TCP/IP Attack Lab

**Task1**

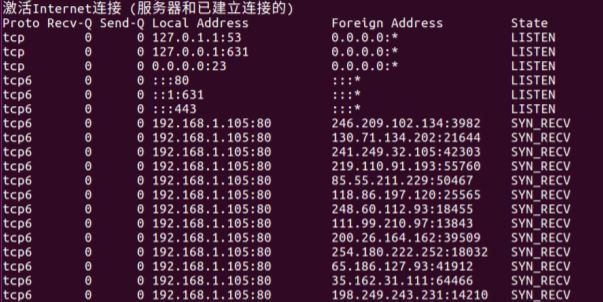
攻击者 IP 为 192.168.1.104/24，受害者为 192.168.1.105/24 先看攻击前受害者情况：



攻击方命令：



受害者情况：



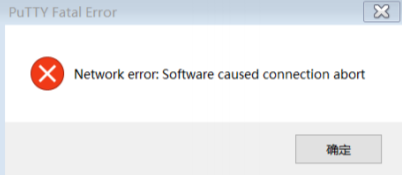
很多 SYN\_RECV 状态，因为我们没有在命令中设置源 ip，所以看到的源 ip 都是随机的

**Task2**

我们先从宿主机（192.168.1.102/24）上用 PUTTY，建立一个与虚拟机 192.168.1.105/24 的 telnet 会话。



结果：



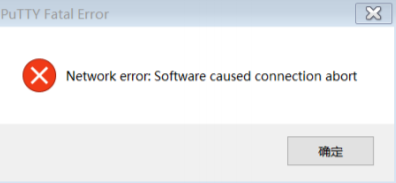
SSH



攻击命令：



结果：



**Task4**

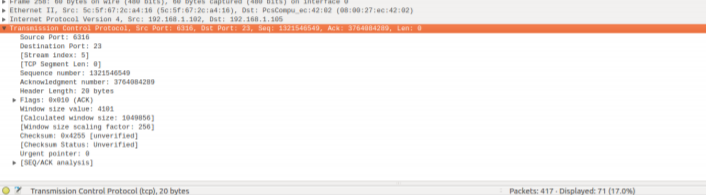
我们在宿主机（192.168.1.102）上使用 putty 与虚拟机 192.168.1.105 建立一个 telnet 会 话。



该虚拟机内我们执行 ls



都看到了 tfile 文件 看 wireshark（在另一台虚拟机 192.168.1.104 上，也是发起攻击的虚拟机）： 目前最后一个包的情况：



那么我们要发送的包的 seq number，ack number，window size 等等都可以延用这个包，数 据即为字符串“rm tflie\r\n” 攻击虚拟机上命令如下：



我们在虚拟机中再次执行 ls：



tfile 删除