**Linux Firewall Exploration Lab实验报告**

机器A：10.0.2.4

机器B：10.0.2.5

机器C：10.0.2.6

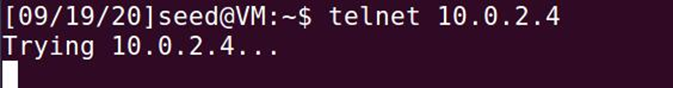
Task1 Using Firewall

a.阻止A telnet B

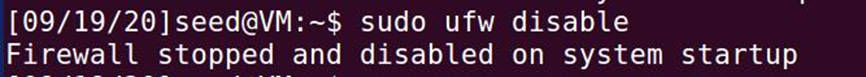
1. 更改主机A中的防火墙设置：

sudo ufw enable

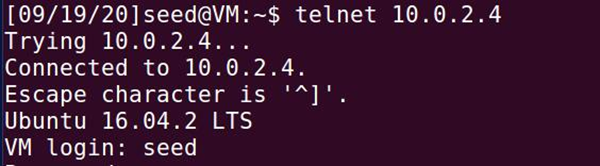
主机B结果：

****

2.主机A:sudo ufw disable



主机B结果：



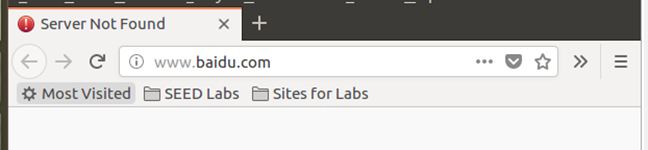
b.阻止B telnet A,同上

c.阻止A浏览一个外部网页，eg:阻止主机A对百度www.baidu.com（112.80.248.76, 112.80.248.75）的访问



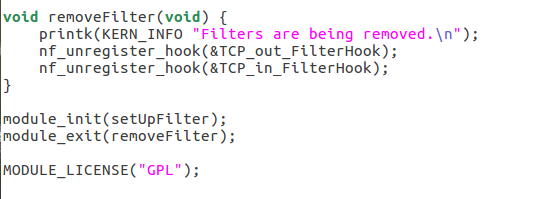
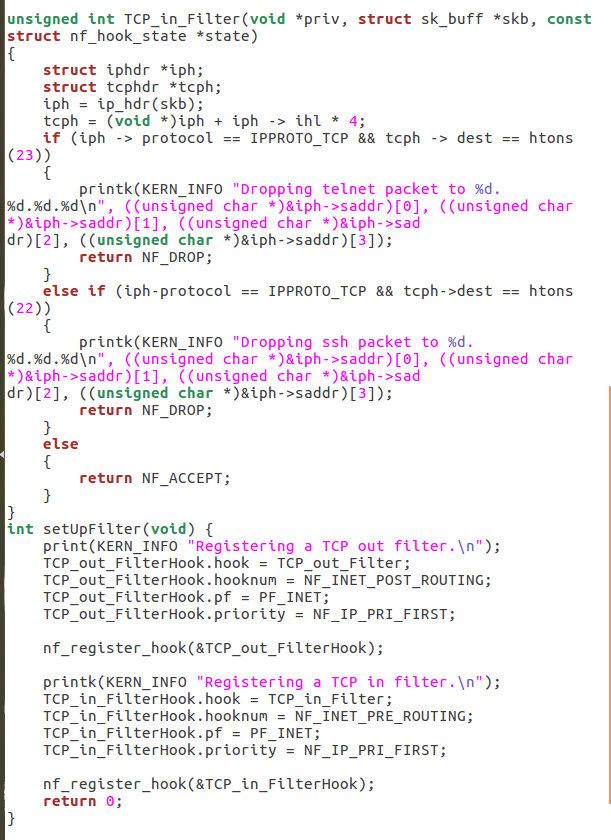
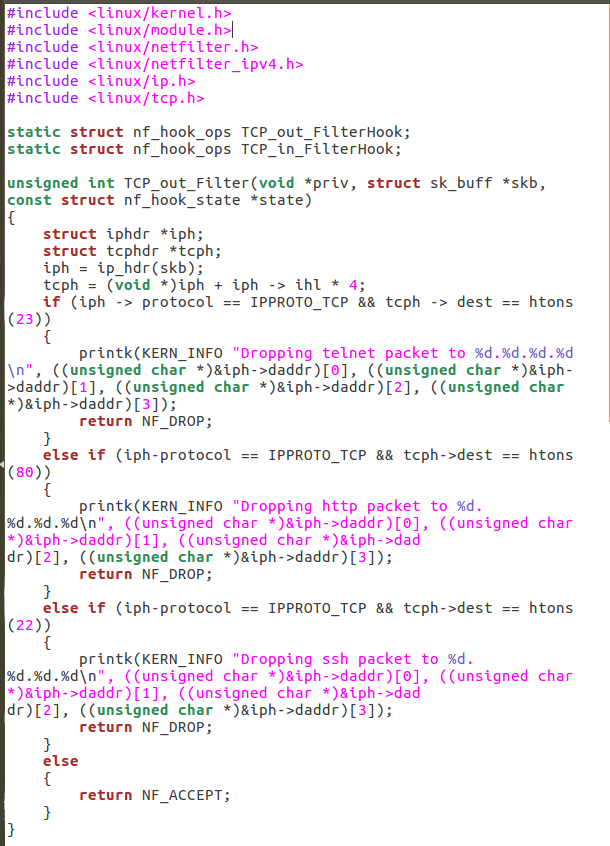


