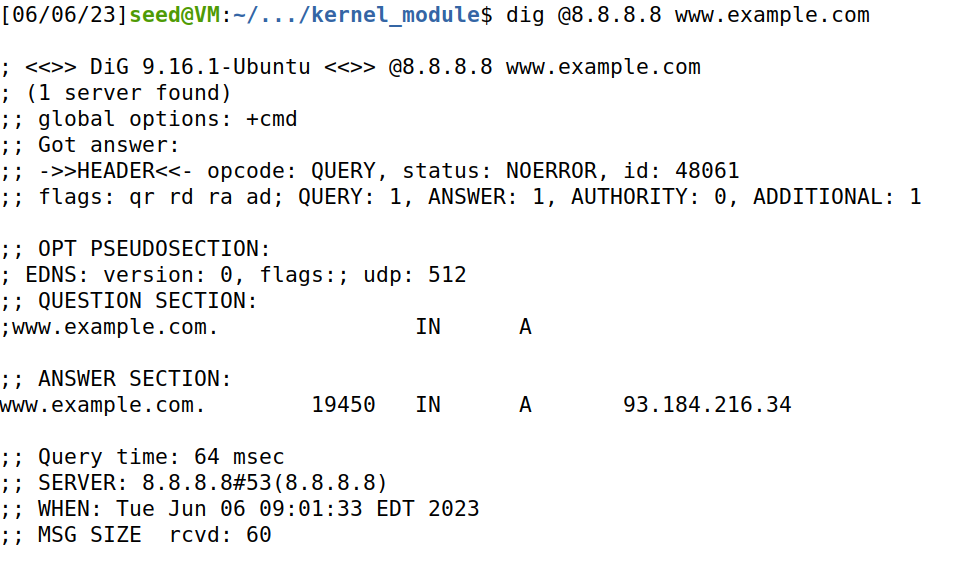
|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验六  防火墙 实验  学 院: 计算机科学与技术   |  |  | | --- | --- | | 姓 名: | 宗晴 | | 学 号: | 200110513 | | 专 业: | 计算机 | | 日 期: | 2023年6月 | |

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。

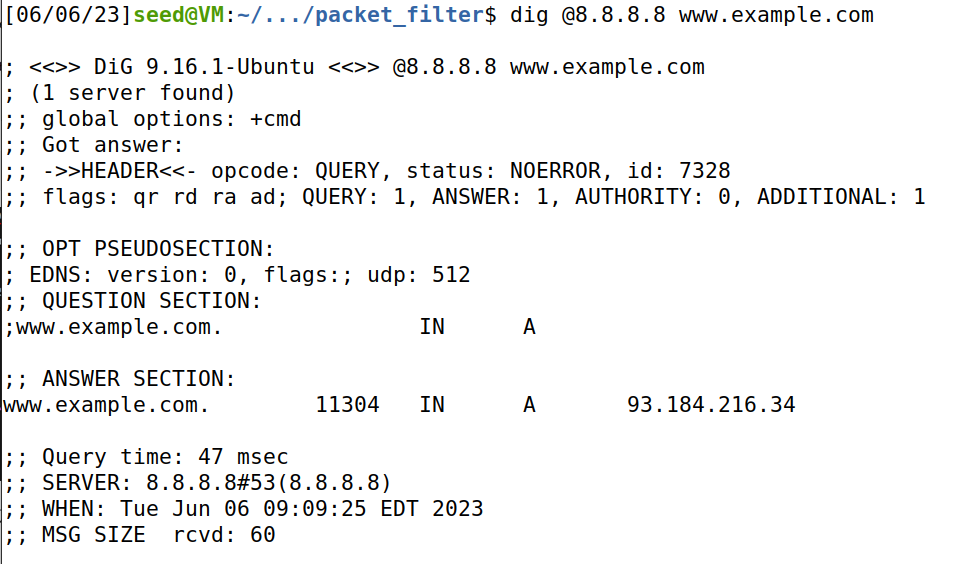
先执行 dig 命令查看，发现有回复，如下图所示：



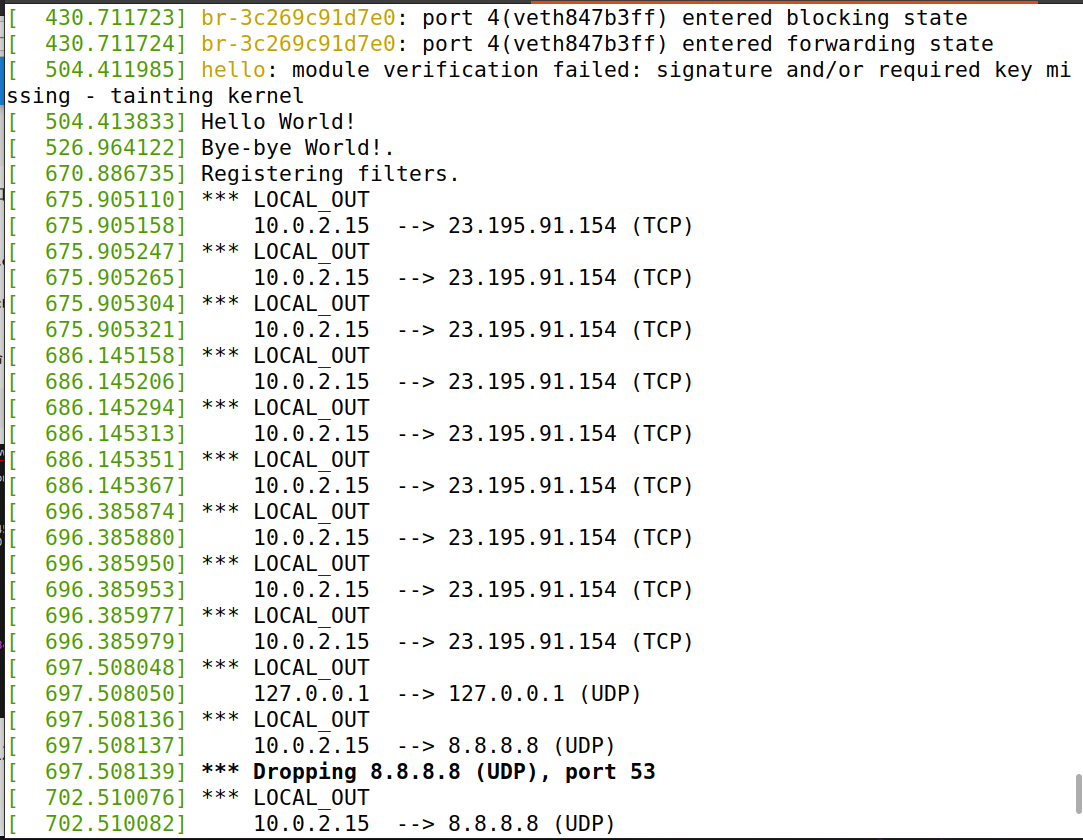
使用 Labsetup/Files/packet\_filter 下的代码，阻止IP地址是 8.8.8.8 和端口为 53 的 UDP 数据包。加载成功后再执行 dig @8.8.8.8 [www.example.com](http://www.example.com/) 命令，查看结果如下图所示，已经得不到任何响应了，说明防火墙设置成功：

