**TCP/IP Attack Lab实验报告**

**57117207 高晓悦**

**实验环境：**

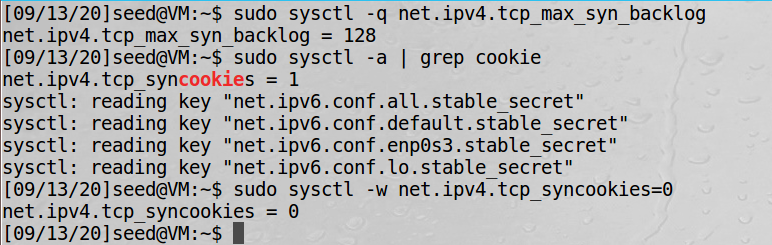
本实验需要三台主机，一台作为攻击机，一台作为受害机，一台作为观察机，这三台主机要位于同一网段，为此，以下实验中安排的主机信息如下：

1. 受害主机（SEED：172.19.204.10）
2. 攻击主机（SEED：172.19.204.20）
3. 观察主机（物理机：172.19.204.124）

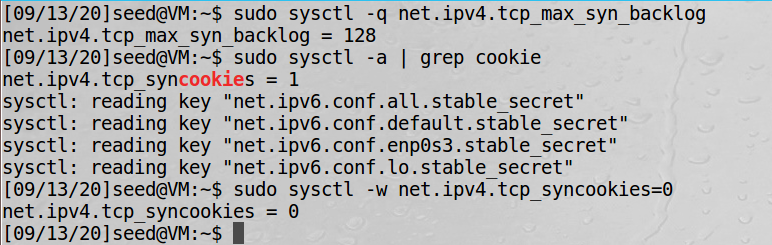
**Task 1: SYN Flooding Attack**

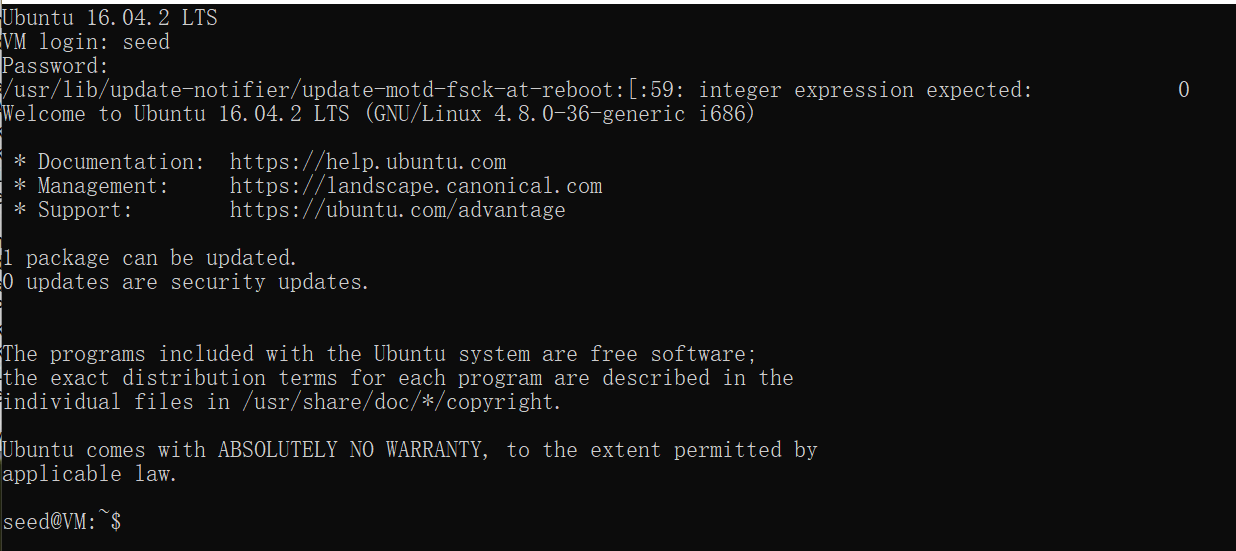
本实验中，攻击者将使用netwox工具向受害者端口发送大量SYN请求来实施泛洪攻击，攻击中，我们不需要受害者发回三次握手中第三步的确认报文，继而使受害者的TCP队列充满未关闭的连接，达到阻止其和其他主机建立TCP连接的目的。

