网络空间安全课程综合设计任务报告六

57117203 姜舒

2020年9月19日

（一）Linux Firewall Exploration Lab

Task 1: Using Firewall

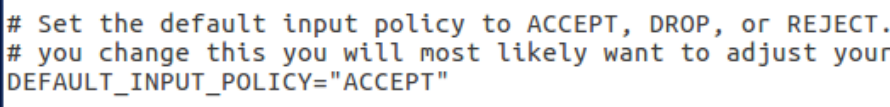
各虚拟机IP地址：

Machine A 虚拟机VA 10.0.2.4

Machine B 虚拟机VB 10.0.2.5

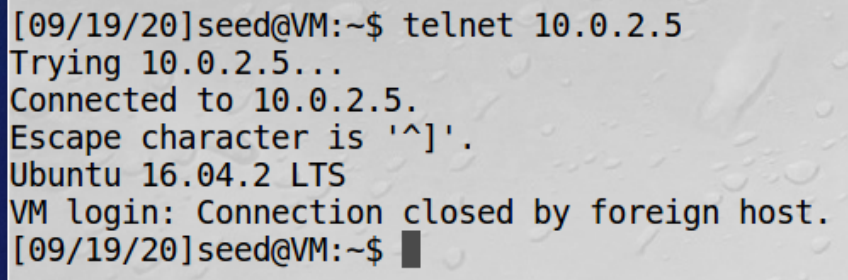
路由器 虚拟机VC 10.0.2.6

在VA中找到默认的policy file /etc/default/ufw并修改，将DROP改为ACCEPT

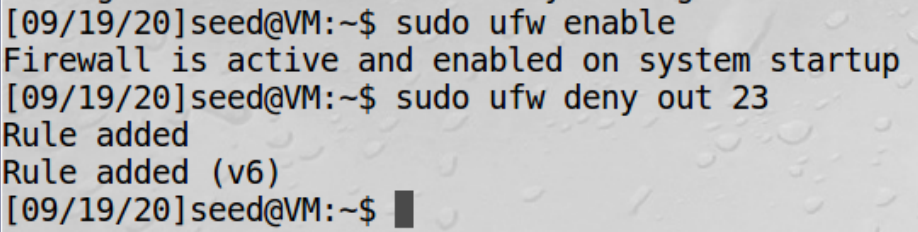


• Prevent A from doing telnet to Machine B. 阻止A对机器B进行telnet

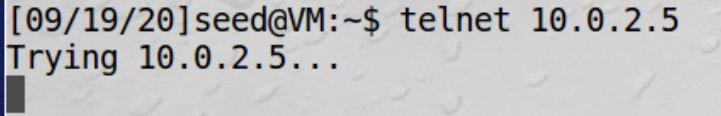
没有禁止访问外部23端口之前，在VA上telnet VB，正常连接



打开ufw设置，禁止VA向外进行telnet连接

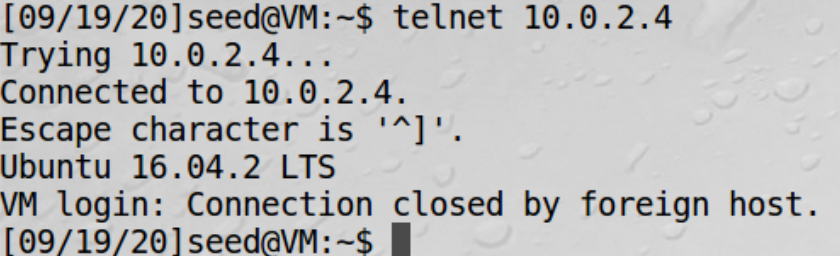


再telnet VB，无法访问

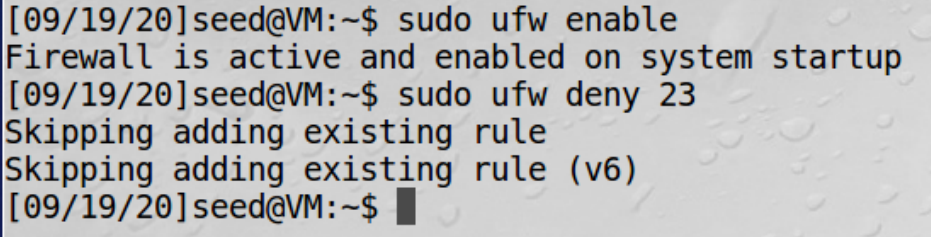


• Prevent B from doing telnet to Machine A. 阻止B对机器A进行telnet

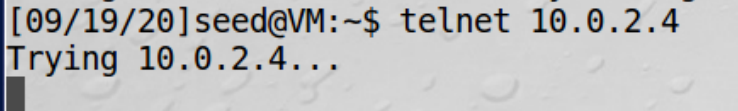
没有禁止访问23端口之前，在VB上telnet VA，正常连接



开启ufw设置，使用ufw命令关闭23端口telnet服务



此时再在VB上telnet VA，无法连接



• Prevent A from visiting an external web site. You can choose any web site that you like to block, but keep in mind, some web servers have multiple IP addresses.