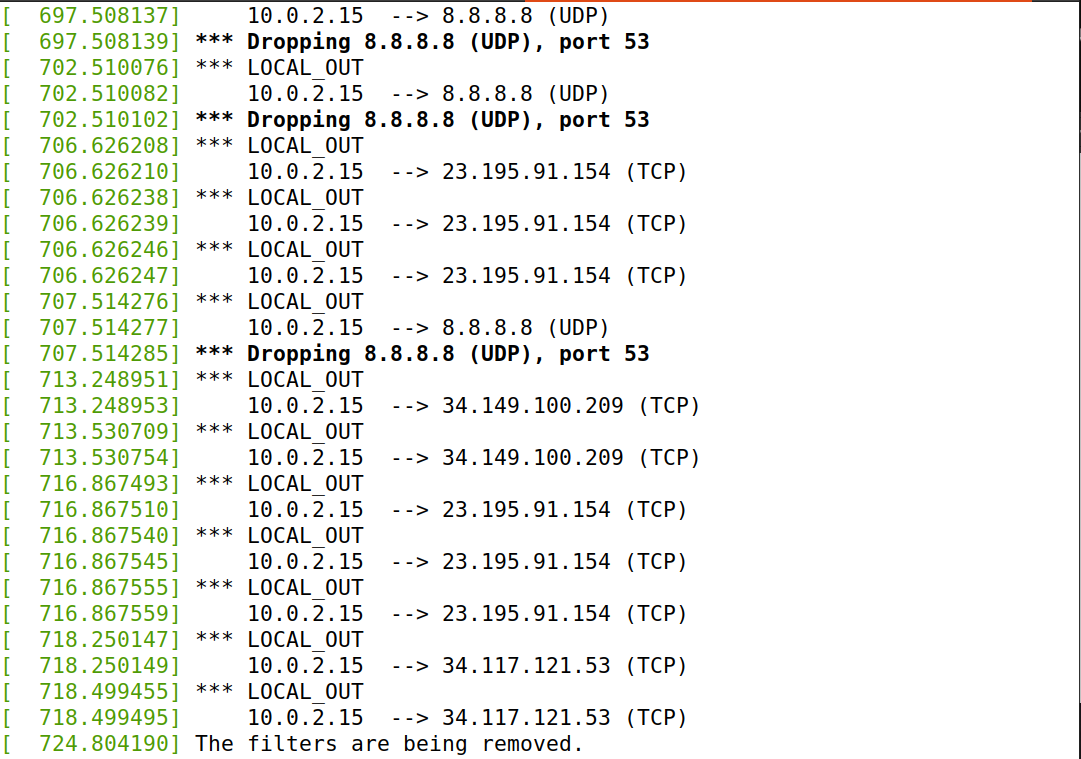


卸载 seedFilter 模块成功后再执行 dig @8.8.8.8 [www.example.com](http://www.example.com/) 命令，又可以收到回复了：



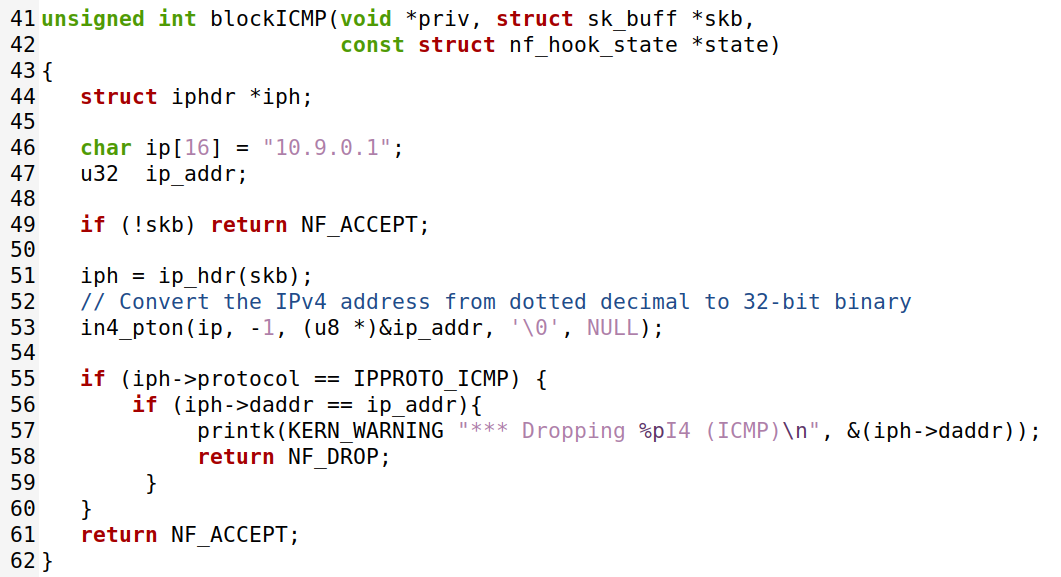
使用 dmesg 命令查看内核日志信息，可以看到注册和卸载的信息，以及防火墙阻止后丢掉的数据包：



