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

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.

SCAPY tool network library does the work of packet generation.

I have used two VM machines for this experiment:

Attacker's IP = 192.168.0.8 Port Number=22000 and Port Number=44000 for second attempt

Victim's IP = 192.168.0.20 Port Number=8000

Source program code written at Attacker's machine is as follows:

>> SYN= TCP (sport=22000,dport=8000, seq=random.random(), flags='S')

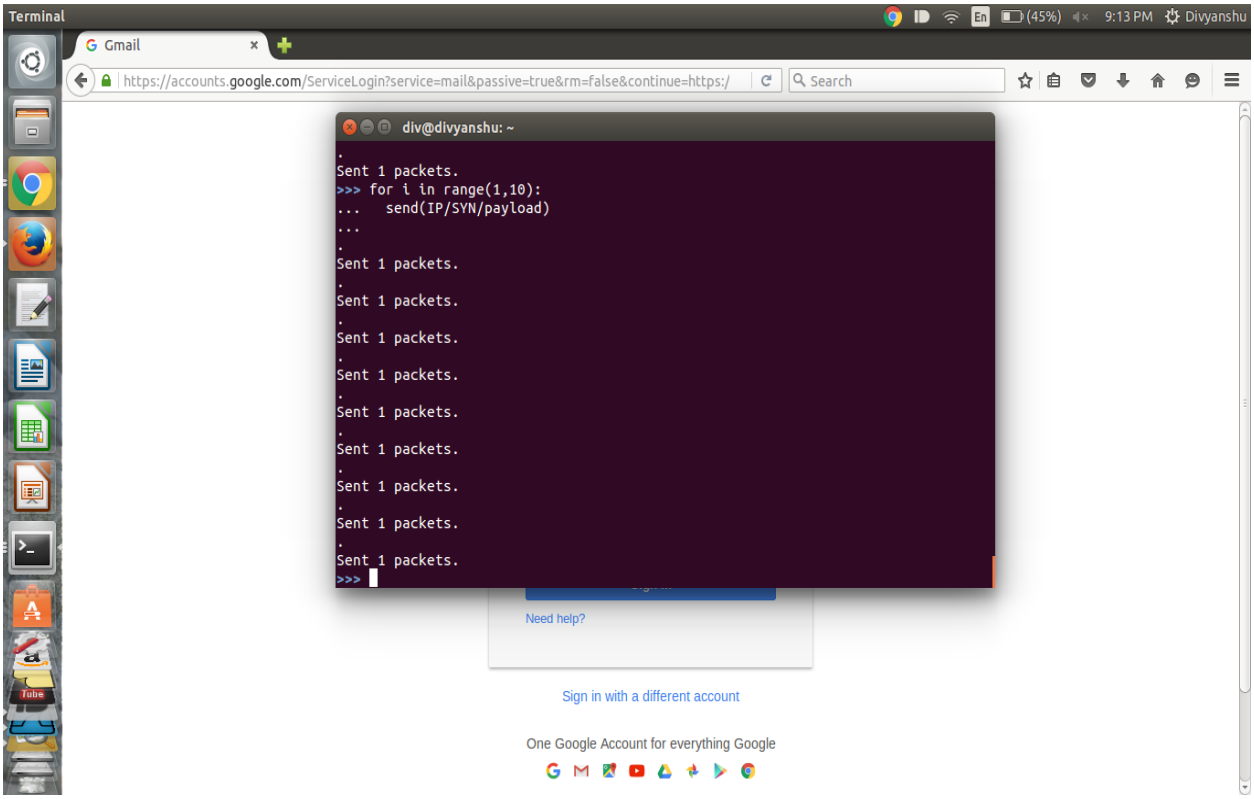
>>IP= IP (src="192.168.0.8",dst="192.168.0.20")

>>payload="Testing SYN packets"

>>for i in range(0,100):

Send (IP/SYN/payload)

