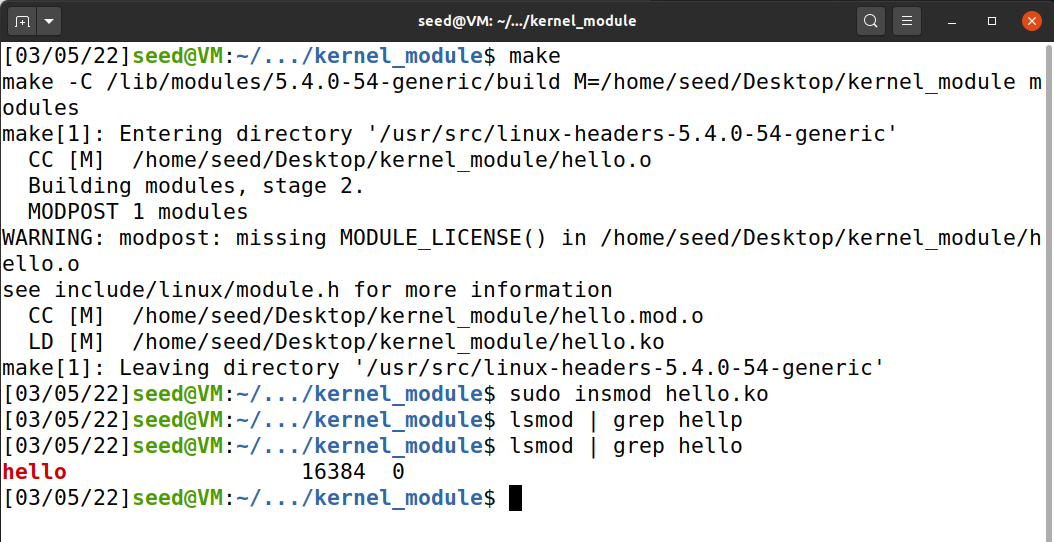
**第六次实验报告**

57118121 刘洪飞

Task1.A

编译加载模块



发现syslog 出现相关记录

Task1.B

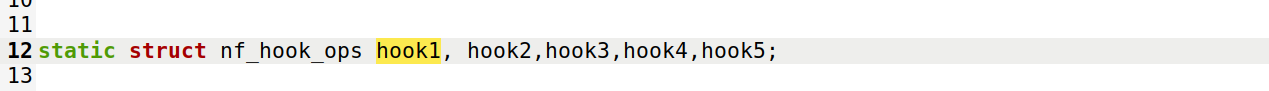
1

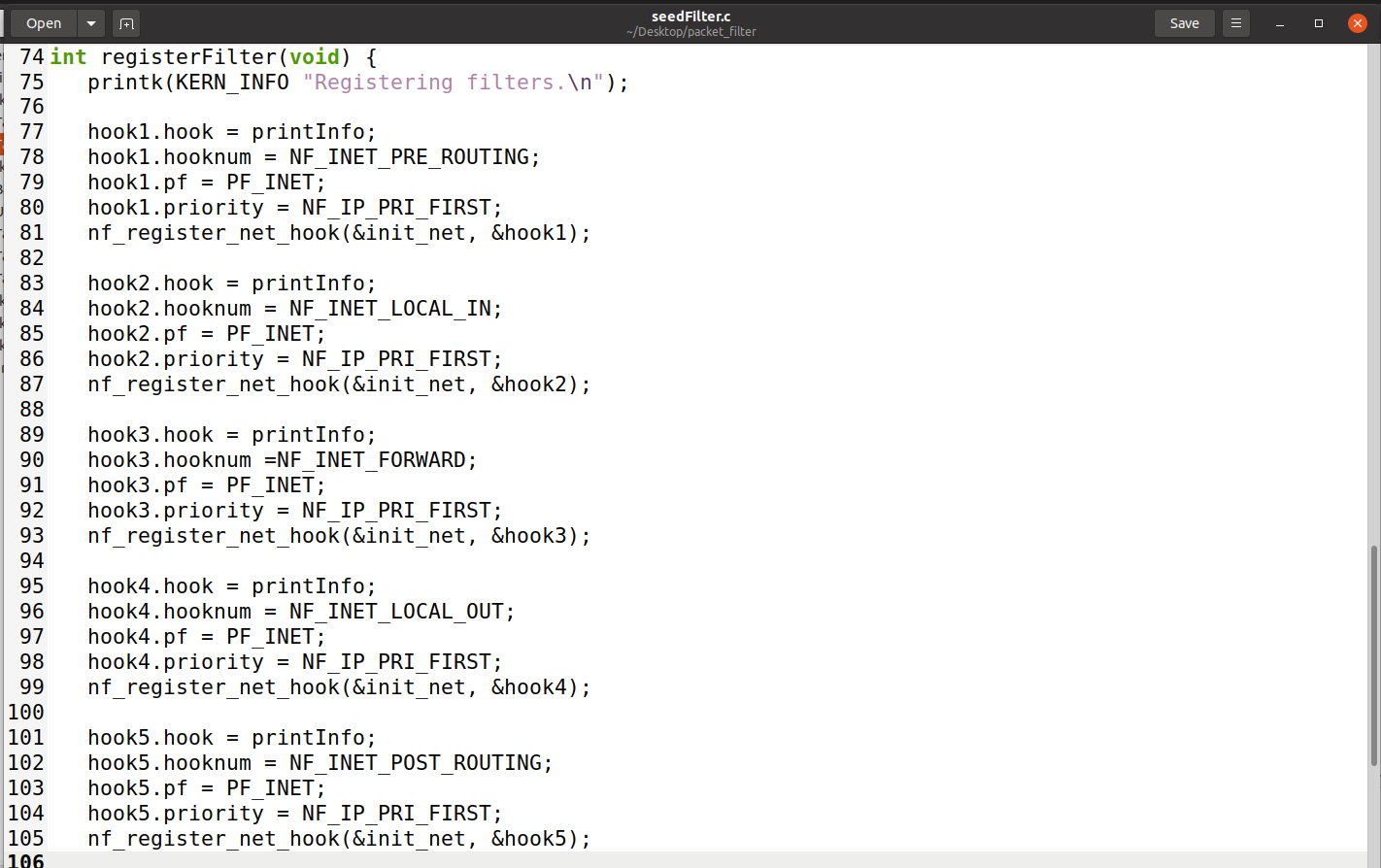