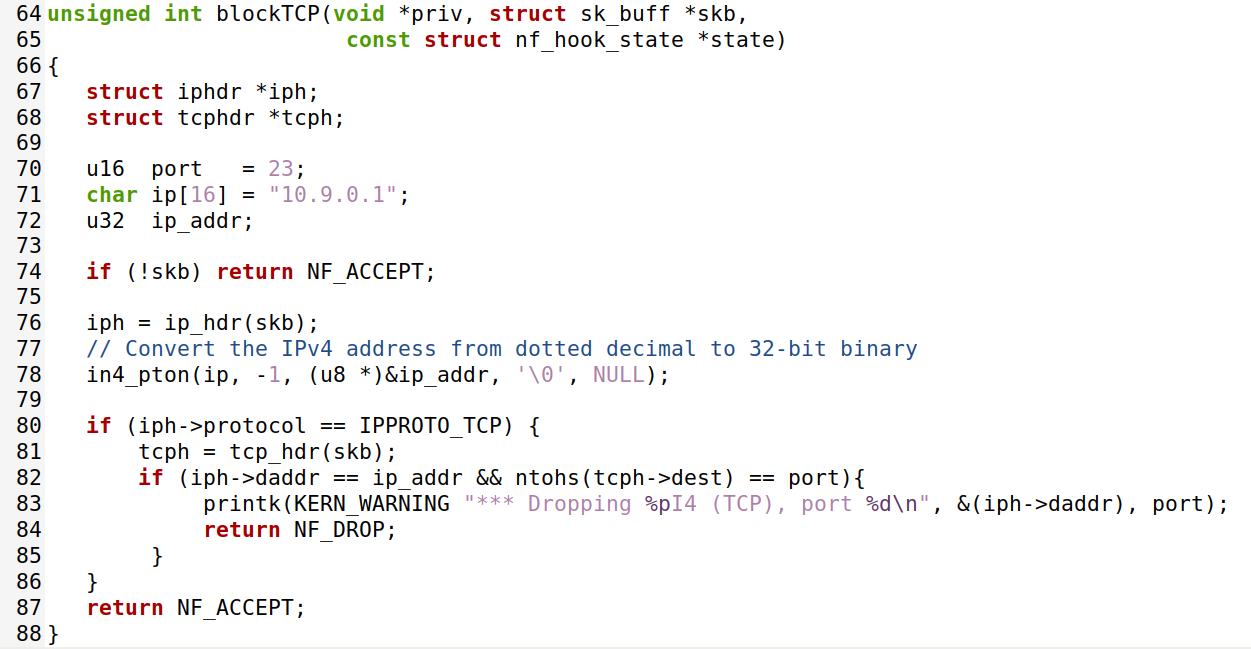


1. Task2：阻止TCP 端口和PING，把增加和修改的代码截图，并在卸载模块后将dmesg的日志信息的截图，并分析说明原因。

增加函数 blockICMP：



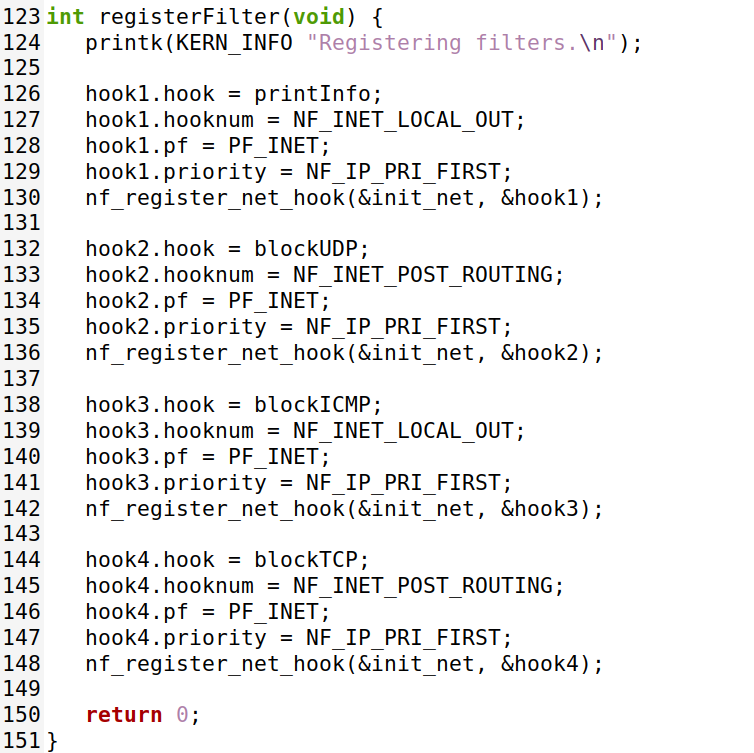
增加函数blockTCP：



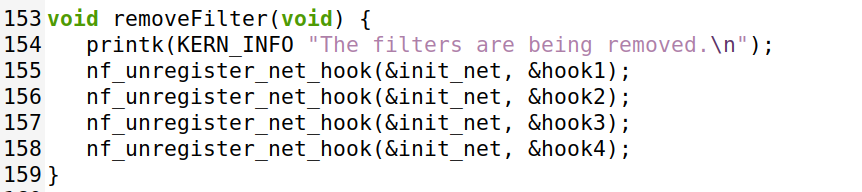
增加两个钩子 hook3，hook4：

C:\Users\lenovo\Documents\WeChat Files\wxid_xgzr63lnxlp912\FileStorage\Temp\1686058905737.png

