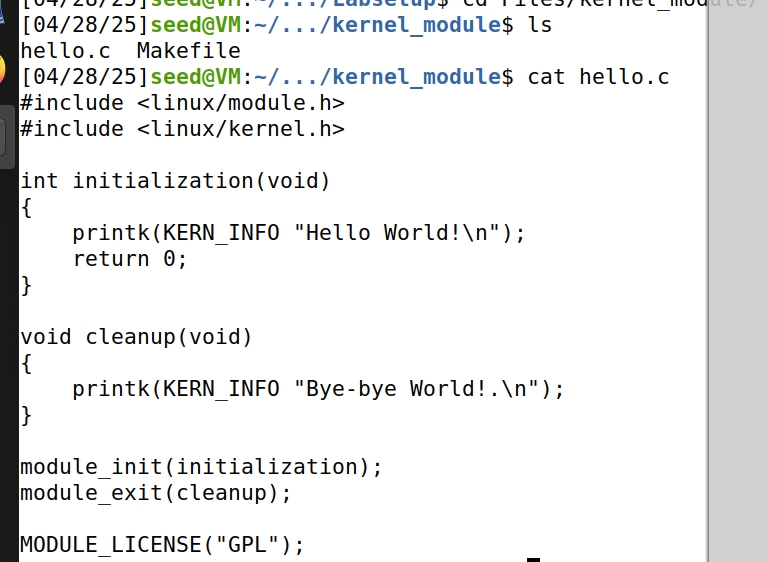
|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验六  防火墙 实验  学 院: 计算机科学与技术学院   |  |  | | --- | --- | | 姓 名: | 覃煜淮 | | 学 号: | 220110803 | | 专 业: | 计算机类 | | 日 期: | 2025年4月 | |

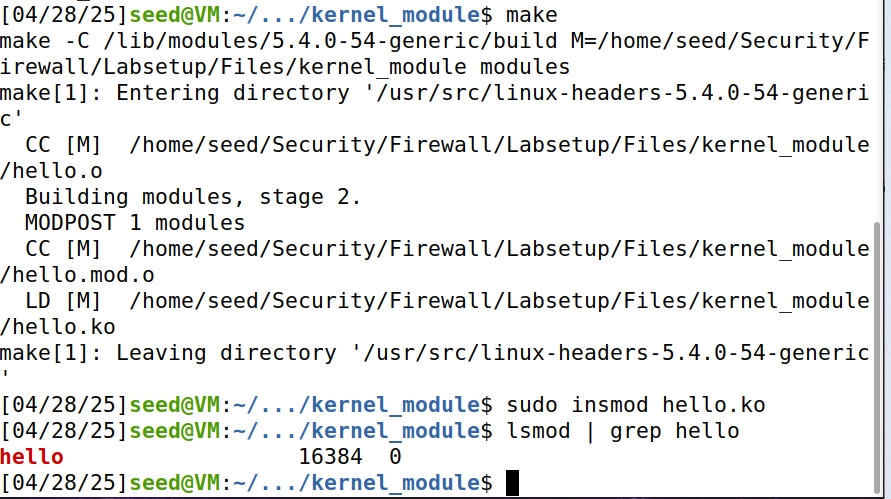
1. Task1: 加载seedFilter模块，执行dig dig @8.8.8.8 [www.example.com](http://www.example.com)，卸载seedFilter后再执行dmesg命令查看内核日志，把日志信息中加载、卸载seefFilter模块以及阻止UDP数据包的信息截图，并进行分析说明。

**（1）了解插入代码进入内核执行的基本操作**

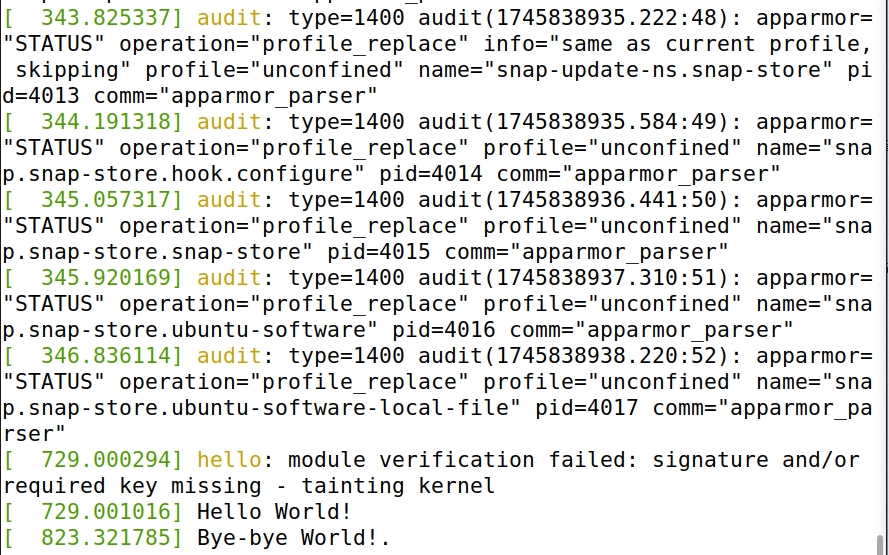
首先查看内核模块初始化加载函数module\_init以及退出执行函数module\_exit