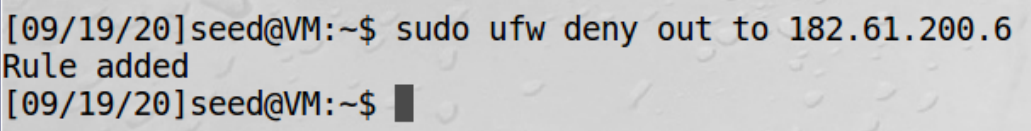
阻止A访问外部网站。 您可以选择要阻止的任何网站，但是请记住，某些Web服务器具有多个IP地址。

使用dig命令获得www.baidu.com的IP地址为182.61.200.6和182.61.200.7

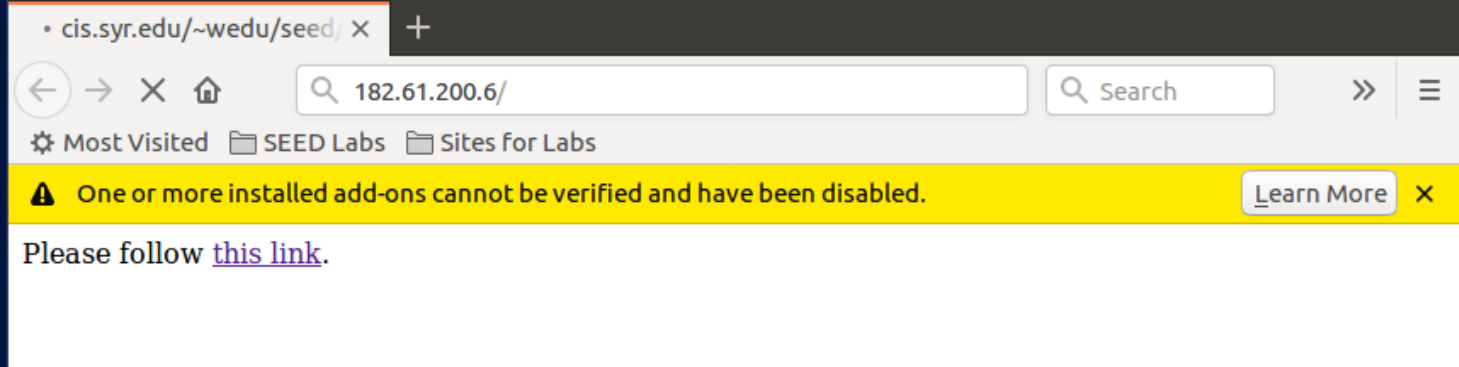
在浏览器里访问182.61.200.6可以打开www.baidu.com的地址