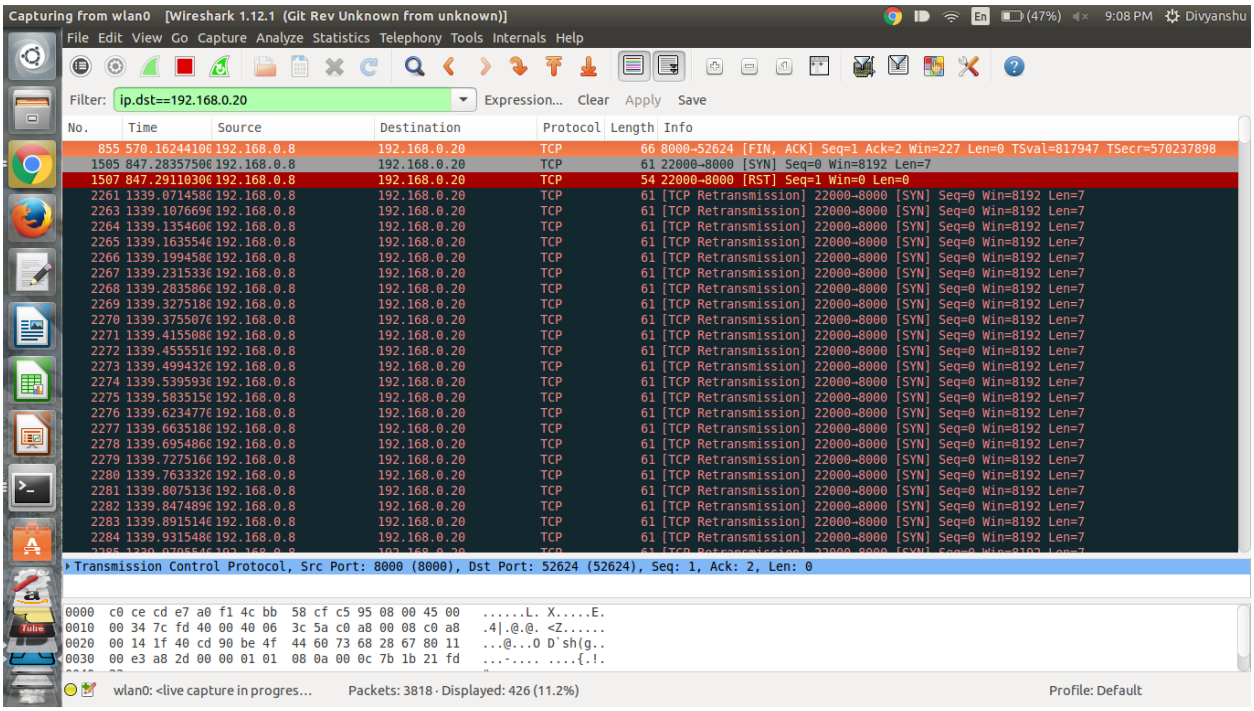
Following Screen shot shows packets in range of 0 to 10



