请编辑高亮部分 提交中或英文版本皆可.

Student Name: 黄敏 HuangMin

Email: huangmin@asu.edu

Submission Date: 2024/4/14

Class Name and Term: CSE 534 Spring B

项目 2.1 异常流量检测实践

I. 项目概述 PROJECT OVERVIEW

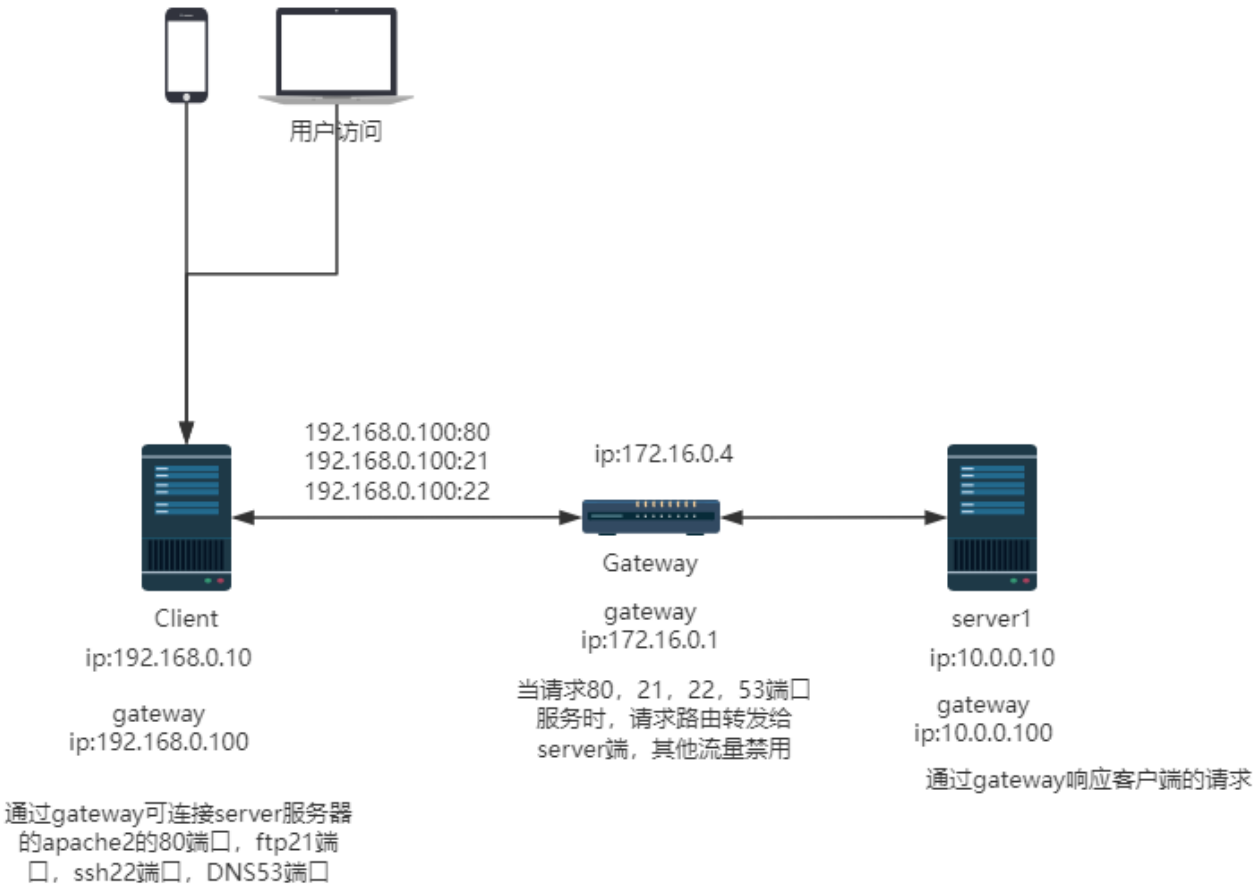
以一段话总结本课程项目以及你达成的目标 One paragraph to describe this project and your accomplishment.
在 client 端安装 hping3，在网关部署防火墙转发请求到 server，并启动 snort 检测异常流量的实践，已完成 3 个试验。

II. 网络配置 NETWORK SETUP

绘制一个网络图来表现你搭建的虚拟网络，需要包括以下内容 Draw a diagraph and provide descriptions about the network setup, include:

- 网络拓扑 topology,

网络拓扑和项目 2.1 没有大的变化，在 client 端安装 hping3，在网关部署防火墙转发请求到 server，并启动 snort 检测异常流量



- 网络配置，如虚拟机的 IP 等，network configurations (IP addresses, etc.)

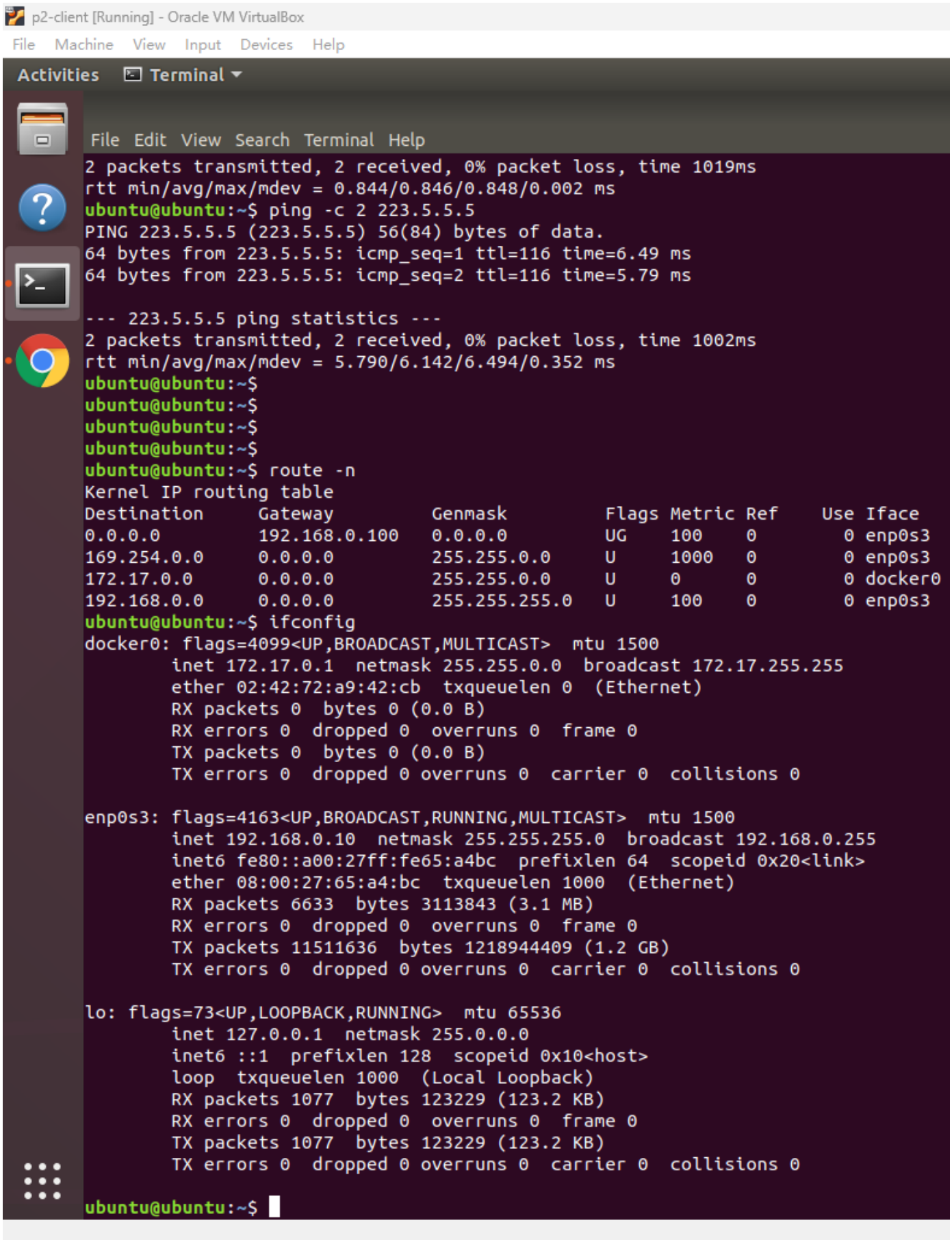
请编辑高亮部分 提交中或英文版本皆可.