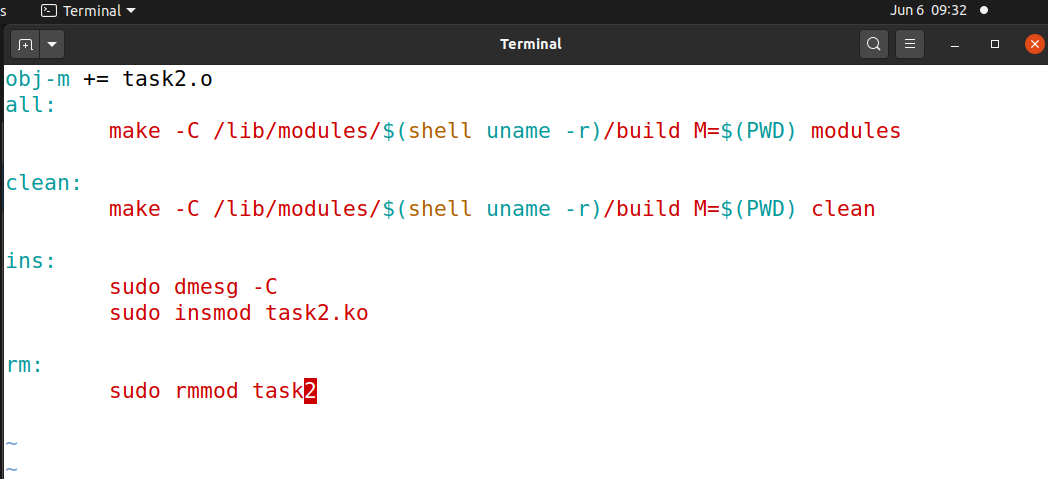
在 registerFilter 函数中注册：



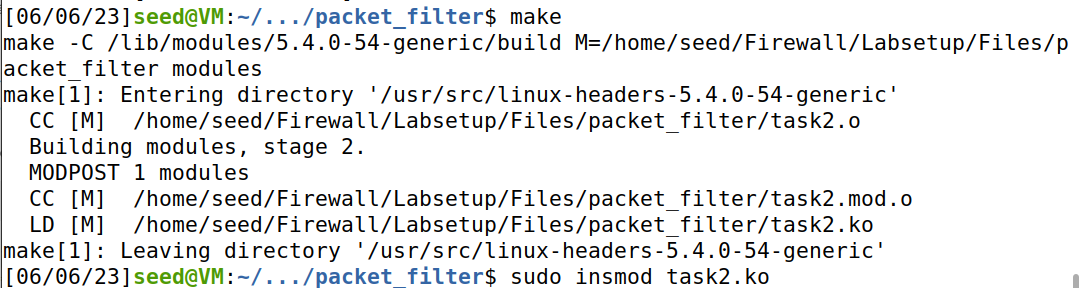
在 removeFilter 函数中删除：

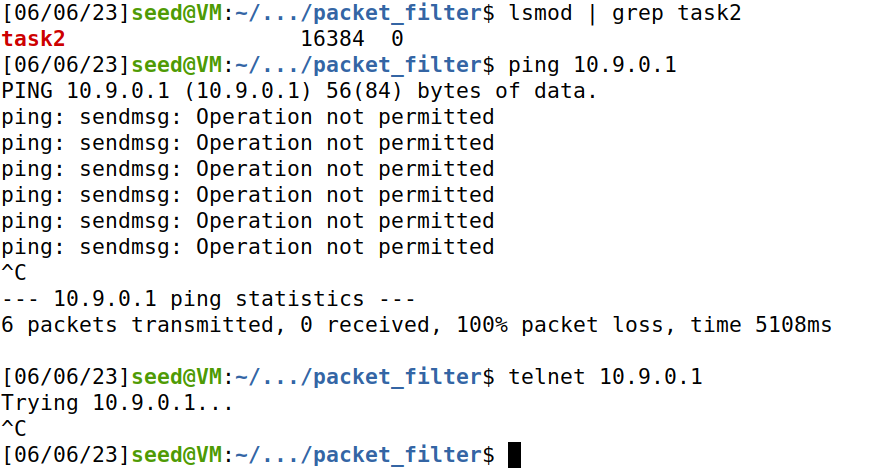


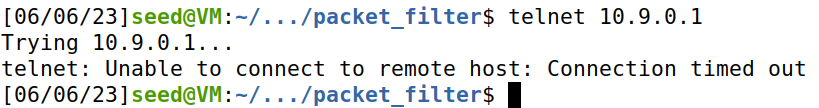
修改 Makefile ，将里面的 seedFilter 相关的内容修改为 task2 的内容：