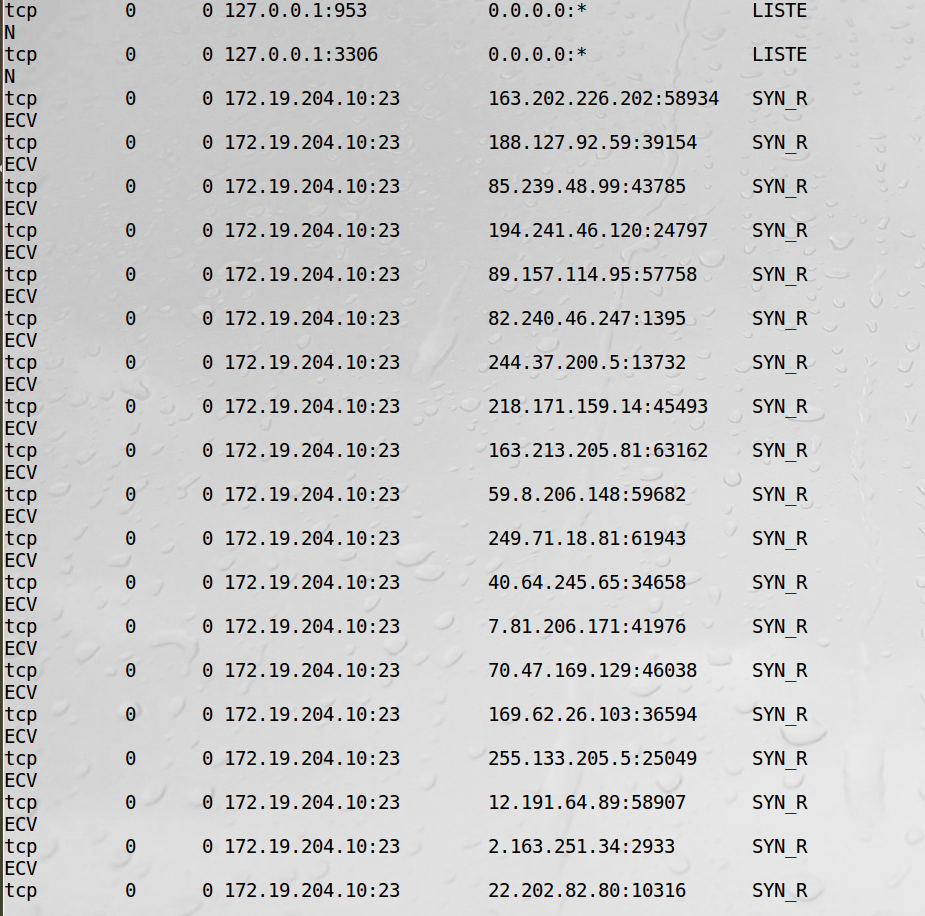
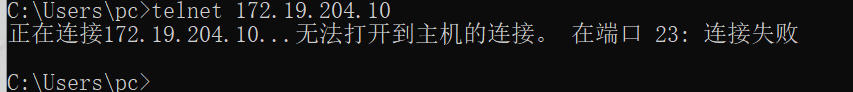
1、查看受害主机的TCP队列的大小：



