**TCP ATTACKS LAB**

2018级 信息安全 管箫 18307130012

一、环境配置

1、主机网络配置

①主机A（Attacker）：IP Addr：192.168.61.138；MAC：00:0c:29:01:41:ae

②主机B（Client）：IP Addr：192.168.61.139；MAC：00:0c:29:a3:8a:e6

③主机C（Server）：IP Addr：192.168.61.140；MAC：00:0c:29:aa:55:ad

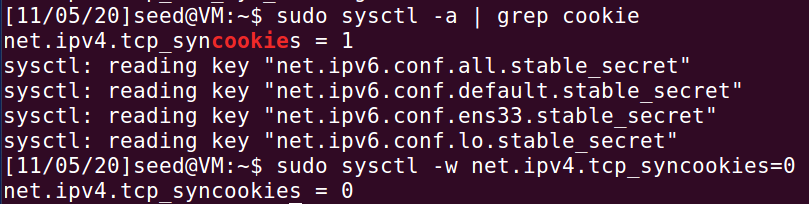
二、报告正文

1、Task 1: SYN Flooding Attack

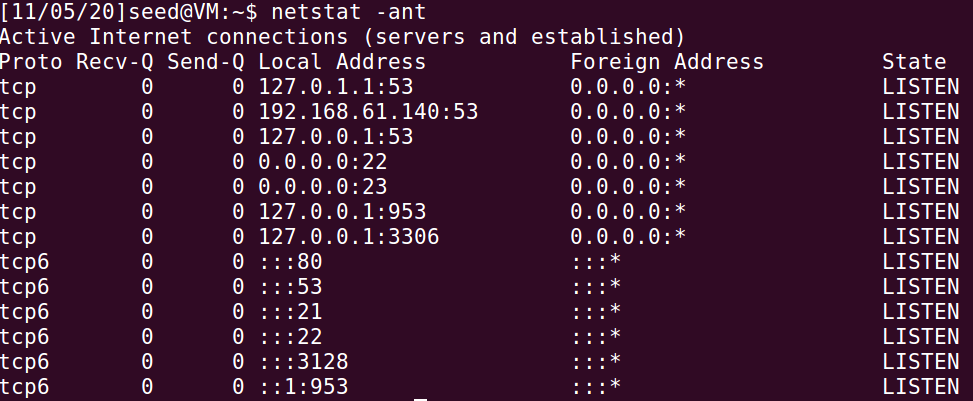
①查看服务器TCP SYN最大连接数：



②关闭服务器的TCP SYN Cookie功能



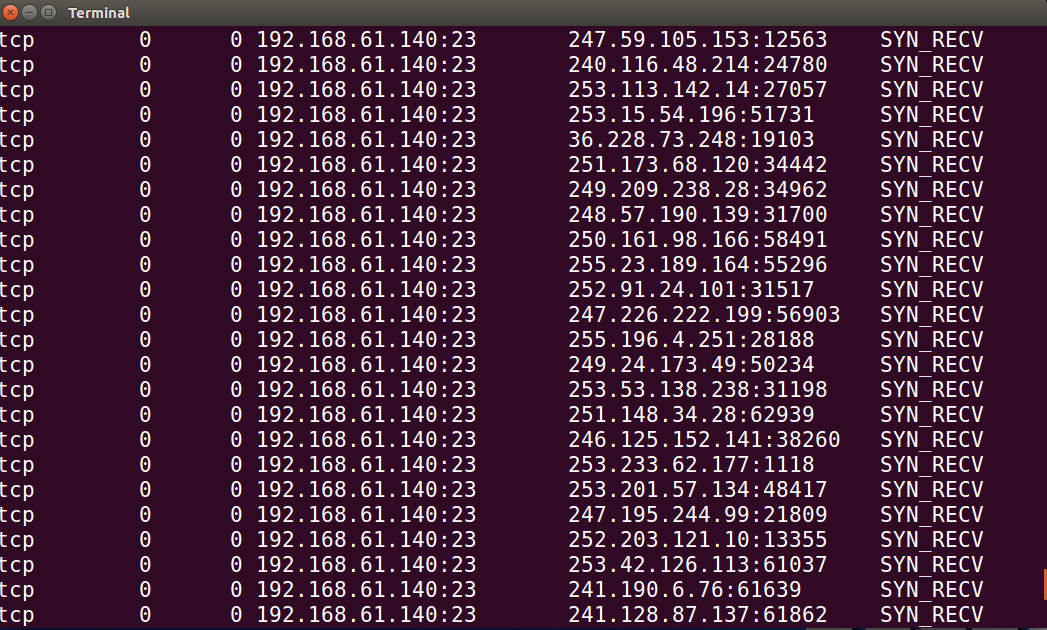
③检查当前半开连接数



④发起SYN 洪泛攻击