网络设置：
通过 Net 3 连接互联网：172.16.0.0/12
客户端 Net 1：192.168.0.0/24
服务器端 Net 2：10.0.0.0/8

IP 地址的设置如下：
- 客户端 IP：192.168.0.10
- 网关的入口 IP：192.168.0.100
- 网关的出口 IP：10.0.0.100
- 服务器 IP：10.0.0.10（运行 ssh、web、ftp、dns 服务等 ）

客户端 ifconfig 和 route -n

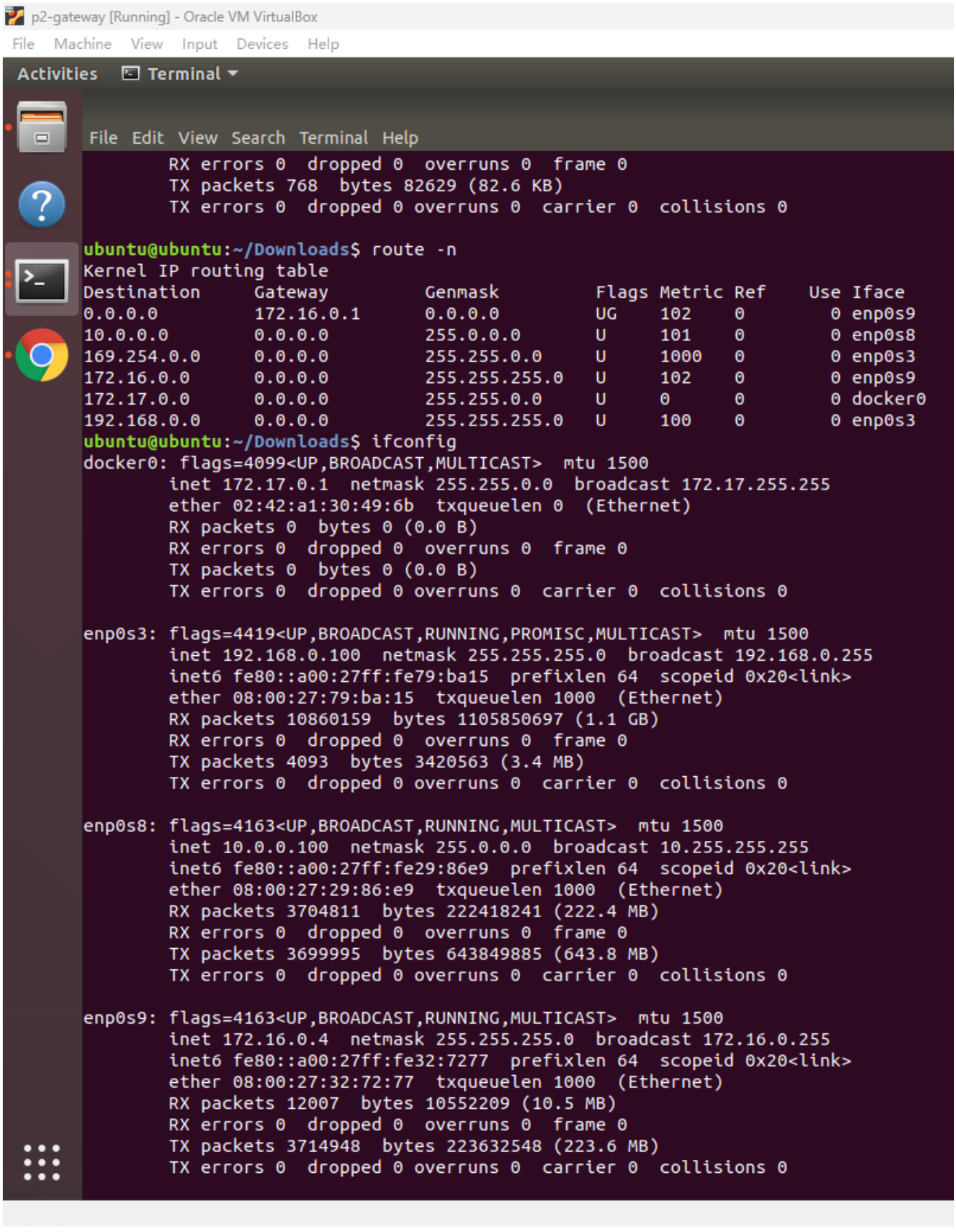
请编辑高亮部分 提交中或英文版本皆可.



请编辑高亮部分 提交中或英文版本皆可.

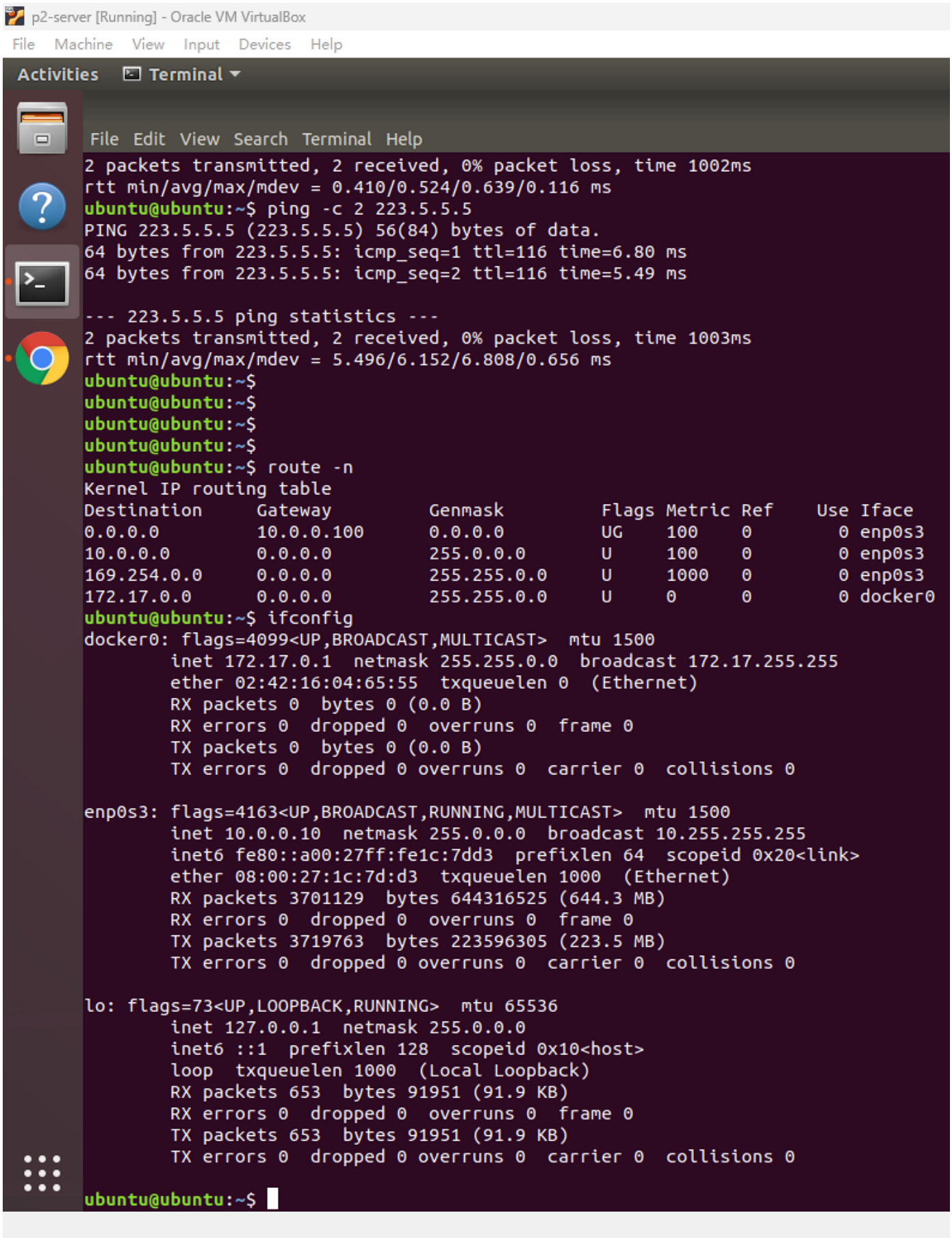
网关 ifconfig 和 route -n，发起攻击测试前，删除了 172.16.0.1 对外网关

请编辑高亮部分 提交中或英文版本皆可.



