**网络安全综合课程设计实验6**

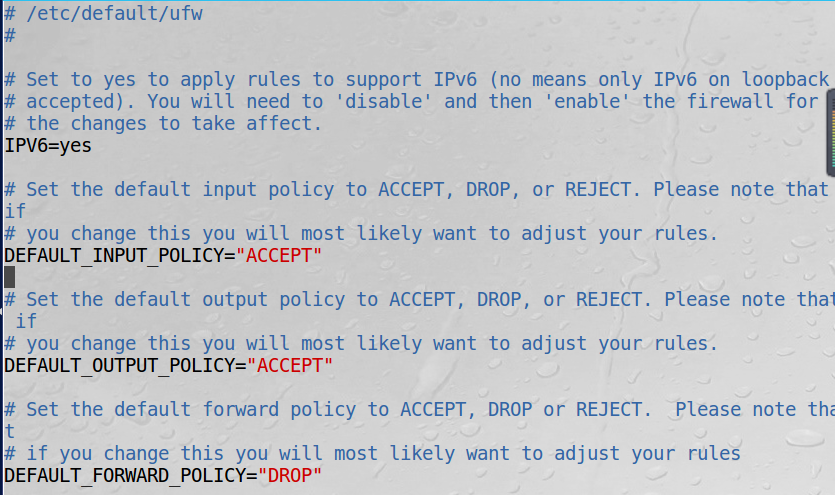
57117204 姚晓

2020/9/18

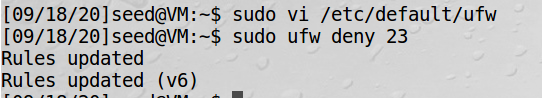
本次实验用三台虚拟机：Ubuntu01（IP地址为10.0.2.4）；Ubuntu02（IP地址为10.0.2.15）；Ubuntu03（IP地址为10.0.2.5）。

**Task1: Using Firewall**

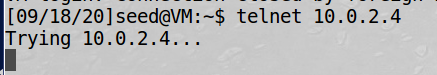
首先在Ubuntu01上修改/etc/default/ufw文件，将DEFAULT\_INPUT\_POLICY改为”ACCEPT”：



然后在Ubuntu01上添加防火墙规则，禁止访问Ubuntu01的23号端口（telnet服务）：



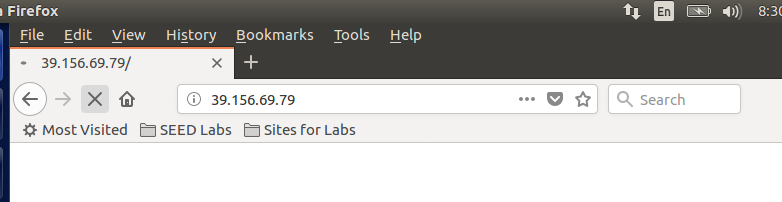
在Ubuntu02上用telnet访问Ubuntu01，发现不能访问：



在Ubuntu01上添加规则，阻止Ubuntu01对[www.baidu.com (IP地址为39.156.69.79](http://www.baidu.com (IP地址为39.156.69.79))的访问：

