**Lab4实验报告**

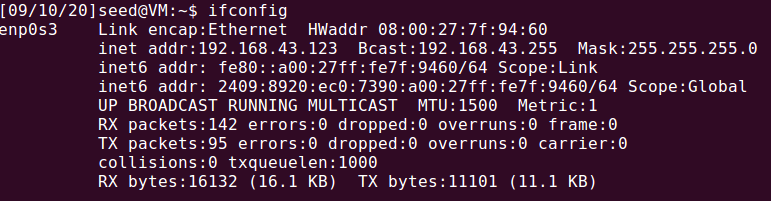
57117138 吴伊杰

**TCP/IP Attack Lab**

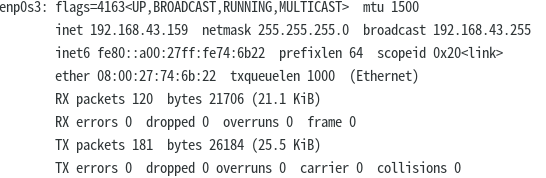
# Lab Environment

实验环境的配置：需要三台虚拟机A,B,C，A为攻击者，B为被攻击者，C为观察者。具体配置如下：

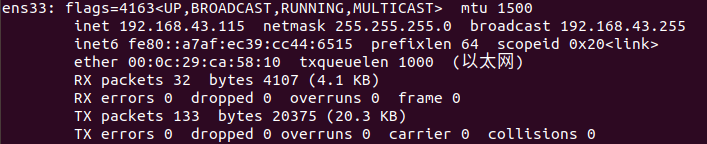
主机A——IP地址：192.168.43.123



主机B——IP地址：192.168.43.159



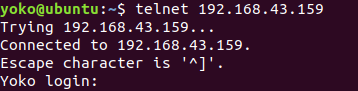
主机C——IP地址：192.168.43.115



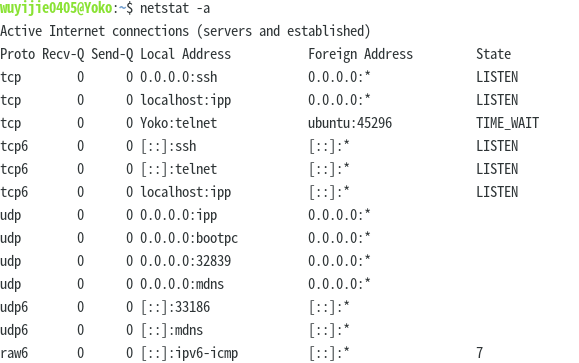
# Task 1: SYN Flooding Attack

SYN泛洪攻击。实验中使用telnet服务，在23号端口发起该攻击。这里令A对B攻击，C对B进行观测。

首先给主机B开启telnet服务。之前的实验中有做过配置，所以不赘述。然后尝试用C对B进行telnet连接，成功：



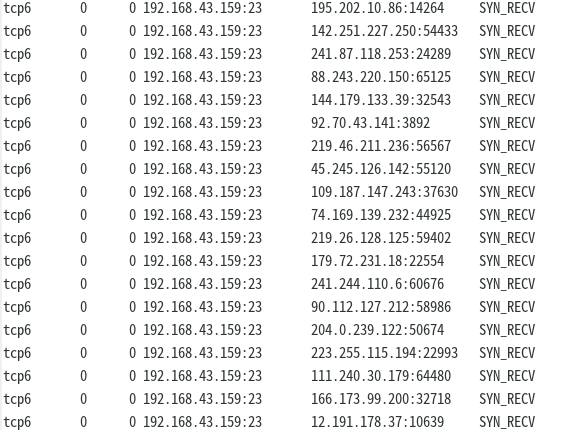
在主机B中使用netstat -a命令：



此时一切正常。然后在主机A中使用如下命令进行泛洪攻击：



此时再次在主机B中使用netstat -a命令查看，发现有大量状态为SYN\_RECV的TCP连接请求，可见攻击成功：



此时，主机C尝试与B进行telnet连接，但是连接超时。



如果在主机B中开启SYN Cookie防御

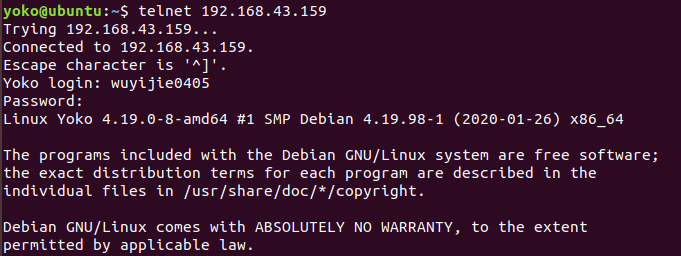


则虽然仍有大量半连接存在，但是telnet连接却依旧能成功。

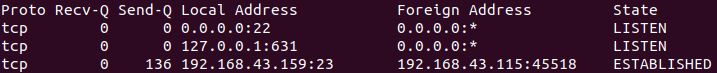
# Task 2: TCP RST Attacks on telnet and ssh Connections

主机A通过启动TCP RST攻击来中断B和C之间的telnet连接。

首先主机C和B建立telnet连接，连接成功后：



使用netstat -na查看登陆端口号为23：



在主机A中发起攻击，利用netwox所提供的78号工具

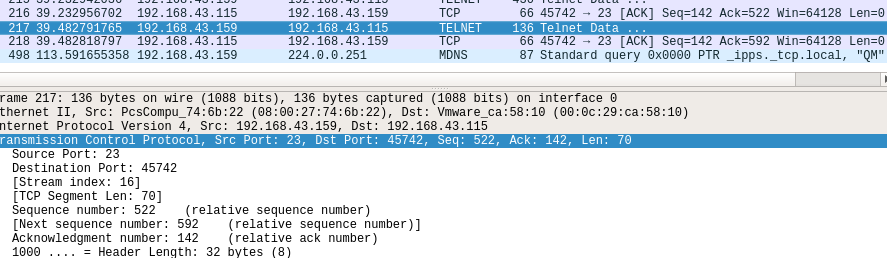


攻击后，主机C断开了对B的telnet连接。

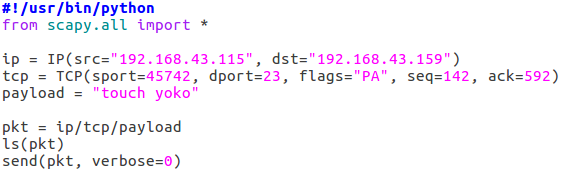
可以用同样的办法中断B和C之间的ssh连接，一般来说ssh连接的端口号是22，只需要把攻击指令中的port改成22即可。

# Task 4: TCP Session Hijacking

TCP会话劫持攻击。首先我们开启Wireshark，对B和C的telnet通信进行监测。然后令主机C向B发起telnet连接，此时Wireshark里可以抓包该通信过程，重点关注最后一次通信。



根据最后的报文，构造攻击程序：



在攻击方主机A中执行此代码。此时Wireshark中能监测到该活动：



在受攻击主机下查看，发现名称为”yoko”的文件被创建。