编译加载模块，防火墙效果为UDP报文被拦截，没有响应



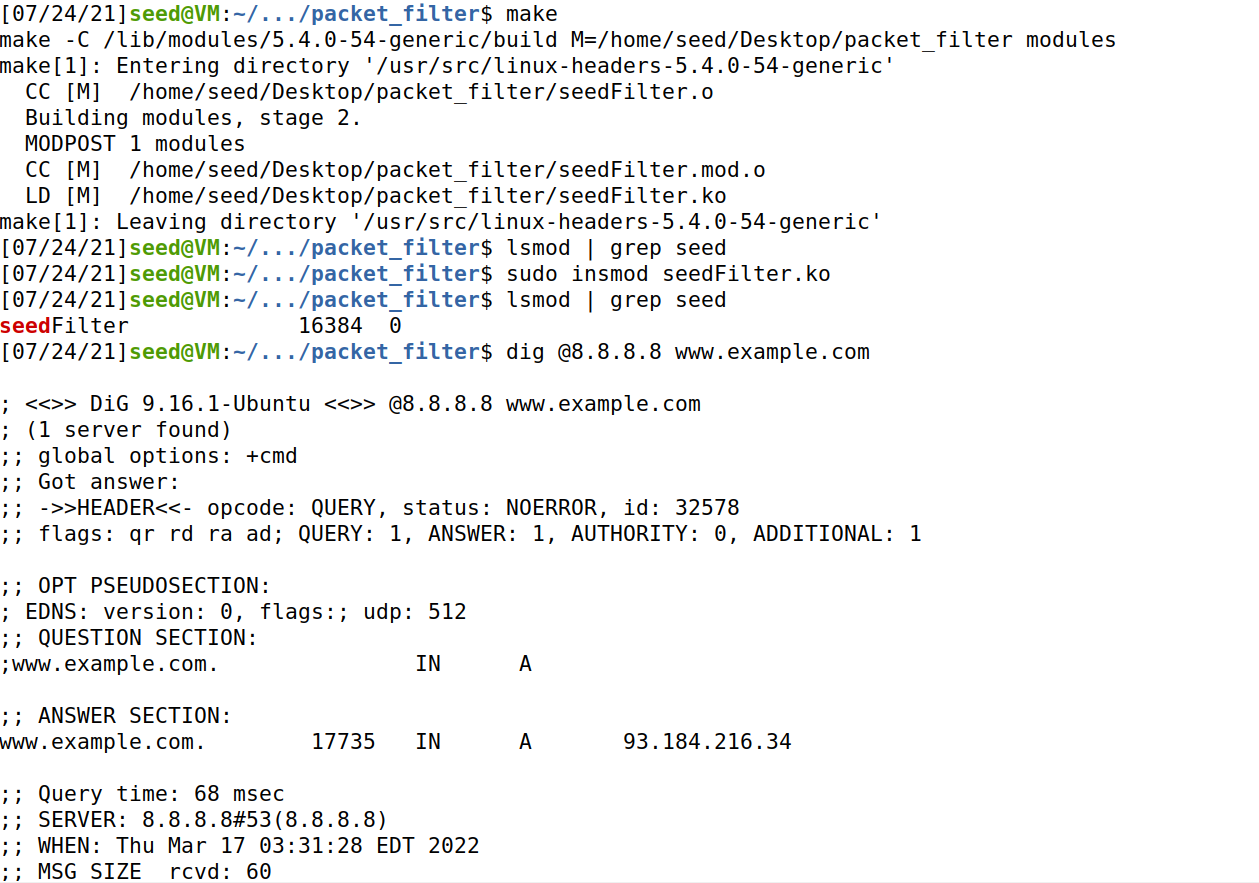
2

代码修改如下

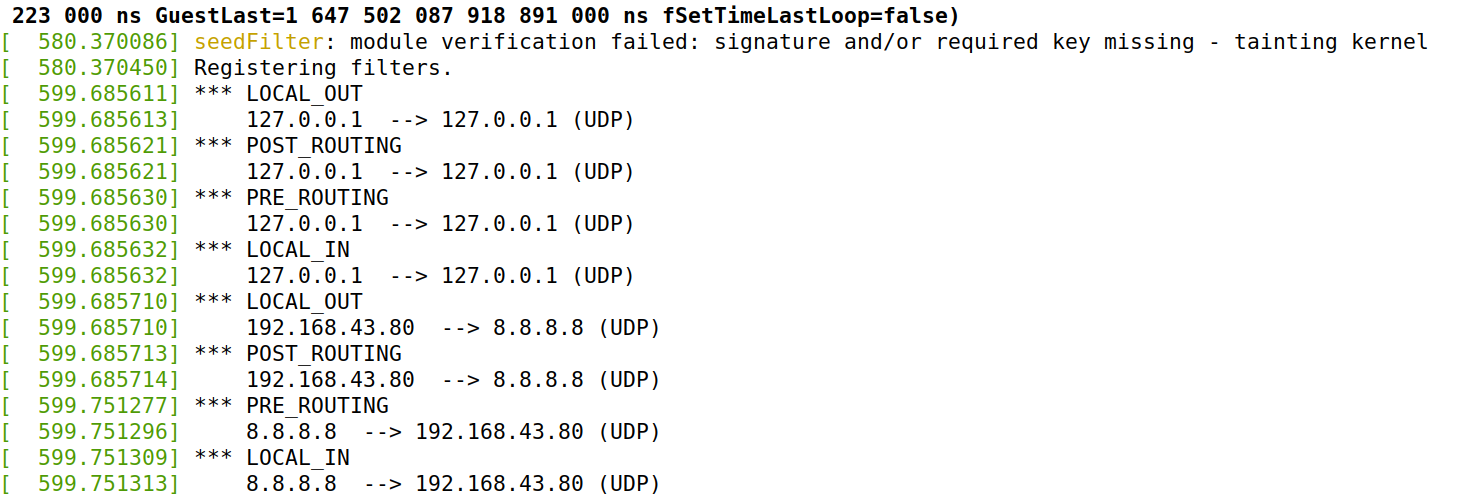




编译内核加载，使用dig进行测试

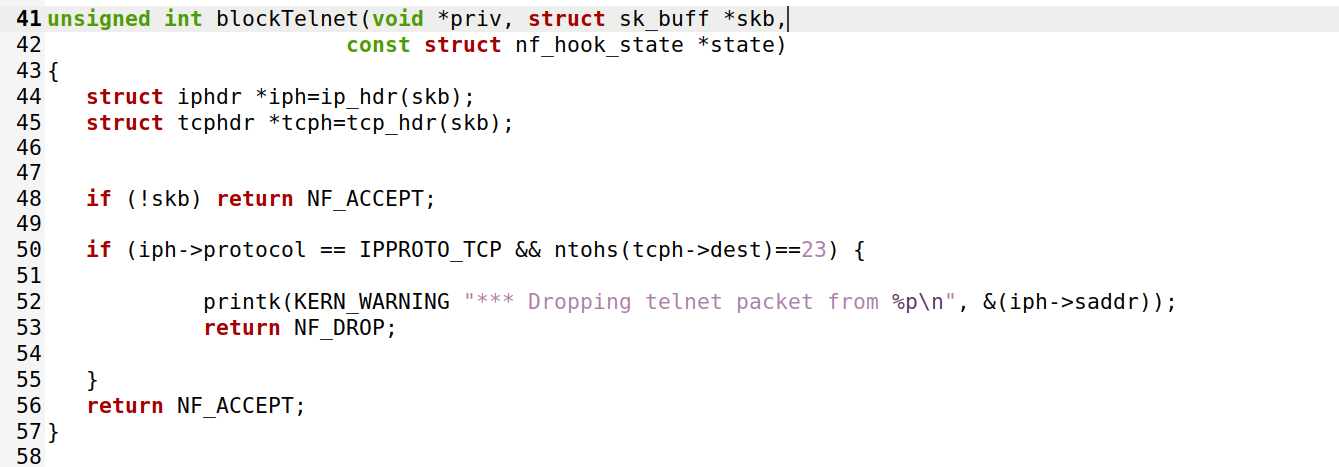