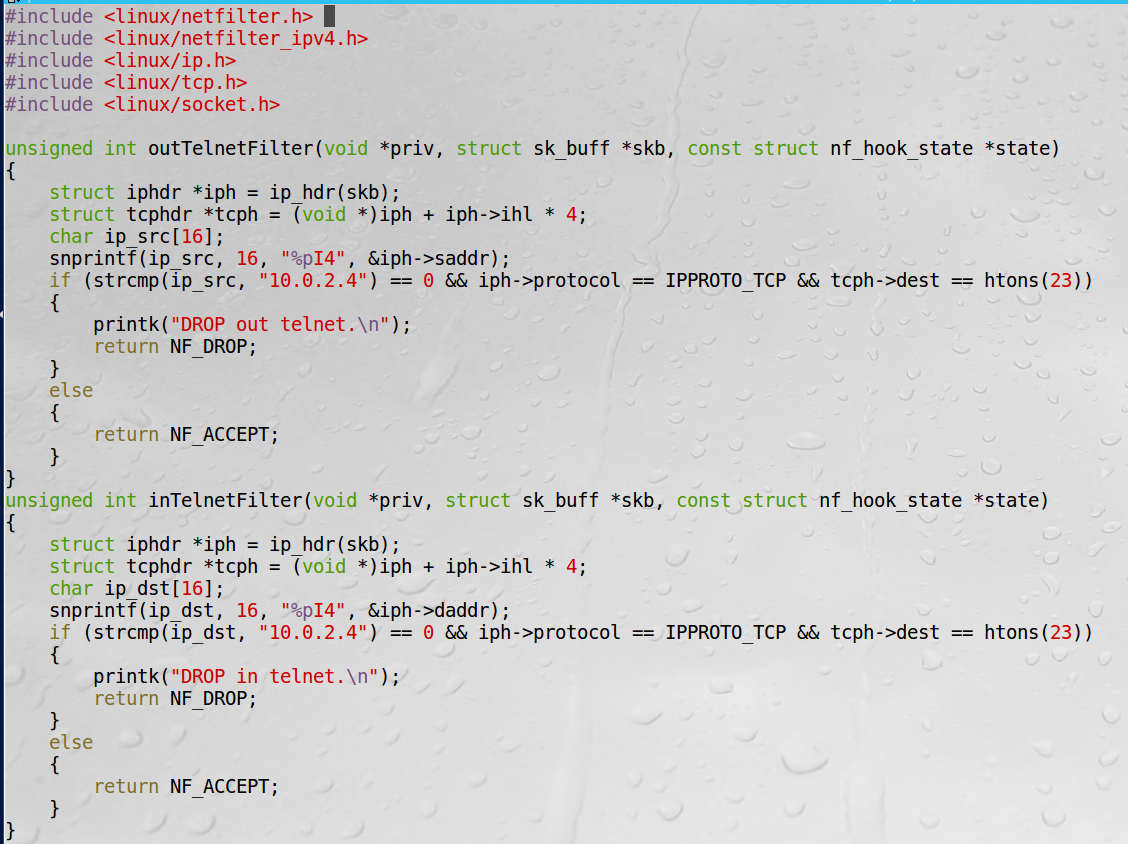


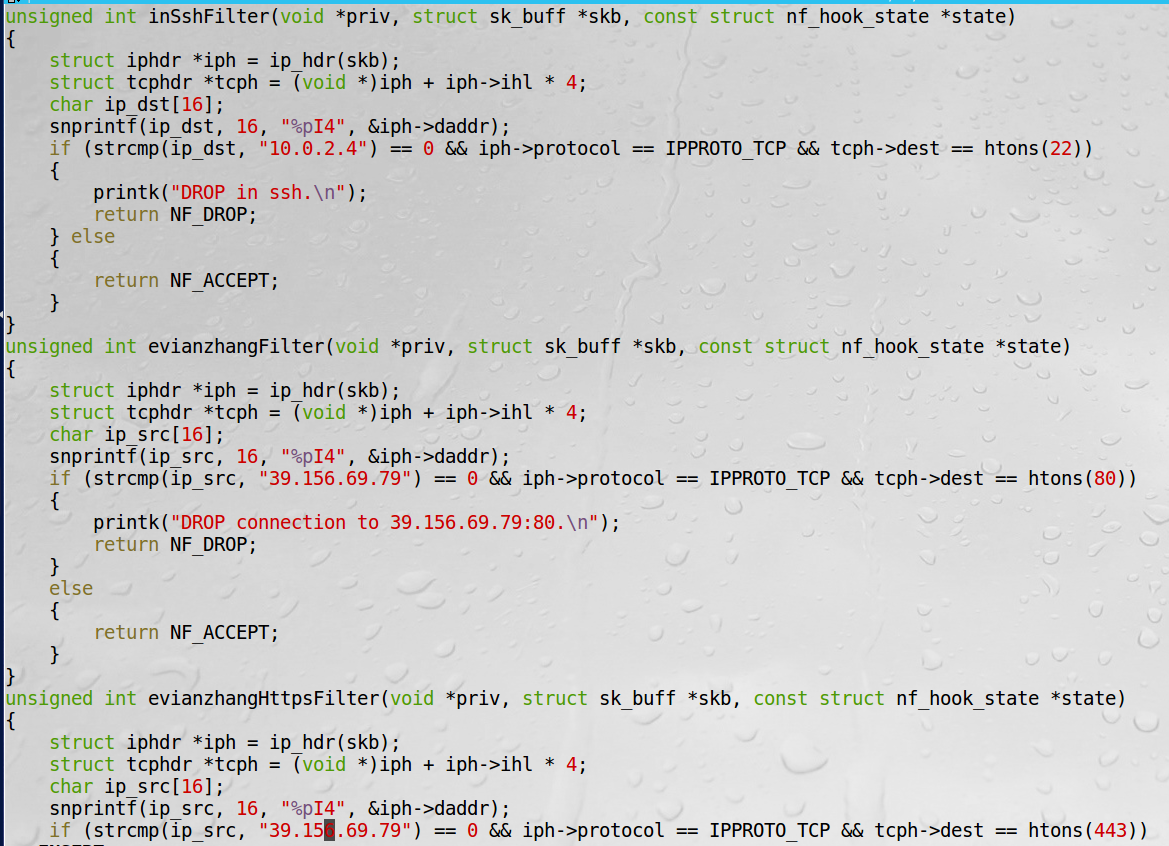
在浏览器访问39.156.69.79，结果无法加载出网页：

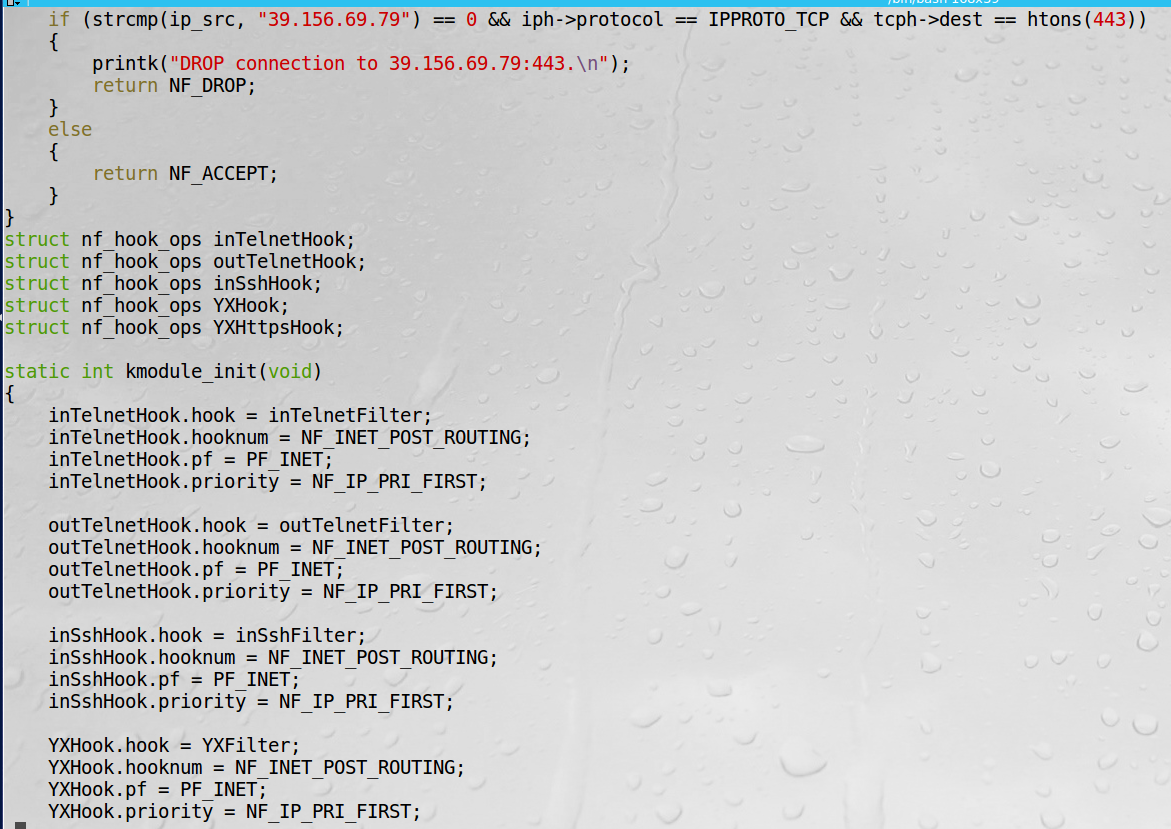


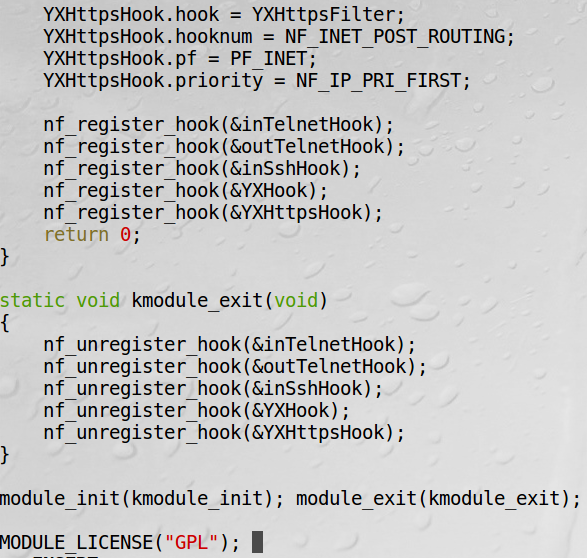
