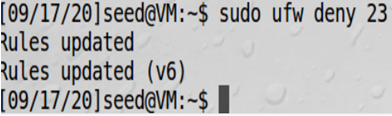
# Linux Firewall Exploration Lab

## 2.1 Task 1: Using Firewall

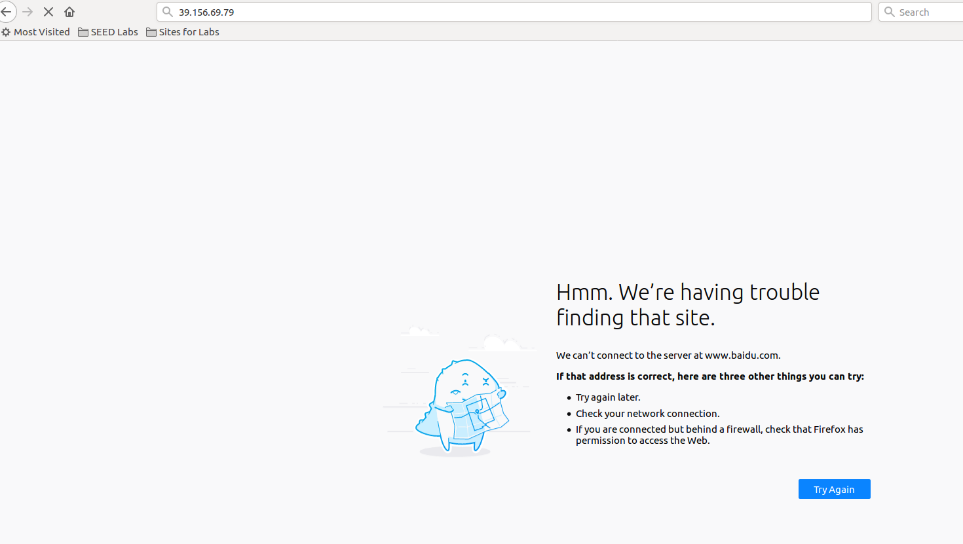
将/etc/default/ufw文件中DEFAULT\_INPUT\_POLICY设置为ACCEPT，在主机中添加规则，禁止访问本机的23号端口。



