Machine A ：10.0.2.8

Machine B ：10.0.2.9

Machine C ：10.0.2.10

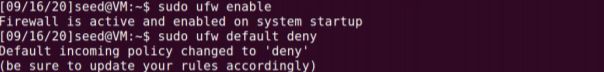
**Task 1: Using Firewall**

首先修改默认策略文件：



阻止 A 对 B 做 telnet 连接

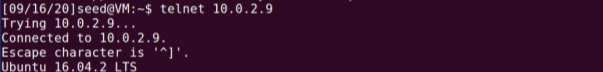
开启主机 B 的防火墙：



关闭主机 B 的防火墙：

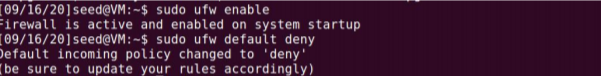


主机 A 可以通过 telnet 连接到主机 B



阻止 B 对 A 做 telnet 连接

开启主机 A 的防火墙：



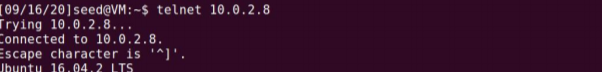
主机 B 无法通过 telnet 连接到主机 A：



关闭主机 A 的防火墙：

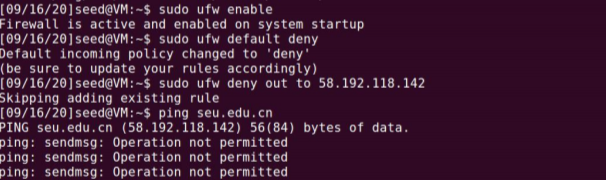


主机 B 可以通过 telnet 连接到主机 A：



阻止 A 访问外部网站

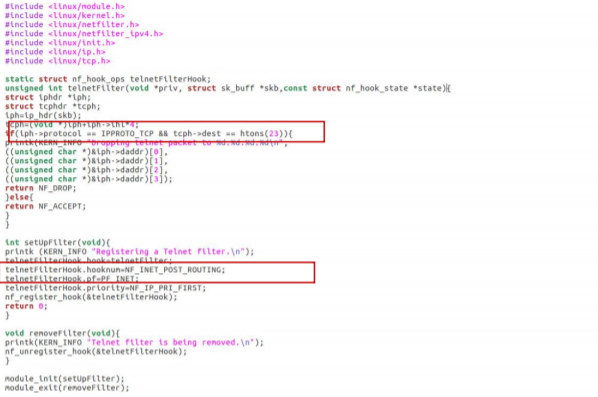
禁用主机 A 特定 IP 地址 58.192.118.142 ：



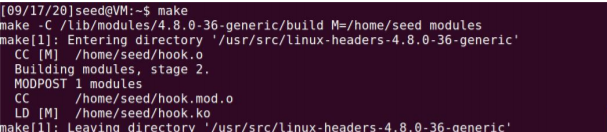
A 访问连接外网失败。

**Task 2: Implementing a Simple Firewall**

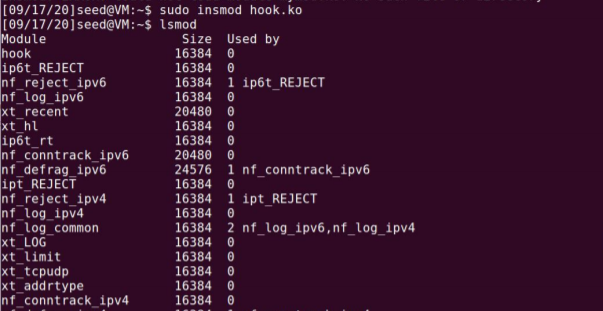
编写代码模块，拒绝目标 TCP 端口是 23 (telnet)的数据包，同时设置外出检测点 HOOK： NF\_INET\_POST\_ROUTING ：



加载编写好的模块：



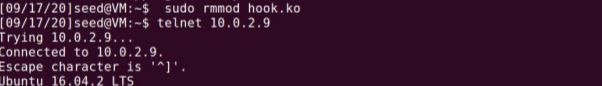
安装内核模块：



telnet 访问连接失败：



移除内核模块，telnet 访问连接成功：

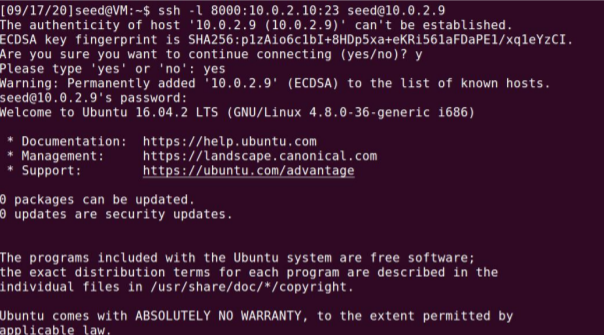


通过 LKM 向内核添加一个新的模块， Netfilter 设置外出检测点 HOOK，不需要重新编译整 个内核即可实现防火墙功能。

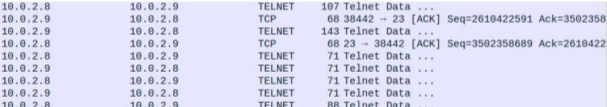
**Task 3: Evading Egress Filtering**

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

上一个实验 Task2 已建立防火墙阻止所有向外部 telnet 服务器发送流量，为了绕过防火墙与 B 建立 telnet 连接，需要在主机 A 和主机 B 之间建立 SSH 隧道：