服务端 ifconfig 和 route -n

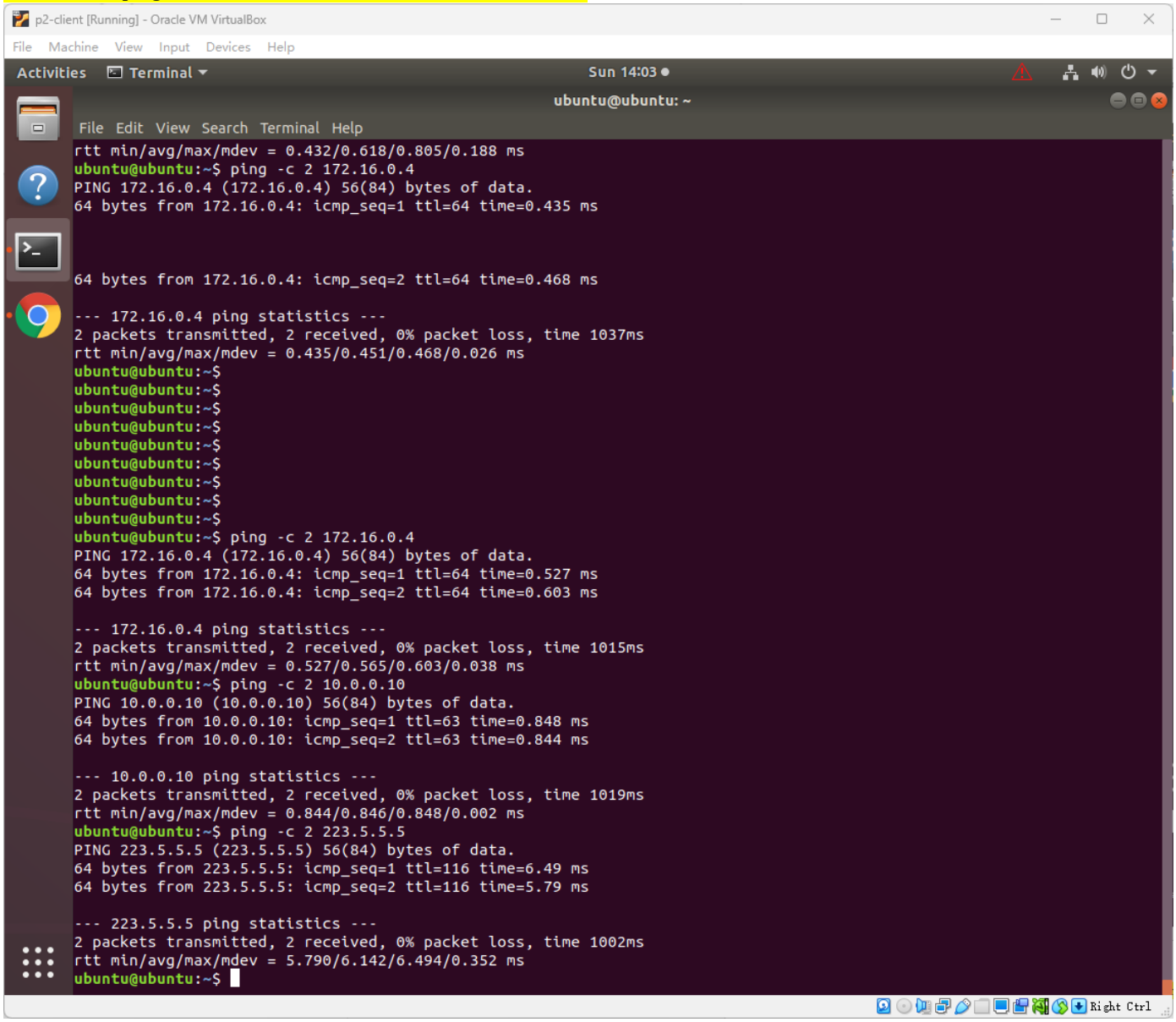
请编辑高亮部分 提交中或英文版本皆可.



请编辑高亮部分 提交中或英文版本皆可.

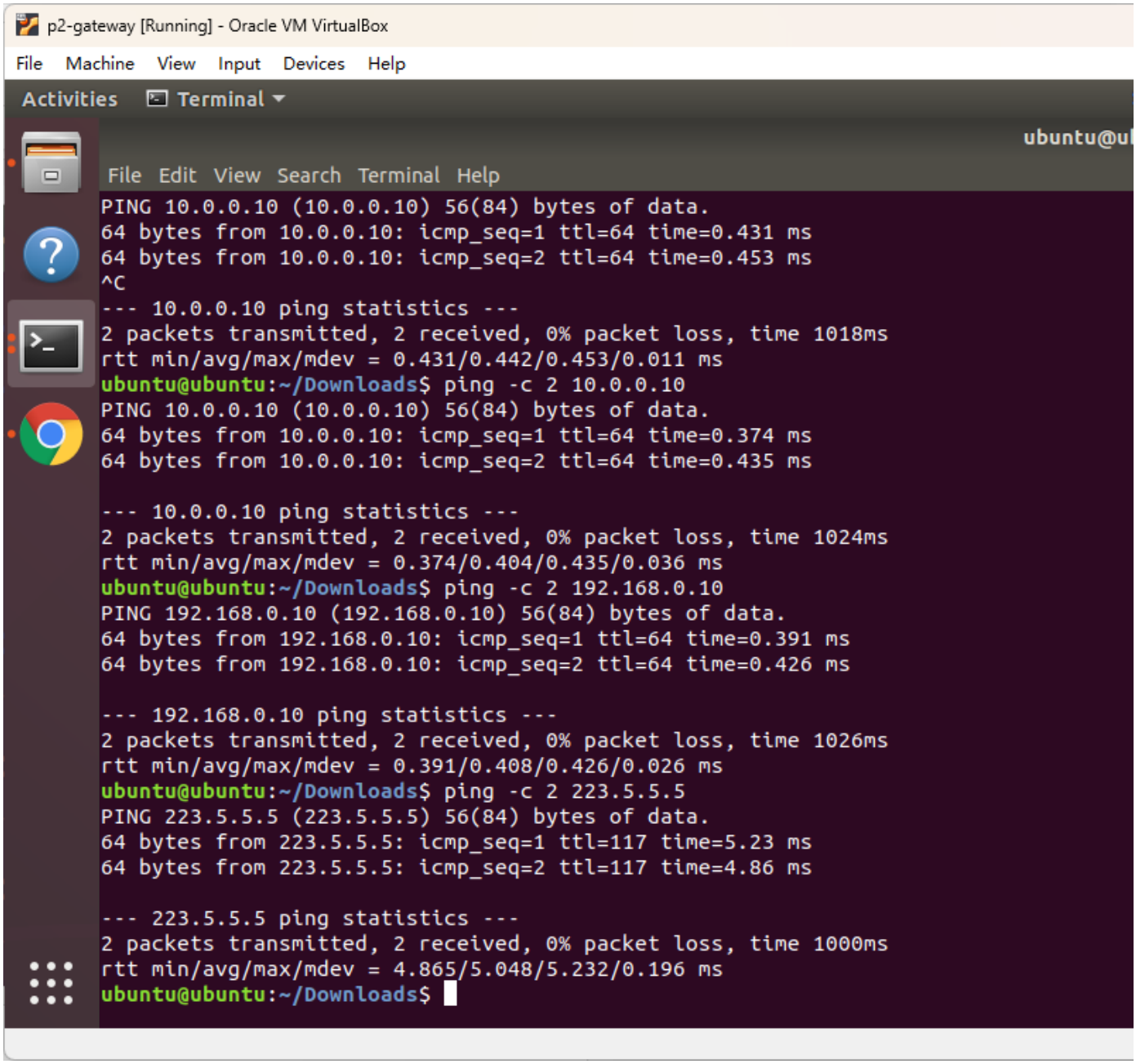
- 虚拟机之间的连接状况 initial reachability among network nodes