结果：浏览器访问百度，访问不了



Task 2: 实现一个简单的防火墙

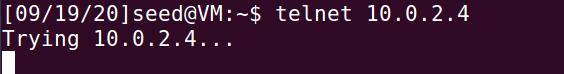
1、编写程序Filter.c：



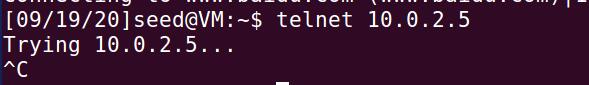
2、编译后加载进内核：



3、载入之后，发现主机A无法telnet主机B，主机B无法telnet主机A，wget也无法访问[www.baidu.com](http://www.baidu.com)：



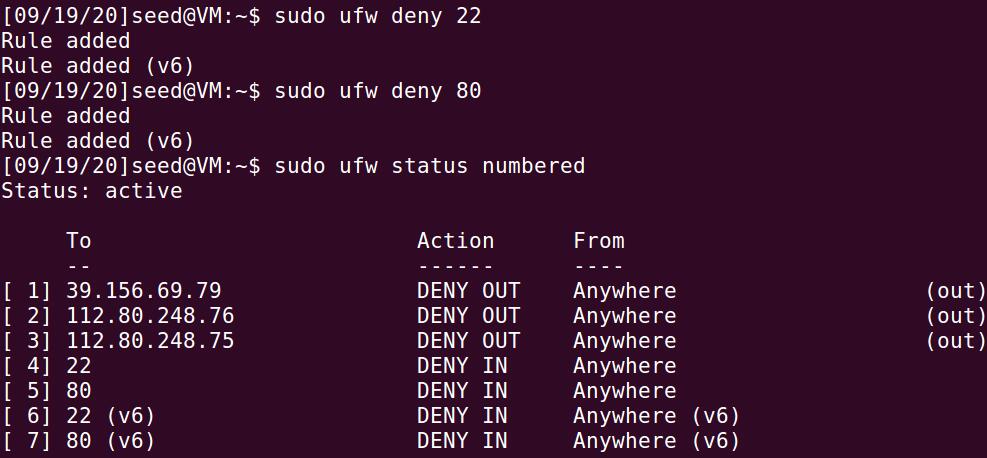




4.移除模块后，恢复正常。

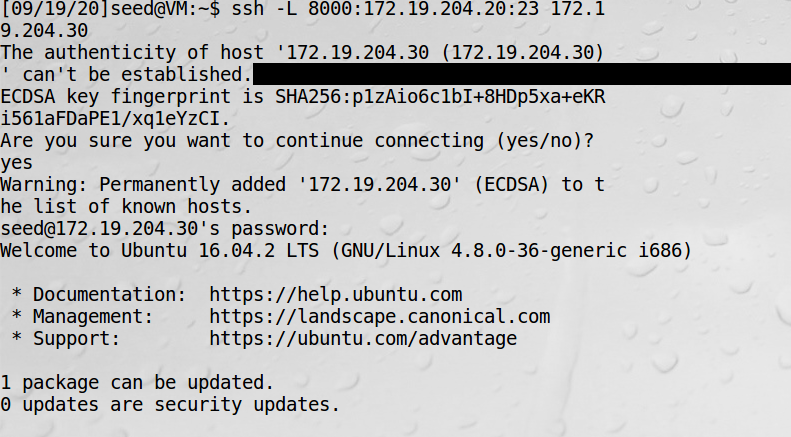
Task 3: 避开出口过滤

主机A中添加规则：

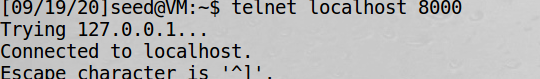


Task 3.a: Telnet to Machine B through the fifirewall

主机A向主机B发送ssh请求：