在主机中ufw添加规则阻止对39.156.69.79的访问。

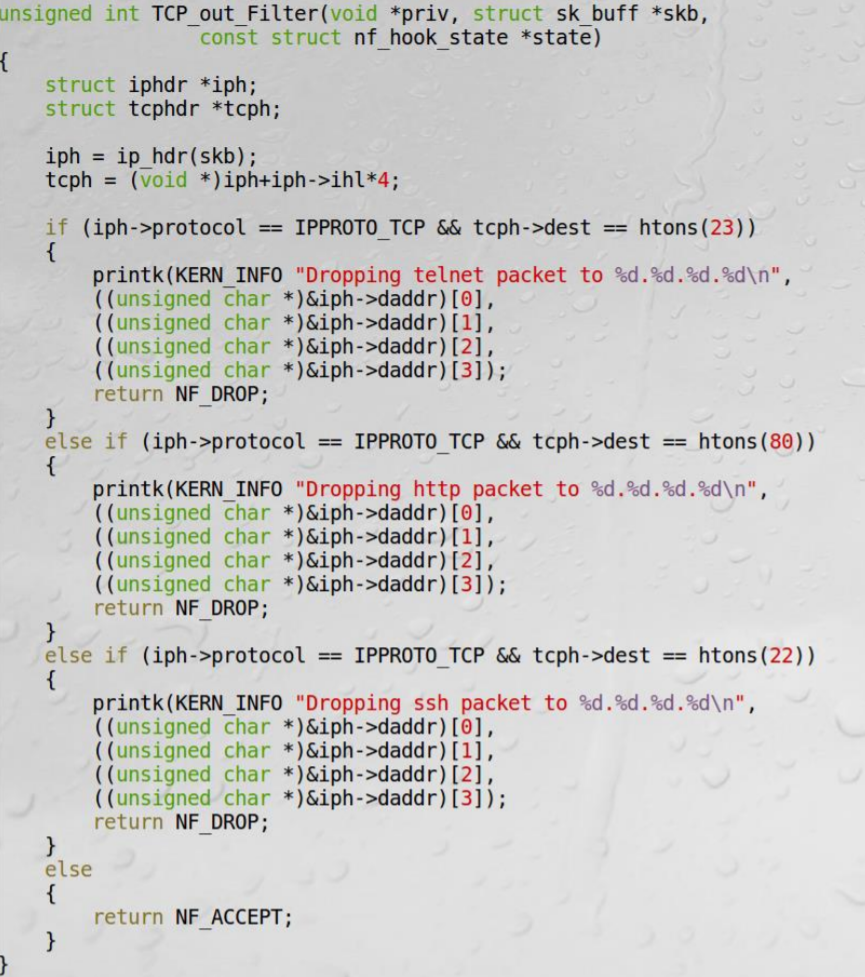


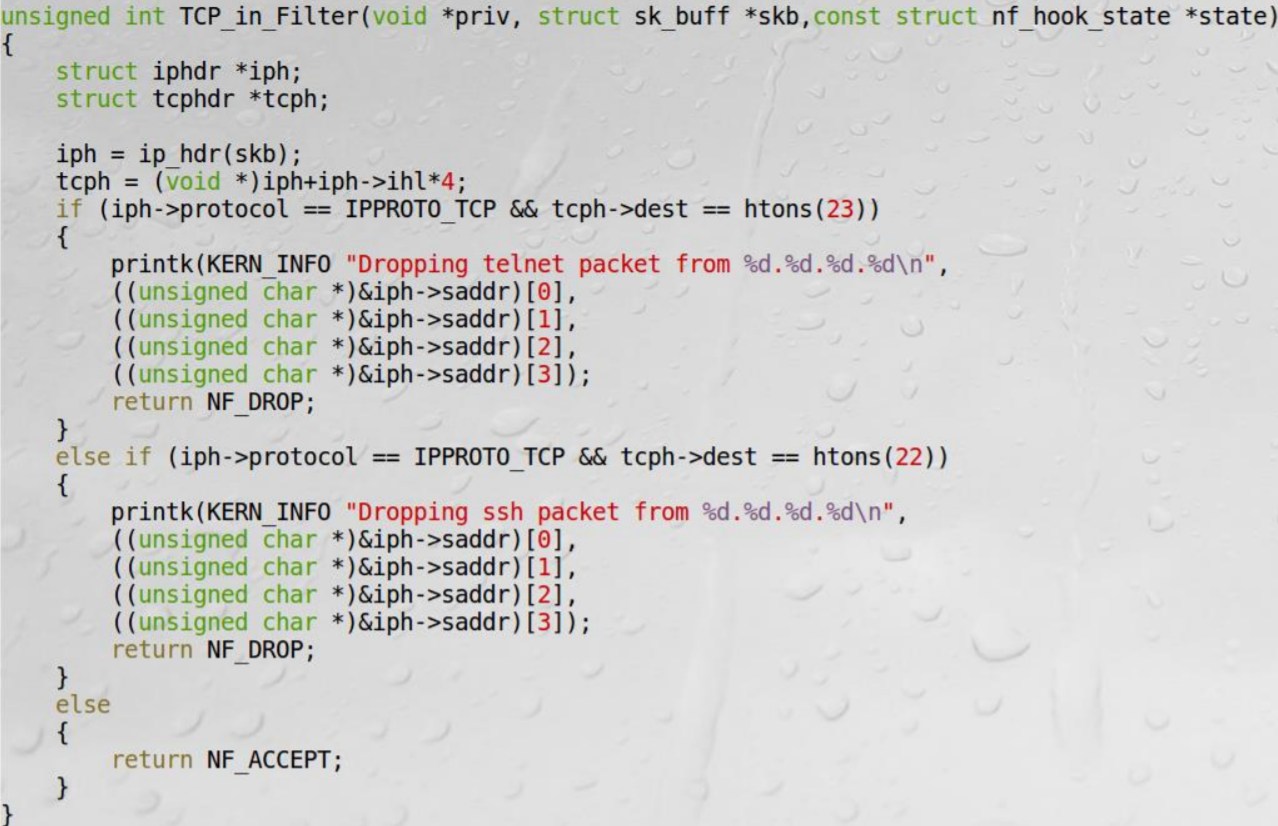
被禁止的网站不能被成功访问



可见禁止对Telnet访问后的操作成功