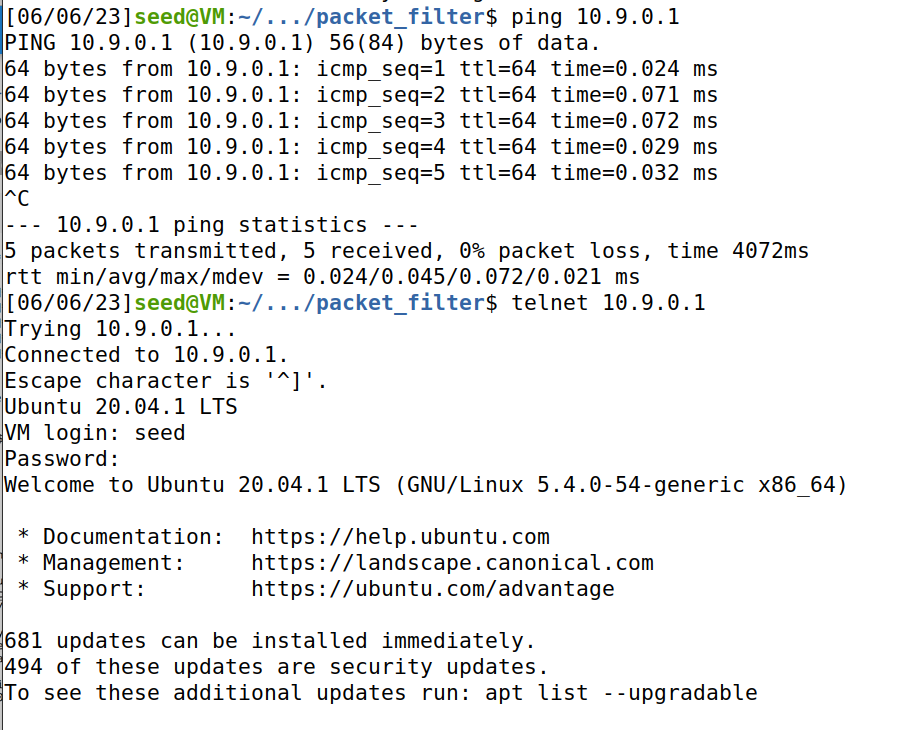
分别输入 ping 10.9.0.1 和 telnet 10.9.0.1 命令，发现没有响应：

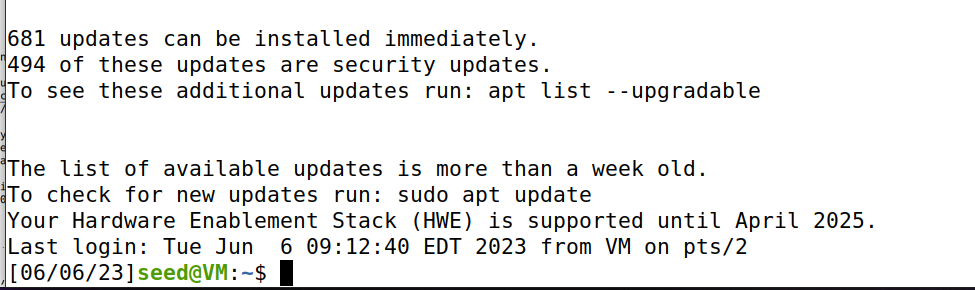




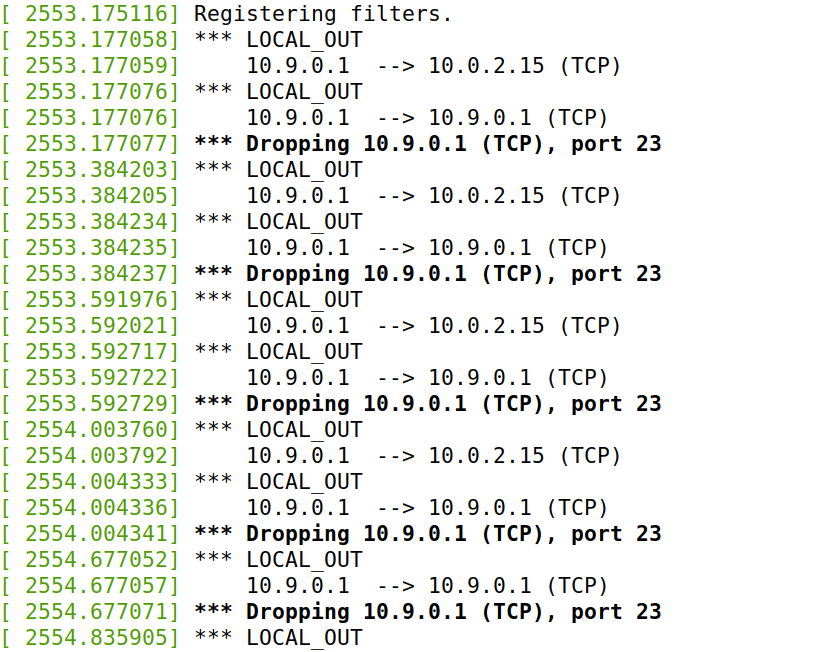


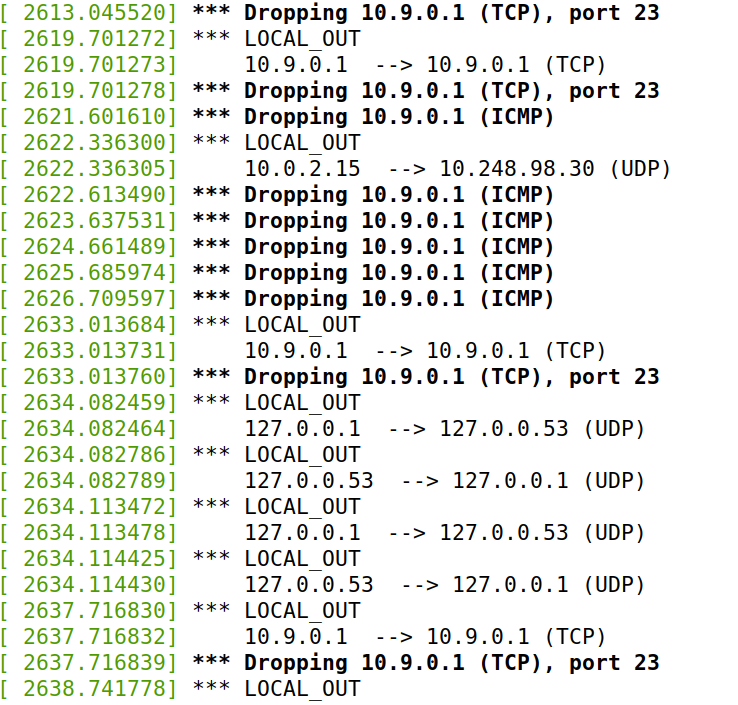
卸载 task2 模块成功后再执行 ping 10.9.0.1 和 telnet 10.9.0.1 命令，恢复正常：