完成后，可以telnet到lcalhost的8000端口：

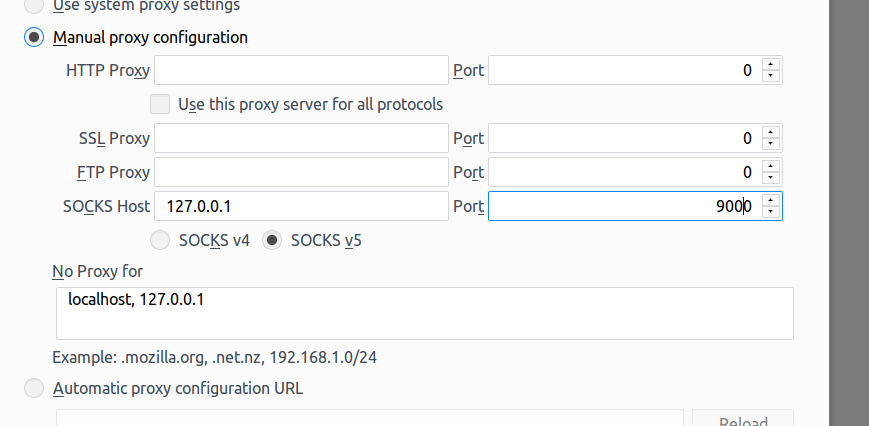


Task 3.b: Connect to Facebook using SSH Tunnel.

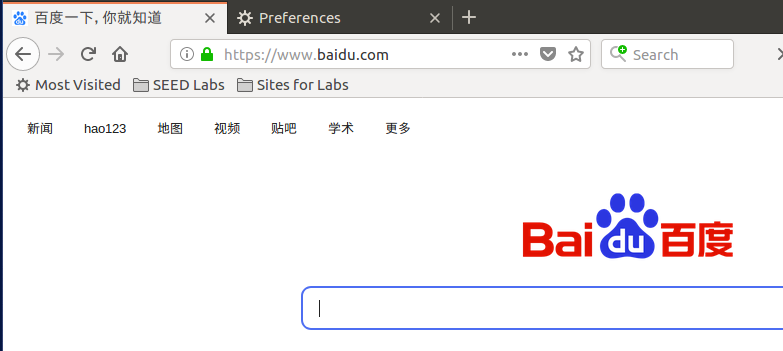
设置ssh隧道，映射主机A的9000端口到主机B：



浏览器中设置代理：

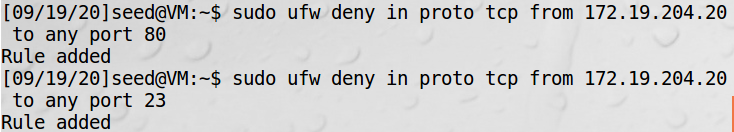


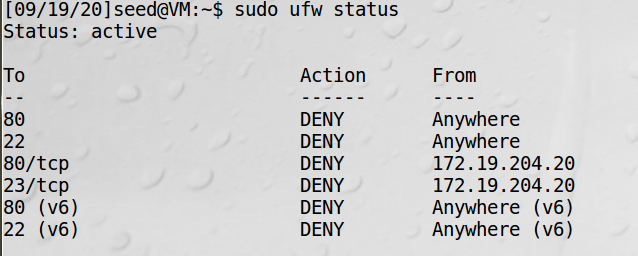
设置完成后成功访问到本该被拦截的百度：



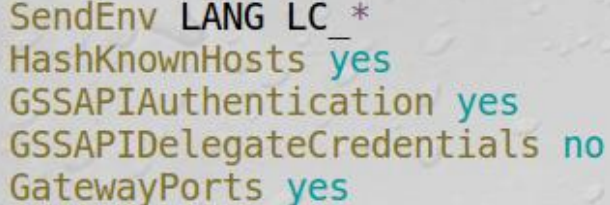
Task 4: Evading Ingress Filtering

主机A中添加规则，禁止主机B访问23、80端口

：



配置主机C的相关文件：



设置ssh隧道，使主机B可通过主机C访问主机A：



结果发现主机B能通过6667号端口成功访问：