使用ufw命令关闭182.61.200.6地址的访问

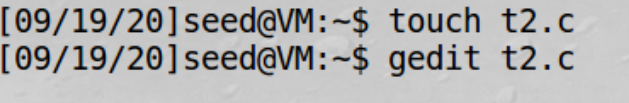


此时无法访问182.61.200.6

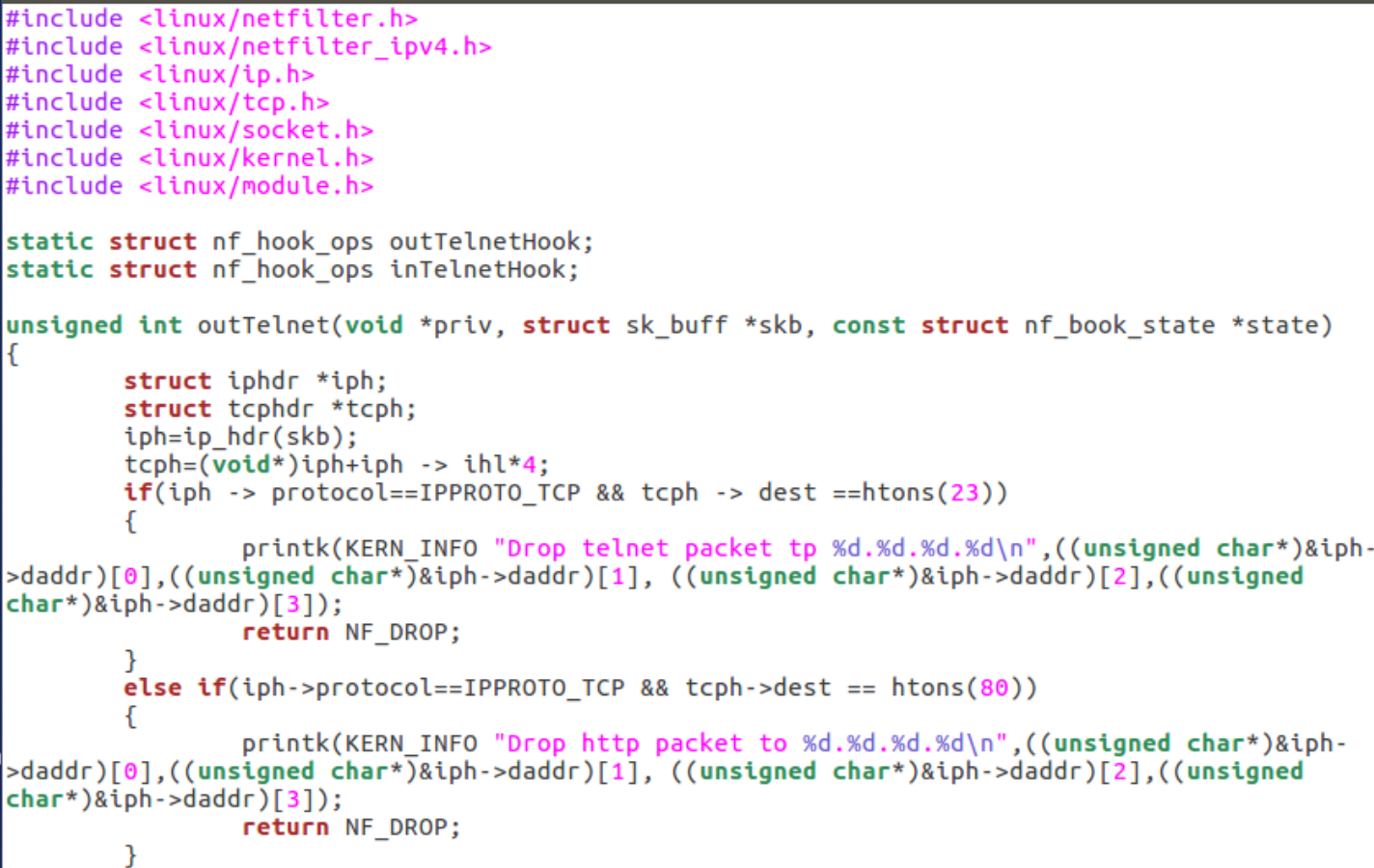


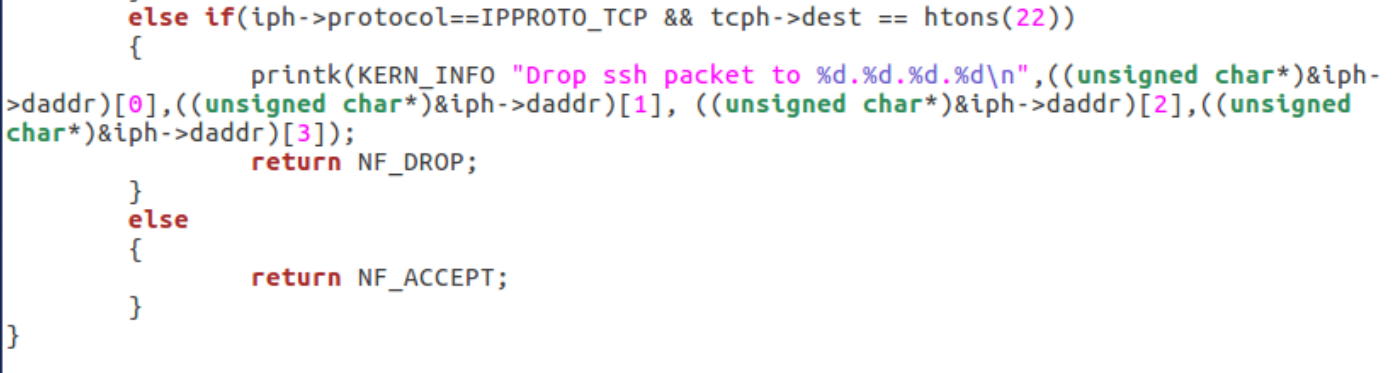
Task 2: Implementing a Simple Firewall