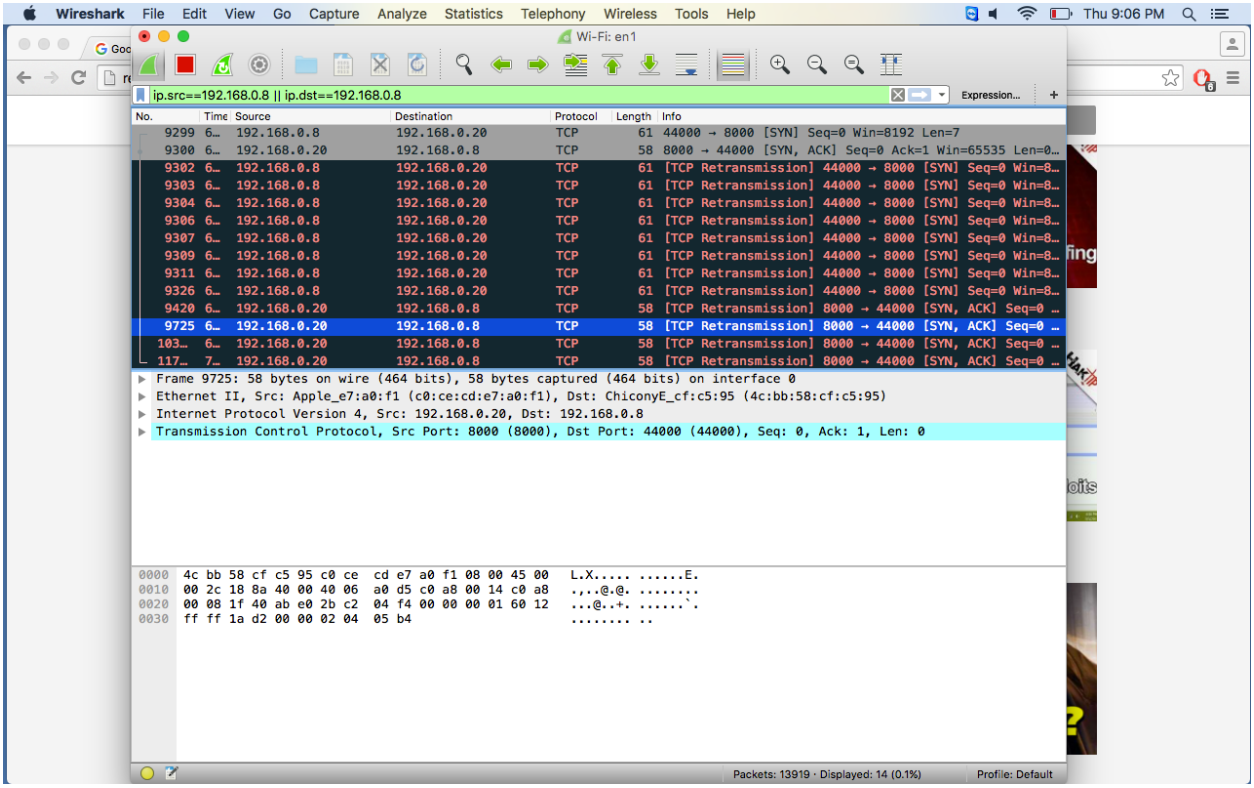
I used command to start HTTP server on VM machine at port no.8000