dmesg的日志信息如下，发现有防火墙阻止后丢掉的数据包：

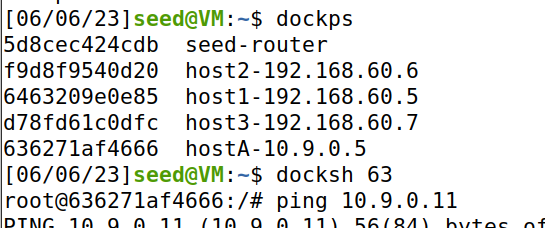


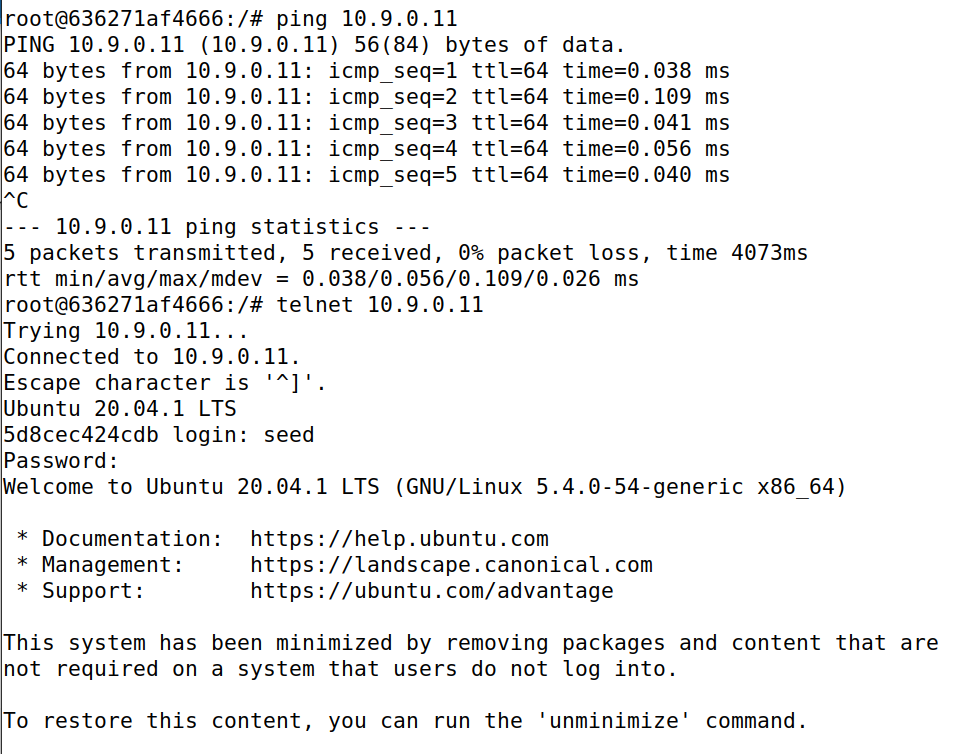


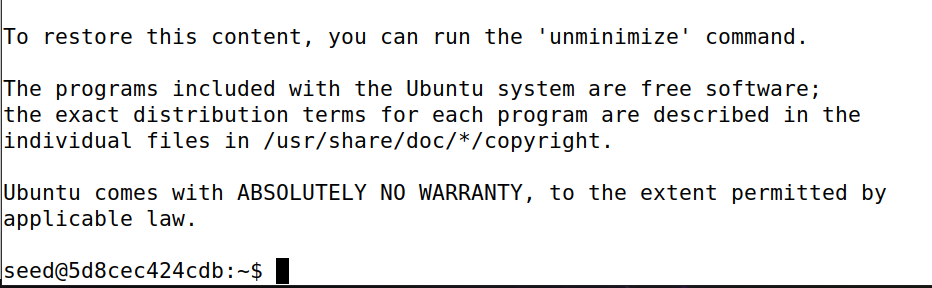
ping 10.9.0.1 和 telnet 10.9.0.1均没有响应，是因为在task2中实现了防火墙，从而拦截并丢弃了 IP地址是 10.9.0.1 的 ICMP 数据包以及IP地址为 10.9.0.1、端口号为23的TCP数据包。