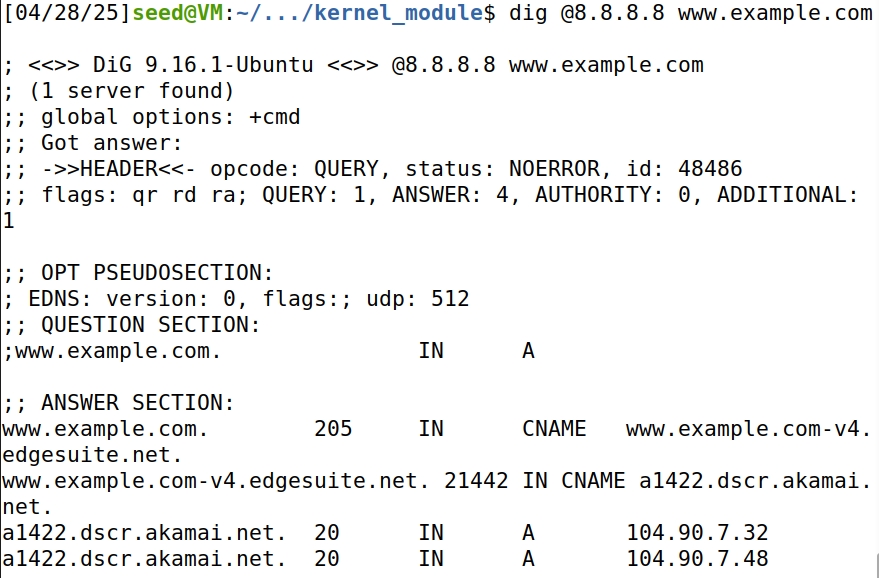
编译并插入模块，检查插入情况



Dmesg输出内核日志：

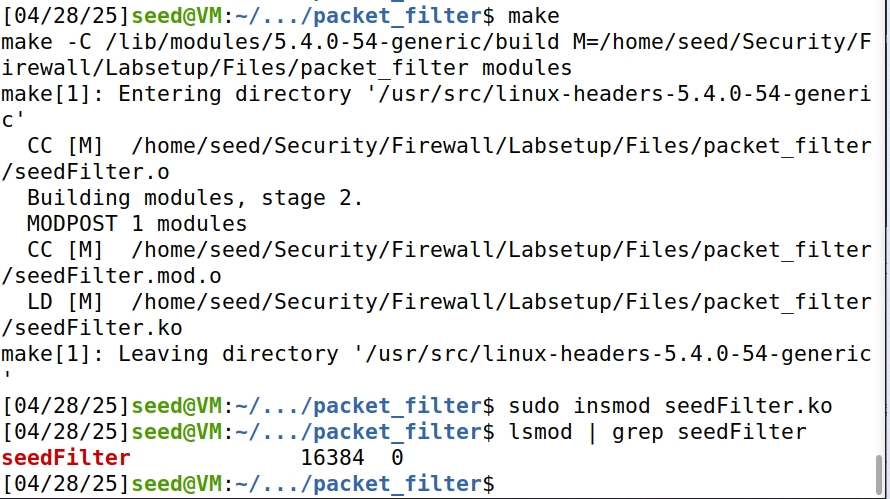


**（2）阻止UDP数据包**

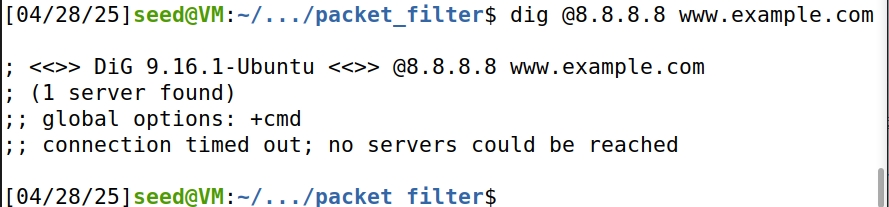


使用dig命令能够访问并且解析出目标域名的IP为answer section的104.90.7.32

编译并插入相关内核模块组织UDP包后：

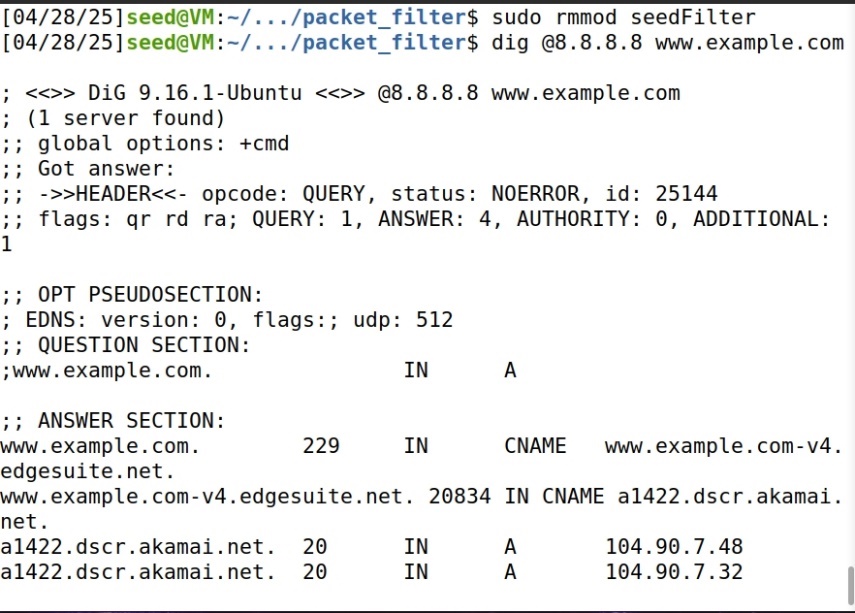


再次dig：

