网安综合课程设计

实验报告

（57117105 杨哲君）

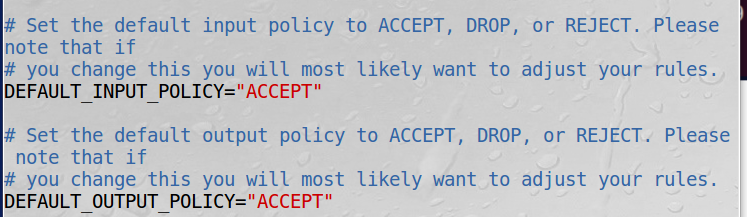
***Linux Firewall Exploration Lab***

**主机A:192.168.80.137**

**主机B：192.168.80.138**

**Task 1: Using Firewall**

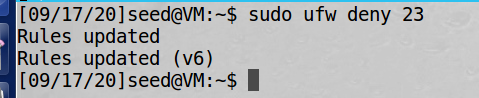
实验前，先将/etc/default/ufw文件的DEFAULT\_INPUT\_POLICY设置为ACCEPT。



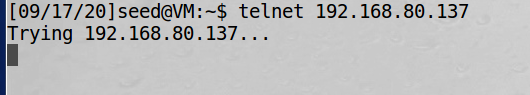
开启防火墙服务。



在主机A中添加规则，禁止访问本机23端口，即telnet服务。



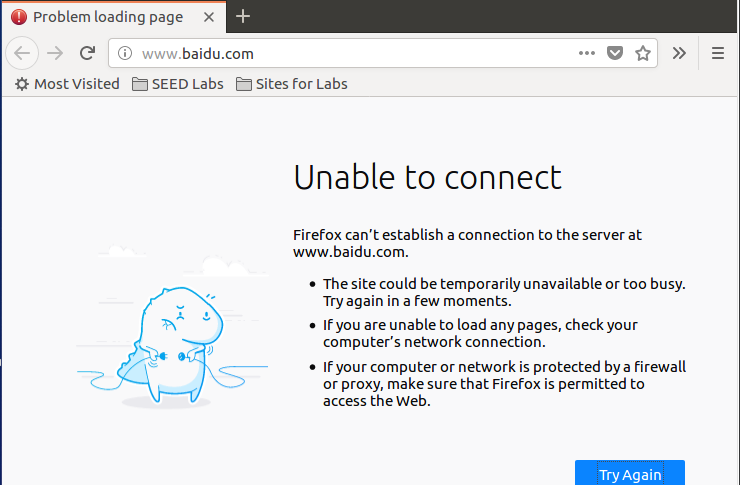
在主机B使用telnet服务，发现其无法访问主机A的telnet服务。同理，在主机B添加一条这样的规则，可以禁止其他主机访问主机B的telnet服务。



