299	6..	192.168.0.8	192.168.0.20	TCP	61	44000 → 8000 [SYN] Seq=0 Win=8192 Len=7
9300	6..	192.168.0.20	192.168.0.8	TCP	58	8000 → 44000 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0...
9302	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9303	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9304	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9306	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9307	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9309	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9311	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9326	6..	192.168.0.8	192.168.0.20	TCP	61	[TCP Retransmission] 44000 → 8000 [SYN] Seq=0 Win=8...
9420	6..	192.168.0.20	192.168.0.8	TCP	58	[TCP Retransmission] 8000 → 44000 [SYN, ACK] Seq=0 ...
9725	6..	192.168.0.20	192.168.0.8	TCP	58	[TCP Retransmission] 8000 → 44000 [SYN, ACK] Seq=0 ...
103..	6..	192.168.0.20	192.168.0.8	TCP	58	[TCP Retransmission] 8000 → 44000 [SYN, ACK] Seq=0 ...
117..	7..	192.168.0.20	192.168.0.8	TCP	58	[TCP Retransmission] 8000 → 44000 [SYN, ACK] Seq=0 ...

Frame 9725: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
 Ethernet II, Src: Apple_e7:a0:f1 (c0:ce:cd:e7:a0:f1), Dst: ChiconyE_cf:c5:95 (4c:bb:58:cf:c5:95)
 Internet Protocol Version 4, Src: 192.168.0.20, Dst: 192.168.0.8
 Transmission Control Protocol, Src Port: 8000 (8000), Dst Port: 44000 (44000), Seq: 0, Ack: 1, Len: 0

Wireshark packet details for packet 9725, showing the TCP header and flags. The SYN flag is set.

Sequence number: 0 (relative sequence number)
 [Next sequence number: 7 (relative sequence number)]
 Acknowledgment number: 0
 Header Length: 20 bytes

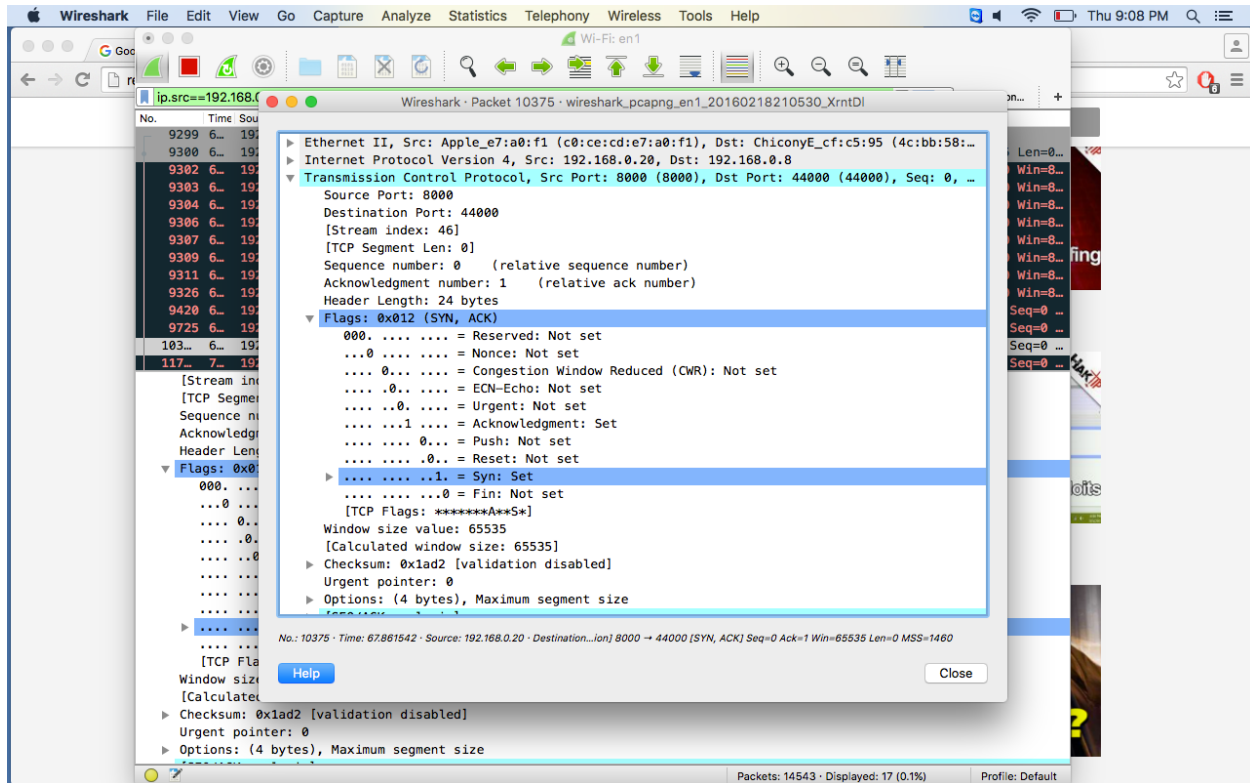
▼ Flags: 0x002 (SYN)

- 000. = Reserved: Not set
- ...0 = Nonce: Not set
-0... = Congestion Window Reduced (CWR): Not set
-0... = ECN-Echo: Not set
-0... = Urgent: Not set
-0... = Acknowledgment: Not set
-0... = Push: Not set
-0... = Reset: Not set
-0... = Syn: Set
-0... = Fin: Not set

[TCP Flags: *****S*]
 Window size value: 8192
 [Calculated window size: 8192]
 Checksum: 0x8b05 [validation disabled]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 Retransmitted TCP segment data (7 bytes)

Step3: Attacker machine receives SYN+ACK packets from victim.

Src Port=8000 Dst Port=44000. In flag (SYN,ACK) Syn=set



Wireshark Filter Used for Experiment:

ip.src==192.168.0.8 || ip.dst==192.168.0.8 and

ip.src==192.168.0.20 || ip.dst==192.168.0.20