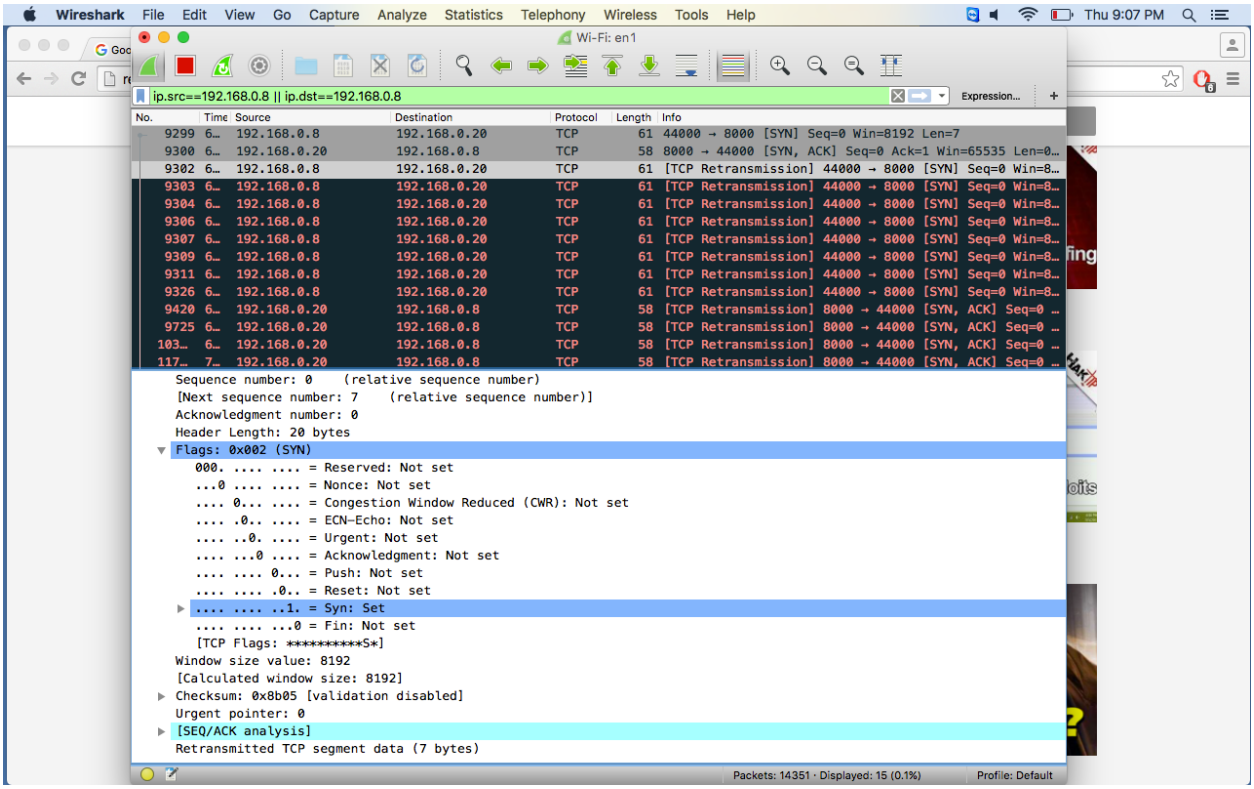
python -m SimpleHTTPServer

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



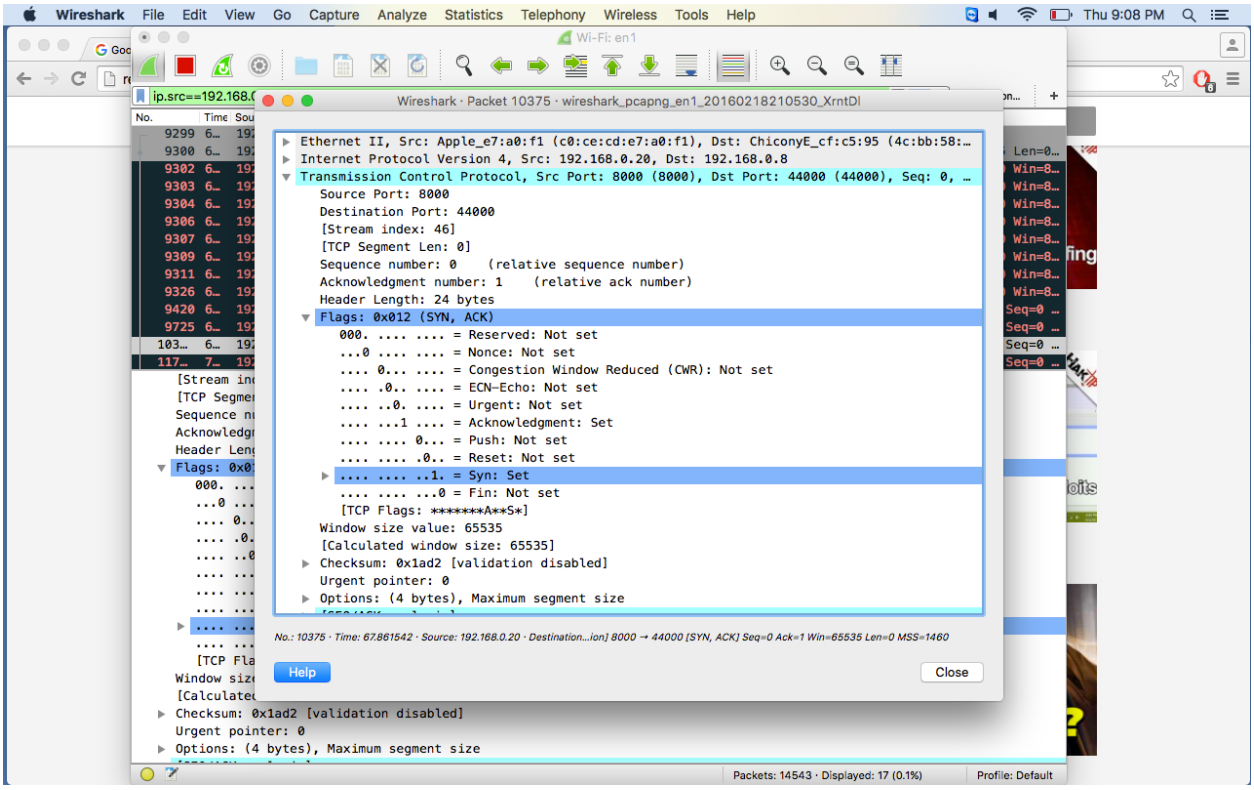
Step2 : Victim machine receives SYN Packets and it sends back “SYN+ACK” packets Flag(SYN) Syn:Set





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