在主机A中添加下面的规则，可阻止其对39.156.69.79，即[www.baidu.com](http://www.baidu.com)的访问。

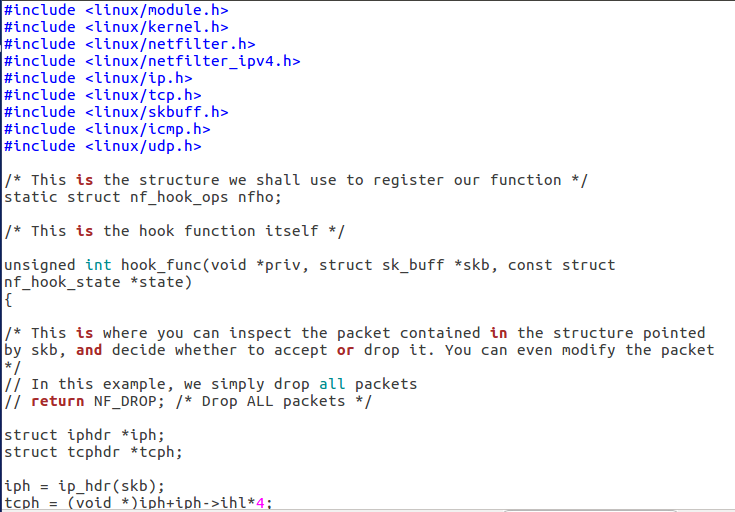


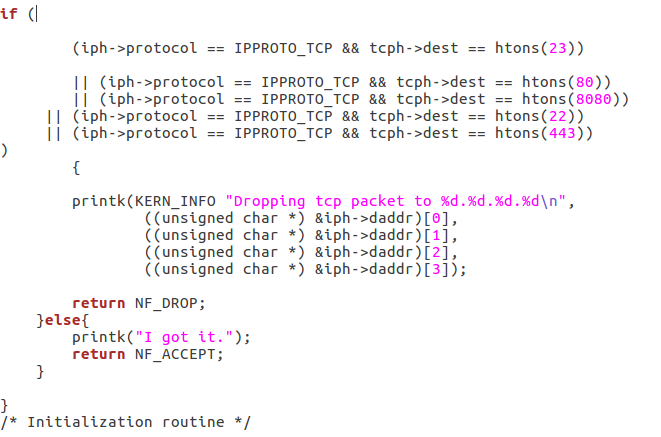
在浏览器输入39.156.69.79，发现其无法加载出百度的网页。实验成功。

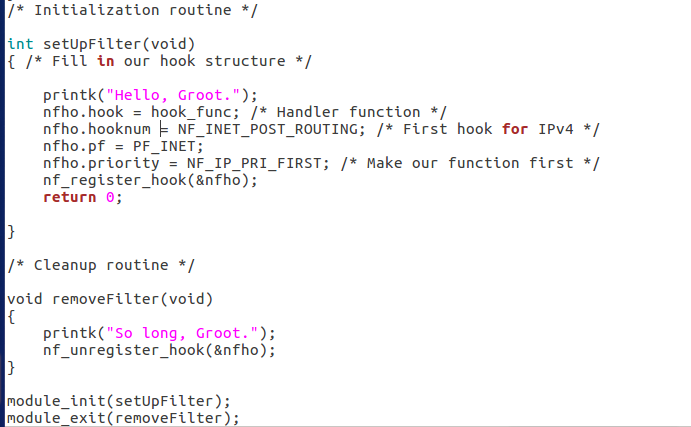


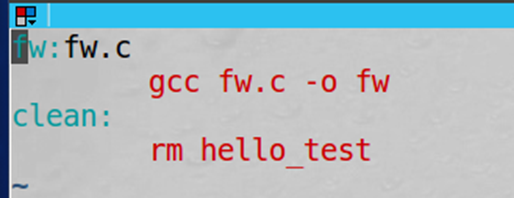
**Task 2: Implementing a Simple Firewall**

编写下面的代码。

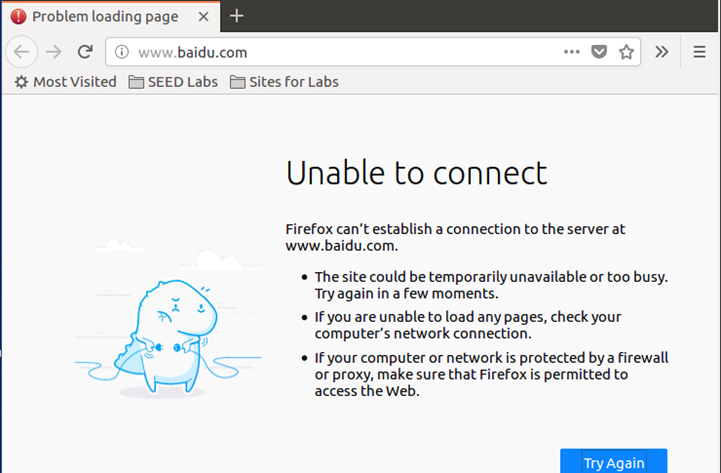




Makefile:

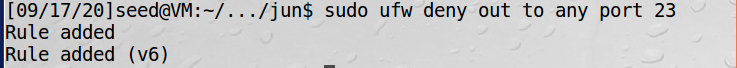
****

将模块编译好后加入内核，限制即可生效，与task1类似，如无法加载百度的网页。



**Task 3: Evading Egress Filtering**

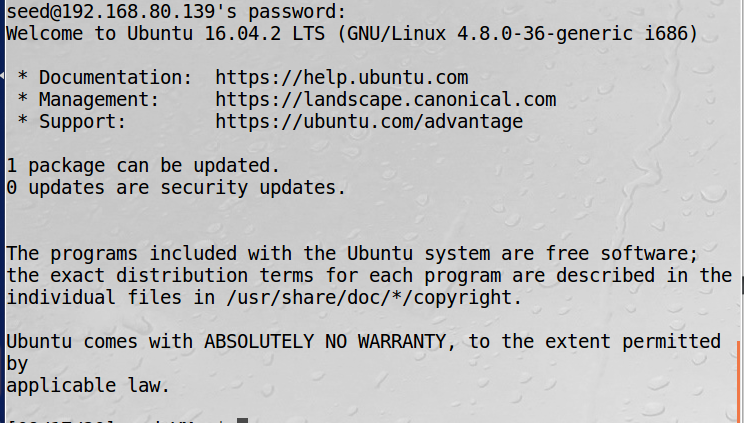
添加ufw规则：

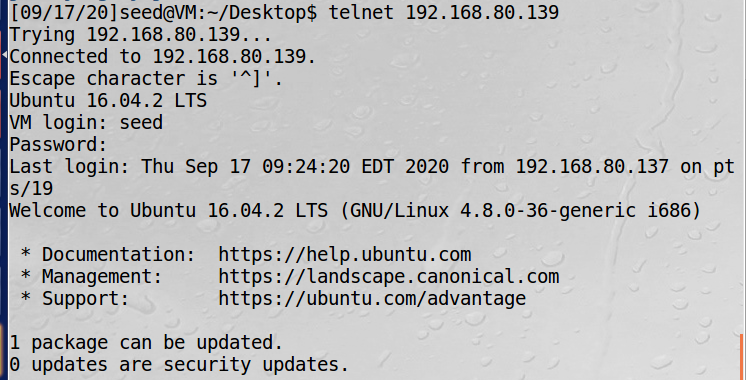


**Task 3.a: Telnet to Machine B through the firewall**

利用SSH连接服务器192.168.80.139，并执行telnet命令，实验成功。

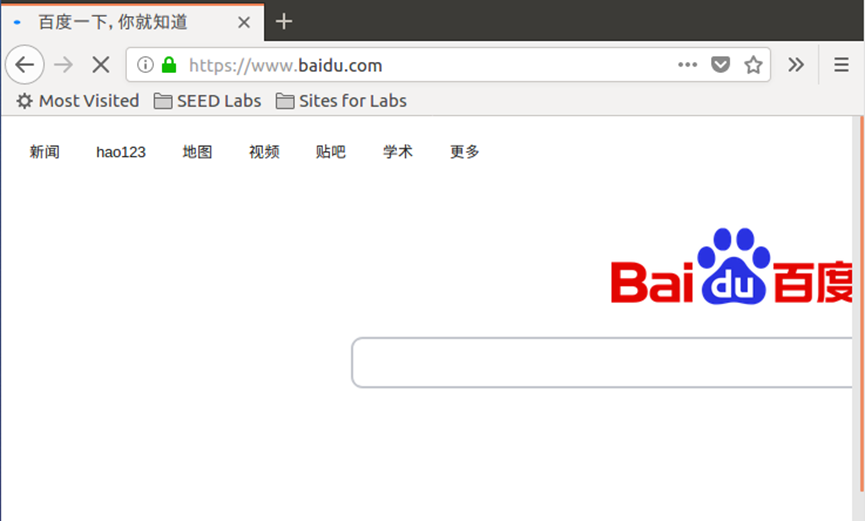






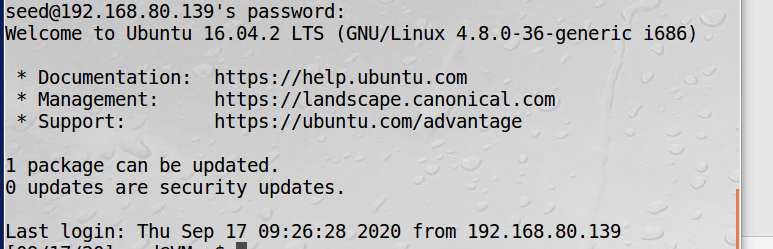
**Task 3.b: Connect to Baidu using SSH Tunnel**