客户端通过 ping 连接网关，服务端，公网阿里 dns 223.5.5.5



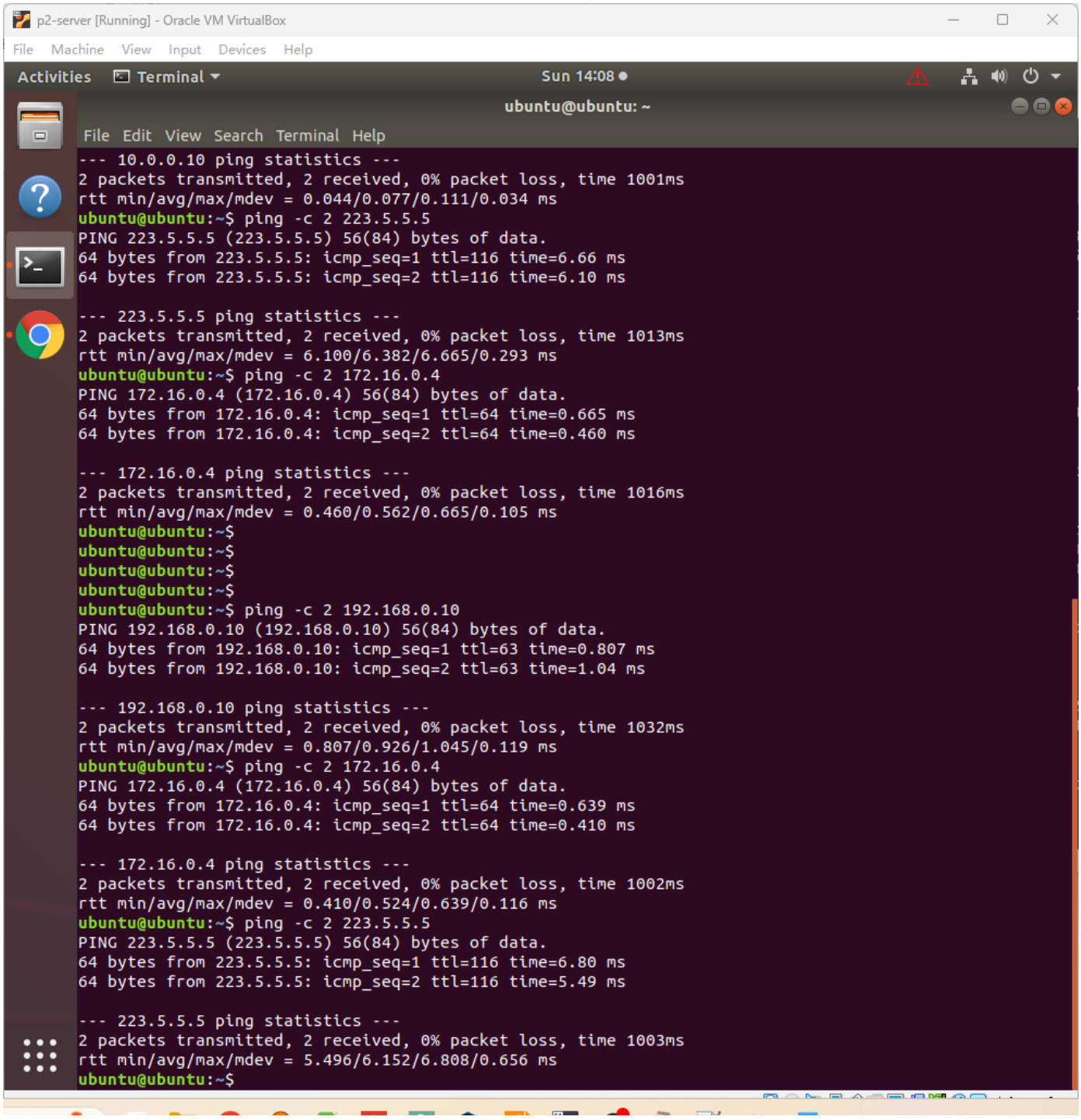
网关通过 ping 连接服务端，客户端，公网阿里 dns 223.5.5.5

请编辑高亮部分 提交中或英文版本皆可.



服务端通过 ping 连接客户端，网关和公网阿里 dns 223.5.5.5

请编辑高亮部分 提交中或英文版本皆可.



III. 软件 SOFTWARE

列出完成本项目时你所用到的软件 Describe major software and network services are used in this project to accomplish your goal.

Apache2，ssh，vsftp，防火墙脚本 iptables，chrome，Ubuntu，nmap，vim，Oracle VM VirtualBox，notepad++，Linux 网络工具 ifconfig/route/ping 等，新增：DNS，hping3，snort