**Task2: Implementing a Simple Firewall**

在Ubuntu01编写代码：







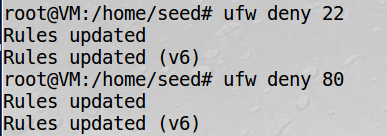


将模块编译好，加载进内核，该代码实现的功能有：禁止Ubuntu01向外部发起telnet连接；禁止外部向Ubuntu01发起telnet连接；禁止外部向Ubuntu01发起ssh

连接；禁止Ubuntu01访问[www.baidu.com](http://www.baidu.com)。

**Task3: Evading Egress Filtering**

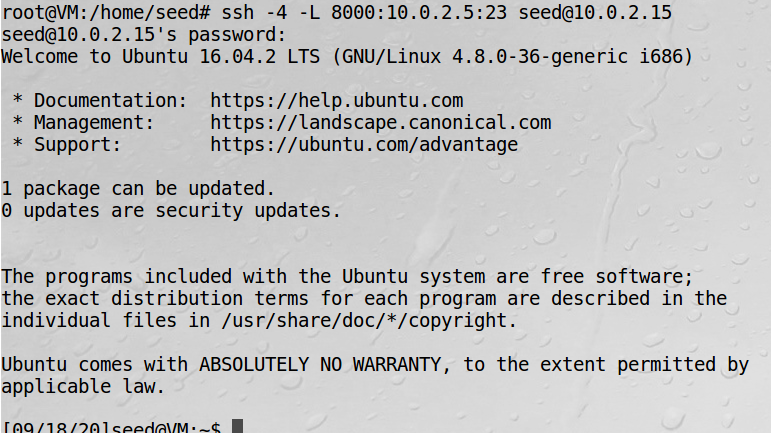
在Ubuntu01添加规则，阻断向外的telnet连接请求，阻断对39.156.69.79的web访问请求：



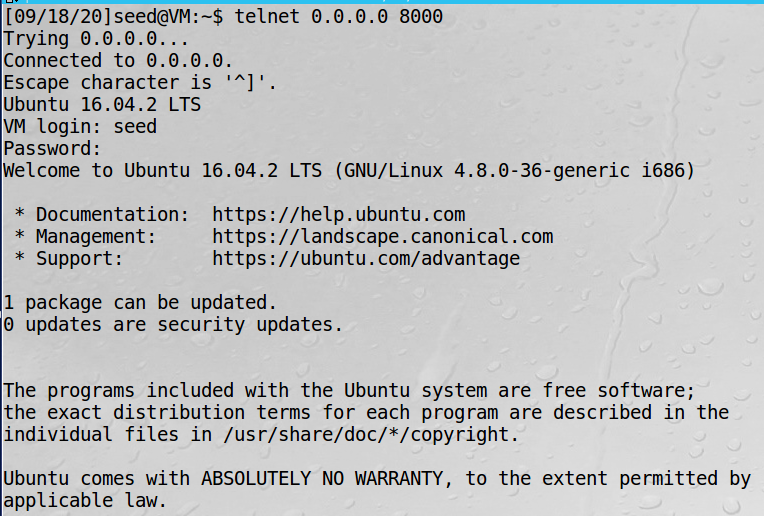


Task3.1:

Ubuntu01向Ubuntu02发起ssh请求，该实验中Ubuntu01以Ubuntu02为跳板访问Ubuntu03，在Ubuntu01中输入命令，会先通过ssh将命令发送给Ubuntu02，然后Ubuntu02将命令发送给Ubuntu03的telnet，Ubuntu03的telnet返回给Ubuntu02后，Ubuntu02再把结果返回给Ubuntu01：

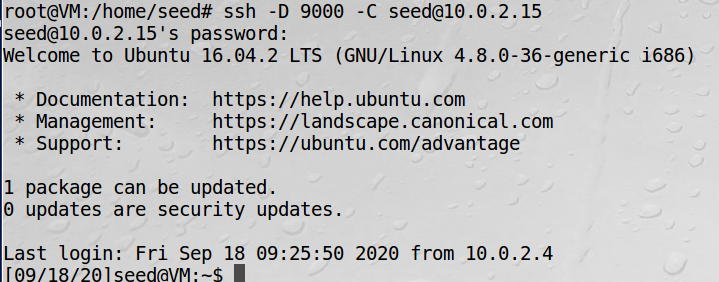


再在Ubuntu01中开一个终端，对0.0.0.0的8000端口发起telnet连接，可以看到成功连接到Ubuntu03：

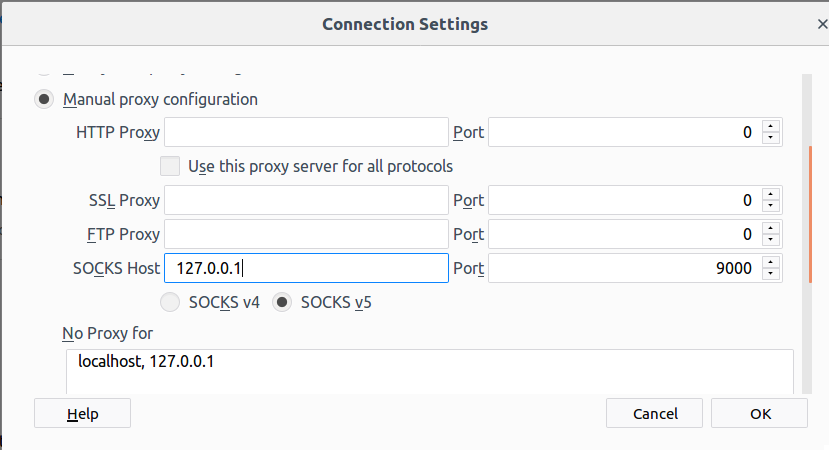


Task3.2:

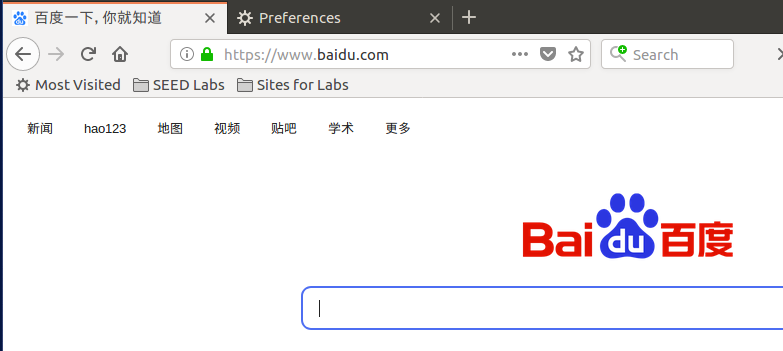
该实验采用动态端口转发方式，映射Ubuntu01的9000端口到Ubuntu02：



