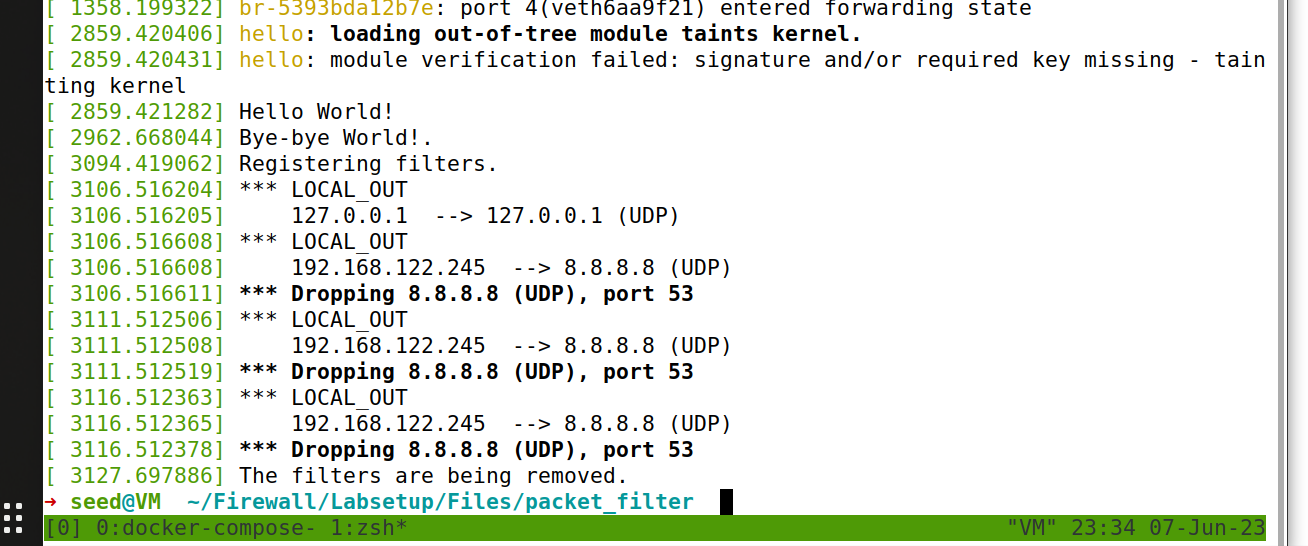
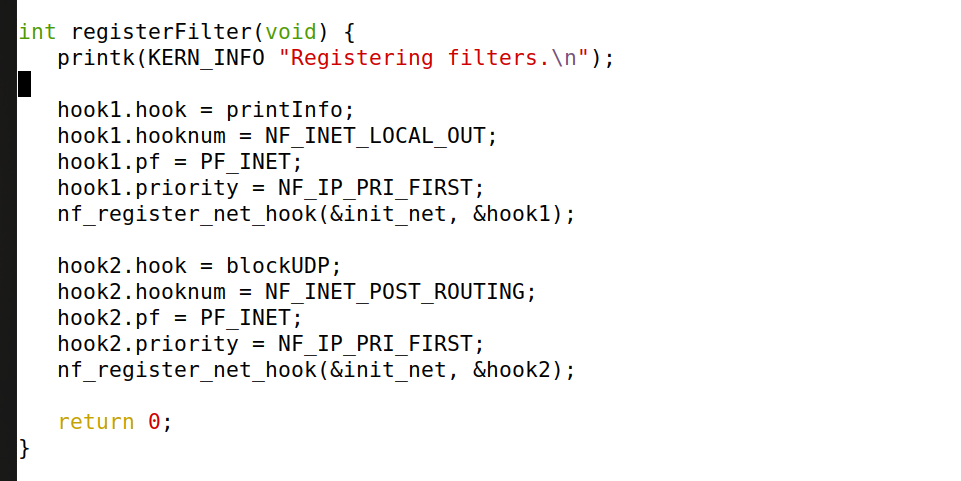
|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验六  防火墙 实验  学 院: 计算机科学与技术学院   |  |  | | --- | --- | | 姓 名: | 梁鑫嵘 | | 学 号: | 200110619 | | 专 业: | 计算机科学与技术专业 | | 日 期: | 2023年4月 | |

1. Task1: 加载seedFilter模块，执行dig dig @8.8.8.8 [www.example.com](http://www.example.com)，卸载seedFilter后再执行dmesg命令查看内核日志，把日志信息中加载、卸载seedFilter模块以及阻止UDP数据包的信息截图，并进行分析说明。