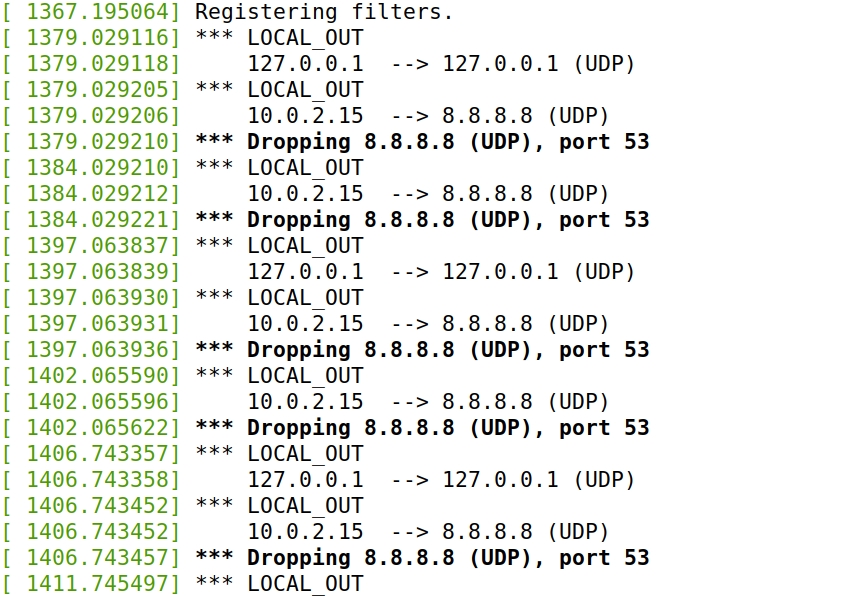


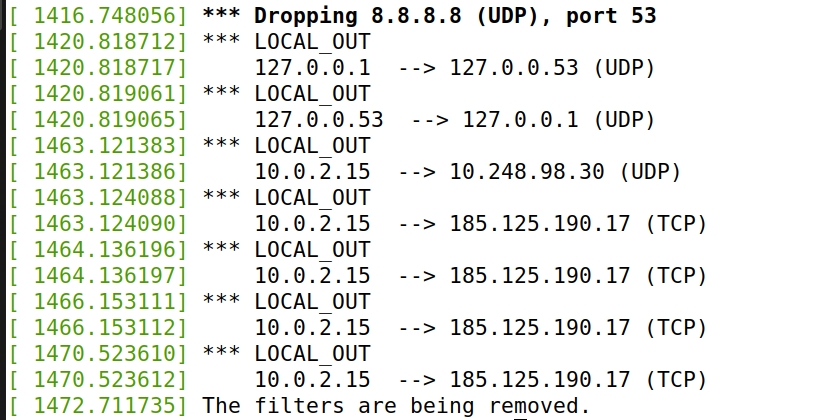
发现失败，域名服务器没响应

移除内核模块重新dig检查域名服务器状态：



观察内核日志：

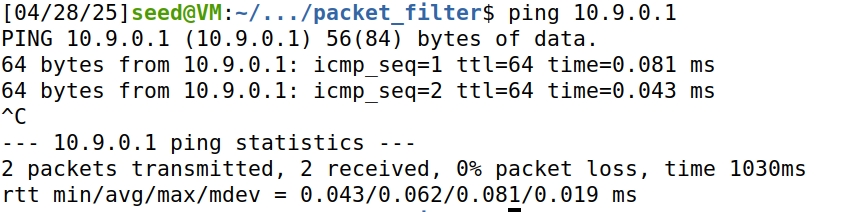


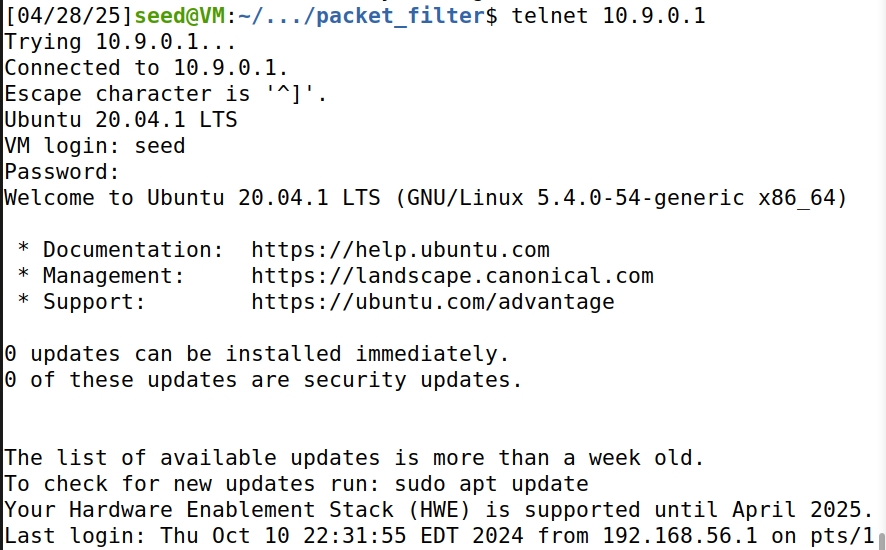


发现内核日志显示注册了过滤包，并且丢弃了来自8.8.8.8的UDP包，之后过滤包被移除

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。