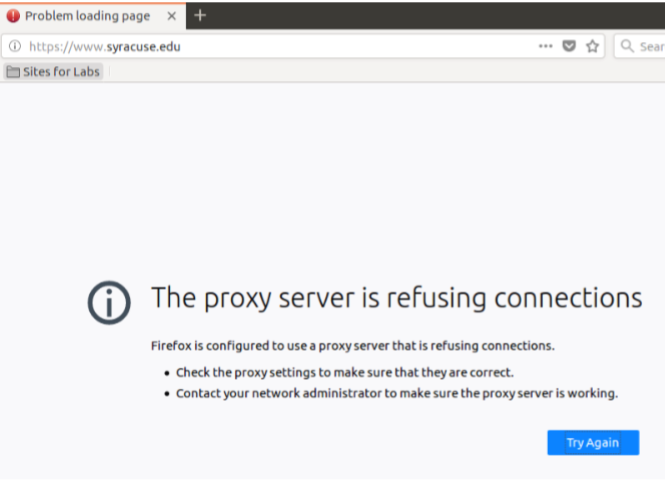
在浏览器中设置代理到本地端口9000：



成功访问到被拦截的网站：

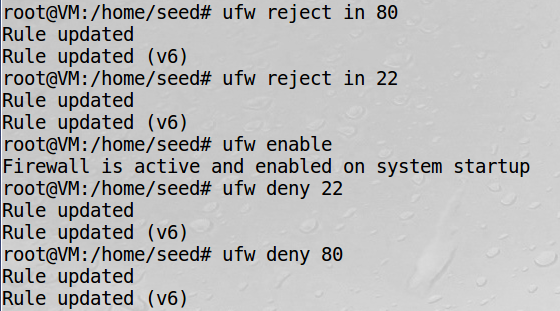


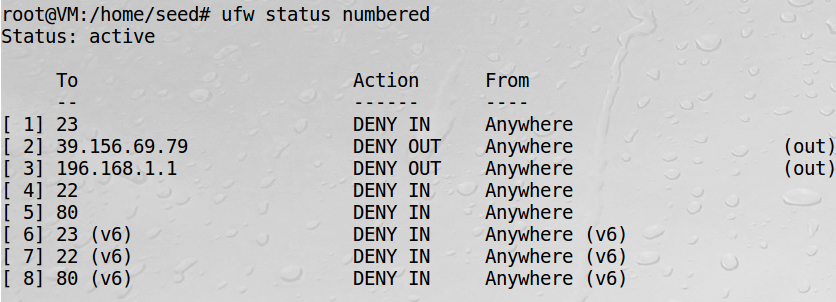
断开ssh连接后不再能访问该网页：



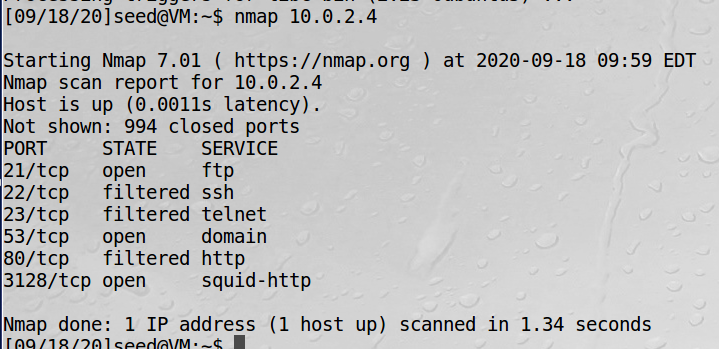
**Task4: Evading Ingress Filtering**

在Ubuntu01中添加如下规则，拦截ssh服务并将自己设为内网web服务器：

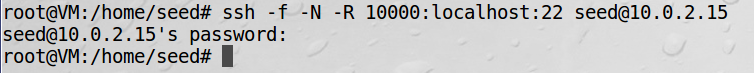




在Ubuntu02中使用Nmap扫描10.0.2.4，可以看到Ubuntu01的22端口和80端口被防火墙过滤：



在Ubuntu01中运行如下命令，将Ubuntu02的10000端口转发到本地的22端口：



在Ubuntu02中运行如下命令，通过反向ssh隧道成功建立与Ubuntu01的ssh连接：