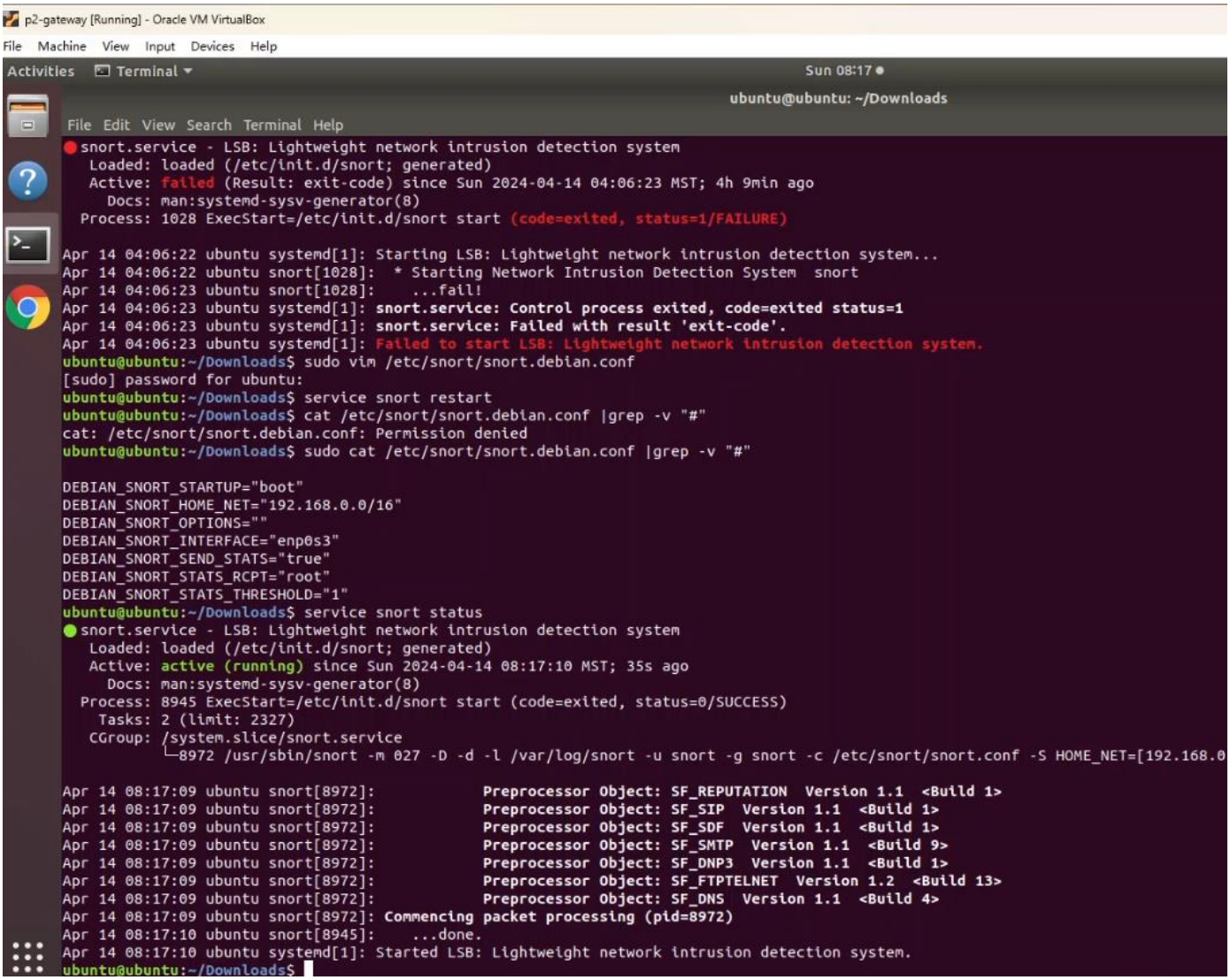
IV. 项目描述 PROJECT DESCRIPTION

详细叙述你完成本项目的步骤，并给出佐证，如截图，配置文件等，以第一个项目为例，你需要在附录中附上你虚

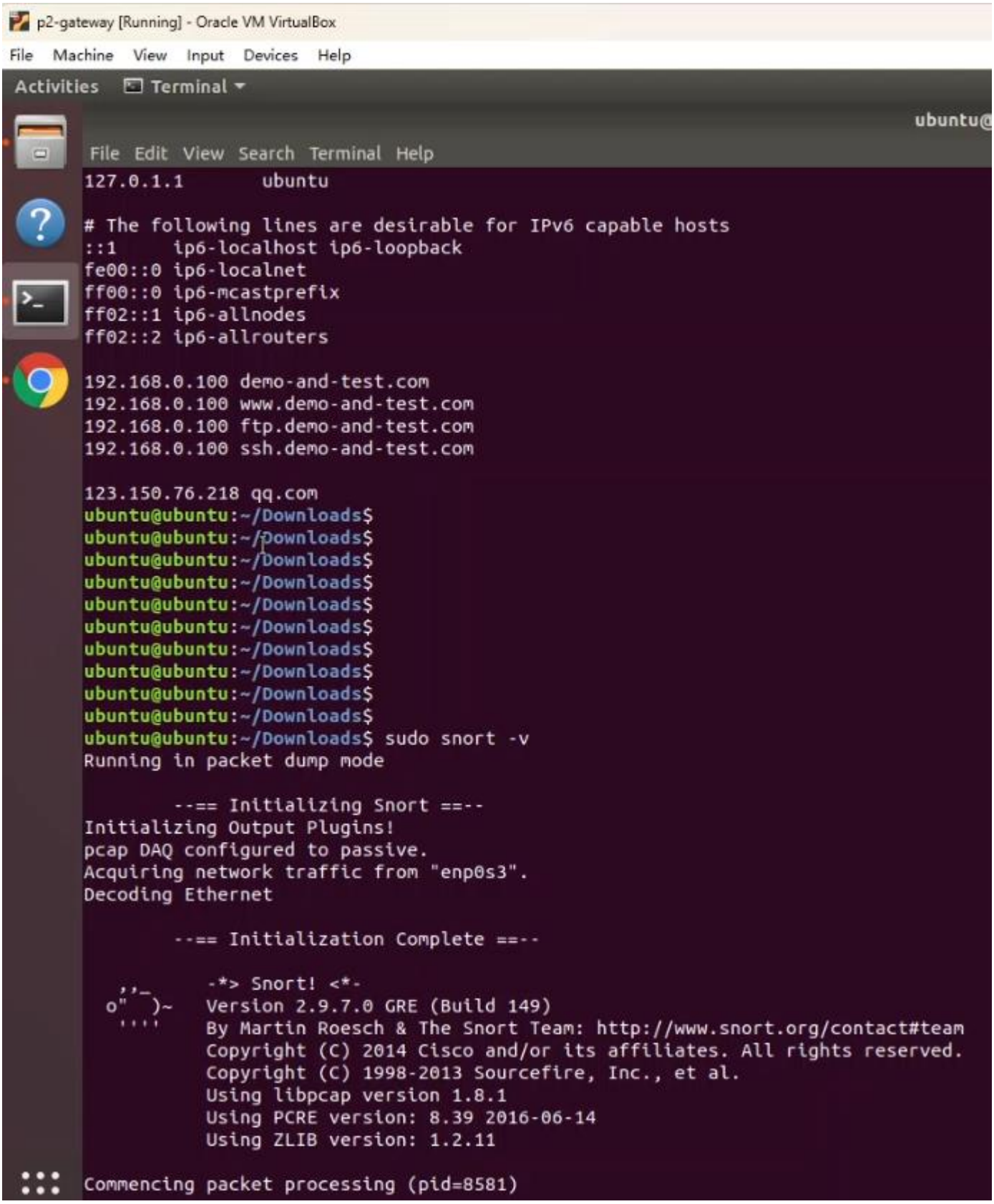
请编辑高亮部分 提交中或英文版本皆可.

拟机中的 netplan 配置文件 Your work should have evidence and corresponding illustrations, e.g., providing configuration files as attachment in the appendix.

