网安综合课程设计

实验报告

（57117105 杨哲君）

***TCP/IP Attack Lab***

**实验环境：**

**VM1（攻击者）192.168.80.137**

**VM2（靶机）192.168.80.138**

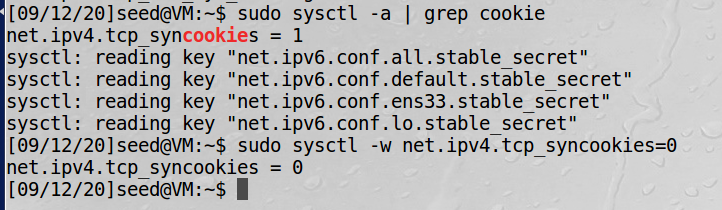
**VM3（监听机）192.168.80.139**

**Task 1: SYN Flooding Attack**

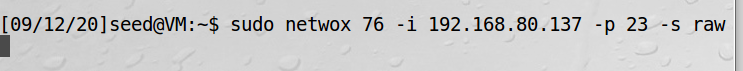
查看VM2中tcp队列的最大容量，为128。



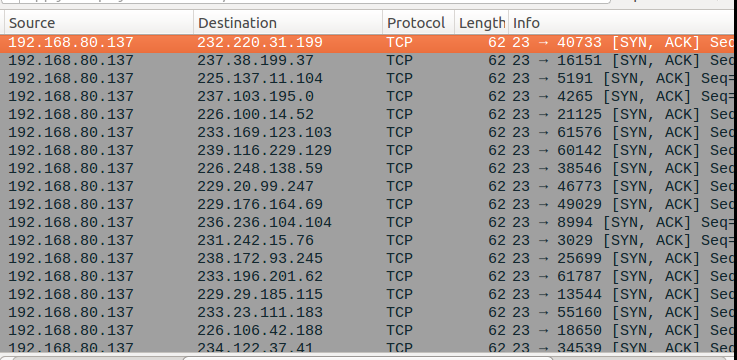
在VM2中将SYN cookies防御机制关闭。



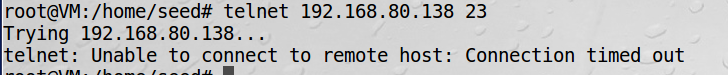
在VM1中输入命令，对VM2的23端口执行攻击指令。



用wireshark抓包可以观察到，靶机收到大量的TCP包。



再次用VM3对靶机进行telnet连接时会连接超时，证明靶机的Telnet服务已经丧失，攻击成功。

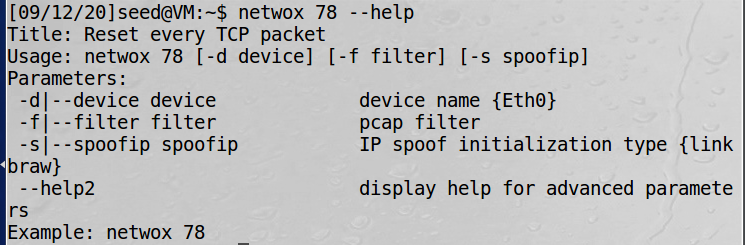


**Task 2: TCP RST Attacks on telnet and ssh Connections**

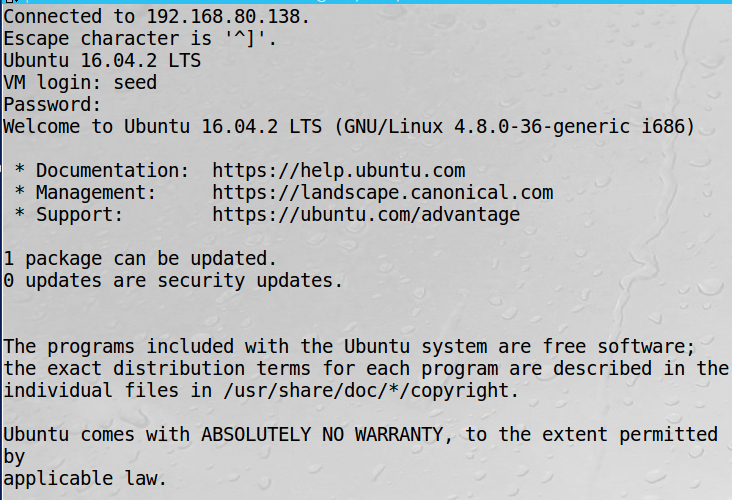
1. **使用Netwox 78进行攻击**

**（1） 对telnet的攻击**

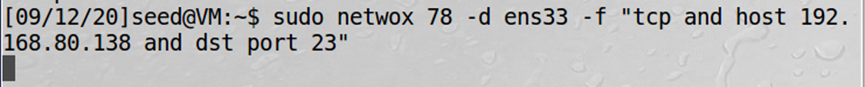
查看一下help，找到过滤器的命令。