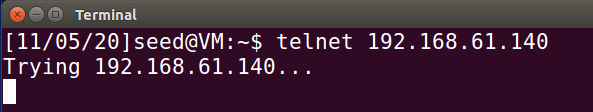


⑤观察被攻击服务器半开连接数



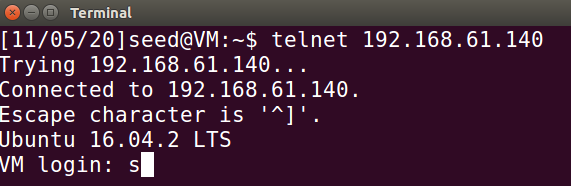
观察到服务器的TCP连接数被大量来自随机IP和端口的请求占满。

⑥检验攻击效果



在主机B上尝试连接作为服务器的主机C，发现主机C无响应。

⑦打开SYN Cookie，重试攻击



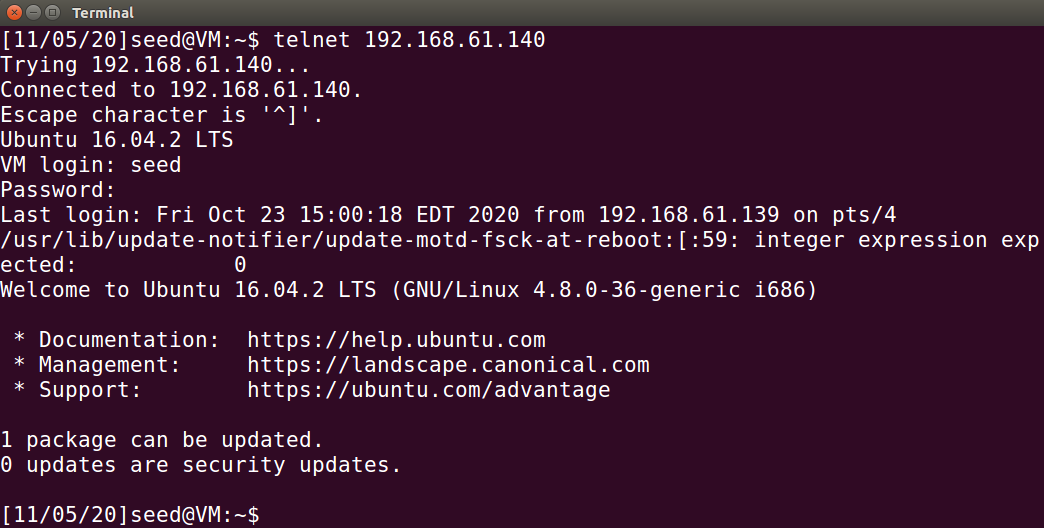
观察到作为服务器的主机C的telnet可以正常连接。

SYN Cookie防范洪泛攻击的原理是：在TCP服务器接收到TCP SYN包并返回TCP SYN + ACK包时，不为该半开连接分配资源，而是根据这个SYN包计算出一个cookie值。这个cookie作为将要返回的SYN ACK包的初始序列号。当客户端返回一个ACK包时，根据包头信息计算cookie，与返回的确认序列号(初始序列号 + 1)进行对比，如果相同，则确认其是一个正常连接，然后再分配资源，建立连接。