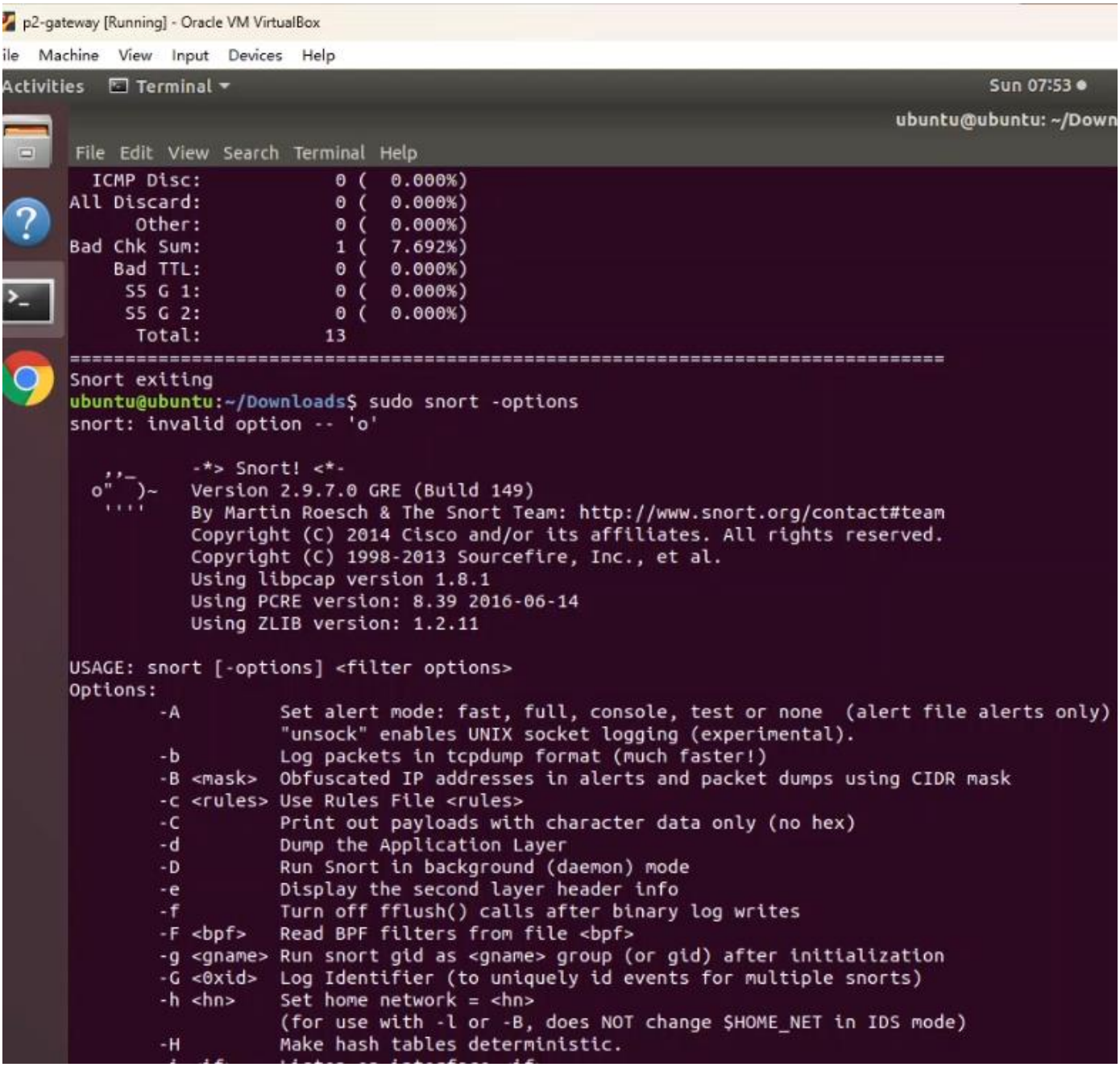
在网关上完成如下任务



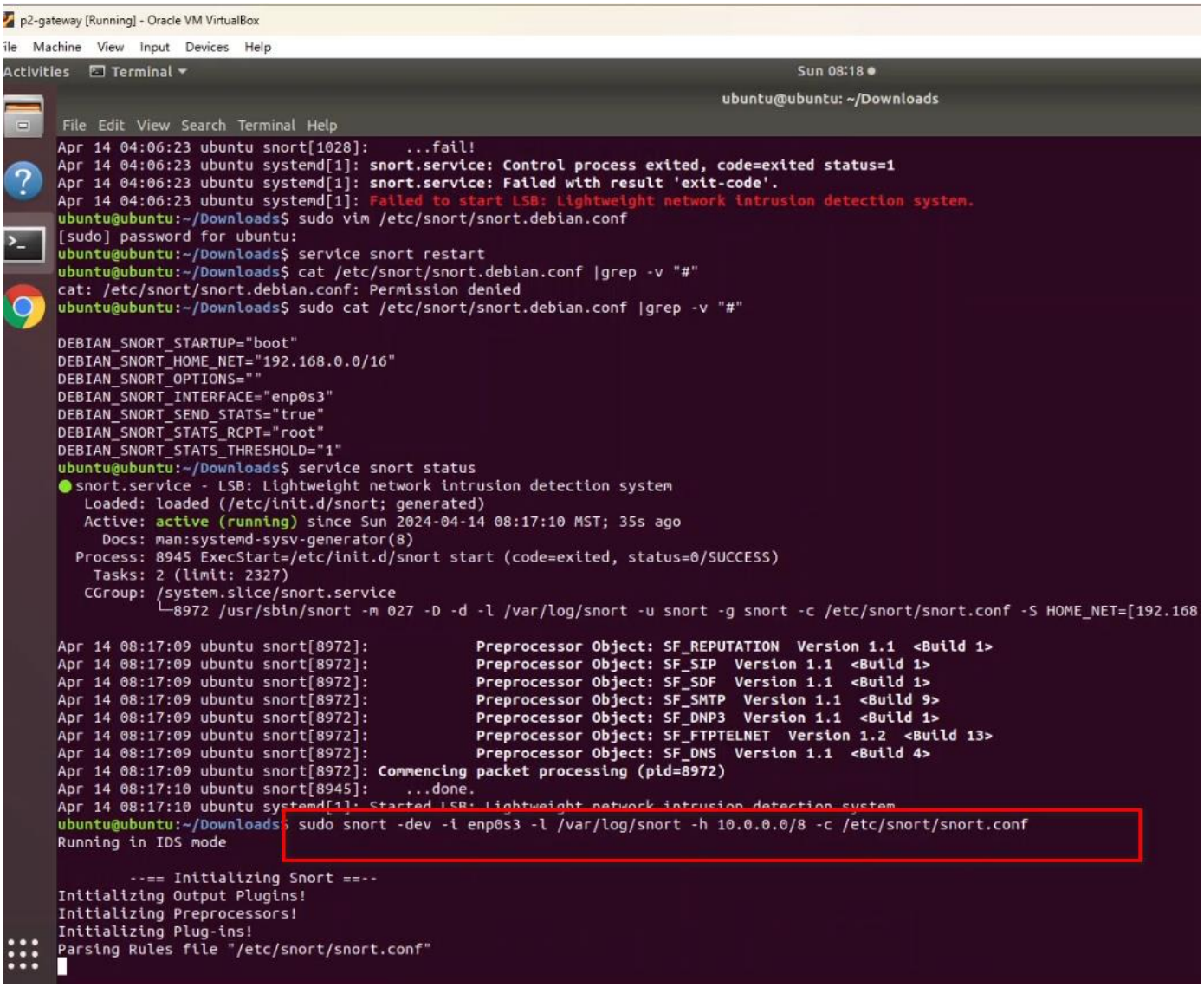
请编辑高亮部分 提交中或英文版本皆可.



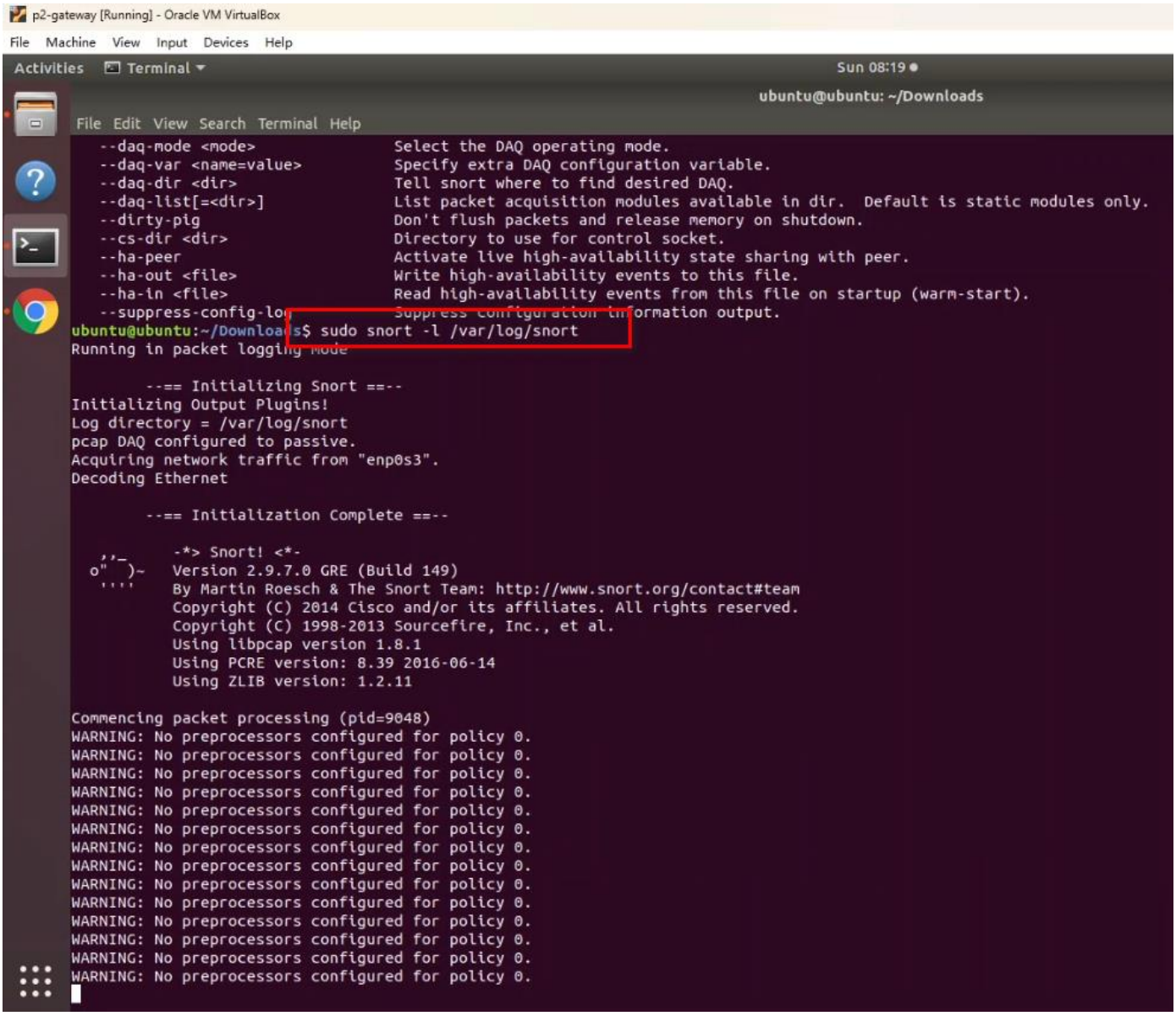
请编辑高亮部分 提交中或英文版本皆可.