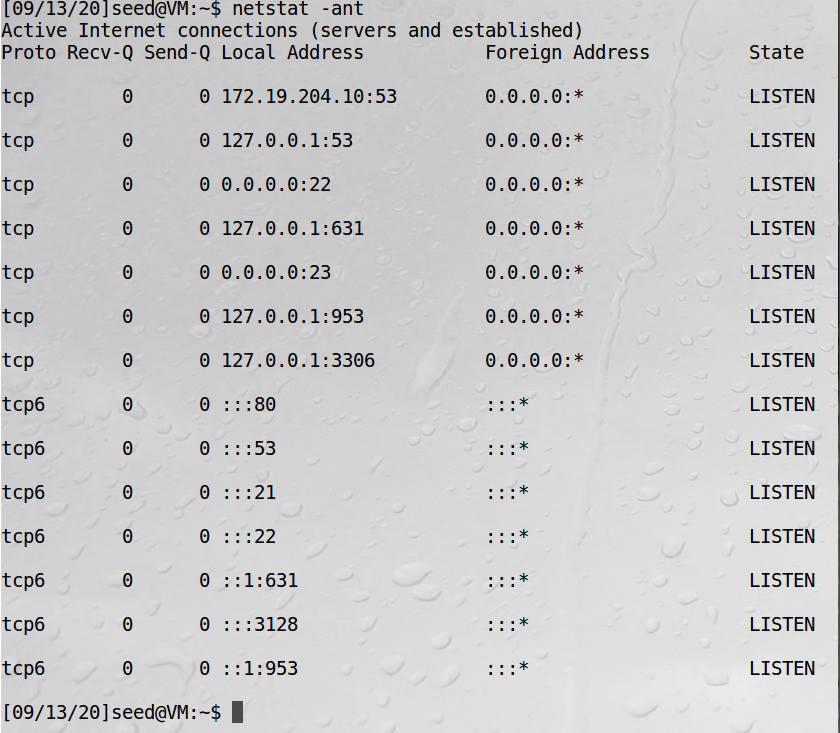
2、在受害主机上关闭SYN cookie：



3、观察主机远程登录受害主机：

1. 攻击主机执行下列命令来实施攻击：
2. 攻击实施后，在受害主机上用netstat查看连接发现出现很多处于SYN\_RECV状态的TCP连接：
3. 再次让观察主机远程登录受害主机，发现连接失败，说明受害主机的TCP队列已被未关闭的连接充满，不能和其他主机进行连接，即攻击成功：

7、将受害主机的TCP队列恢复正常：

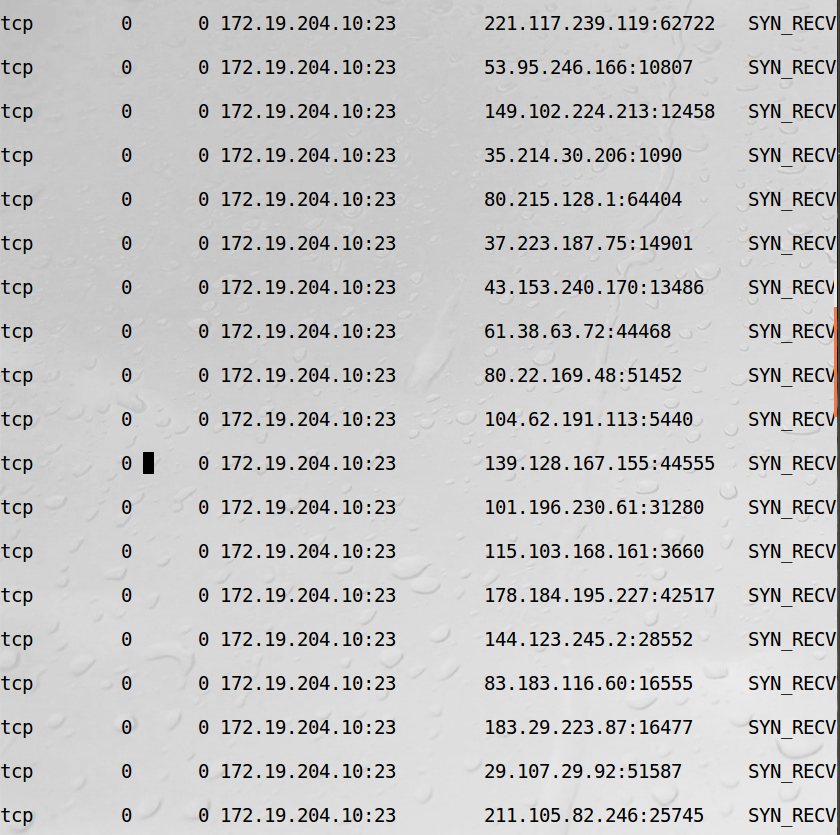


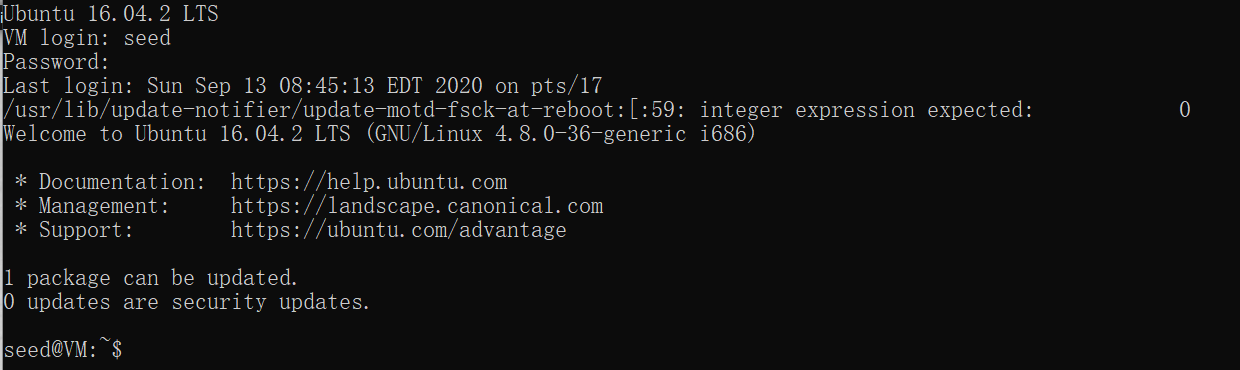
8、sudo sysctl -w net.ipv4.tcp\_syncookies=1打开受害主机的SYN cookie机制