这一设计使得攻击者使用大量SYN请求以建立半开连接消耗服务器资源的攻击方法变得不可行。

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

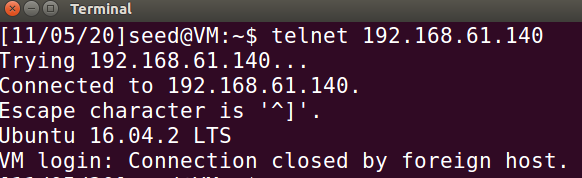
①确认连接可以被正常建立



②发起TCP RST攻击



③尝试telnet连接服务器



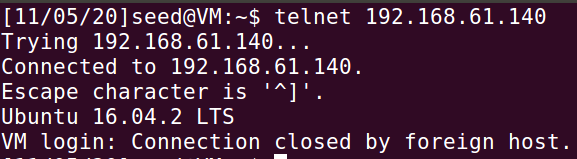
观察到连接被拒绝（也即被TCP RST）

④尝试ssh连接服务器



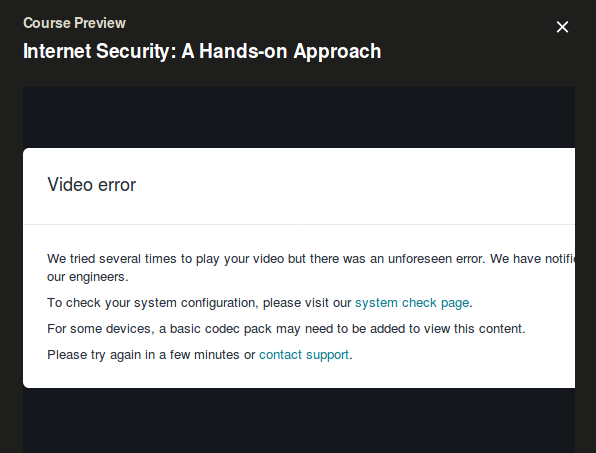
同样被TCP RST

⑤使用scapy



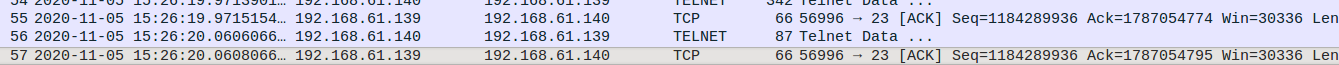
3、Task 3: TCP RST Attacks on telnet and ssh Connections

①直接阻断和远程服务器连接，发送RST命令至主机C即可

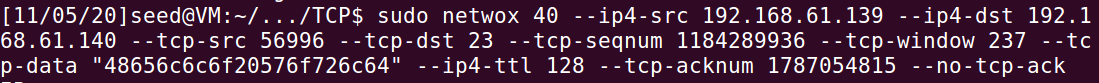


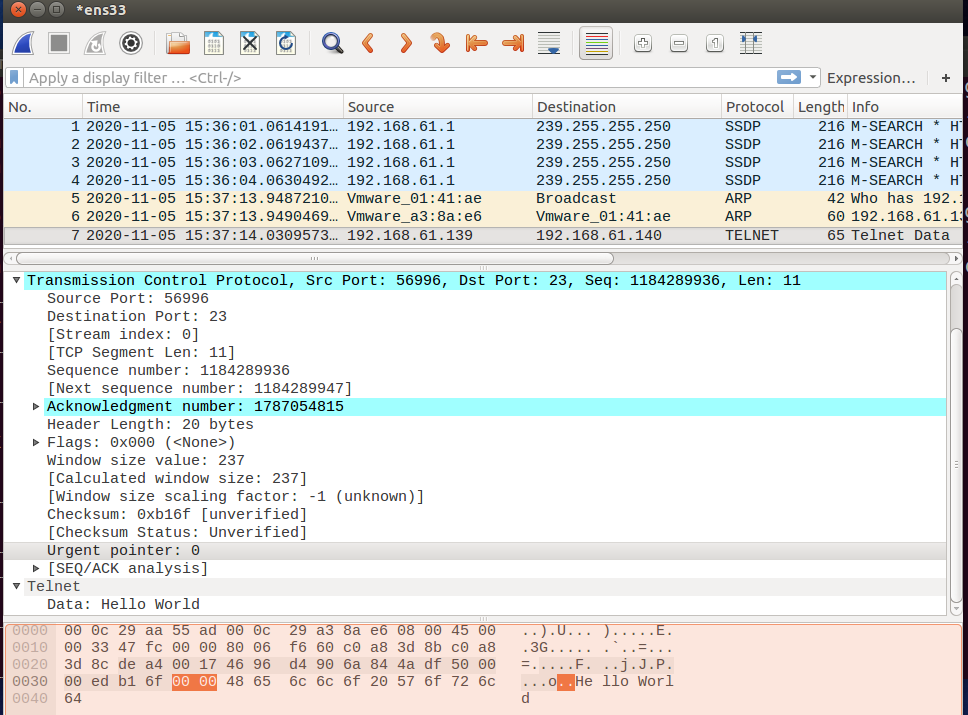
4、Task 4: TCP Session Hijacking

①抓包



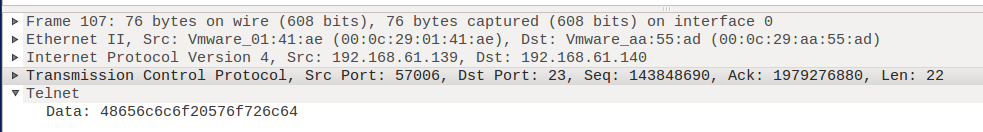
②发包





观察到包正常发送

③使用scapy重现

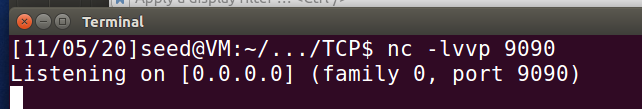


5、Task 5: TCP Session Hijacking

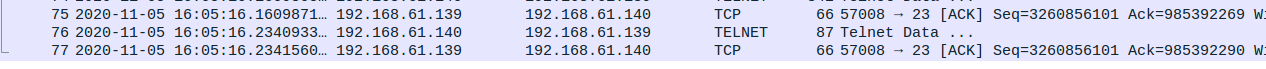
①转换攻击命令：



②开启监听：



③同task4中一样抓包



④成果