初始时执行ping（ICMP）和telnet（TCP）操作：



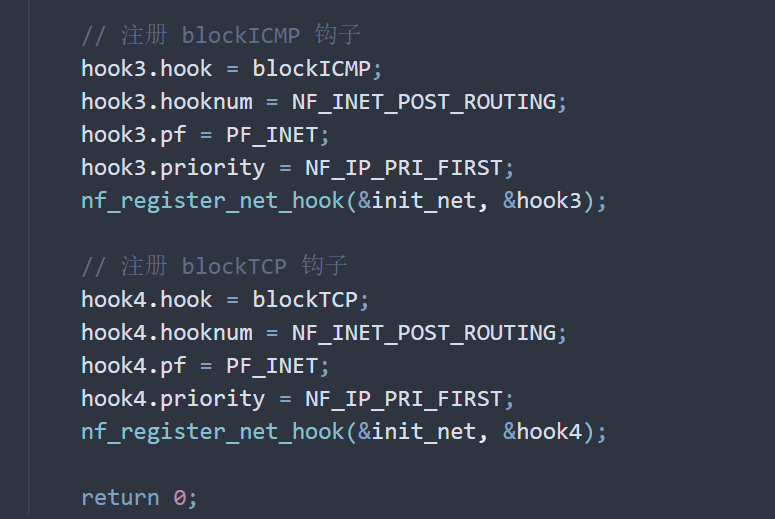


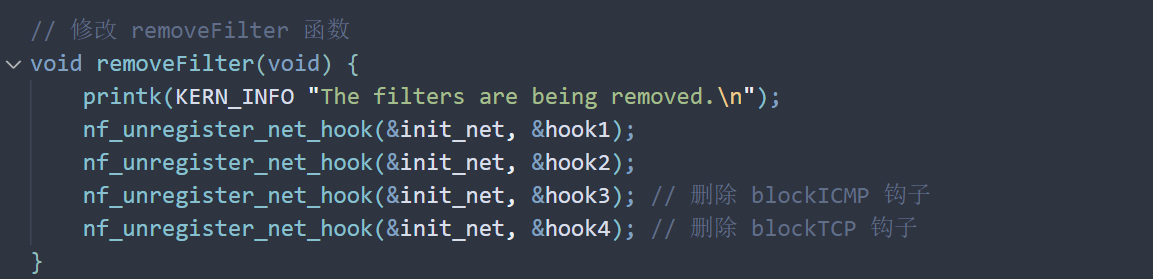
修改的关键代码：

参考blockUDP依次实现blockICMP和blockTCP，在对应的地方注册钩子与删除钩子

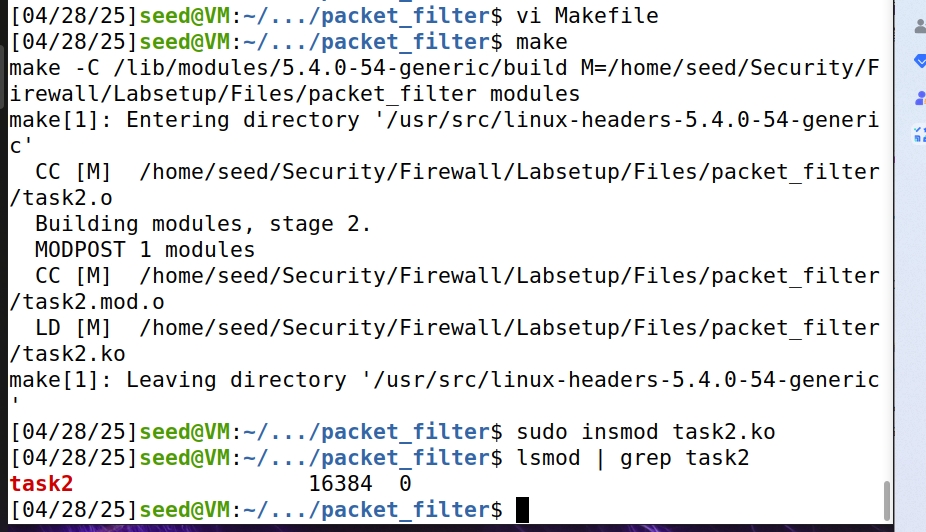




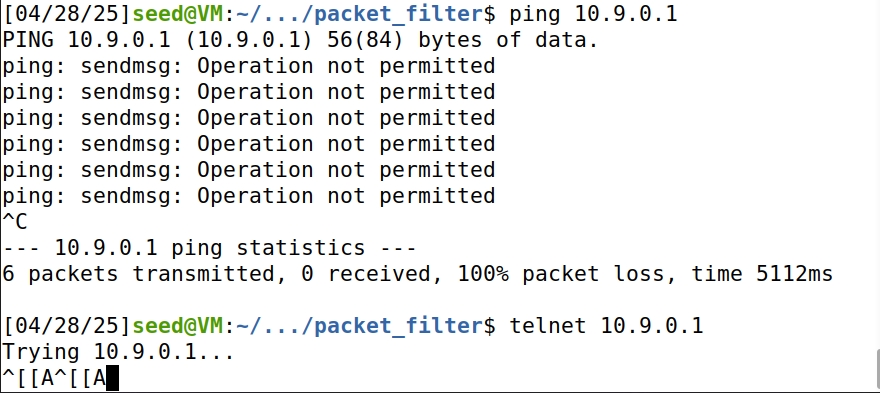




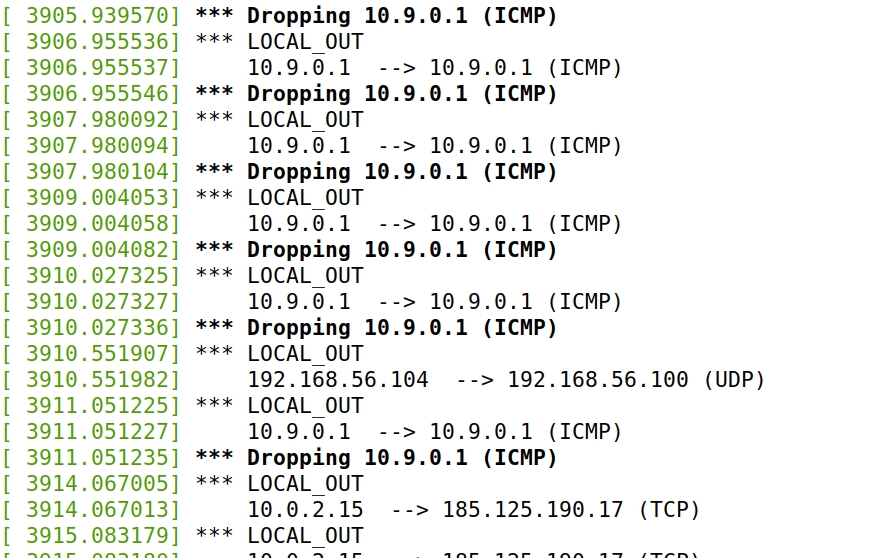