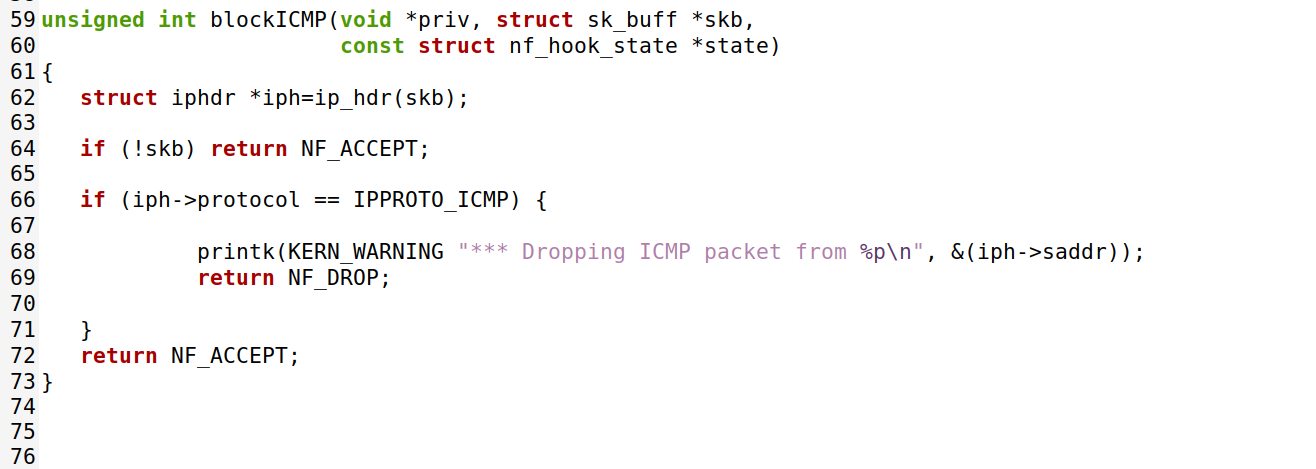
VM向8.8.8.8发送报文，先通过LOCAL OUT ，然后路由后的报文POST ROUTING ，从8.8.8.8发回的的顺序为PRE ROUTING ，然后通过LOCALIN ，有可能因为FORWARD 不进入内核，所以没有出现