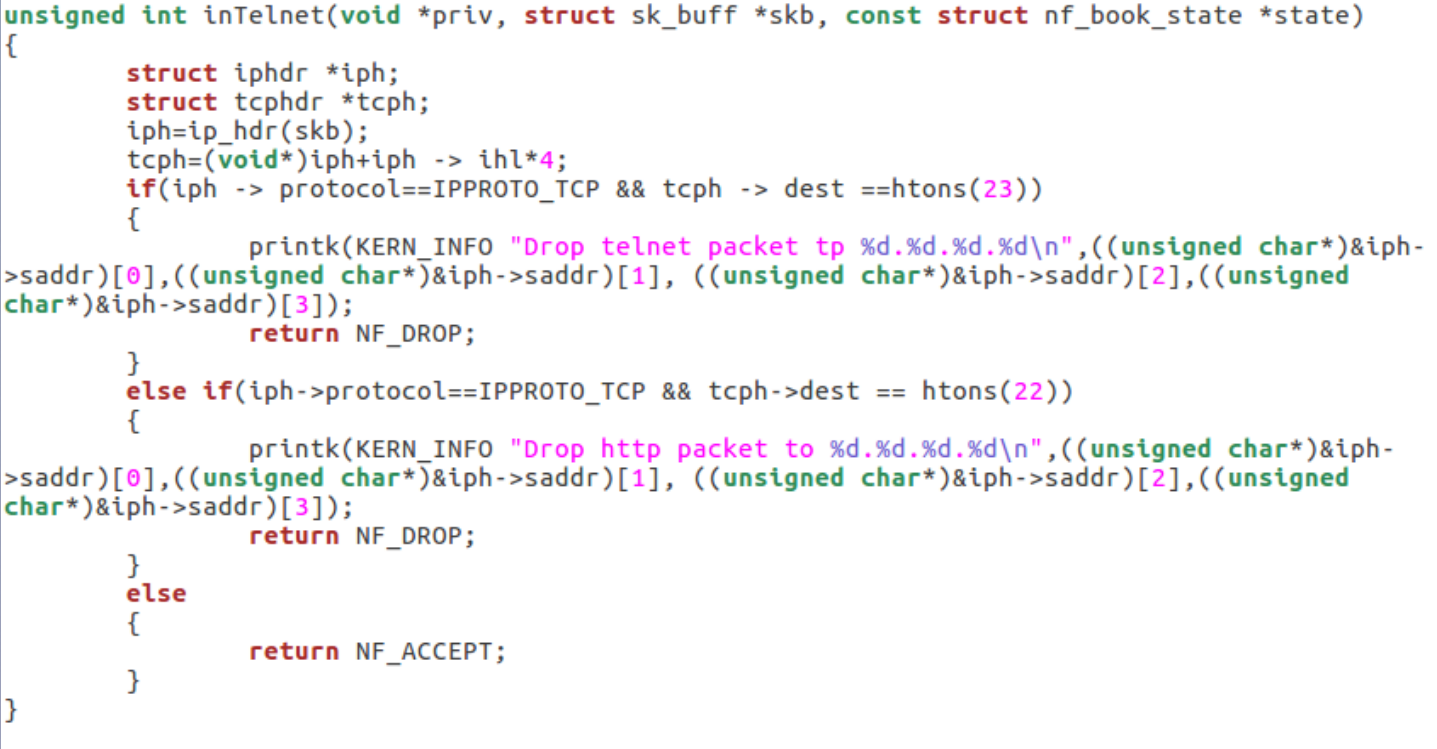
新建t2.c编写代码

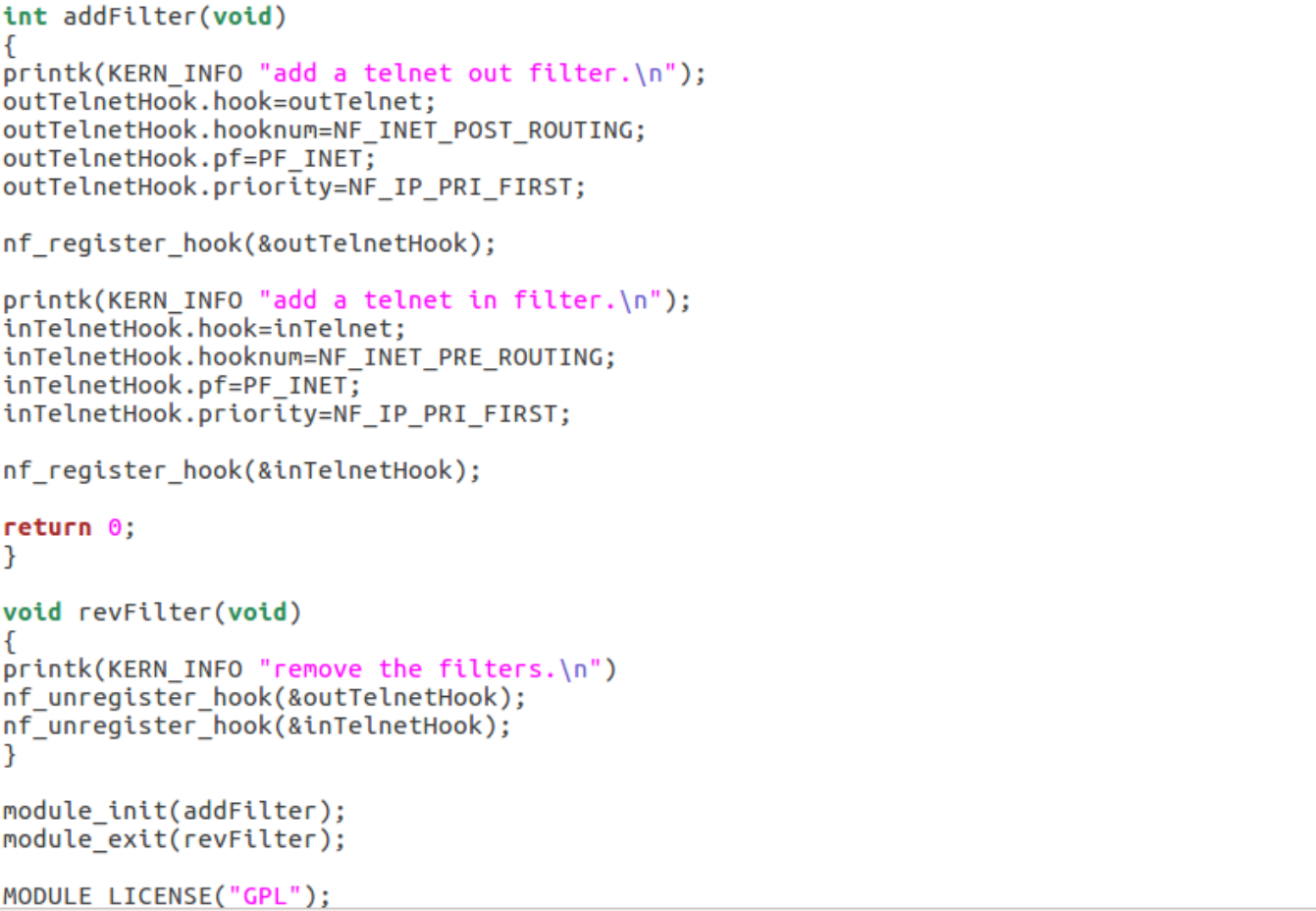


设置了向外telnet连接和其他主机向本机telnet连接的两个hook、增加和删除过滤器的操作





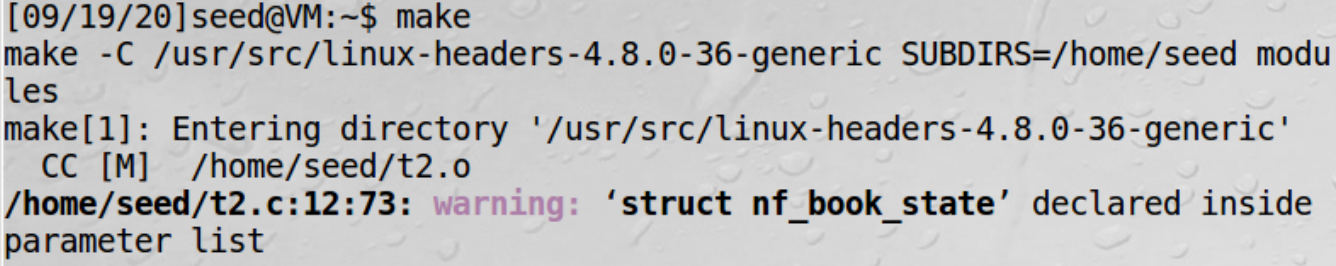




编写Makefile