加载 seedFilter模块：Registering filters

此时seedFilter模块被加载进入内核模块。



注册模块时注册了两个网络钩子，分别监听LOCAL\_OUT和ROUTING，前者是本机发出包的钩子，后者是本机接收包的钩子。其中hook2监听ROUTING，是可以监听接收到的包，对应函数blockUDP。

组织UDP包：Dropping 8.8.8.8 (UDP), port 53

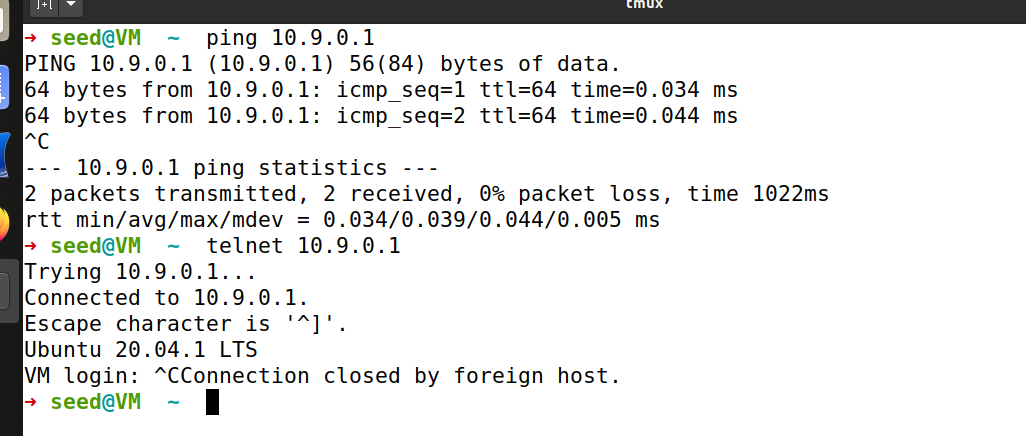
此时blockUDP检查到接收包源地址为8.8.8.8，端口为53，类型为UDP，则丢弃了这个包，组织了DNS请求。

卸载seedFilter模块：The filters are being removed

模块被卸载，之后的包不会经过之前注册的两个钩子路径。

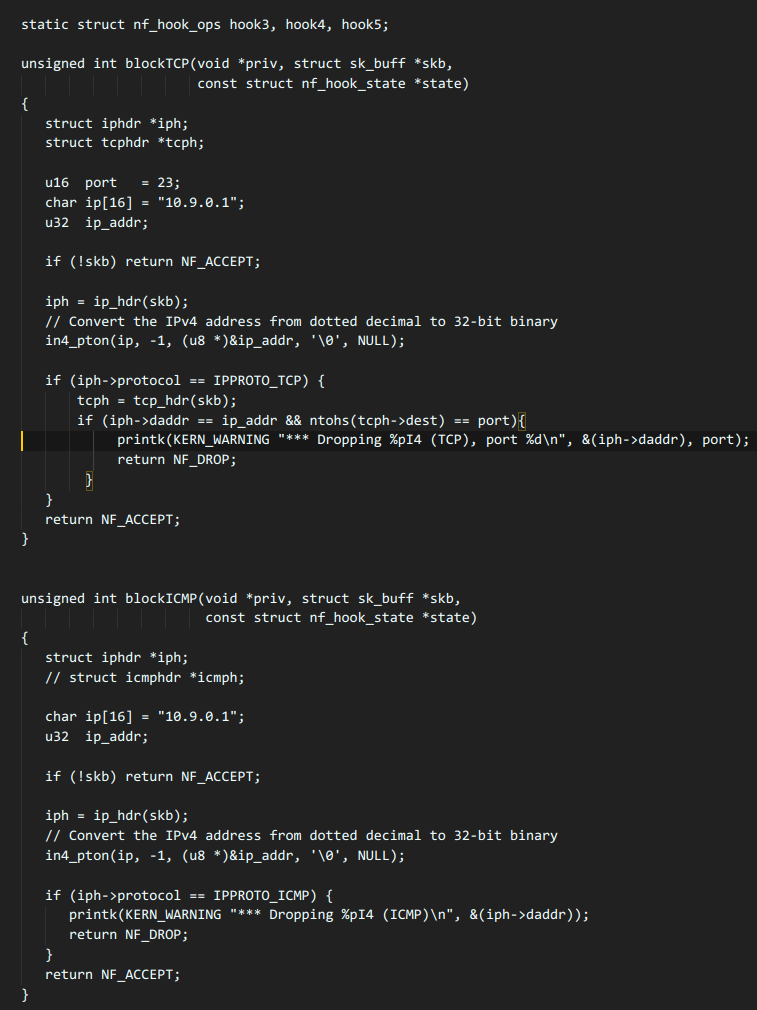
1. Task2：阻止TCP 端口和PING，把增加和修改的代码截图，并在卸载模块后将dmesg的日志信息的截图，并分析说明原因。