先使VM3与靶机进行telnet连接

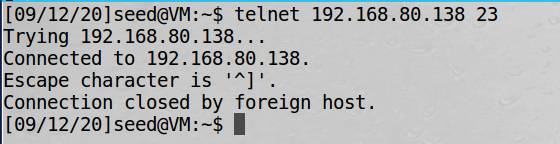


在攻击机上运行命令，进行TCP RST攻击，设置过滤器。



发现VM3和靶机的telnet断开了，并且无法重新连接。可以证明攻击成功。



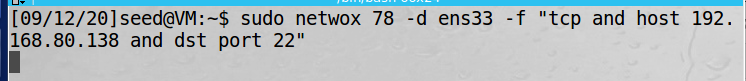


**（2）对ssh的攻击**

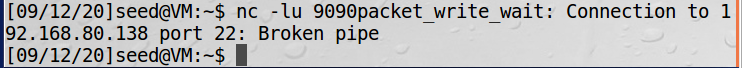
在VM3和靶机间建立ssh连接

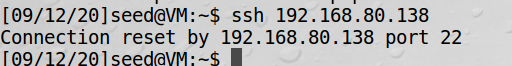


在VM1中使用netwox对目标端口22进行TCP RST攻击：



在观察机VM3中发现ssh连接被断开，再次尝试连接也没有用。可以证明攻击成功。

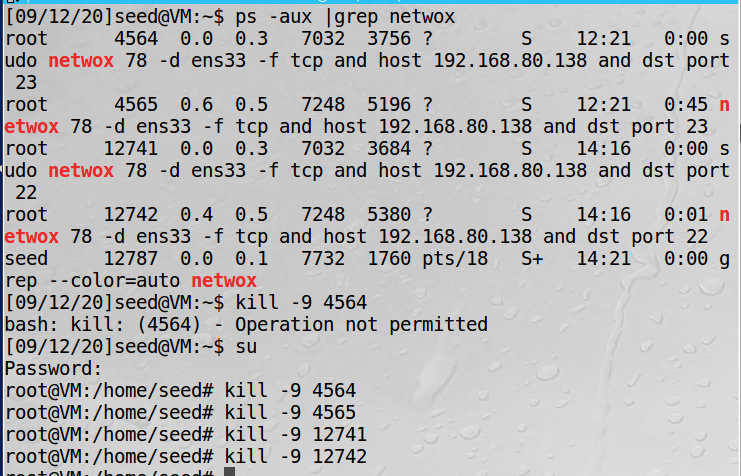




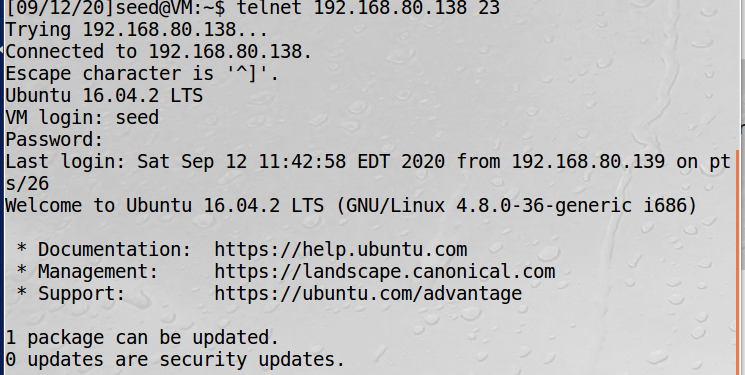
1. **使用scapy进行攻击**

下面使用scapy来进行攻击

先将netwox进程杀死，否则会影响后续实验的连接。

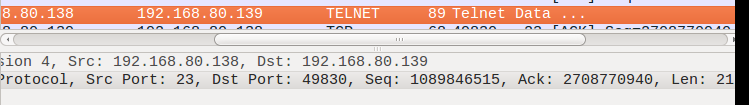


然后重新将VM3与靶机建立连接。发现连接正常。

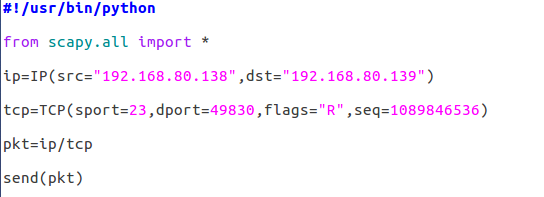


**（1） 对Telnet进行攻击**

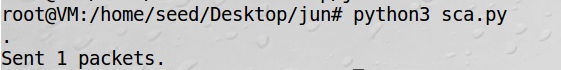
VM3与靶机进行telnet连接时，用wireshark抓包，选择靶机向VM3发送的最新一个telnet数据包，记录源地址，目的地址，源端口，目的端口，序列号和len。