虚拟机192.168.80.139可以正常访问baidu.com，虚拟机192.168.80.137不能正常访问baidu.com。

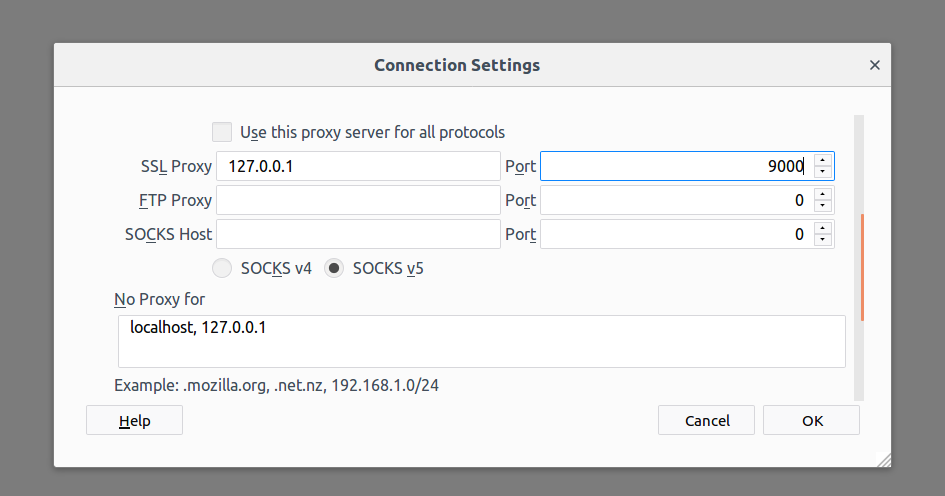


建立192.168.80.137到192.168.80.139的SSH连接。

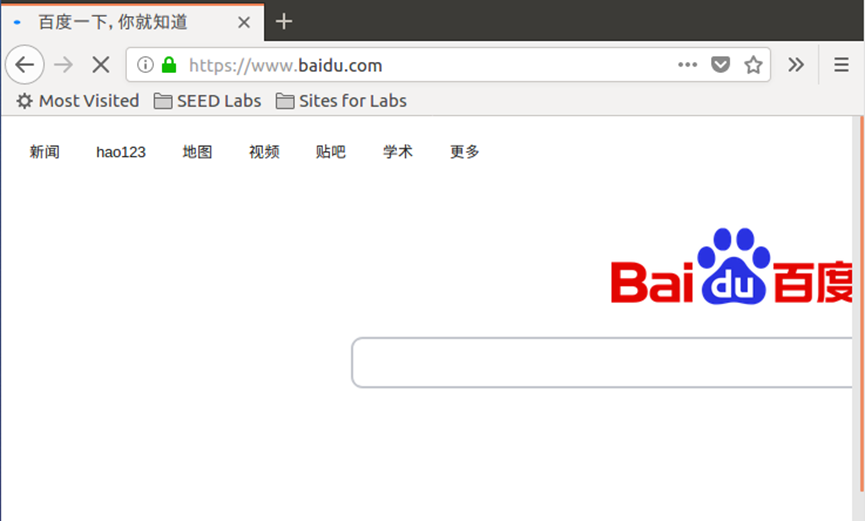




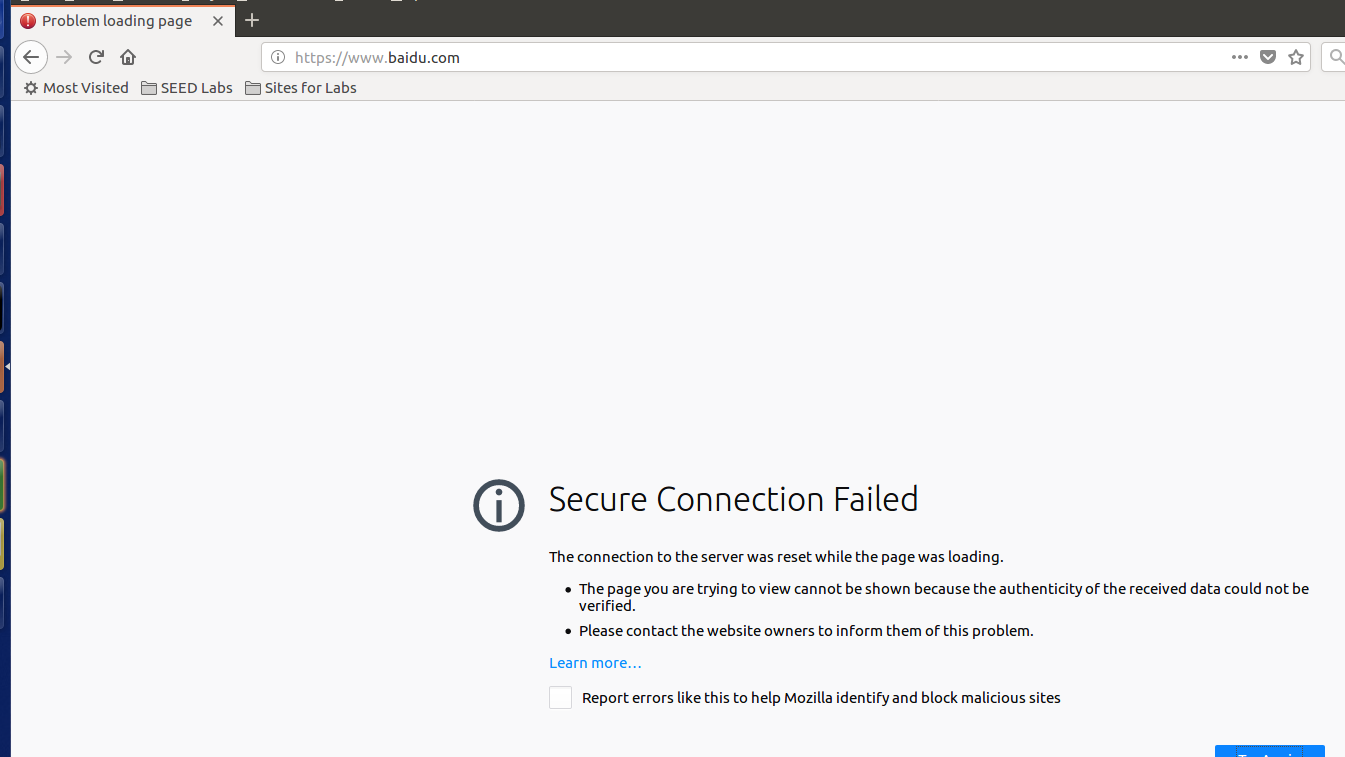
Firefox设置代理.