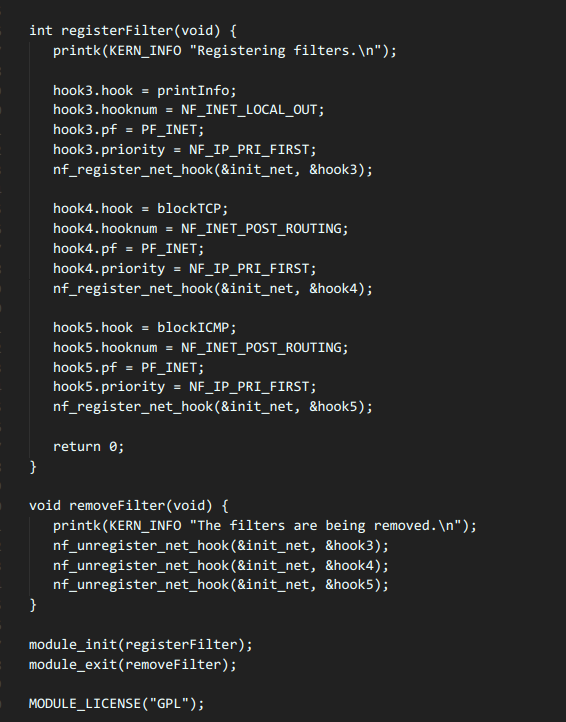
首先检查联通性：



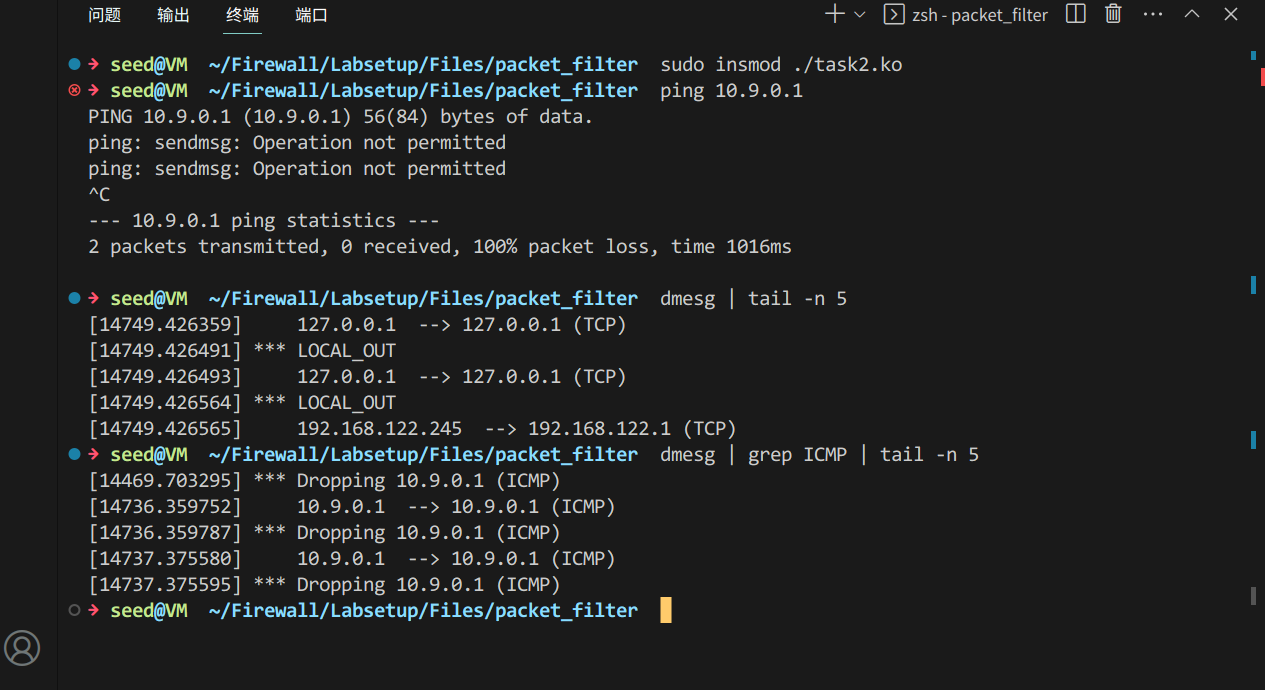
ping和telnet是可以通到服务器上。

编写代码：

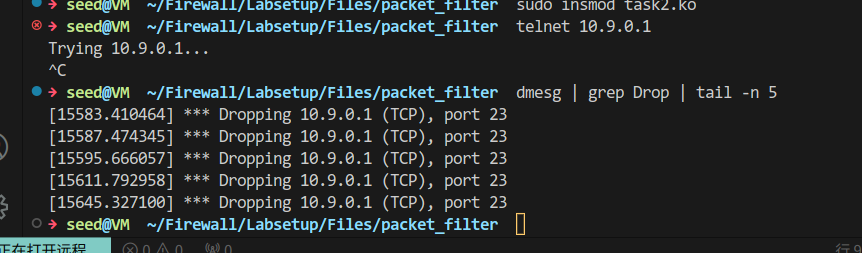




测试 ICMP：

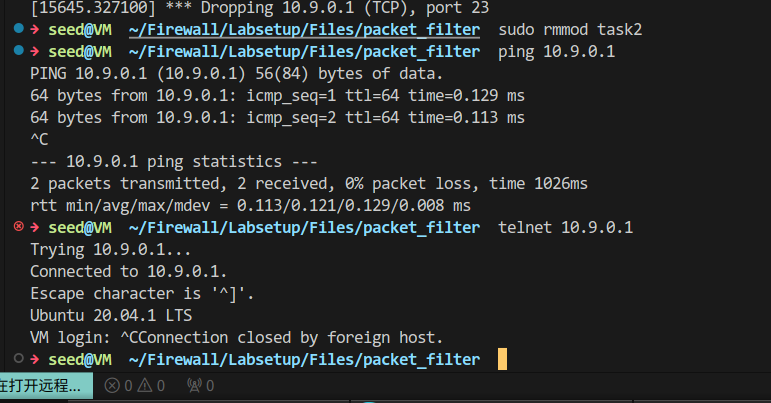


ICMP 请求被拦截。

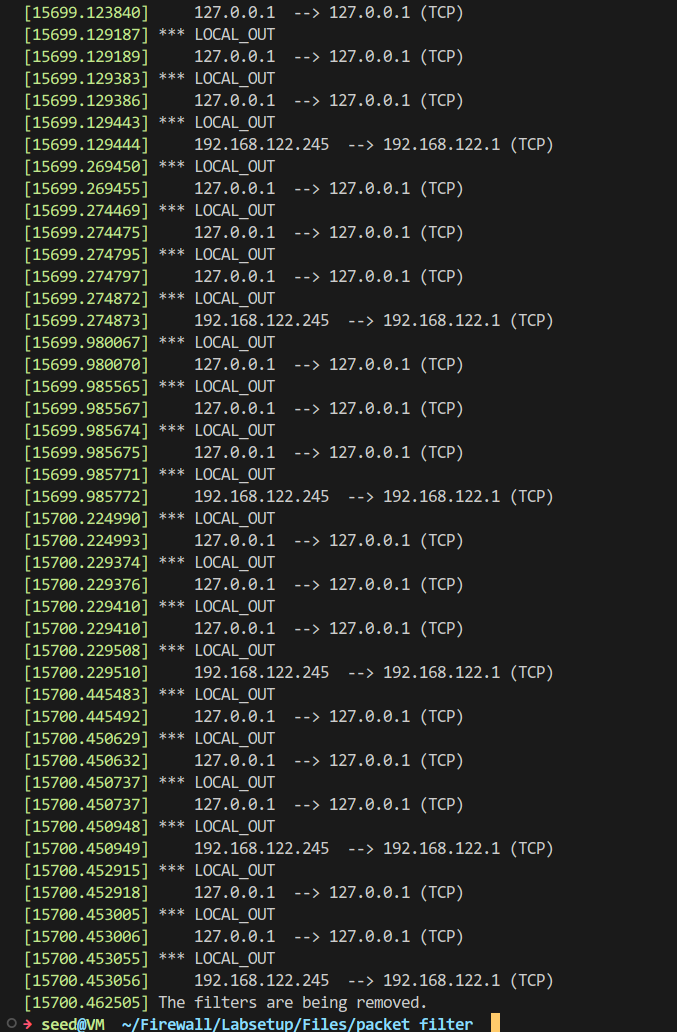
测试 TCP：  


目标 TCP 被拦截。

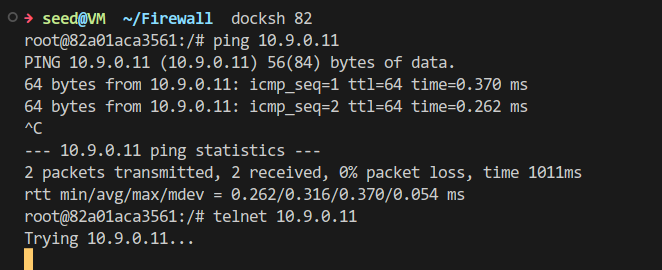
卸载模块后正常ping和telnet：



比较完整的 dmesg：



1. Task3：保护Router，将配置iptables规则前后ping和telnet的连通性测试结果截图，并分析说明原因。