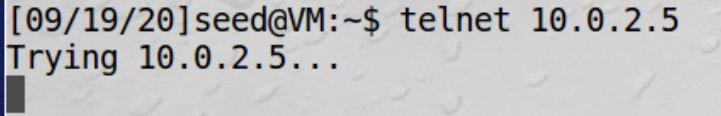


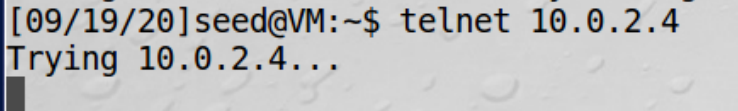
编译成可加载的内核模块





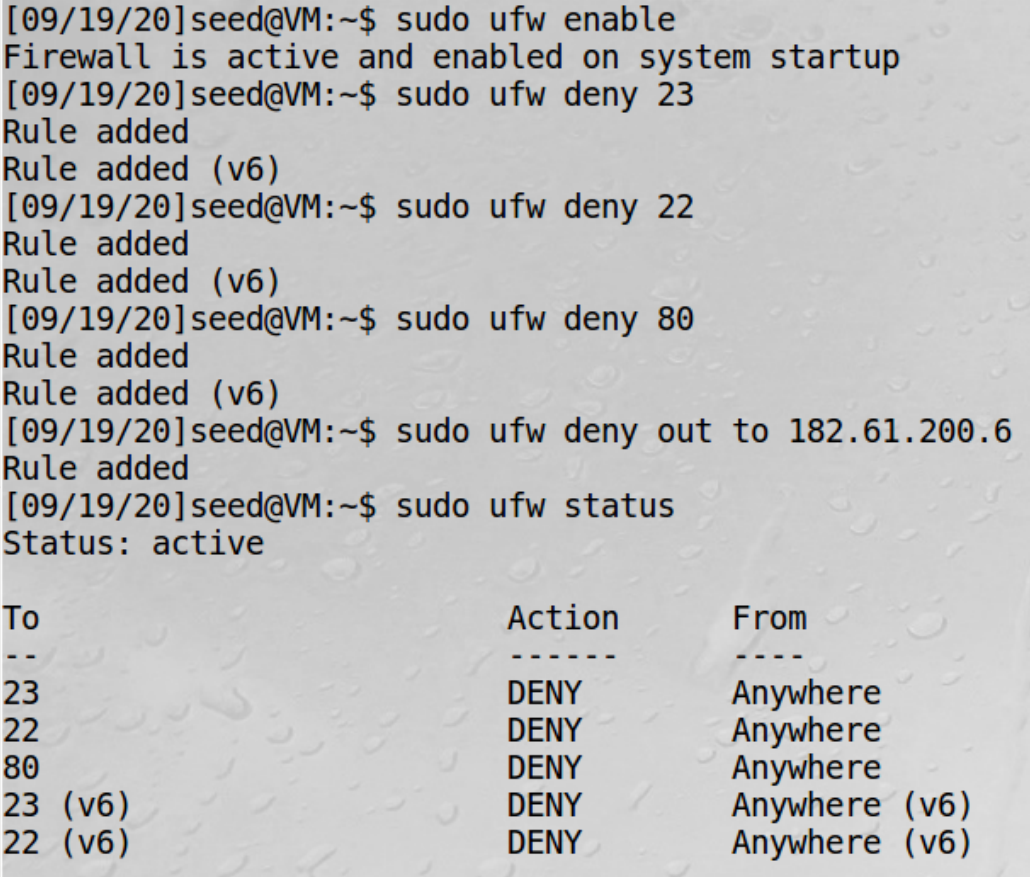
此时VA无法telnet VB，也无法被VB telnet连接到

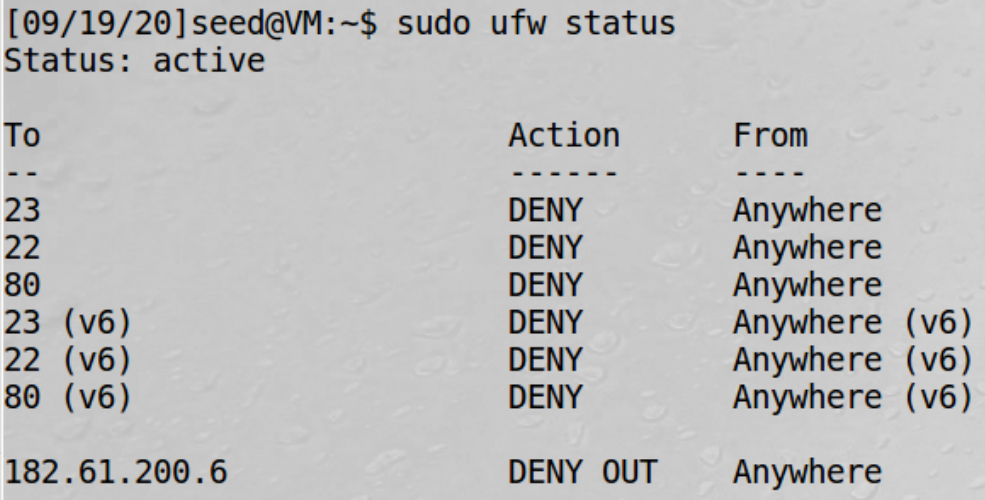