编译，插入内核模块并检查插入情况：

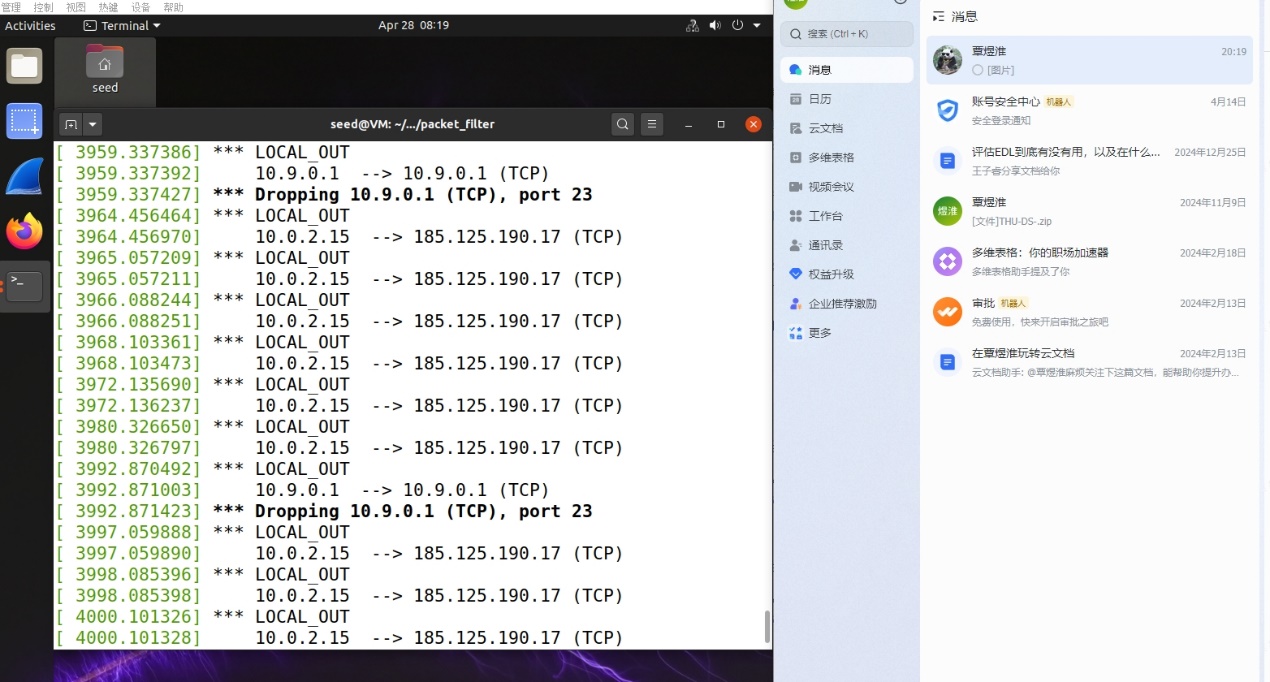


检验TCP（telnet）和ICMP（ping）结果：



使用dmesg获取内核日志：

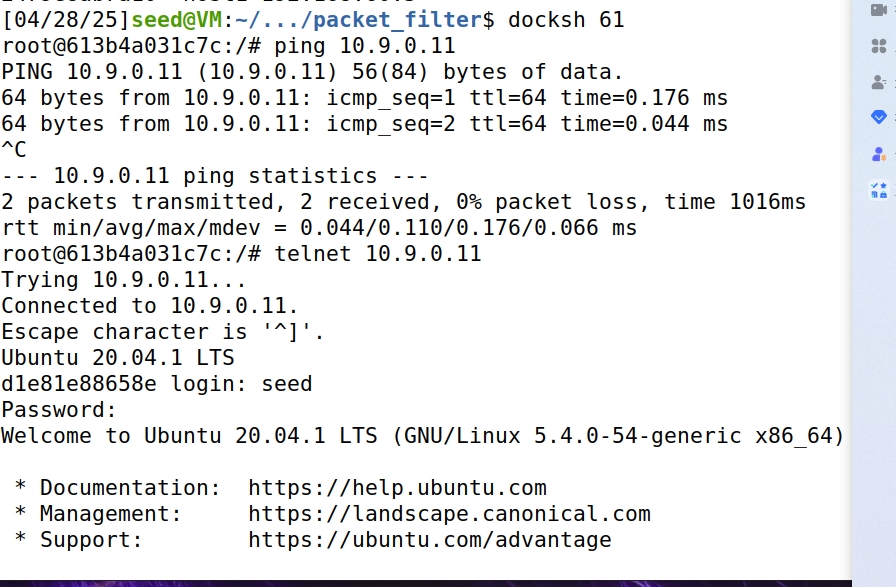




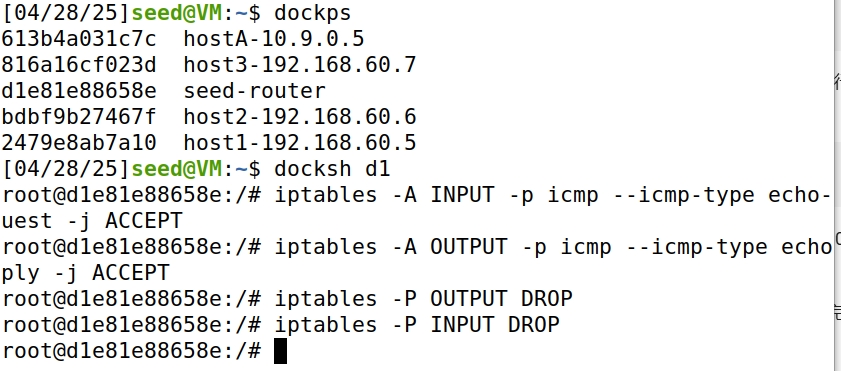
观察到TCP和ICMP都被拦截

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。

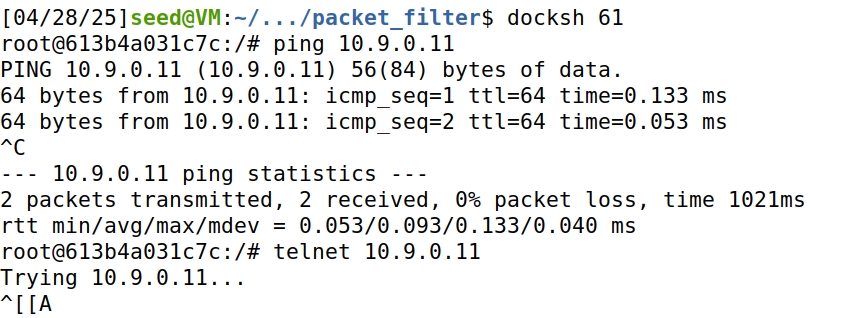