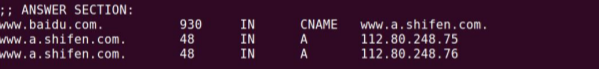
wireshark 检测到主机 A 和主机 B 之间的 telnet 数据包：



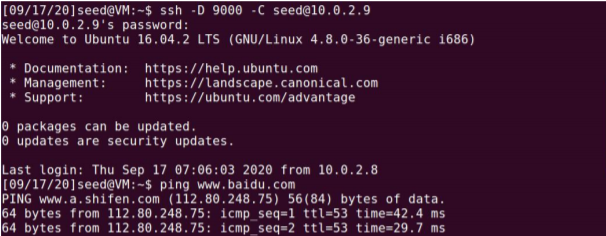
由此，通过建立 SSH 隧道，可以绕过防火墙实现 telnet 连接。

Task 3.b: Connect to Facebook using SSH Tunnel

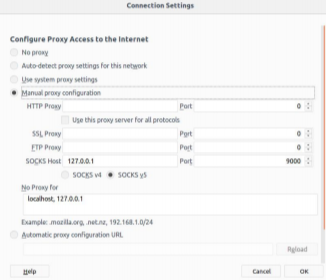
首先通过 ufw 工具禁止主机 A 访问 [www.baidu.com](http://www.baidu.com)：



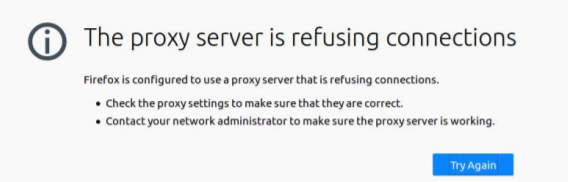
建立主机 A 和主机 B 之间的 SSH 隧道，在主机 A 上即可访问 [www.baidu.com](http://www.baidu.com)：



对浏览器进行连接设置：



在浏览器可以访问 [www.baidu.com](http://www.baidu.com)，断开 SSH 隧道，清除浏览器缓存，则该网站无法访问



重新建立 SSH 隧道，可以重新访问

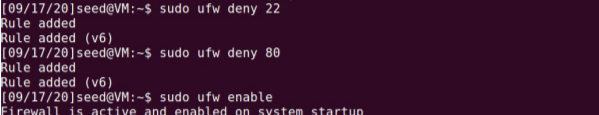
使用 wireshark 检测主机 A 和主机 B 之间的 TCP 数据包：



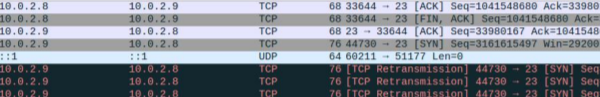
主机 B 相当于一个中介，事实上是主机 B 去访问 www.baidu.com，然后 www.baidu.com 返 回一些 TCP 数据包给主机 B，主机 B 再返回一些 SSH 数据给主机 A，最后实现了主机 A 虽 然被禁止访问却通过 SSH 隧道访问到了 [www.baidu.com](http://www.baidu.com)。

**Task 4: Evading Ingress Filtering**

首先关闭主机 A 的 22 和 80 端口，拒绝主机 B 的 SSH 和 WEB 访问：



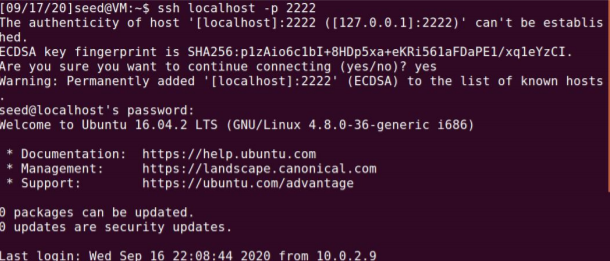
此时，wireshark 检测到主机 A 和主机 B 之间的 tcp 数据包无法正常通信



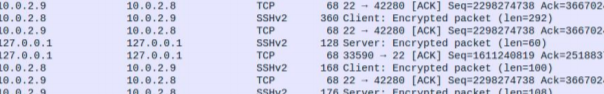
为了能使主机 B 访问主机 A，需要使用反向 SSH 隧道技术，主机 A 通过 SSH 的 2222 端口 连接主机 B:



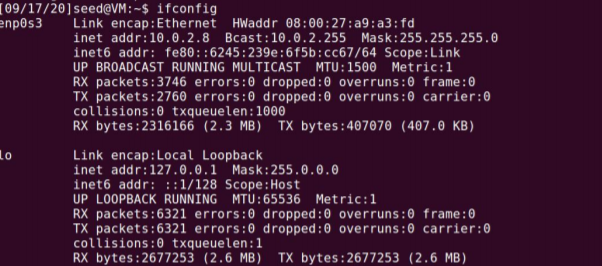
在主机 B 上使用如下命令进行确认，输入主机 A 的密码则访问成功：



使用 wireshark 检测主机 A 和主机 B 之间的访问流量：



在主机 B 上查询 IP 地址，得到的 IP 地址为主机 A 的地址 10.0.2.8，说明远程登录成功：



利用反向 SSH 隧道技术，可以实现外网访问内网主机。