在VM1中编写scapy脚本，端口号与上述数据包中的一致，序列号为上述数据包中的序列号加上len。



运行脚本，向VM3发送伪造的TCP RST报文。



此时观察到VM3中与靶机的telnet断开了。

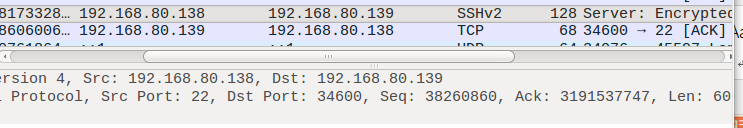


同时wireshark中也抓到了TCP RST报文，证明攻击成功。

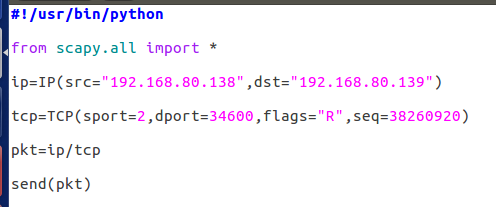


**（2） 对ssh进行攻击**

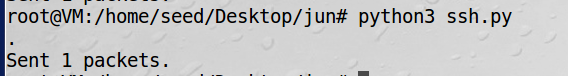
按同样的方法对ssh服务进行TCP RST攻击。



编写脚本，端口号与上述数据包中的一致，序列号为上述数据包中的序列号加上len。



在VM1中执行脚本



观察VM3中的wireshark抓到了TCP RST报文，与靶机的ssh连接断开，可以证明攻击成功。

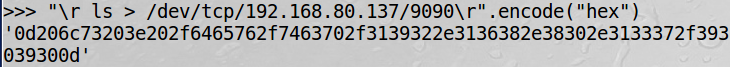


**Task 4: TCP Session Hijacking**

首先在VM3中通过Telnet连接靶机，在wireshark中查看最新一个由靶机发给VM3的telnet数据包的信息。记录下来信息



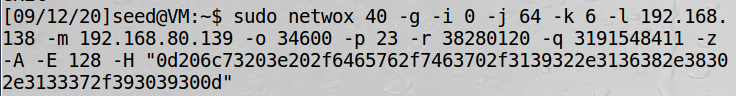
利用Python的encode工具对攻击命令进行16进制编码。



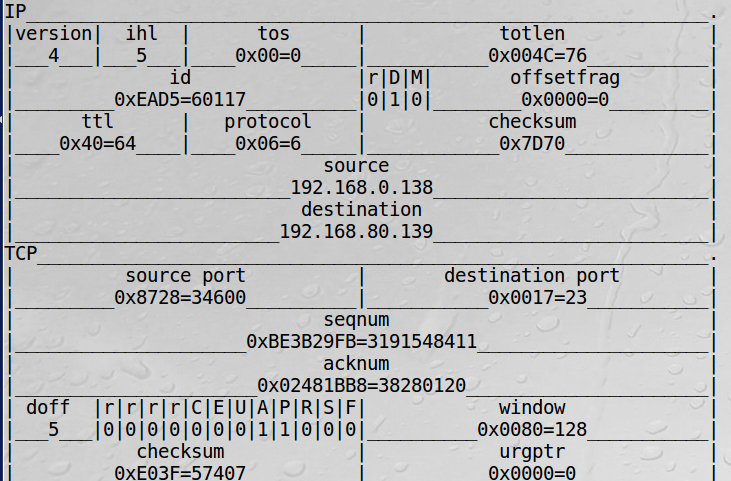
编写脚本。

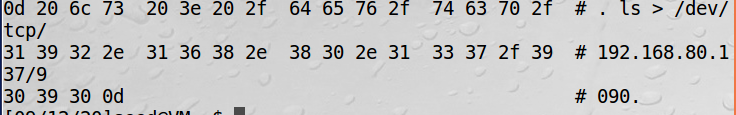


构造数据包发送服务器，进行攻击



结果如下：





在VM3中的wireshark也抓到了伪造的数据包，证明攻击成功。

