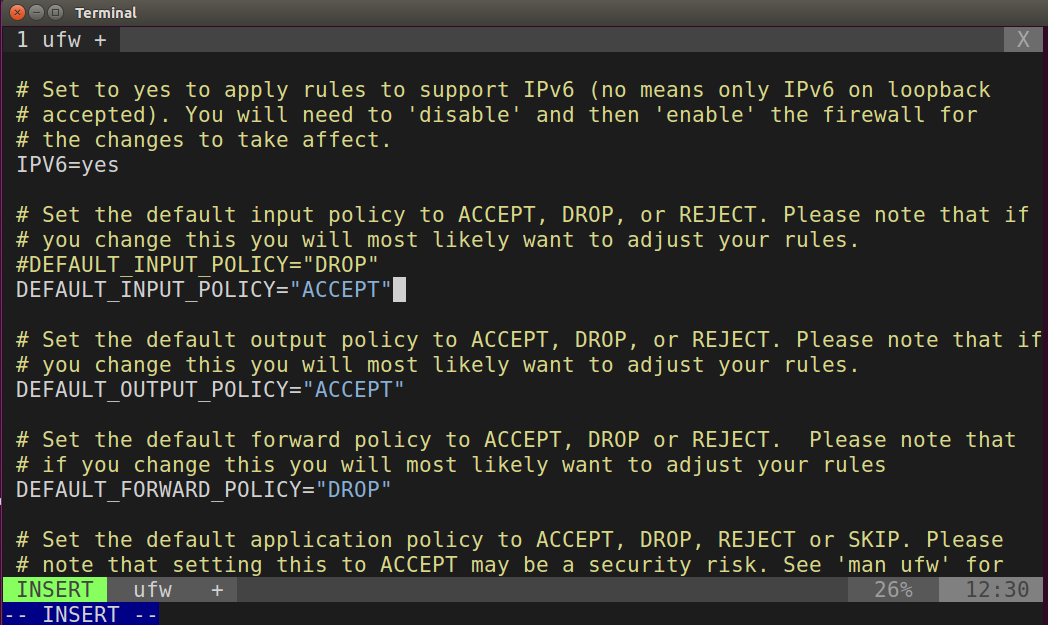
Linux Firewall Exploration Lab

Machine A: 10.0.2.18

Machine B: 10.0.2.17

Task1 Using Firewall

根据任务，首先设置防火墙输入策略默认为允许



在Machine A中输入如下命令：

sudo ufw enable

sudo ufw deny out on enp0s3 proto tcp to 10.0.2.17 port 23

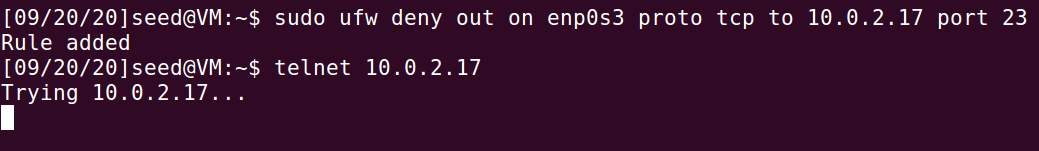
sudo ufw deny out on enp0s3 proto tcp to 93.184.216.34