9、攻击主机执行命令实施攻击：



10、查看受害主机的TCP连接，它仍被攻击：

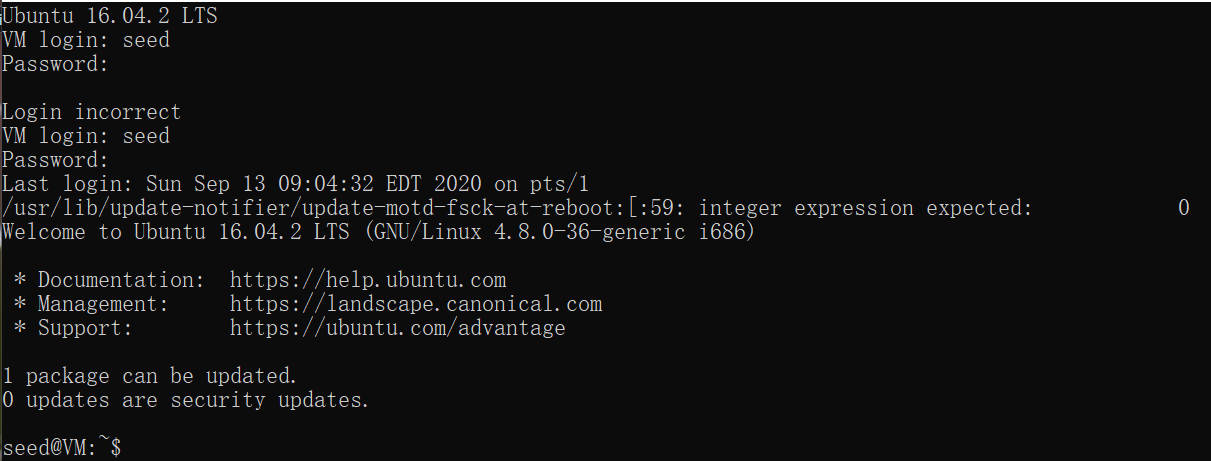


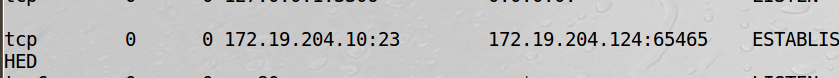
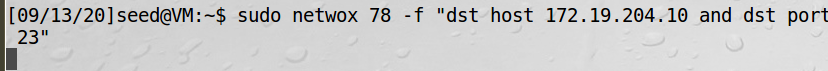
11、再次让观察主机远程登录受害主机，发现可以连接上，说明SYN cookie机制对SYN泛洪攻击有一定防御作用：

**Task 2: TCP RST Attacks on telnet and ssh Connections**

本实验中我们用netwox工具伪造TCP RST报文，使受害主机与其他主机中断连接。

1、观察主机远程登录受害主机：

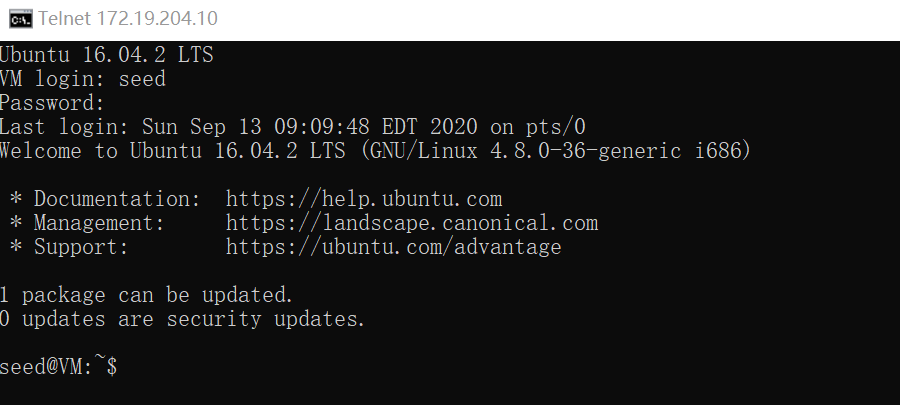


1. 查看TCP连接，发现已建立telnet连接：
2. 攻击主机实施攻击（对telnet连接的TCP RST攻击）后，发现上述连接断开：
3. 重新建立连接，攻击主机执行命令实施攻击（对SSH的TCP RST攻击）后，观察主机上与受害主机建立的连接被断开：