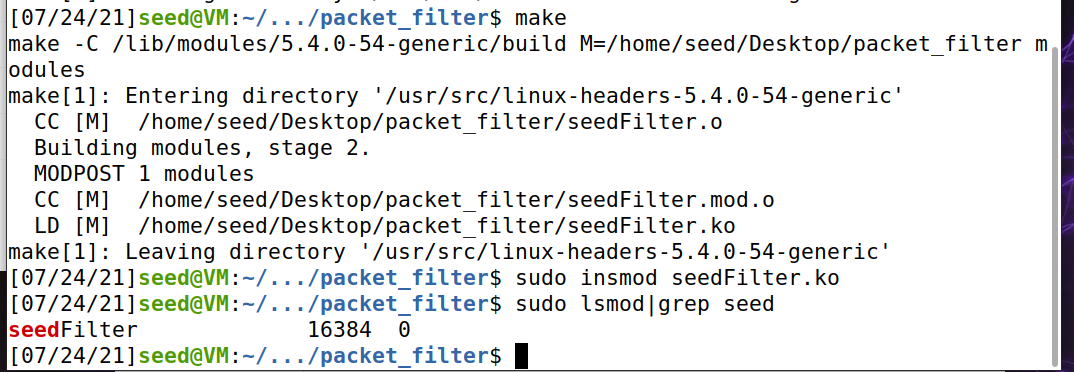
3

修改代码如下

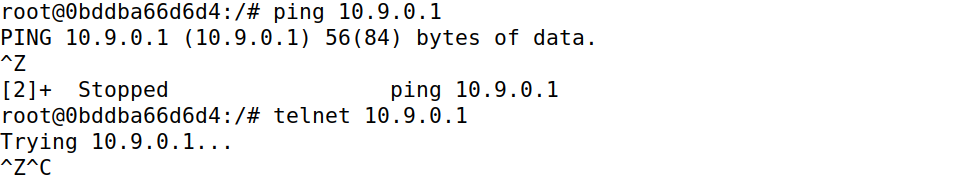




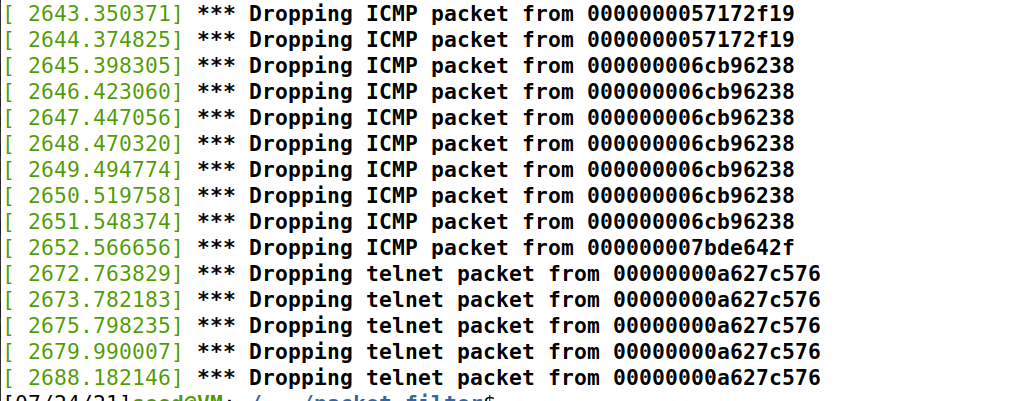
编译内核加载



Ping 和 Telnet 10.9.0.1的结果如下，都被拦截



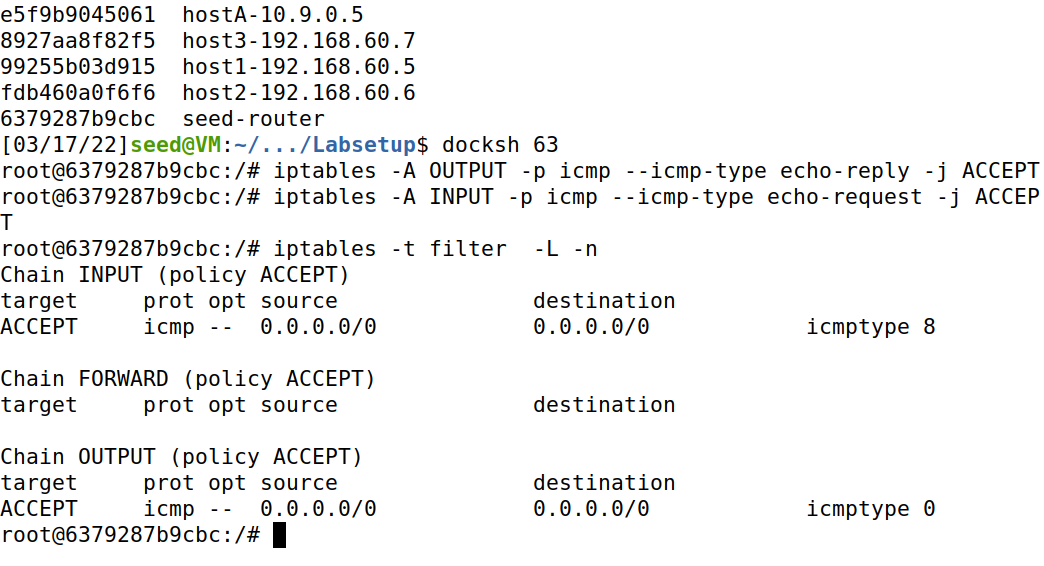
Syslog出现防火墙过滤策略的记录

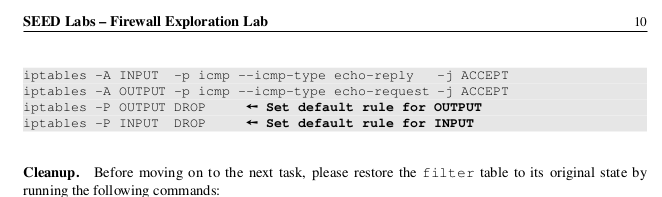


Task2.a

配置路由器







四条规则的解释依次如下

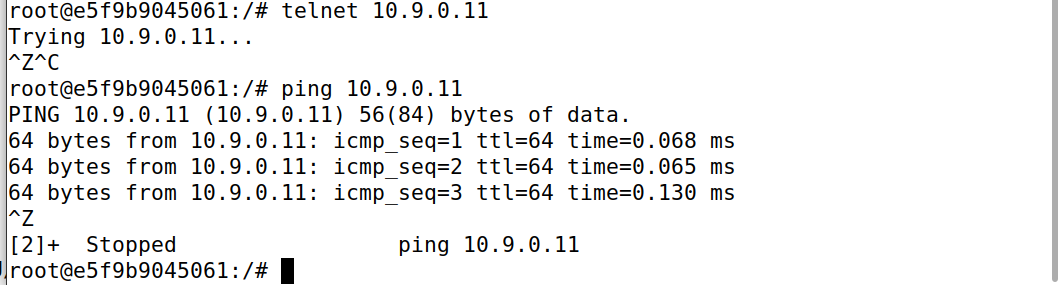
允许发出ICMP的响应报文

允许接收ICMP的请求报文