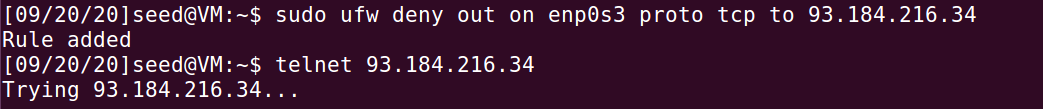
在Machine B中输入如下命令：

sudo ufw deny out on enp0s3 proto tcp to 10.0.2.18 port 23

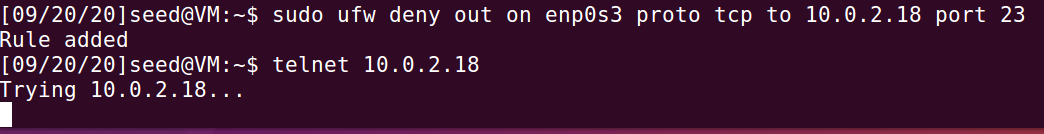
然后尝试telnet连接，发现不能连接：

Machine A





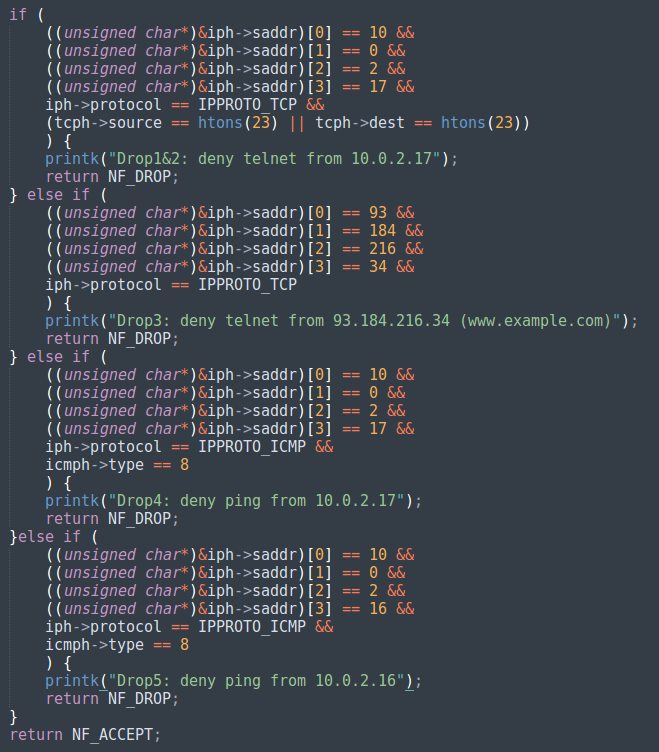
Machine B



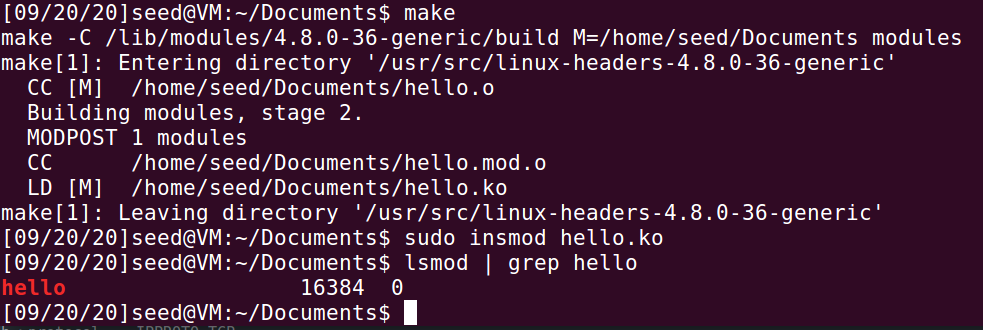
Task2 Implementing a Simple Firewall

实现的规则有：

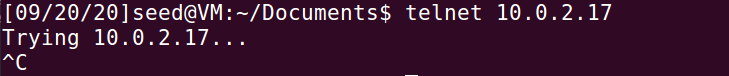
1. 禁止Machine A向Machine B发起telnet连接
2. 禁止Machine B向Machine A发起telnet连接
3. 禁止Machine A向93.184.216.34发起telnet连接
4. 禁止Machine B向Machine A发送ping报文
5. 禁止10.0.2.16向Machine A发送ping报文