在 HostA 上，ping能ping通，但是telnet不通。原因：

1. router上设置ICMP的报文是可以接收并回复的：

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

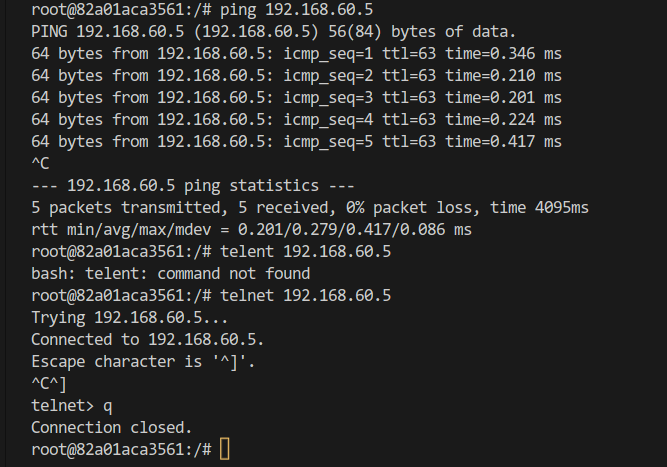
1. 对于telnet，属于TCP协议，在router中未设置，fallback到默认DROP：

iptables -P OUTPUT DROP

iptables -P INPUT DROP

4、Task4：保护内网，将配置iptables规则前后ping的连通性测试结果截图，并分析说明原因。

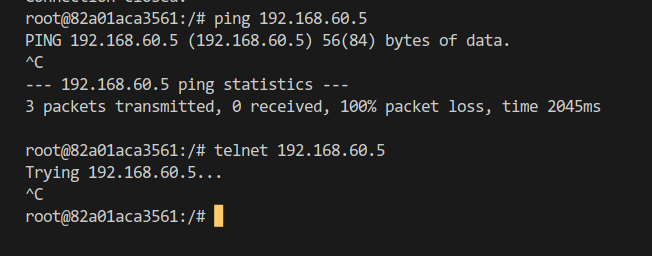
Step1：



1. HostA能够ping通192.168.60.5
