Lab 1 TCP/IP Attack Lab

task 1 SYN Flooding Attack

手机屏幕的截图

描述已自动生成

首先在主机2上建立对主机3的连接，连接成功。

手机屏幕截图

描述已自动生成

此时使用Wireshark查看主机3的状态，发现流量非常大。此时也无法再次ssh连接到主机3上了。

task 2 TCP RST Attacks on telnet and ssh Connections

手机屏幕的截图

描述已自动生成

两主机间可以建立telnet连接



操作完成后，主机1断开连接，主机2处于监听状态。

此时对主机1的攻击还没有结束，当主机1尝试连接主机2，发现最开始能连上，但还没来得及显示后续内容，连接就中断了。

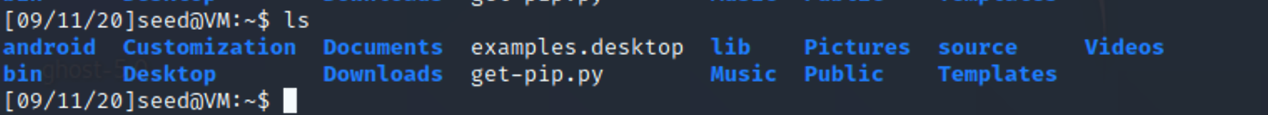
针对ssh的攻击同上。

task 4 TCP Session Hijacking

电脑屏幕的照片上有字

描述已自动生成

可以看到两个主机已经建立telnet连接。



电脑屏幕的截图

描述已自动生成

主机间通过telnet传送命令时可以看到wireshark捕获成功。

屏幕上有字

描述已自动生成蓝色的天空

描述已自动生成

观察捕捉到的数据包，预测下一个数据包的序列号和确认号，使用工具netwox 40 来伪造数据报，我们需要修改五个参数：源IP地址，目的IP地址，序列号，确认号以及数据字段。其中源IP地址为客户端IP地址，目的IP地址为服务器IP地址，序列号和确认号为我们观察所预测的序列号和确认号，数据字段为攻击者想要服务器执行的指令。我们查到可以用netwox来伪造包之后，我们查阅了很多的资料，也请教了很多同学才确定netwox命令的写法，我们根据之前总结出的tcp包的seq和ackseq 确定了如下的指令：当我们回车之后 这个数据包被发出，我们劫持了123和122之间的telnet会话并用自己的伪造数据包使得123来执行我们自定义的命令 mkdir aa，当然要使用16进制编码 不然会出现报错提醒，最后可以看到成功在目标主机上建立了一个文件夹aa。