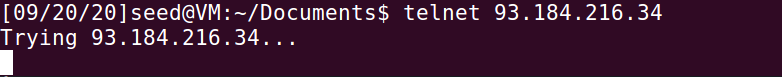


编译并载入到内核

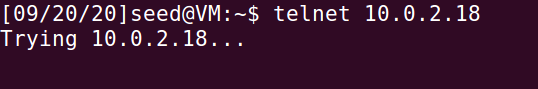


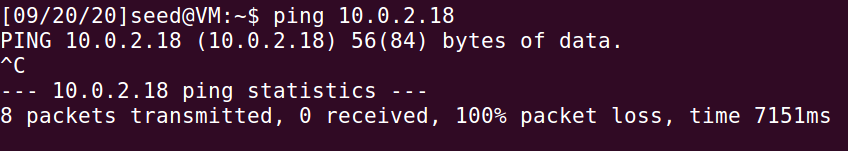
Machine A



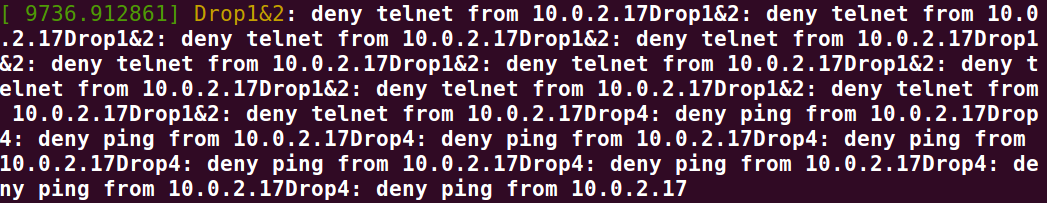