Task 3: Evading Egress Filtering

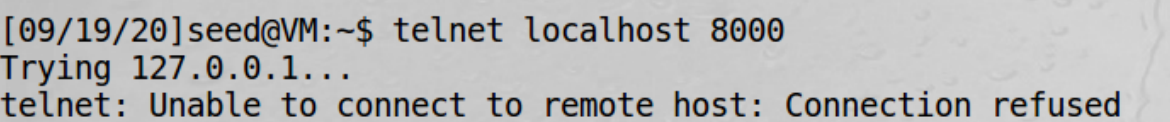
在VA上用ufw命令添加限制



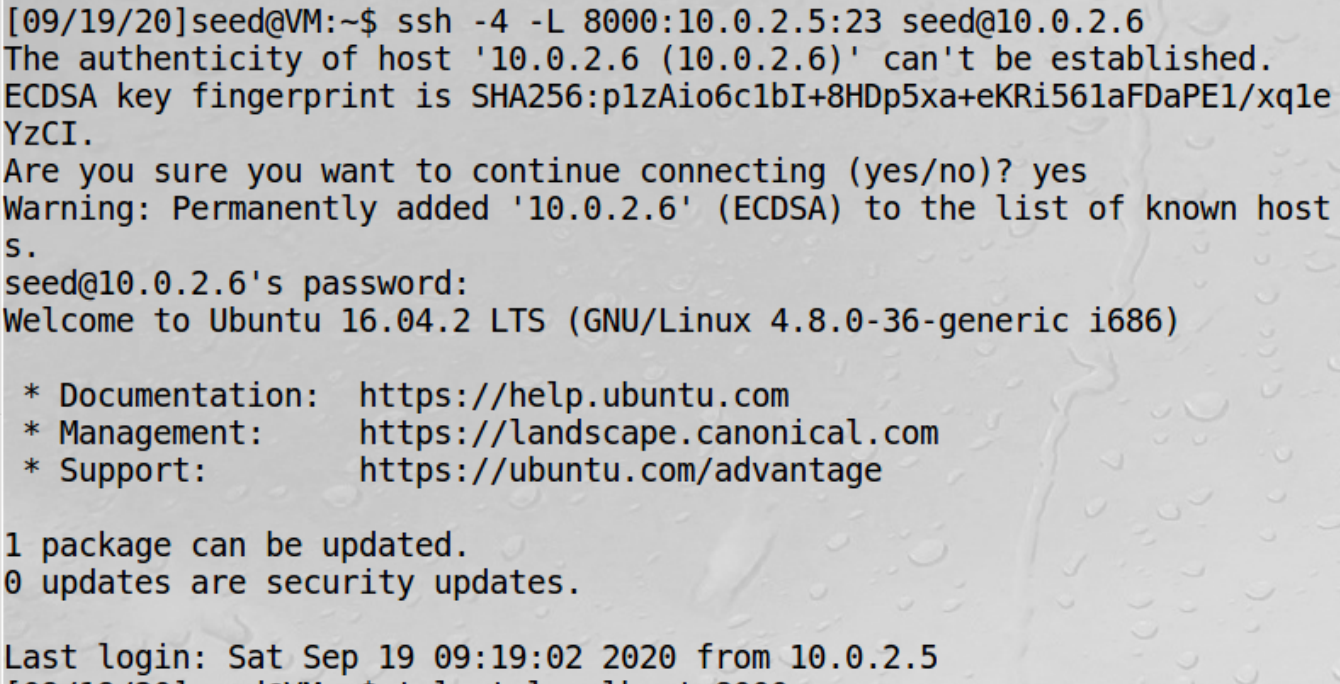


Task 3.a: Telnet to Machine B through the firewall

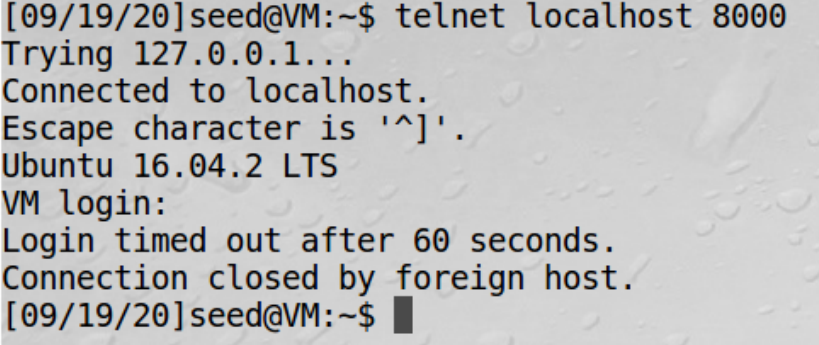