丢弃所有的发送报文

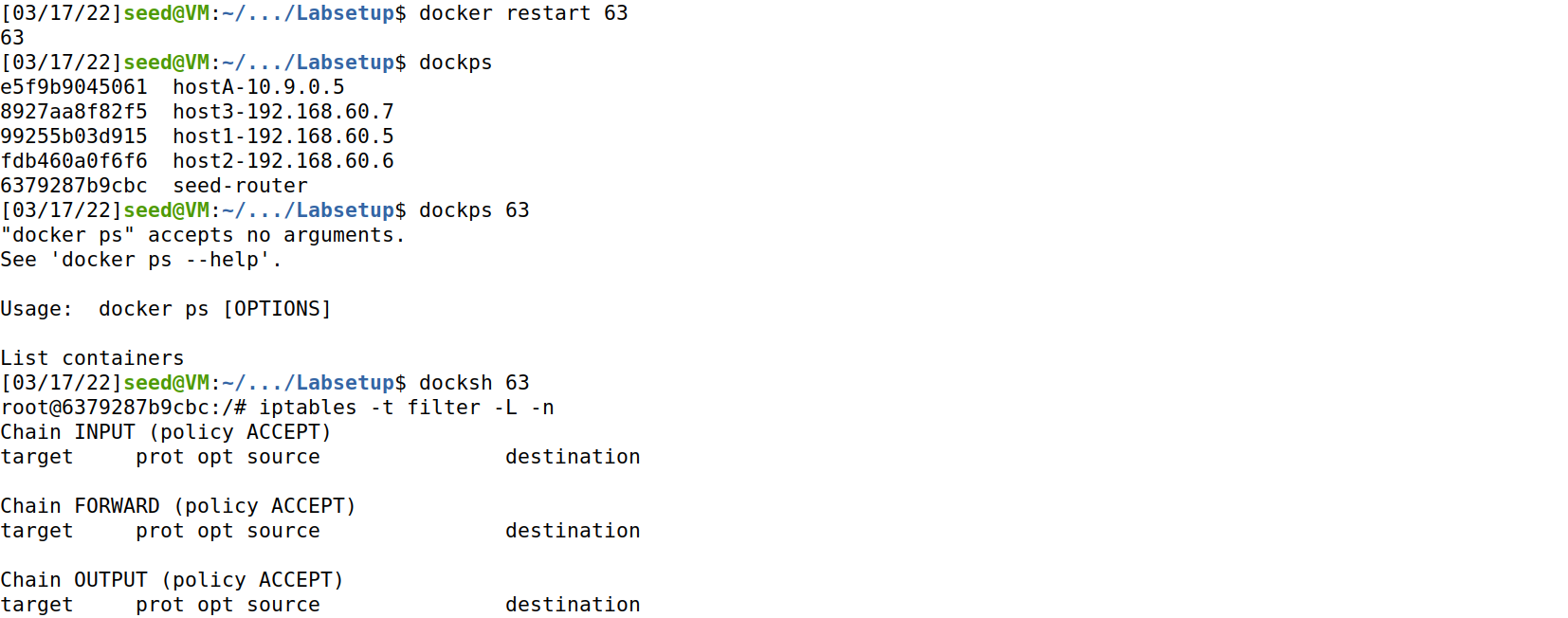
丢弃所有的接收报文

效果如下 Telnet无法连接，ping可以成功

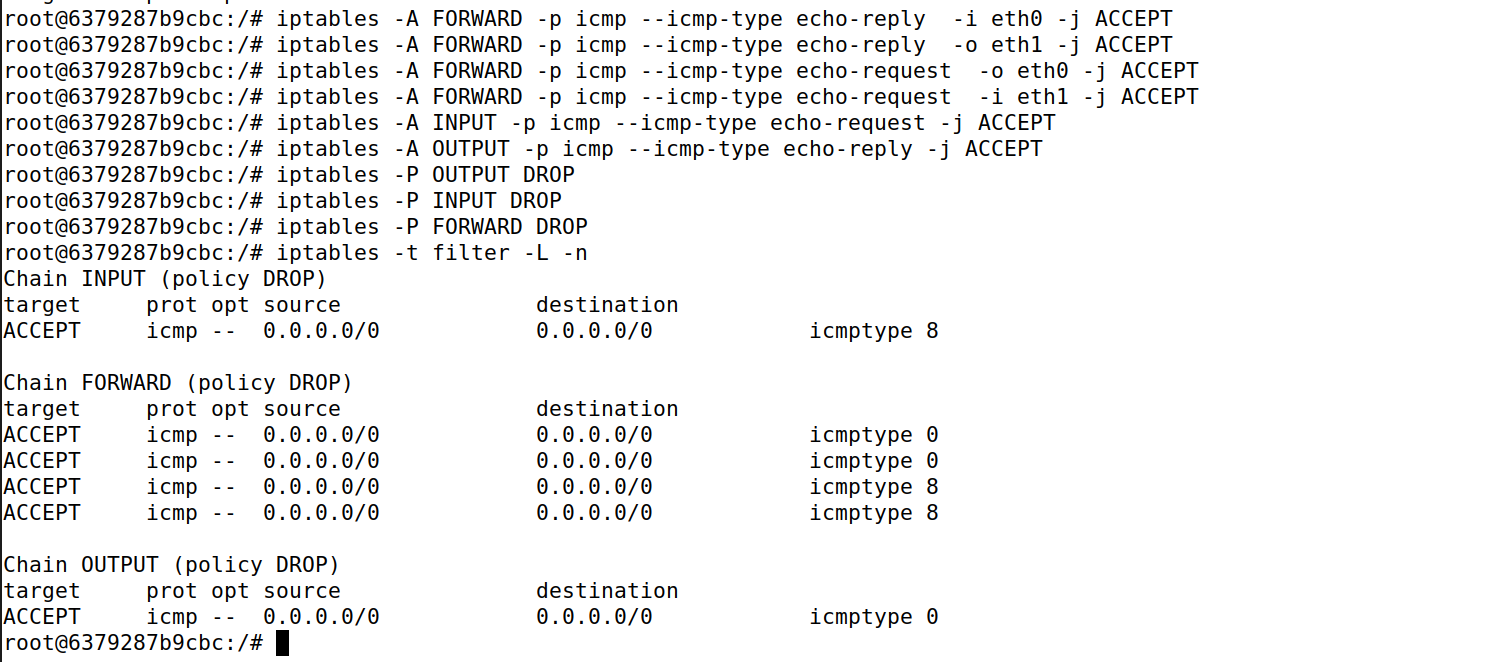


Task2.b

清空配置

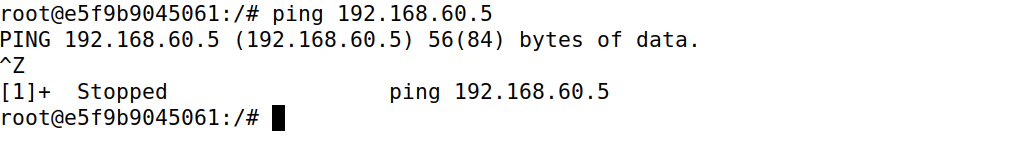


策略配置如下

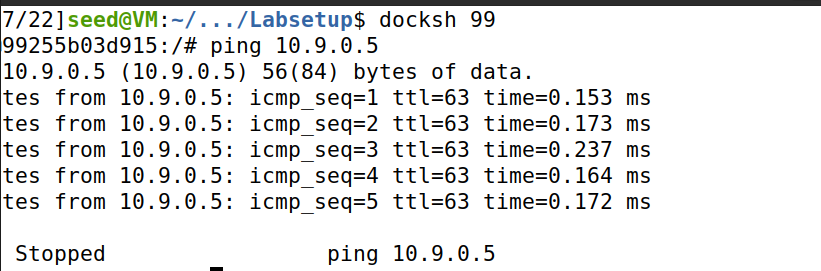


防火墙效果如下

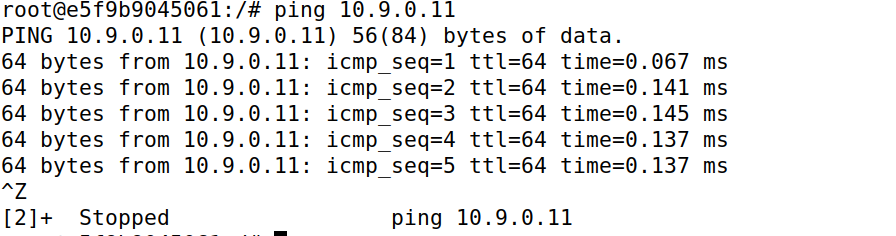
10.9.0.0网段无法ping通192.168.60.0网段



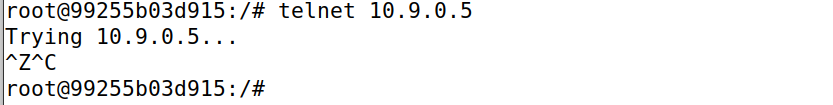
192.168.6.0网段无法ping通10.9.0.0网段

