**lab4**

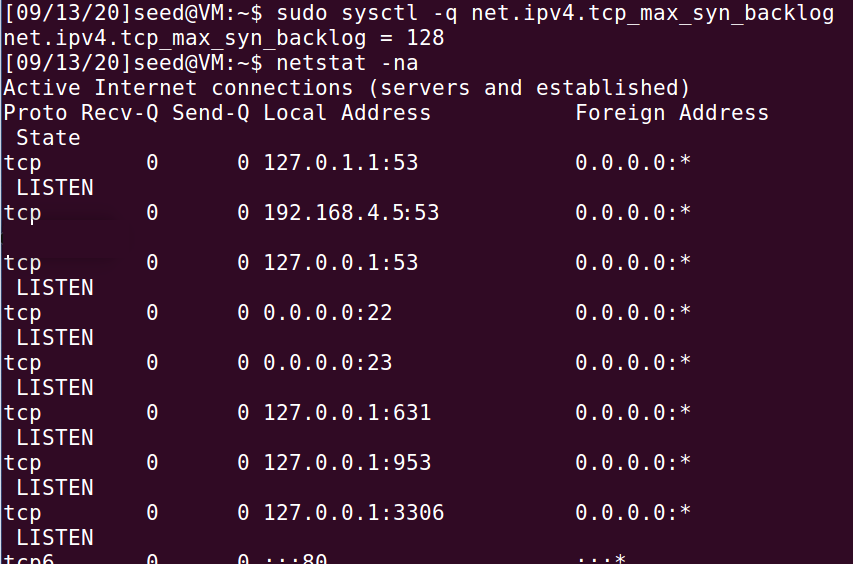
57117208 傅靖邦

攻击机A ip：192.168.4.5

靶机B ip：192.168.4.2

观测机C ip:192.168.4.115

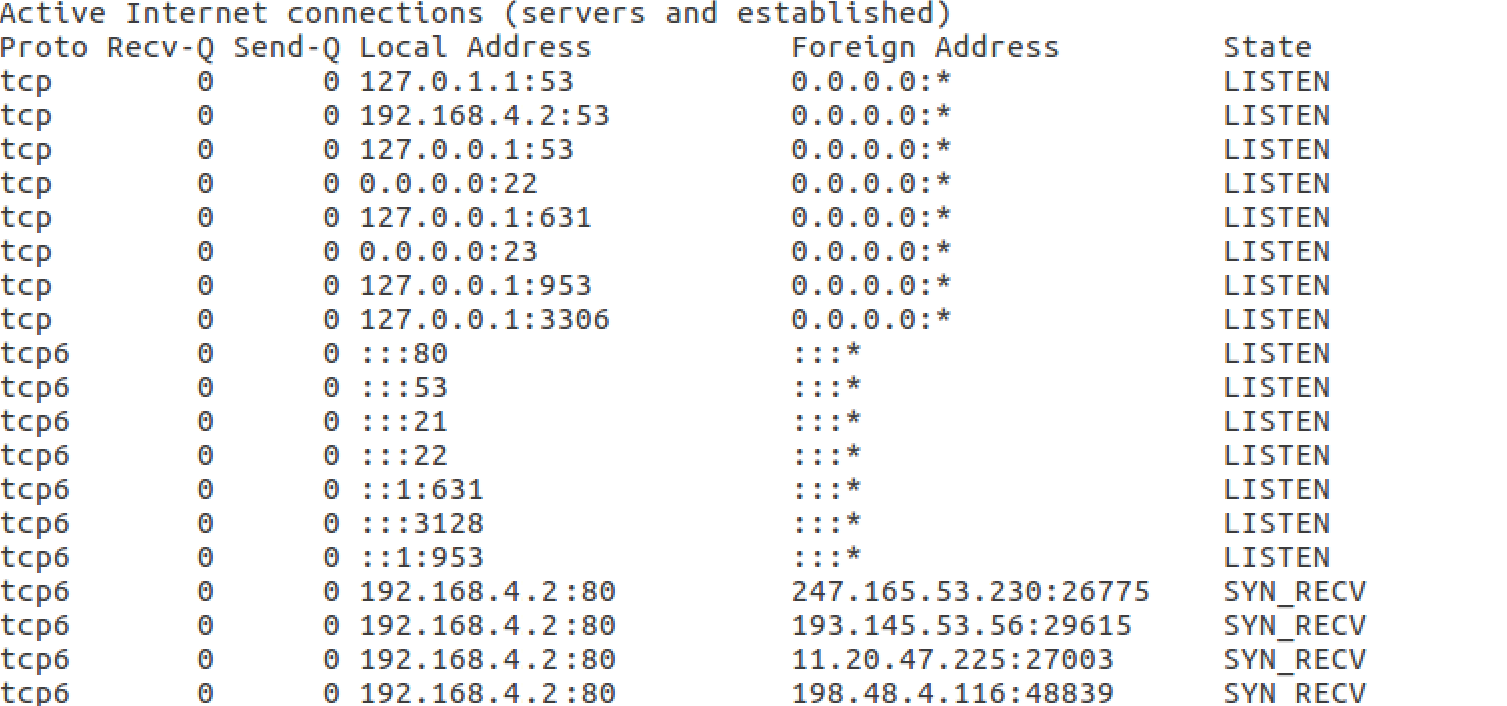
1.



攻击命令：

sudo netwox 76 -i "192.168.4.2" -p "80"

可以发现有很多TCP都处于SYN\_RECV状态。



攻击机与靶机进行到TCP三次握手的第二次后，就不再向靶机发送第三个报文，导致靶机把这个请求暂存到缓存里。攻击机的ip足够多，可以把靶机的TCP缓存塞满，导致靶机的服务失效。

2

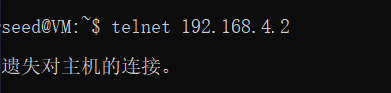
在宿主机的cmd建立与虚拟机的telnet会话



使用命令

sudo netwox 78 -f "dst host 192.168.4.2 and port 23"

进行攻击。



由于telnet运行在TCP协议上，攻击机伪造了TCP RST报文，使TELNET连接重置，从而截断了后续的telnet通信。  
在ssh攻击中也是类似的效果。

4

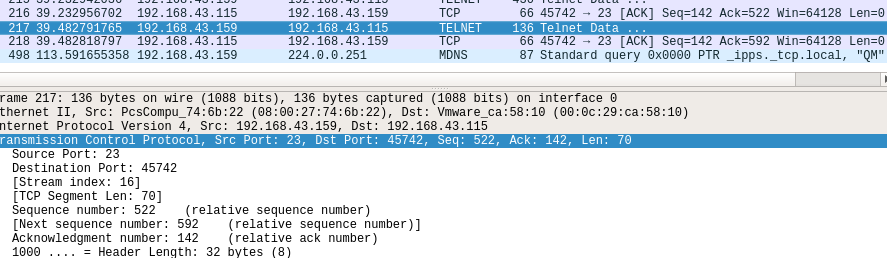
TCP会话劫持攻击。

主机A——IP地址：192.168.43.123

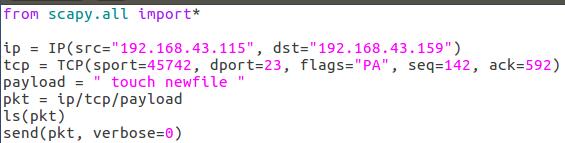
主机B——IP地址：192.168.43.159

主机C——IP地址：192.168.43.115

首先使用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:



A执行，在WireShark中发现：



受攻击主机中被创建了一个newfile文件。