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。

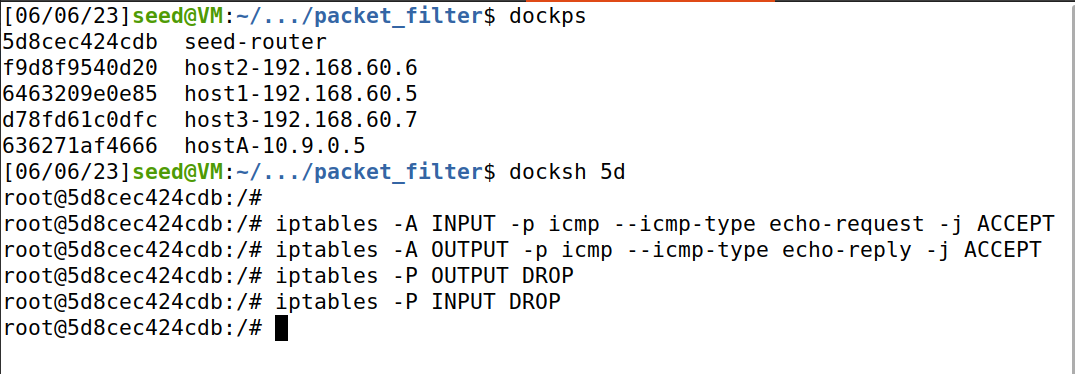
初始时，直接在容器A中执行 ping 10.9.0.11（Router IP）和 telnet 10.9.0.11（Router IP）命令，发现均可以连通：



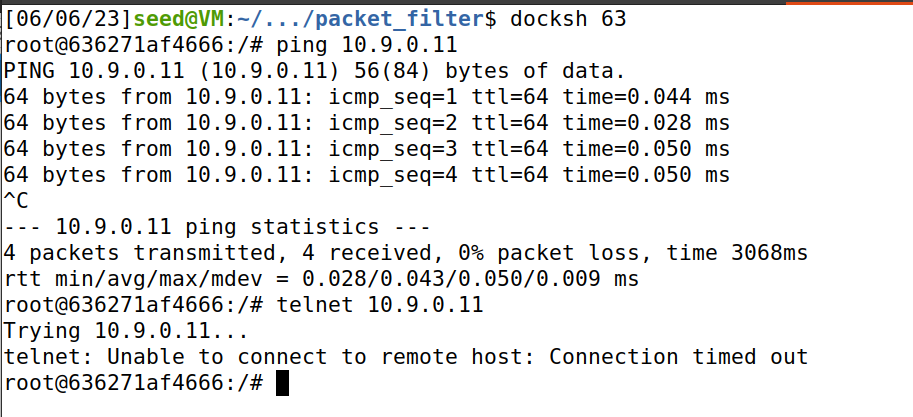




然后，设置Router允许icmp类型协议的应答，其他没有设置的协议类型默认拒绝：



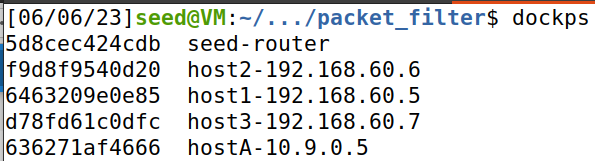
在 HostA 容器中再次执行 ping 10.9.0.11（Router IP）和 telnet 10.9.0.11（Router IP）命令，发现ping 10.9.0.11可以连通，而telnet 10.9.0.11不行：

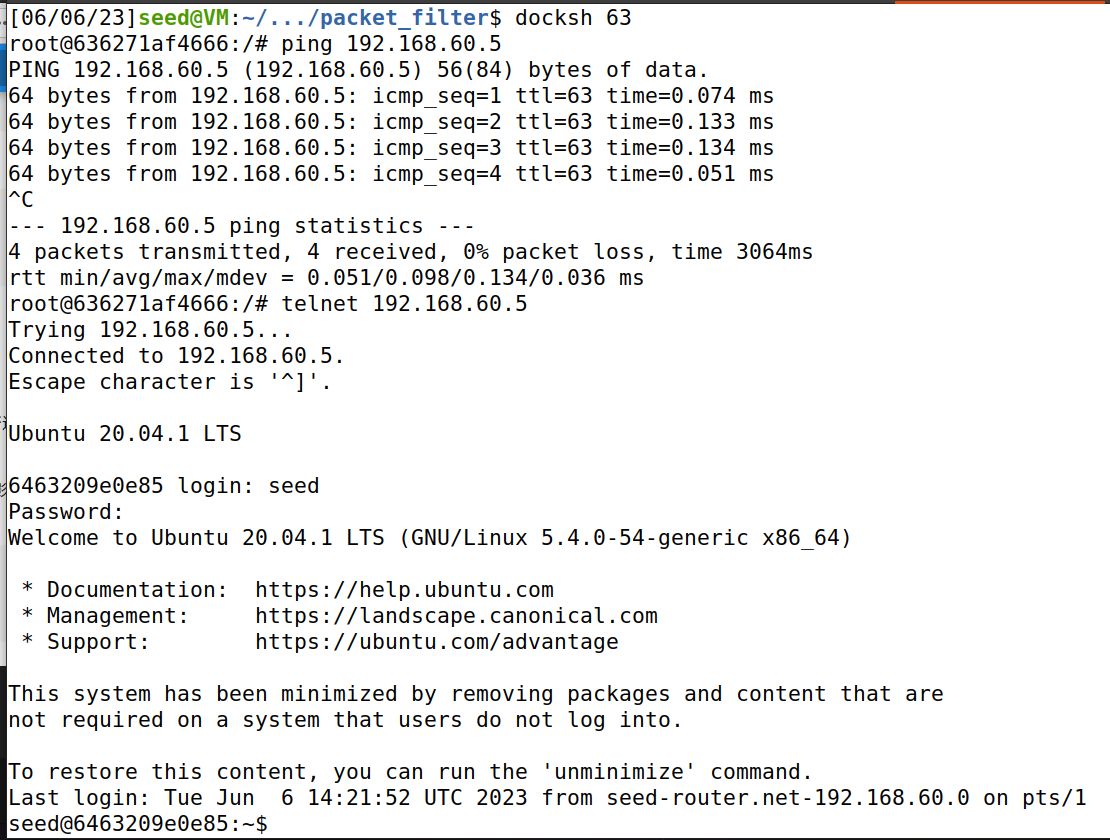


ping 10.9.0.11可以连通，是因为防火墙允许icmp-type echo-request数据包以及icmp-type echo-reply数据包通过。而telnet 10.9.0.11不行，是因为防火墙设置其他没有设置的协议类型都默认拒绝，又由于telnet使用了TCP协议，因此相关的报文将被防火墙拦截并丢弃。