没有建立ssh通道前，无法在VA上telnet连接



VA向VB发送建立ssh通道的请求

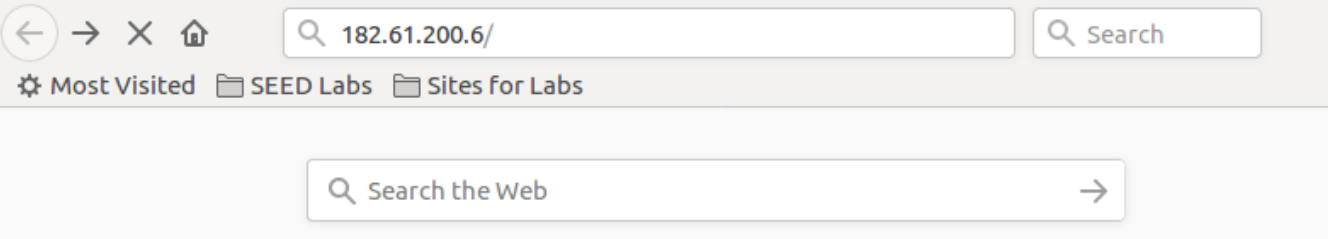


此时可以访问到localhost的8000端口

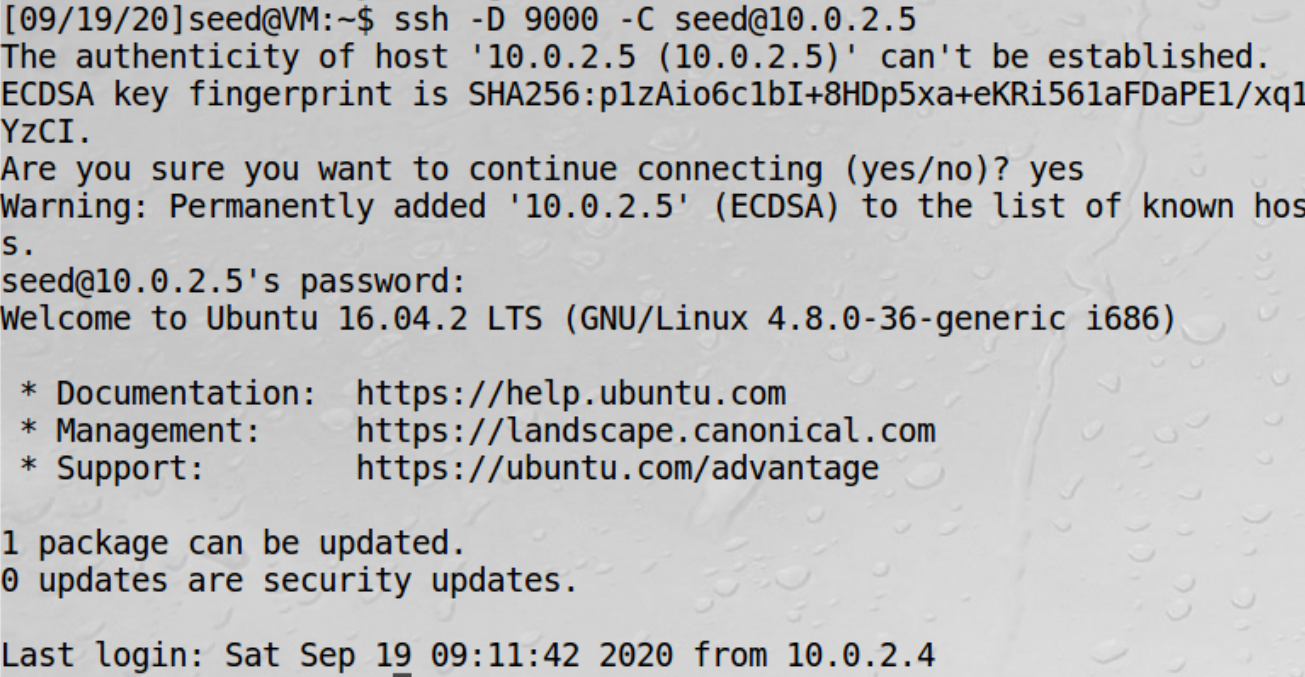


Task 3.b: Connect to Facebook using SSH Tunnel.