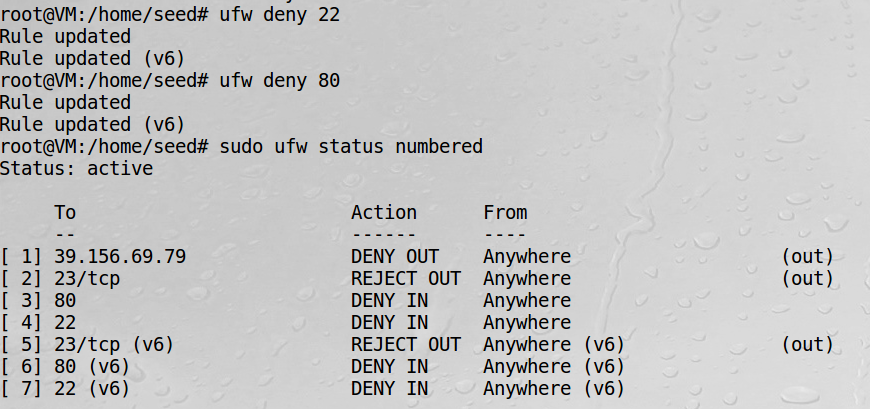
## 2.2 Task 2: Implementing a Simple Firewall





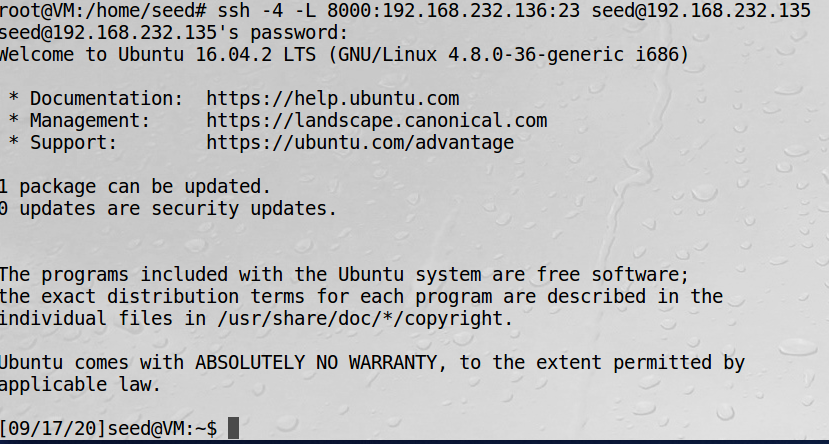
用代码实现功能：禁止本机向外部、外部向本机发起telnet，禁止外部向本机发起ssh，运行后可以看到无法访问。