启动hostA并且尝试ping和telnet命令，结果如下：



进入router容器执行以下规则：



在hostA中再次执行指令

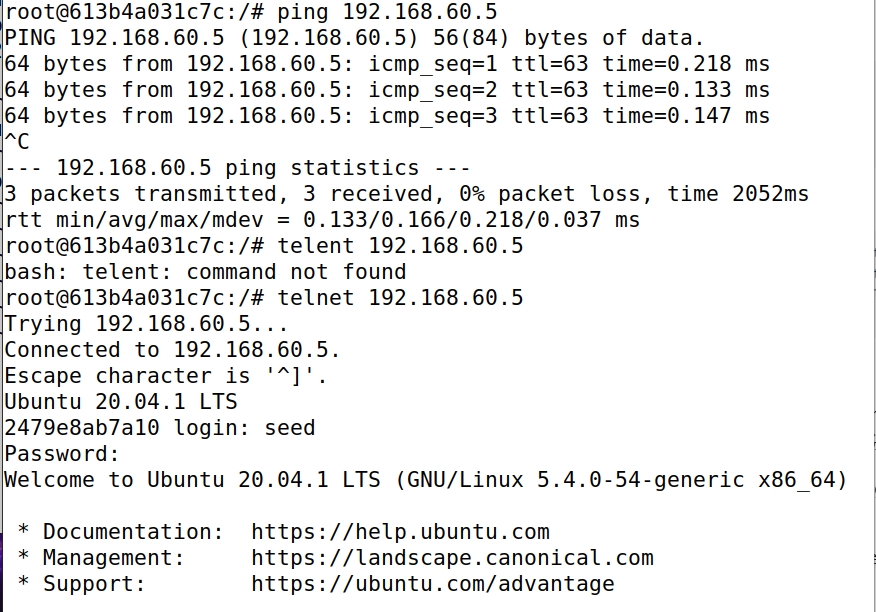


观察到hostA中能够ping通但是无法telnet连接

**分析原因：**10.9.0.11即路由器IP，因为在iptable中设置了允许ICMP报文进和出，并且位置在拒绝所有报文前面，优先级更高，所以能够处理ICMP的请求和应答报文。而设置了默认所有类型协议报文都丢弃，所以基于TCP的telnet报文会被丢弃，无法成功连接

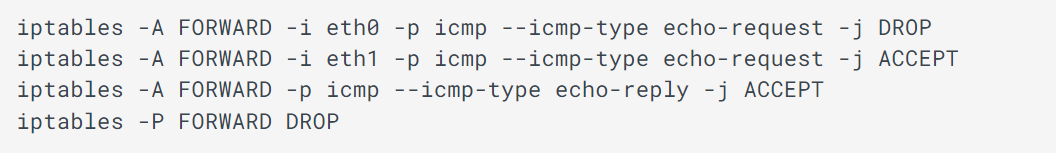