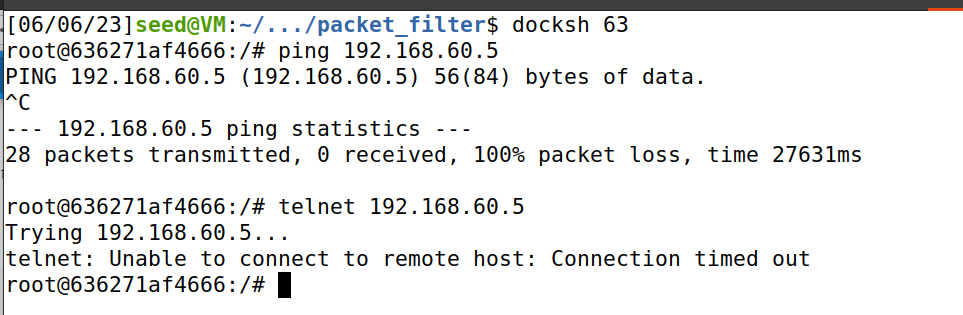
4、Task4：保护内网，将配置iptables规则前后ping的连通性测试结果截图，并分析说明原因。

最初时，在 HostA 容器中执行 ping 192.168.60.5（内网host1 IP）和 telent 192.168.60.5（内网host1 IP）命令，发现均可以连通：





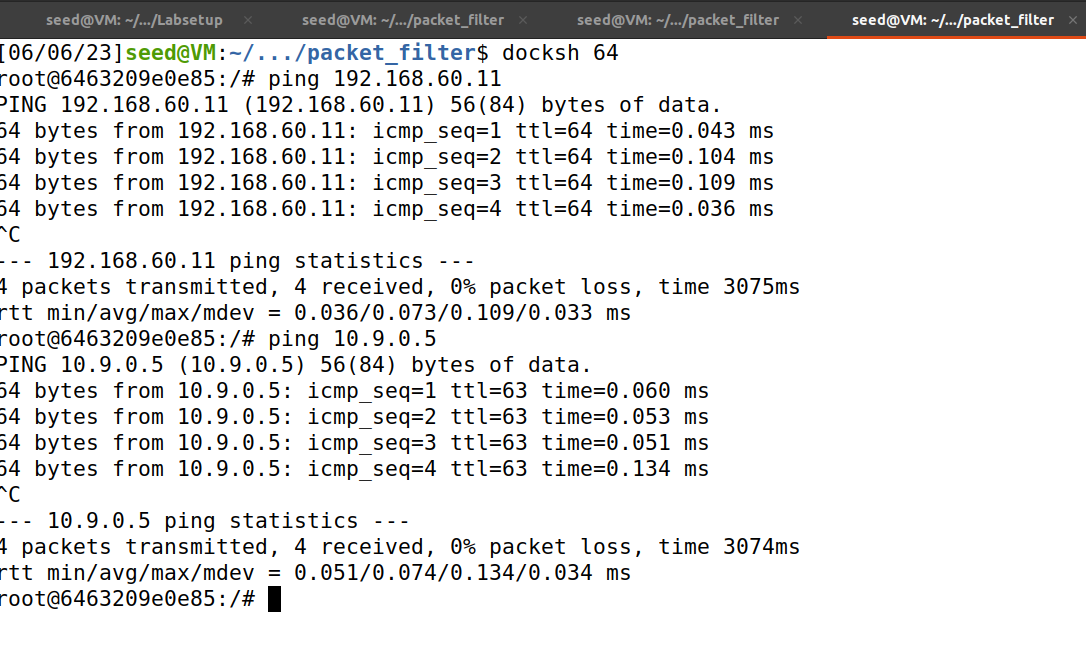
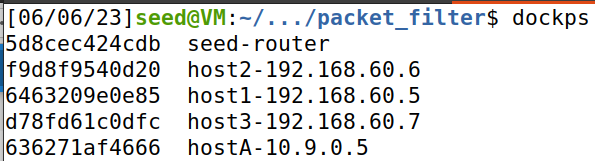
在 Router 容器中配置iptables之后，在 HostA 容器中执行 ping 192.168.60.5（内网Host1 IP）和 telent 192.168.60.5（内网Host1 IP）命令，发现均无法连通：



这是因为配置规则 -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP表示从外网接口eth0来的icmp-type echo-request数据包均需要被拦截并丢弃。因此，HostA无法ping通内网的Host1。

同时，配置规则-P FORWARD DROP 表示除上述三种类别外的其它数据包都将被拦截并丢弃。telnet使用的是TCP协议，因此数据包被丢弃，无法连通。

在 Host1（192.168.60.5）中分别执行 ping 192.168.60.11 和 ping 10.9.0.5（HostA），观察发现均可以连通：



这是因为配置规则 -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT表示从内网接口eth1来的icmp-type echo-request数据包被允许通过。配置规则 -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT表示其它的icmp-type echo-reply数据包均被允许通过。

所以，执行ping 192.168.60.11时，Host1发送icmp-type echo-request数据包到Router（192.168.60.11），防火墙允许该数据包通过；Router收到请求并回复icmp-type echo-reply数据包，防火墙也允许该数据包通过，所以Host1可以收到回复。 因此可以连通。

同理，执行ping 10.9.0.5 时，Host1和HostA之间的数据包也被防火墙允许通过，所以Host1和HostA也能连通。