TCP SYN Flood

1505084

July 30, 2019

1 Definition

A SYN Flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

Normally when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

1.The client requests a connection by sending a SYN (synchronize) message to the server.
2.The server acknowledges this request by sending SYN-ACK back to the client.
3.The client responds with an ACK, and the connection is established.

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol.

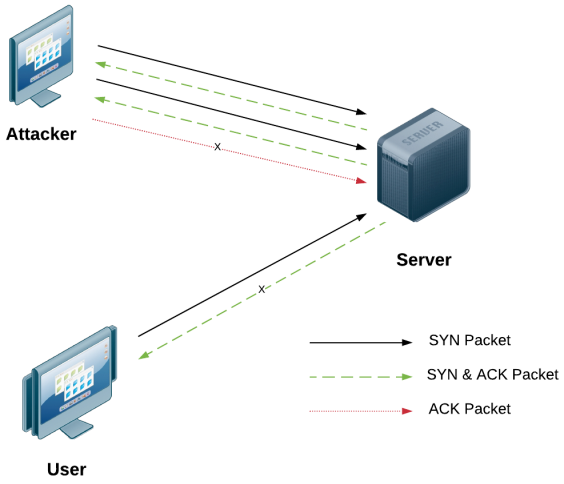

Fig:1 Topology Diagram

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address – which will not send an ACK because it knows that it never sent a SYN.

2 Attacking Strategies

I need to follow some steps to fulfill TCP SYN Flood attack.Steps are given below:
1.First of all i will send a high volume of SYN packets to the targeted server directly or with spoofed IP addresses.

2.Then the server will respond to each one of the connection requests and leave an open port ready to receive the response.

3.While the server waits for the final ACK packet, i will continue to send more SYN packets. The arrival of each new SYN packet will cause the server to temporarily maintain a new open port connection for a certain length of time, and once all the available ports would have been utilized the server will unable to function normally.

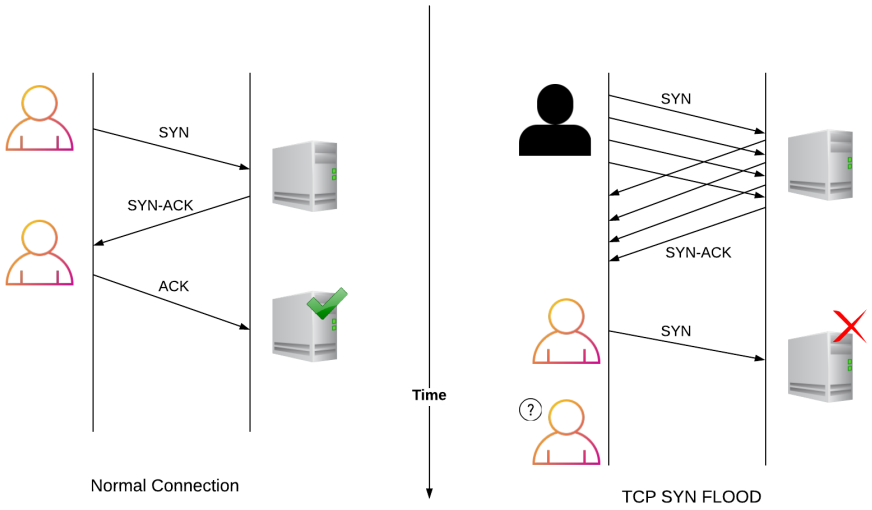

Fig:2 Timing Diagram

I will use Linux platform and a very simple syn flood program in python. This syn flood program will work by creating syn packets which need raw socket support and Linux has raw socket support natively.

3 Packet/Frame details

I will create raw tcp/ip packets.A packet contains IP header,TCP header and data.Format of IP header and TCP header are given below:

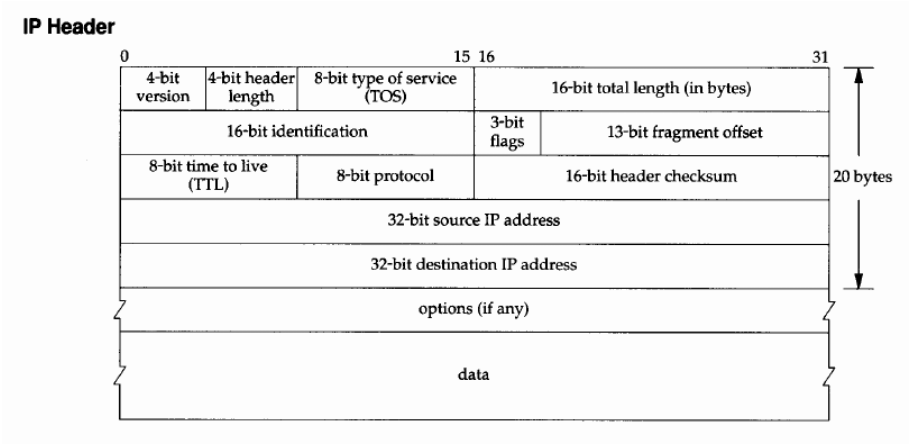

Fig:3 IP Header

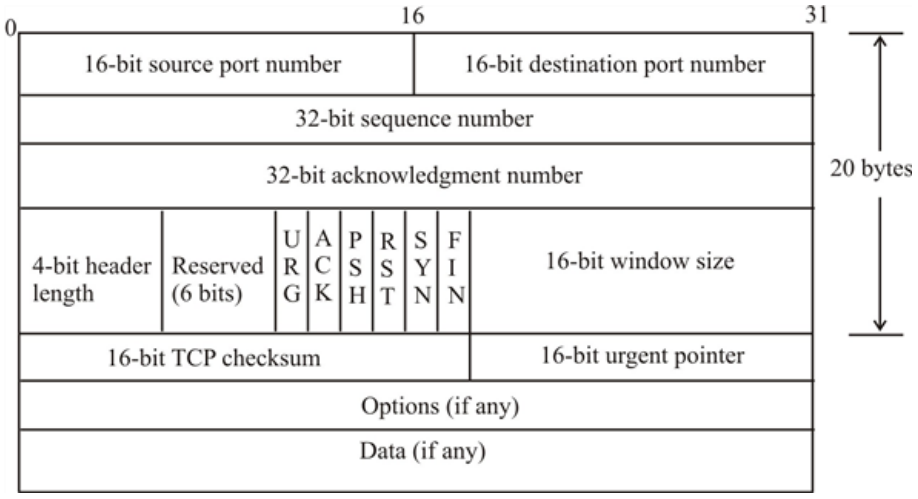

Fig:4 TCP Header

I will use tcp flags URG=0,ACK=0,PSH=0,RST=0,SYN=1,FIN=0.Raw packet can be easily created in python.I am going to paste a snapshot of this part here.

```
#create a raw socket
try:
        s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)
except socket.error , msg:
        print 'Socket could not be created. Error Code : ' + str(msg[0]) + ' Message ' + msg[1]
        sys.exit()
```

Fig:5 Raw packet creation

4 Justification

For implementing the attack I'm going to create a raw socket in python and through which i will generate numerous SYN packet.I will sent them at the victim's side and when it will reply me with SYN-ACK, i will not send ACK packet. Again i will spoof my IP address also. So reply of SYN packet will go to those IP addresses and they will surely not reply to those. As the victim PC has no way to stop receiving SYN packets during its active session in internet, in a few moments all of its resources will be consumed storing SYN information. So it will not be able to take more SYN packets and hence the denial of service will take place.