2. HostA能够正常对192.168.60.5发起telnet

Step2-3：

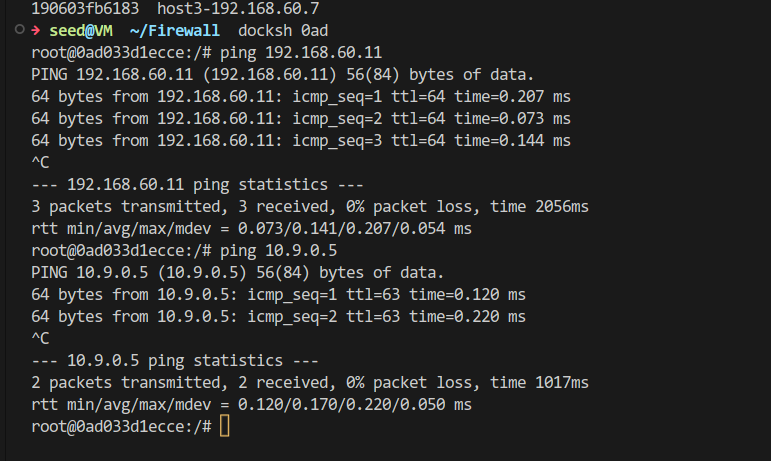
配置了内网保护相关规则后：



1. 外网HostA不能ping通192.168.60.5这个内网地址
2. 外网HostA不能telnet到192.168.60.5这个内网地址

分析原因：路由器不再对外网到内网的指定请求进行转发，但是对内网到内网的相关请求仍有转发。

Step4：



1. 内网host1能够ping通同在内网的router (192.168.60.11)
2. 内网host1能够ping通外网的服务器HostA

分析：内网到外网的请求被路由器转发到外网，且echo-reply的ICMP包也会被转发到内网，所以HostA在外网能够收到内网host1的ping请求，且其回复echo-reply也能被路由器转发到内网从而被host1接收到。

Step5：清理。