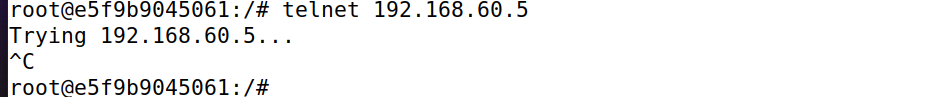


可以ping通路由器



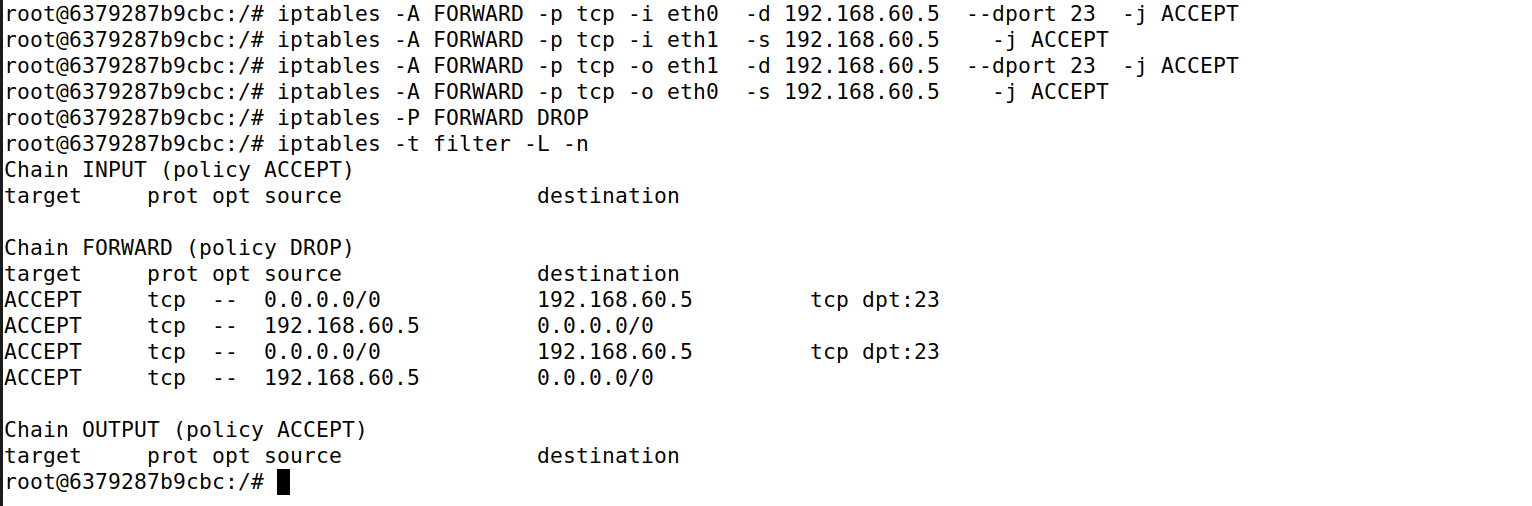
两个网段都无法Telnet



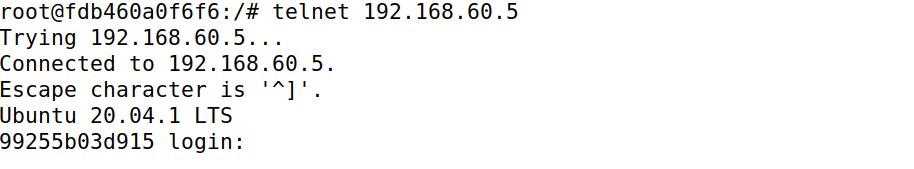


Task2.c

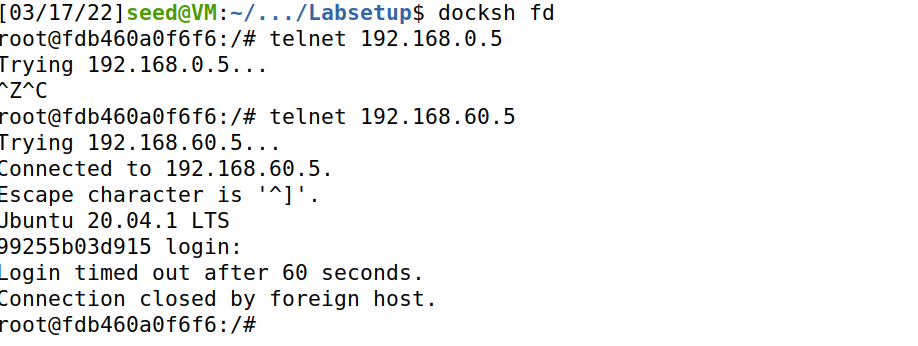
配置如下



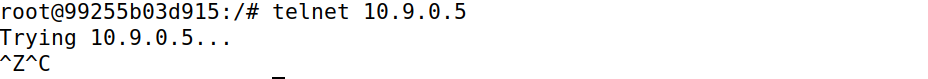
内部相互可以Telnet

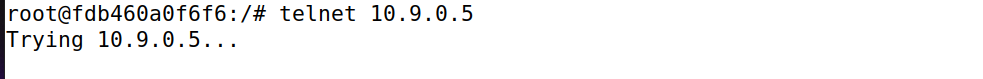


外部可以Telnet 192.168.60.5，但是无法Telnet其他内网IP

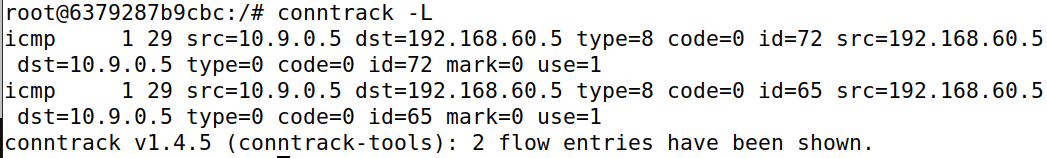