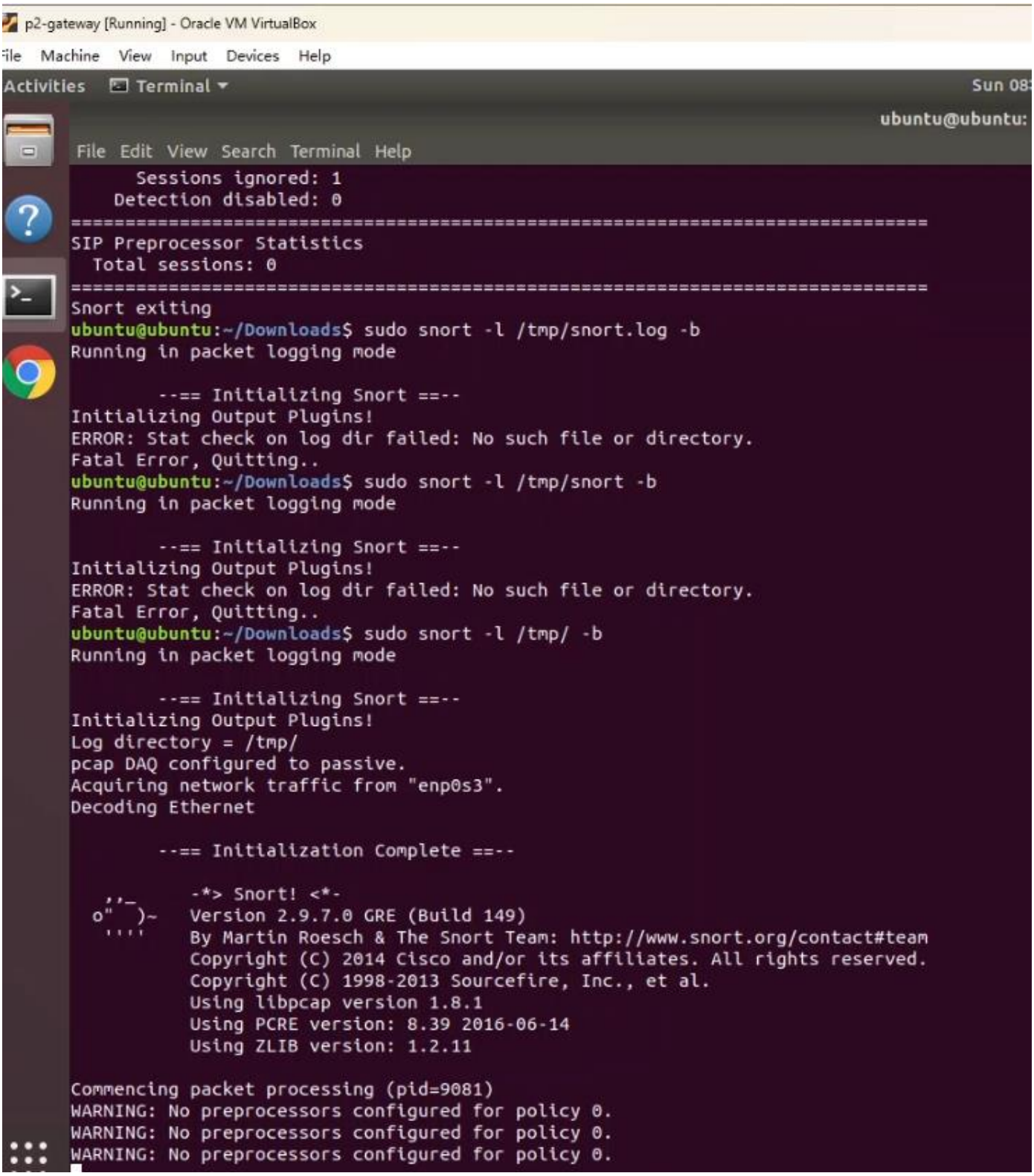
请编辑高亮部分 提交中或英文版本皆可.



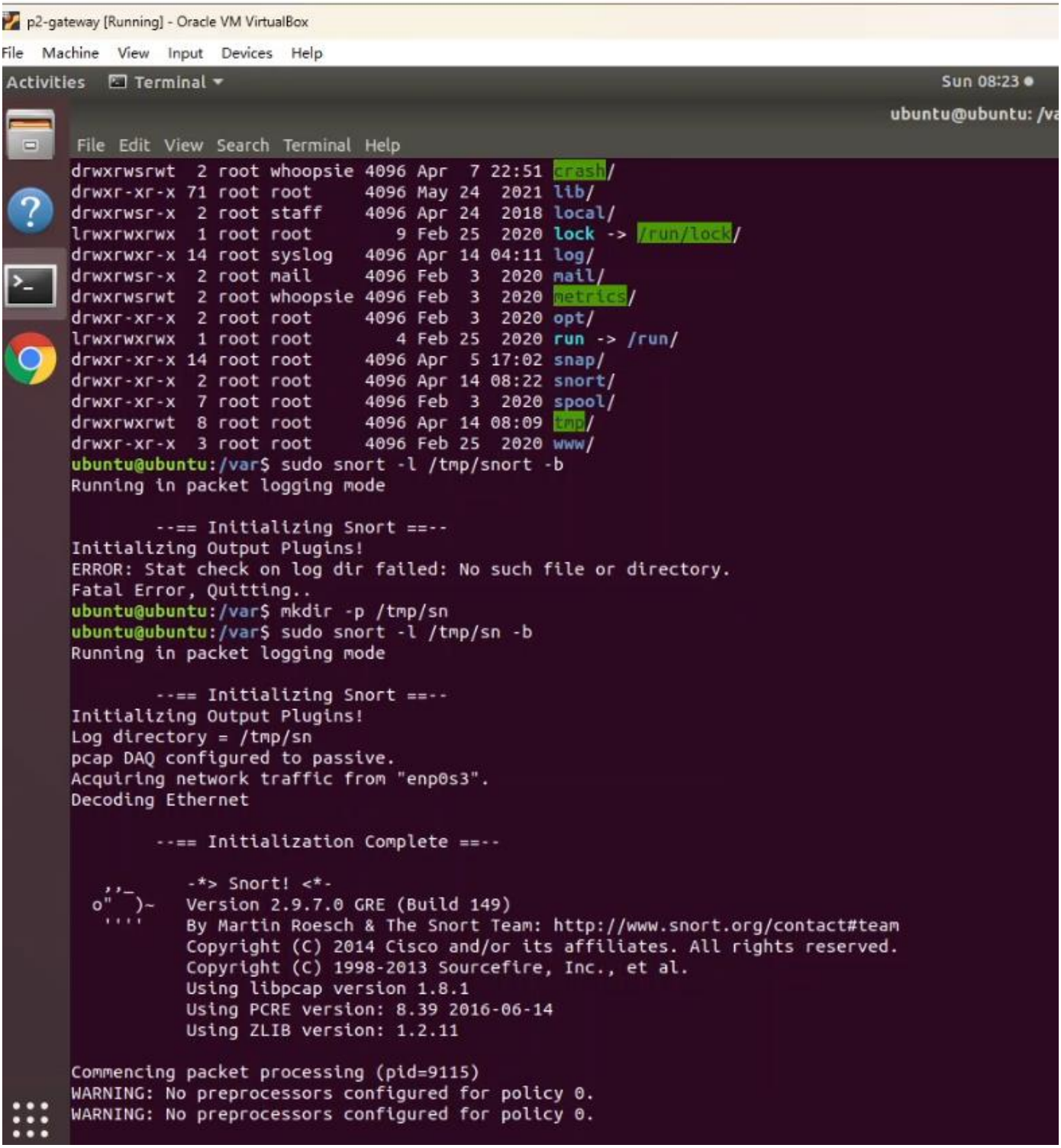
请编辑高亮部分 提交中或英文版本皆可.



请编辑高亮部分 提交中或英文版本皆可.