4、Task4：保护内网，将配置iptables规则前后ping的连通性测试结果截图，并分析说明原因。

先在hostA上执行下述命令：



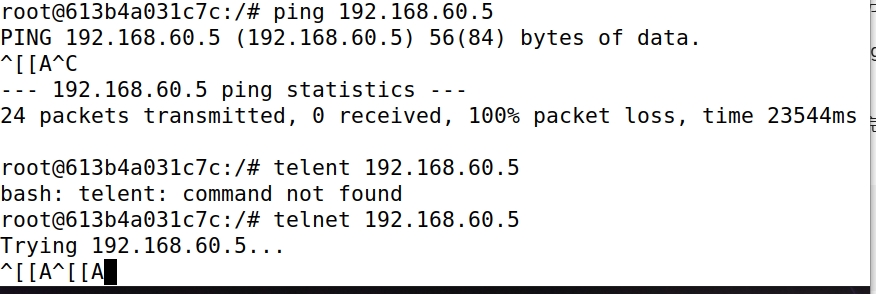
发现HostA都能ping通

之后在router机上执行以下规则：



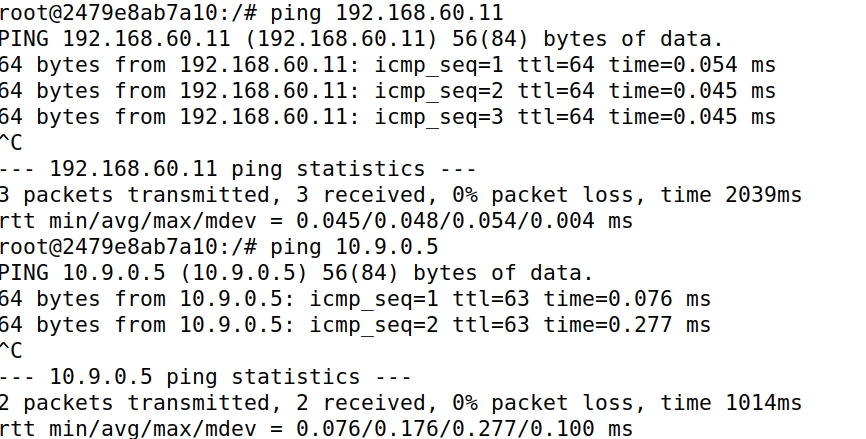
配置路由转发的规则，将命令从上至下定为1234，后面解释不再具体使用命令而是用命令1代指

外网ping内网结果



**分析原因：**外网访问内网要经过router，因为router的iptable配置了丢弃所有外网来的icmp包，因此外网的ping命令无法穿过router,因此ping不通内网

内网host1尝试Ping内网机器与外网结果：



可以观察到全部ping通

**分析原因：**因为router的iptable设置了内网的icmp报文请求都会接受并且路由转发(命令2)，并且router对于icmp的回复报文都会默认转发，因此可以观察到都ping通了

# 二、遇到问题及解决方法

1.代码最初没有注意到IP地址要更改耽误了一点时间

2.对虚拟机进行过类似的联网配置，通过本实验对iptables掌握进一步加深

# 三、对本次实验的建议

建议指导书维护一下命令,是telnet不是tenlet