内网ip包括196.168.60.5都无法Telnet其他主机

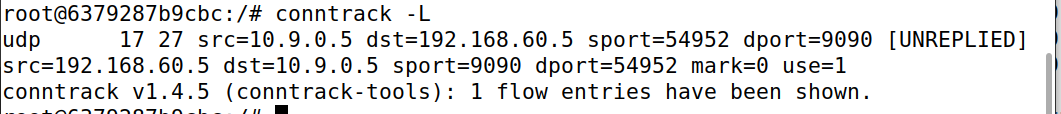




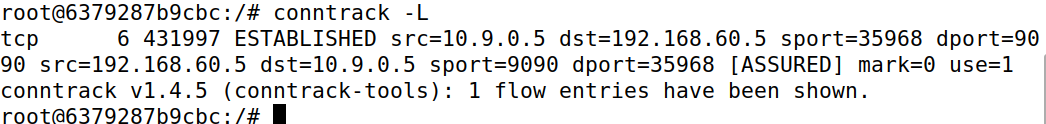
Task3.a



测试发现ICMP持续时间大约为30秒，



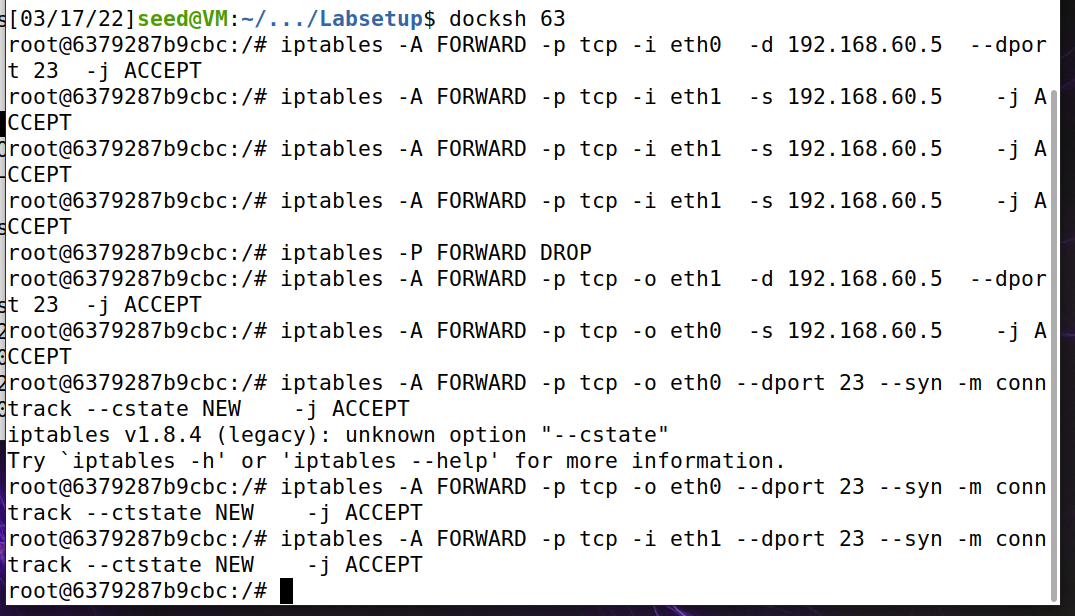
同样，发现UDP的时间大约是30秒



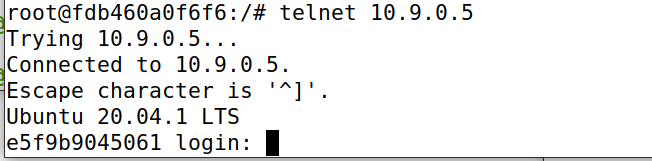
发现tcp时间大约432000秒，

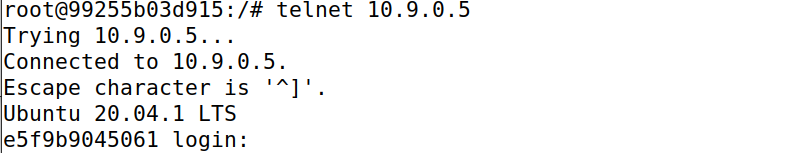
Task3.b

配置如下



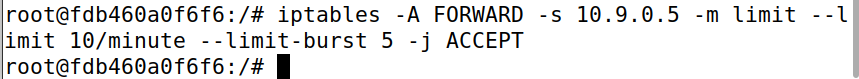
192.168.60.0网段可以Telnet到10.9.0.5