Machine B





Machine A的记录

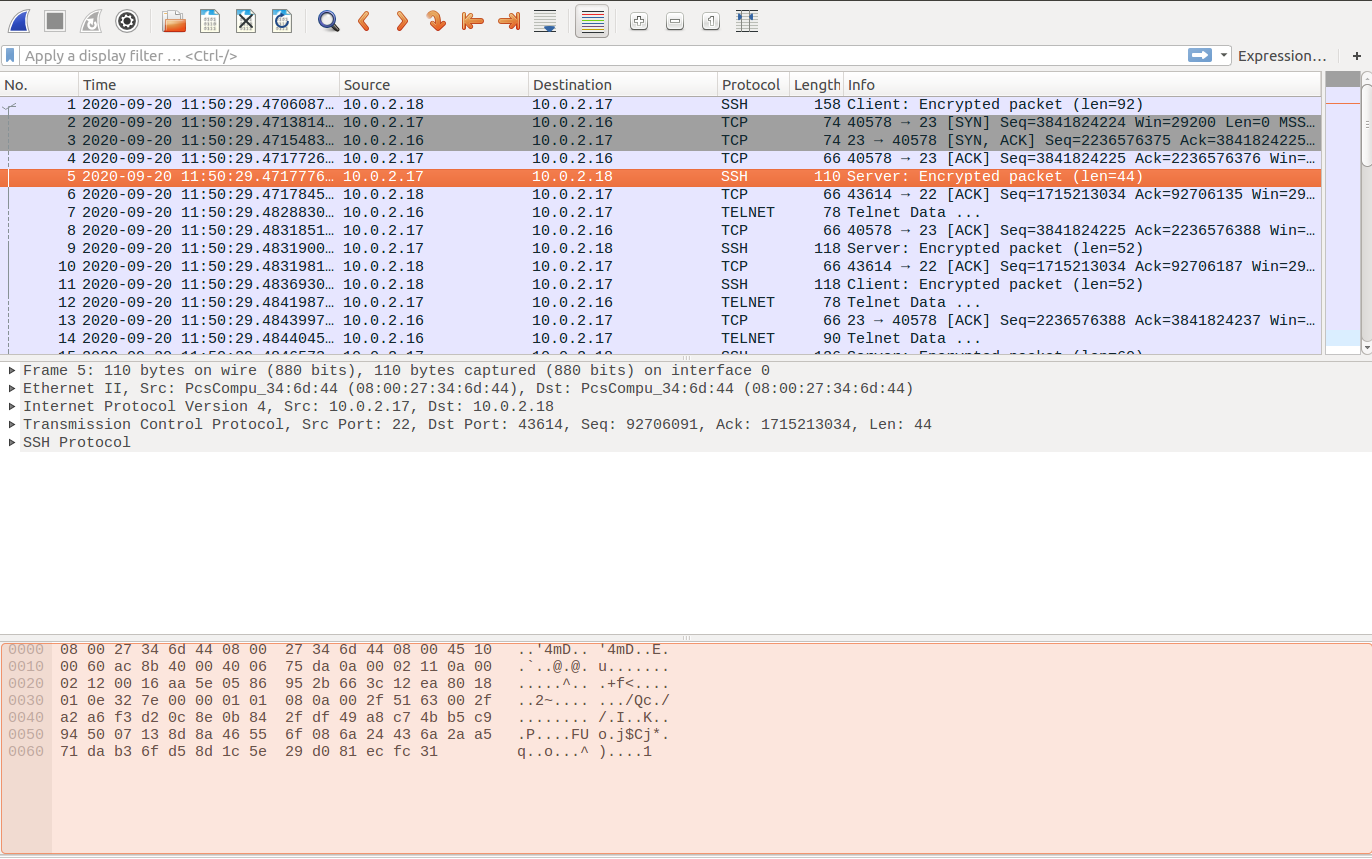


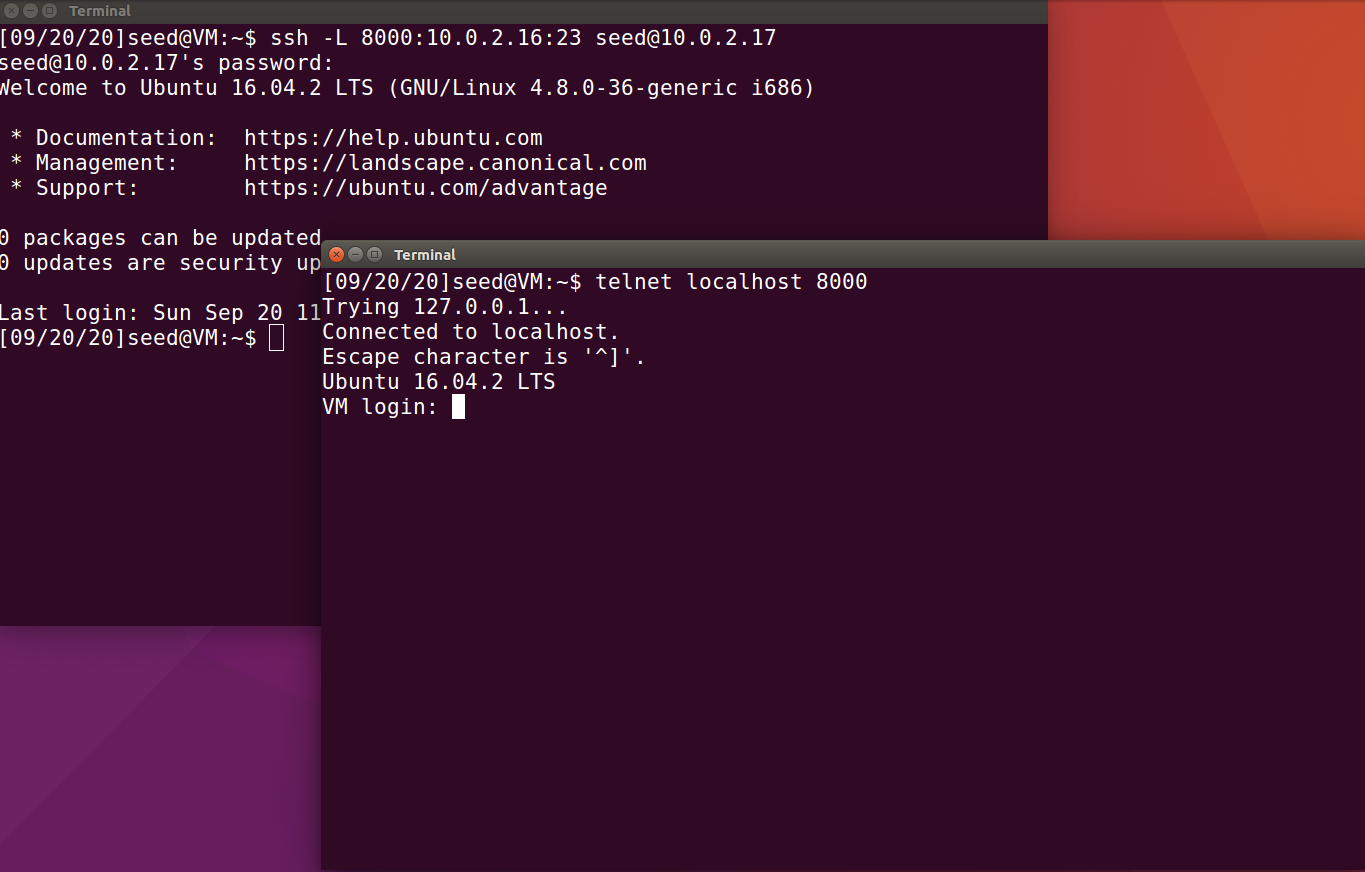
Task3.a Telnet to Machine B through the firewall