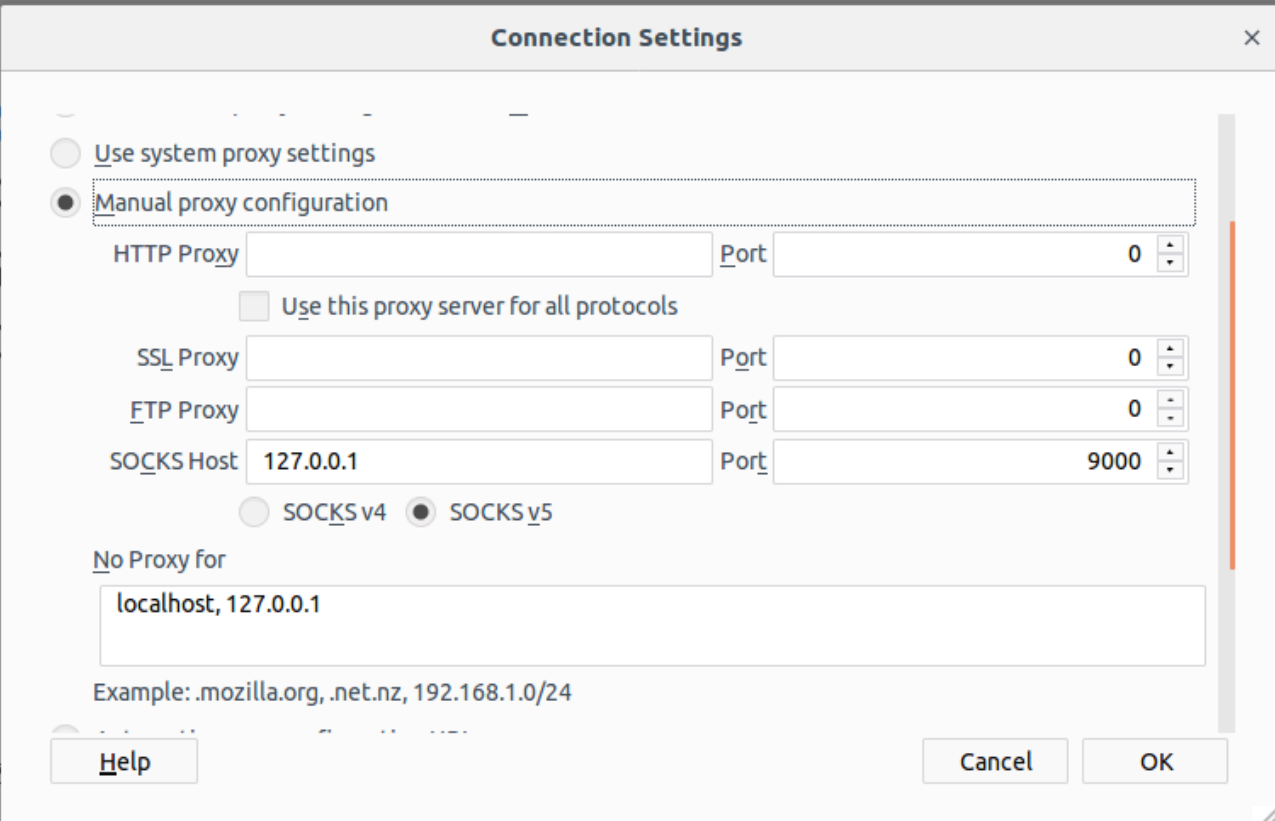
无法访问182.61.200.6



建立ssh通道，映射VA的9000端口到VB



浏览器中设置代理到本地端口9000

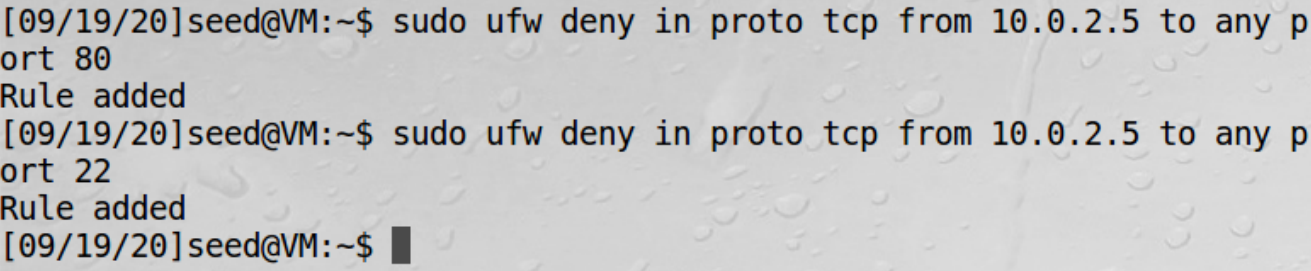


更改后可以访问182.61.200.6



Task 4: Evading Ingress Filtering

禁止VB访问VA的80，22端口



设置ssh隧道，将VB的10000端口转发到本机22端口



在VB上建立反向隧道