设置代理后可正常访问百度，通过wireshark可以发现，虚拟机192.168.80.137和百度之间是通过虚拟机192.168.80.139作为跳板，进行数据转发。

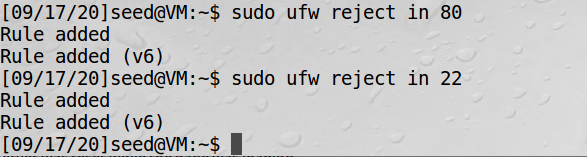


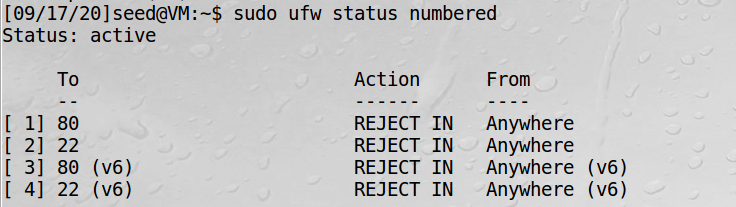
断开SSH连接并且清除浏览器缓存，发现又不能正常访问百度了。



**Task4 Evading Ingress Filtering**

设置主机A的限制规则。





在A端运行下面的命令，通过反向SSH隧道与主机B建立SSH连接，实验成功。

