**Lab6实验报告**

57117138 吴伊杰

**Linux Firewall Exploration Lab**

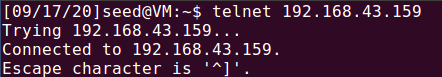
# Task 1: Using Firewall

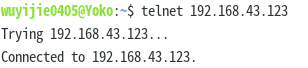
Machine A的IP地址：192.168.43.123

Machine B的IP地址：192.168.43.159

* **阻止A对B进行telnet连接；阻止B对A进行telnet连接**

未进行任何操作时，A和B可以互相连接：

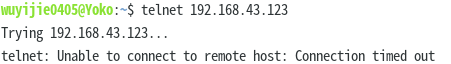




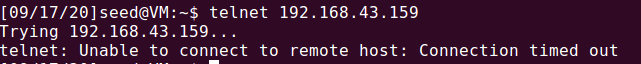
在主机A处开启防火墙——sudo ufw enable



此时主机B无法对A进行telnet连接

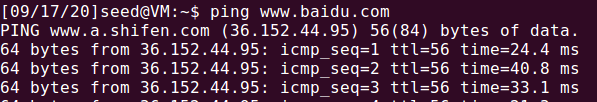


同理，在主机B处开启防火墙，主机A也无法对B进行telnet连接



* **阻止A访问某个外部网页**

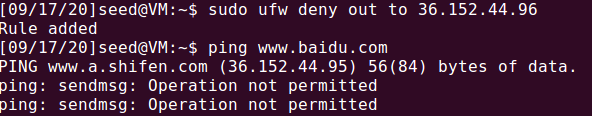
以[www.baidu.com](http://www.baidu.com)为例，先ping一下百度查看其ip地址

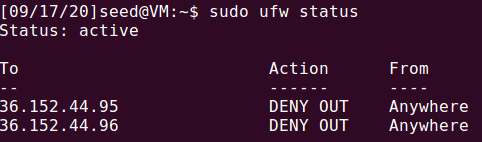


添加规则



此时再去ping百度，如果ping的是该IP地址，会被拒绝访问

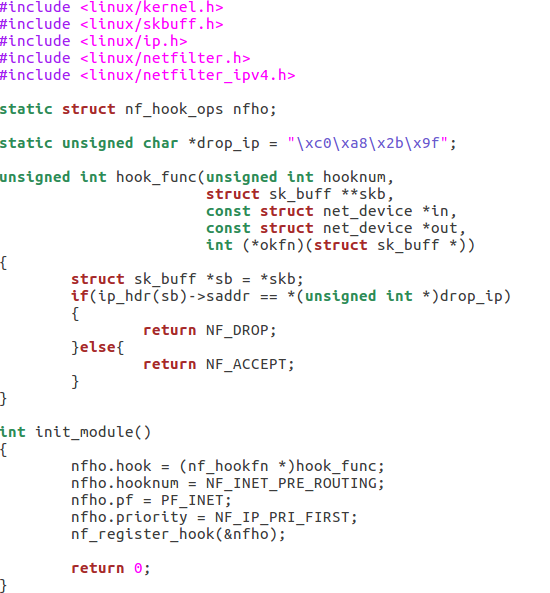




# Task 2: Implementing a Simple Firewall

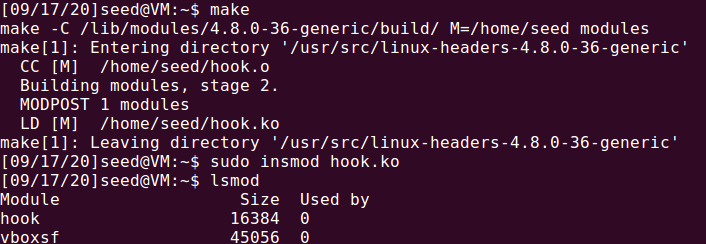
使用LKM和Netfilter来实现包过滤模块。

在监测点NF\_INET\_PRE\_ROUTING设置阻止主机B的任何访问，故代码如下：

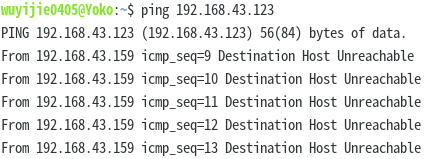


\*drop\_ip为阻止访问主机的IP地址

注意指针的写法，可能seed的gcc编译较为严格，容易报错。

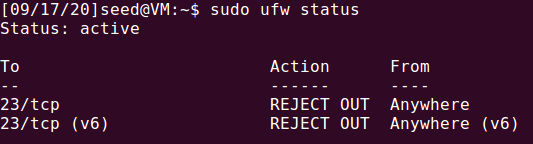


在内核中加载模块，上图为成功的结果。然后在主机B中尝试连接A，失败。可见阻止成功。



# Task 3: Evading Egress Filtering

主机A（192.168.43.123）已经设定防火墙，阻止了所有对外telent访问



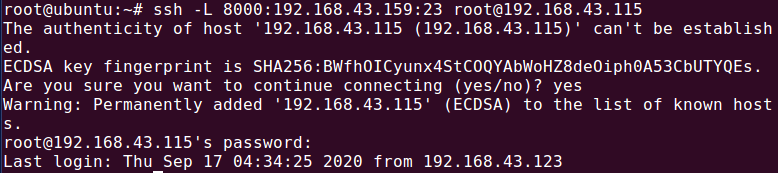
主机B（192.168.43.115）不设定防火墙

主机C（192.168.43.159）作为telnet服务器

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

令主机A穿过防火墙对主机B进行telnet访问。

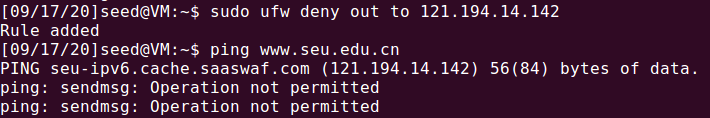
方法：令A向C发起SSH访问请求，然后以其为跳板telnet访问B



然后进行telnet连接，成功。

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

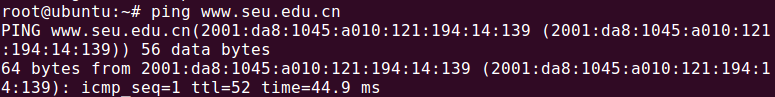
使用SSH请求连接一个被禁止访问的网址，这里以[www.seu.edu.cn](http://www.seu.edu.cn)为例：



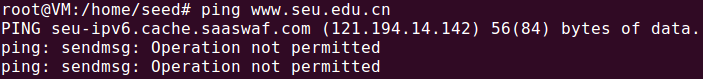
通过SSH通道将主机B作为跳板



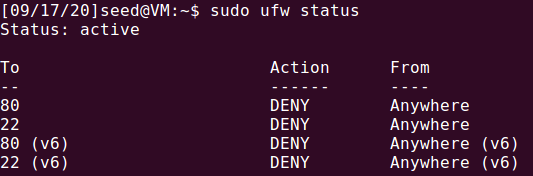
此时可以顺利与[www.seu.edu.cn](http://www.seu.edu.cn)通信



退出SSH后，又不可访问



# Task 4: Evading Ingress Filtering



在主机A中阻止外部对其80端口和22端口的连接

然后通过指令建立ssh通道



这样主机B就可以反向通过该通道访问到主机A的80端口