Machine A: 10.0.2.18

Machine B: 10.0.2.17

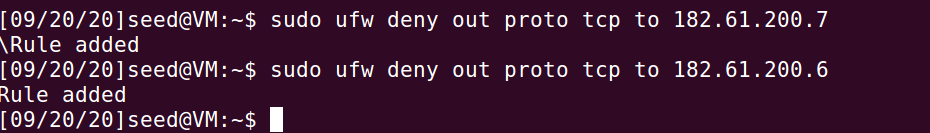
Machine C: 10.0.2.16





Task3.b Connect to XXX using SSH Tunnel

首先在Machine A中设置防火墙策略

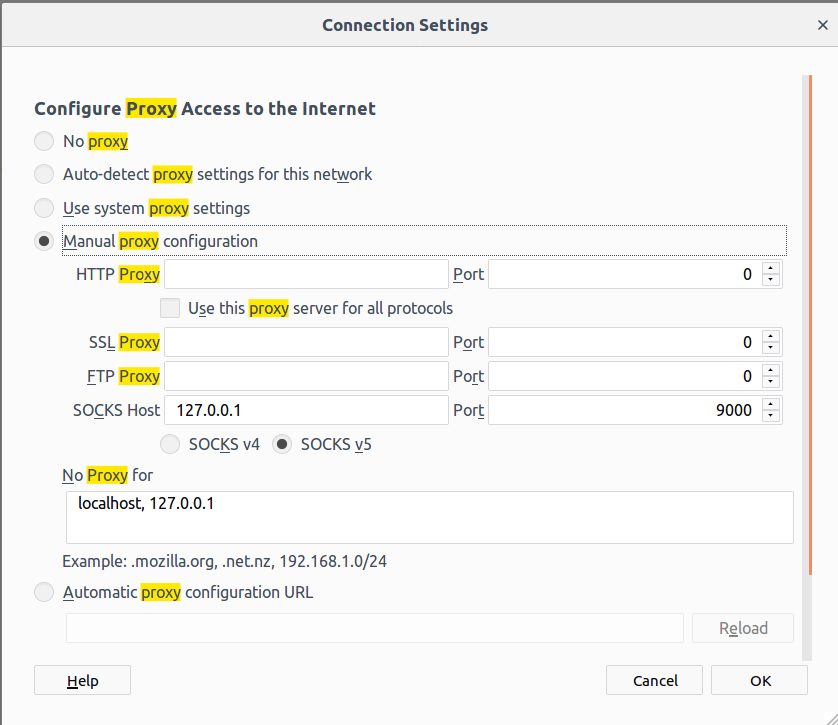


然后发现浏览器无法访问<https://www.baidu.com>

在Machine A中输入以下命令

sudo -D 9000 -C [seed@10.0.2.17](mailto:seed@10.0.2.17)

登录后设置Machine A中的浏览器代理

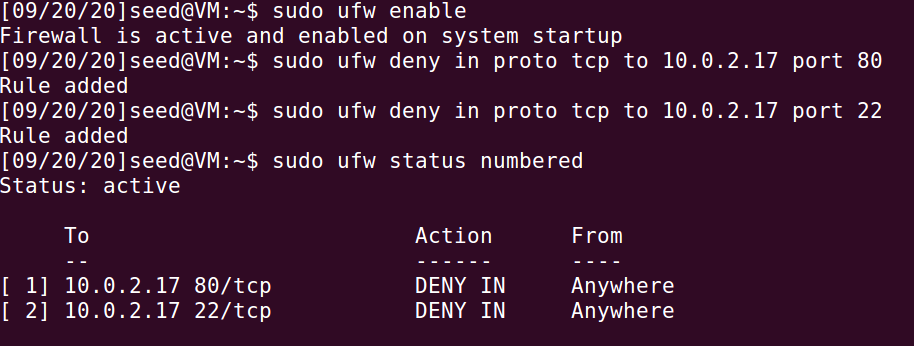


再次登录发现可以访问<https://www.baidu.com>了



Task4 Evading Ingress Filtering

在Machine B中添加防火墙规则



在Machine B中执行以下命令

sudo ssh -D 12345:127.0.0.1:80 [seed@10.0.2.18](mailto:seed@10.0.2.18)

登录成功和打开Machine A中的浏览器，访问<http://localhost:12345>网址，发现连接成功