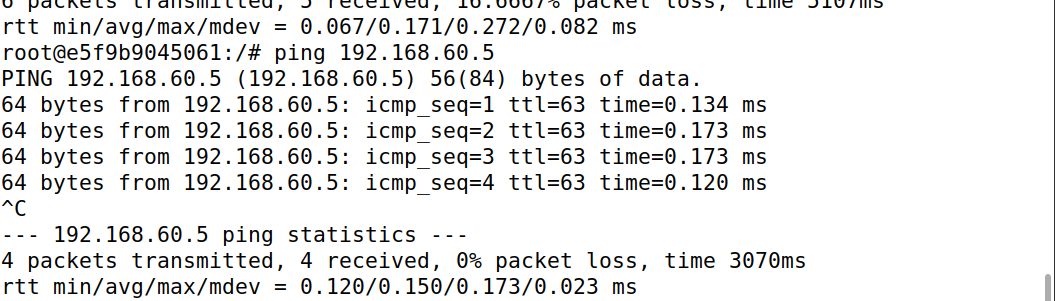


Task4

添加规则



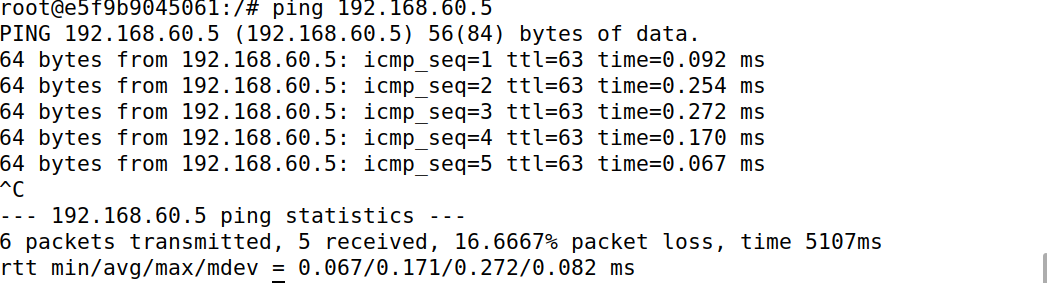
Ping 结果如下



再添加如下规则



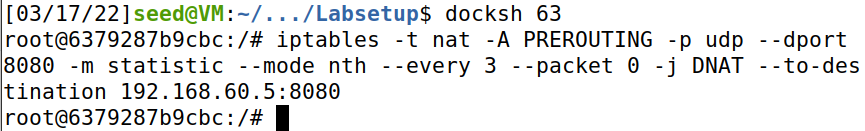
结果如下



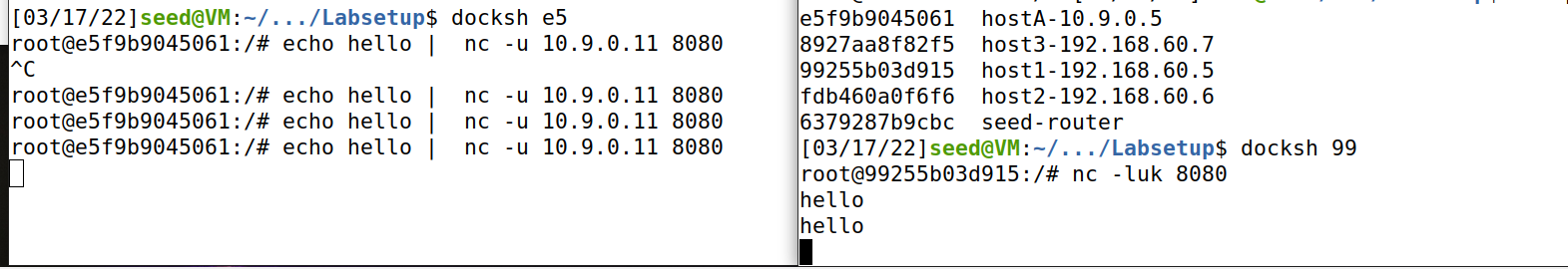
对比发现加上第二条规则才会生效，只有一条的话超出部分会被accept ，而只有添加第二条之后超出流量会被drop

Task 5

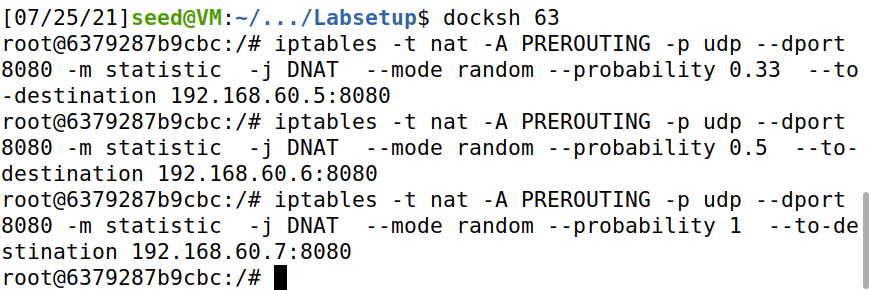
配置如下



发现每三次交互都只有一次会成功，如图所示进行了四次，所以会输出两次成功



设置负载均衡



发现成功