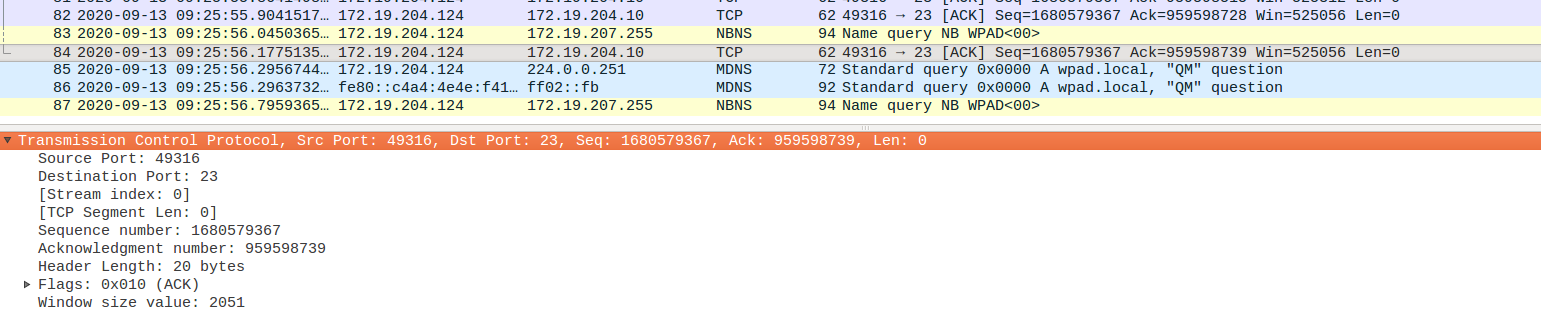
**Task 4: TCP Session Hijacking**

本实验中，我们将劫持一个TCP连接并注入恶意代码。

1. 观察主机远程登录受害主机：



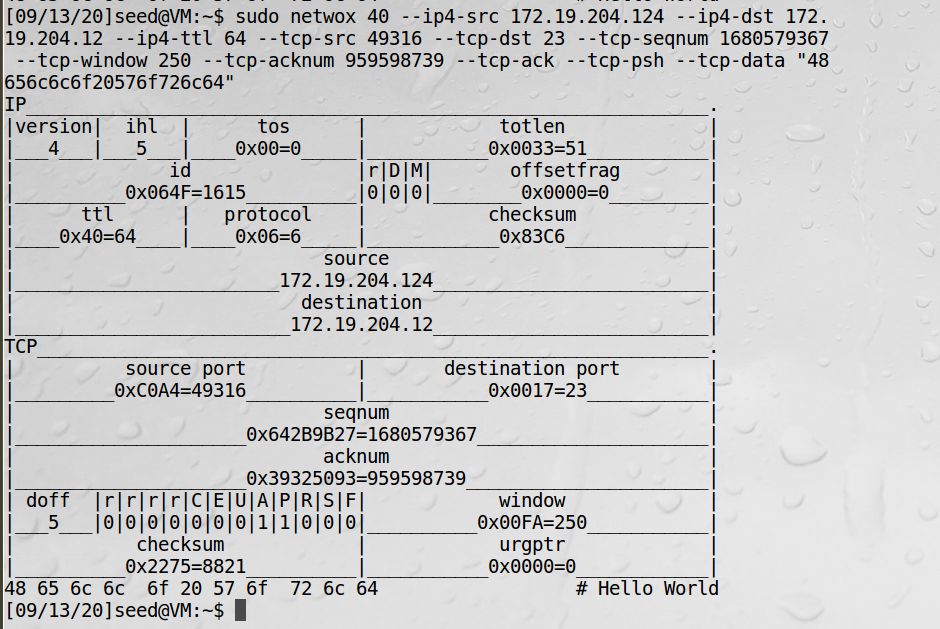
1. 在攻击主机上对上述连接进行抓包，找到观察主机向受害主机发送的最后一个确认报文：



TCP连接的端口信息如下：



1. 伪造报文，源地址为观察主机的地址，目的地址为受害主机的地址，源端口为观察主机的端口号，目的端口为受害主机的端口号，数据部分为”hello world”的编码：



4、进行抓包，观察运行结果：