## 2.3 Task 3: Evading Egress Filtering

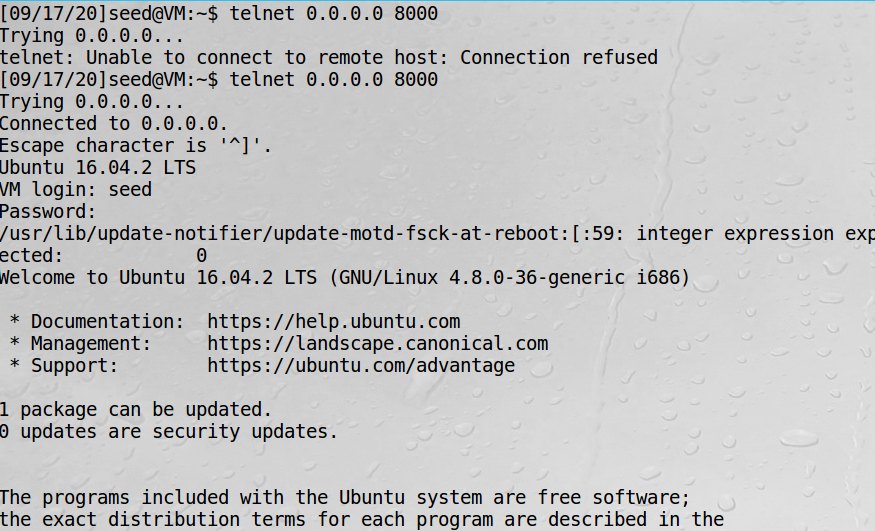


Task 3.a: Telnet to Machine B through the firewall

主机A向主机B发起ssh请求，以B为跳板访问主机C：

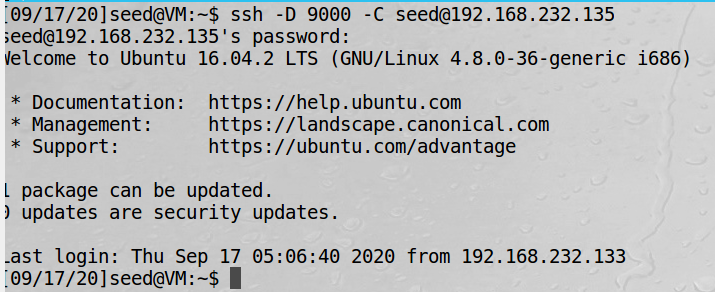


再在主机A中开一个shell，对自身8000端口发起telnet连接：



成功连接到主机C。

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

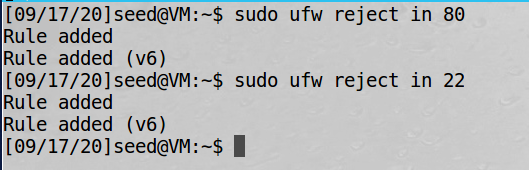


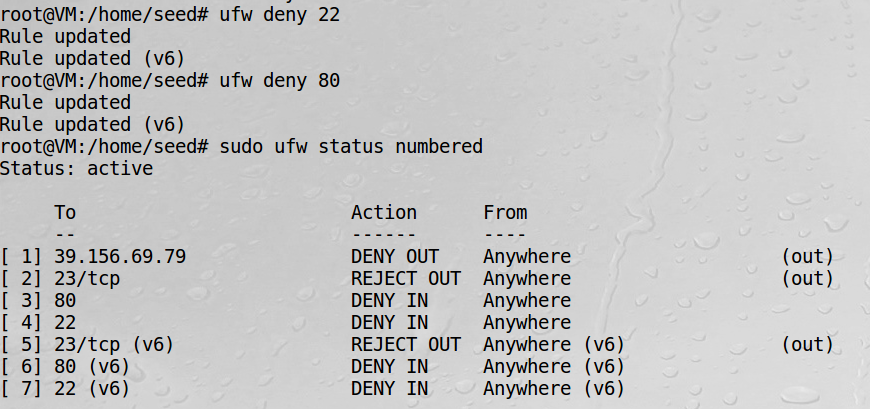
在Firefox浏览器中设置代理到本地端口9000，成功访问被ufw拦截的网站syr.edu。

断开与主机B的ssh连接后不能访问，重新连接ssh后，再次访问，则恢复正常访问。

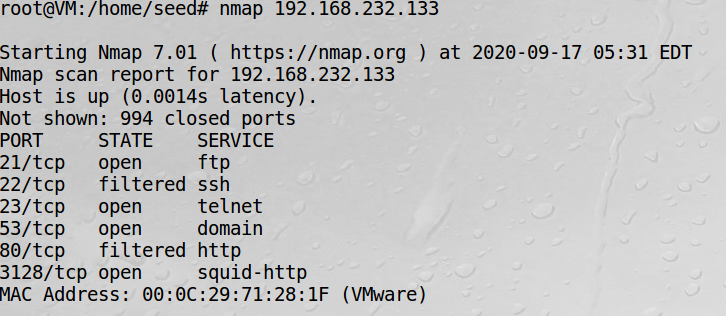
## 2.4 Task 4: Evading Ingress Filtering

在主机A添加规则，将自己设置为内网web服务器，并拦截ssh服务：

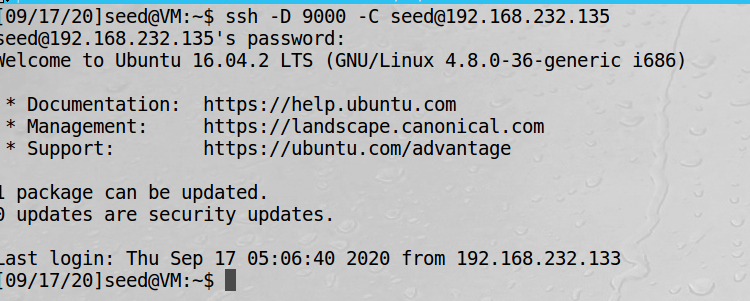
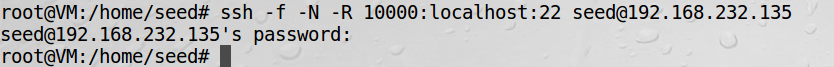




在主机B中使用Nmap可以看到主机A的22端口和80端口被防火墙过滤：



在主机A将主机B的端口10000转发到本地的端口22



主机B通过反向ssh隧道与主机A的ssh连接建立成功