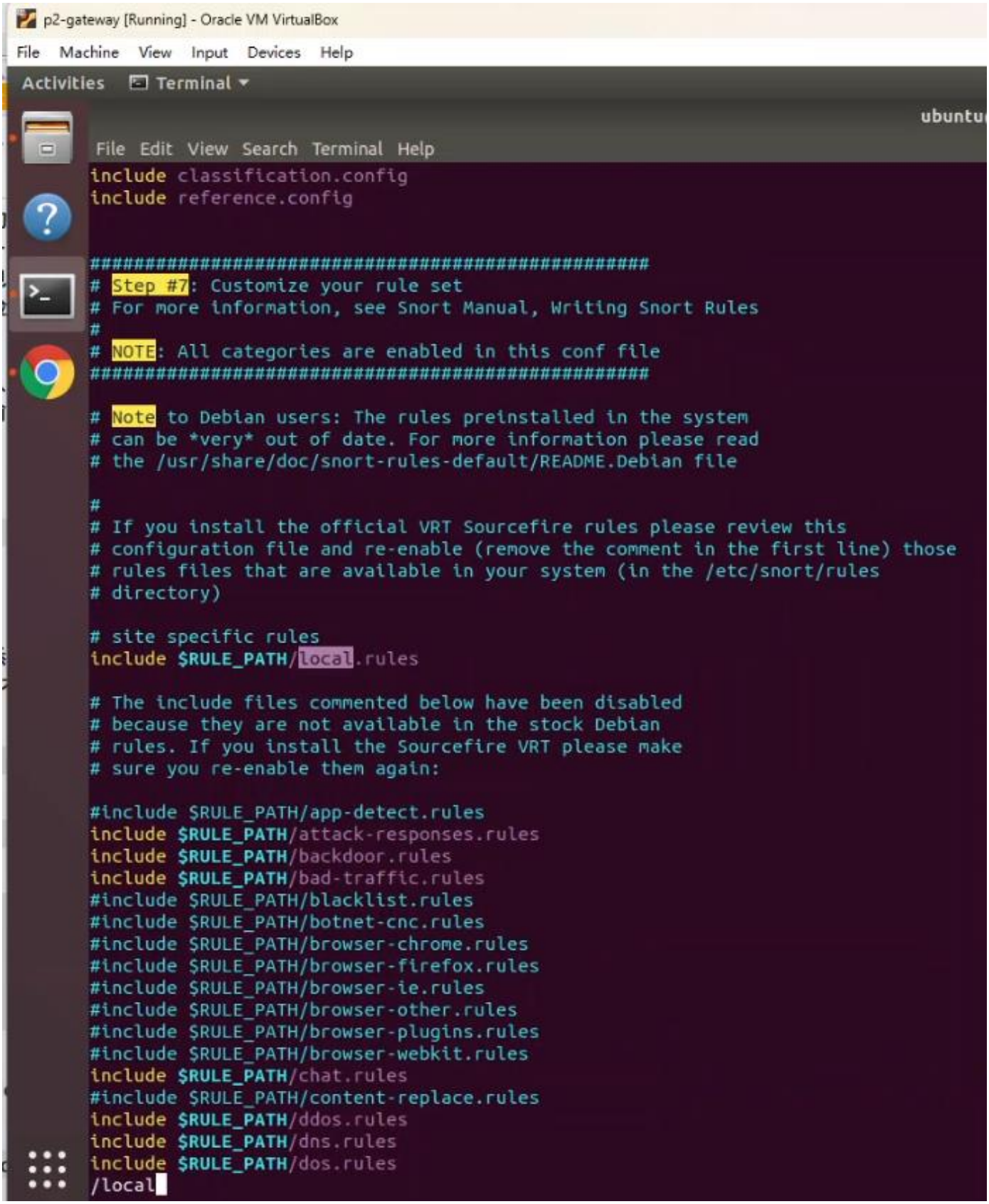


请编辑高亮部分 提交中或英文版本皆可.



3. 任务 3：创建并测试 Snort 规则 13

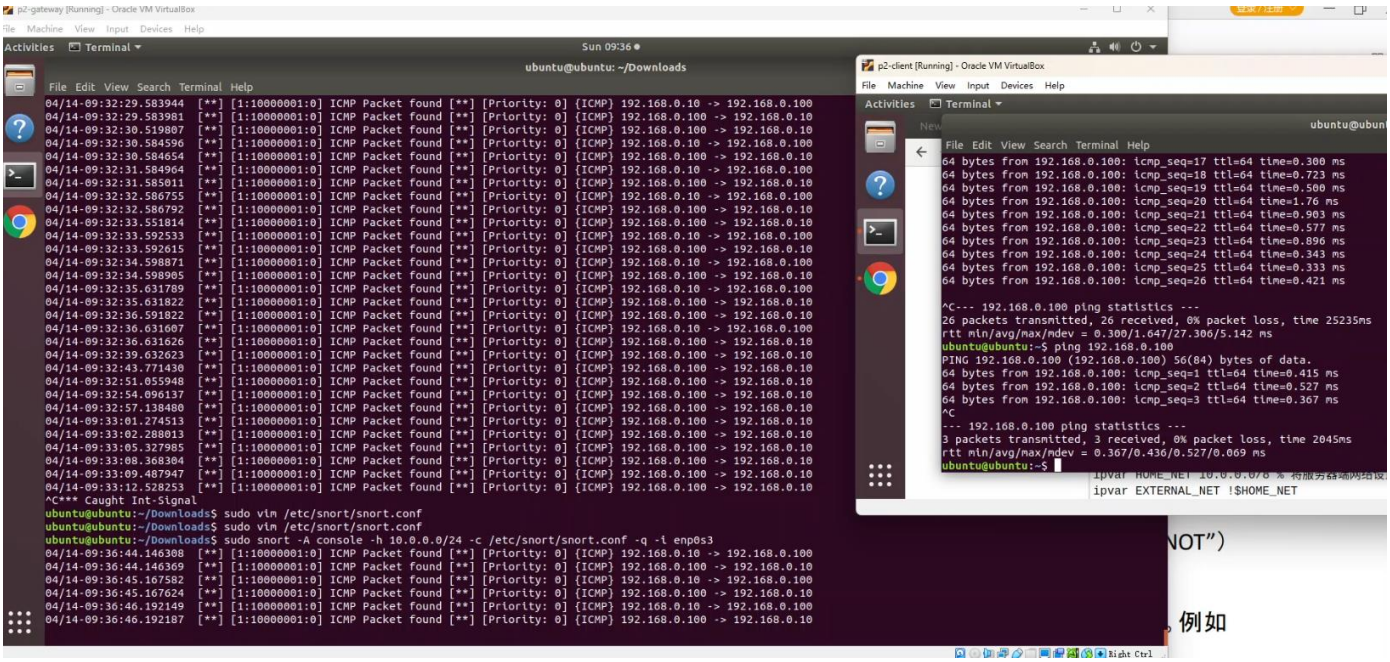
请编辑高亮部分 提交中或英文版本皆可.

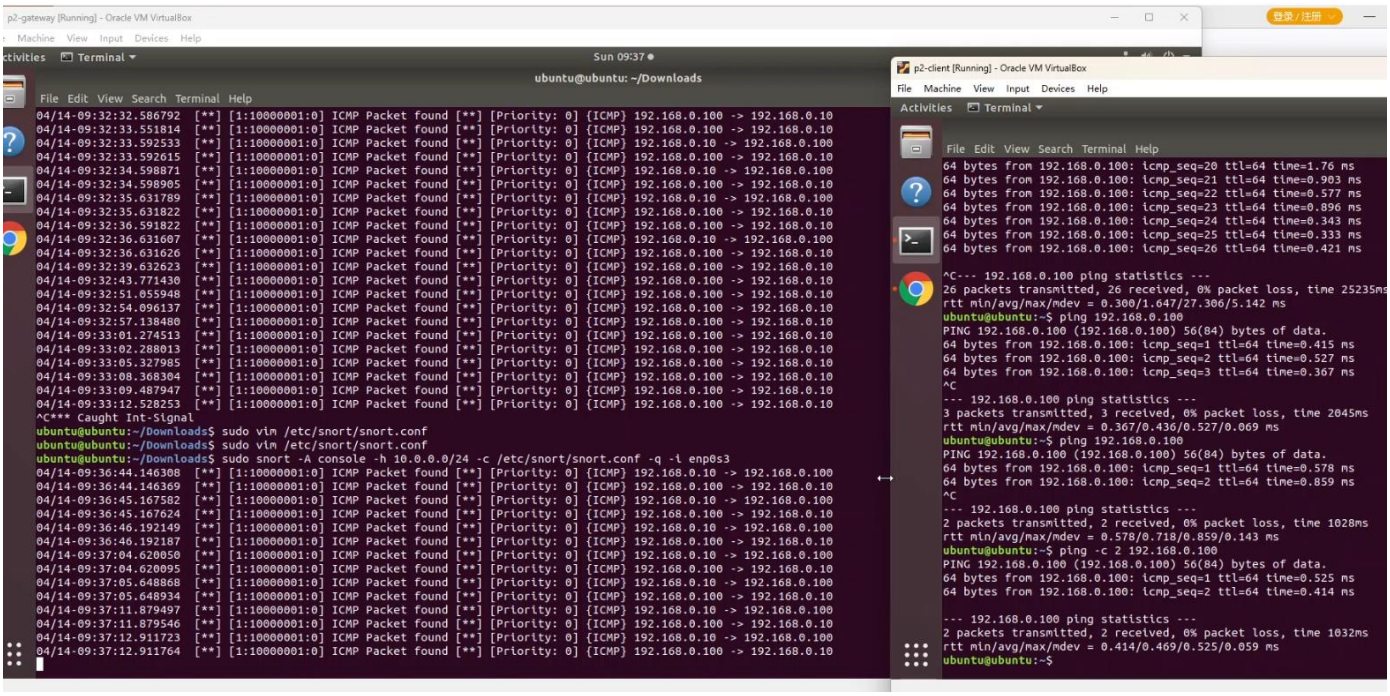


禁用除了 local.rule 以外的所有规则文件

3.1 任务 3.1 创建并测试 icmp 规则 13

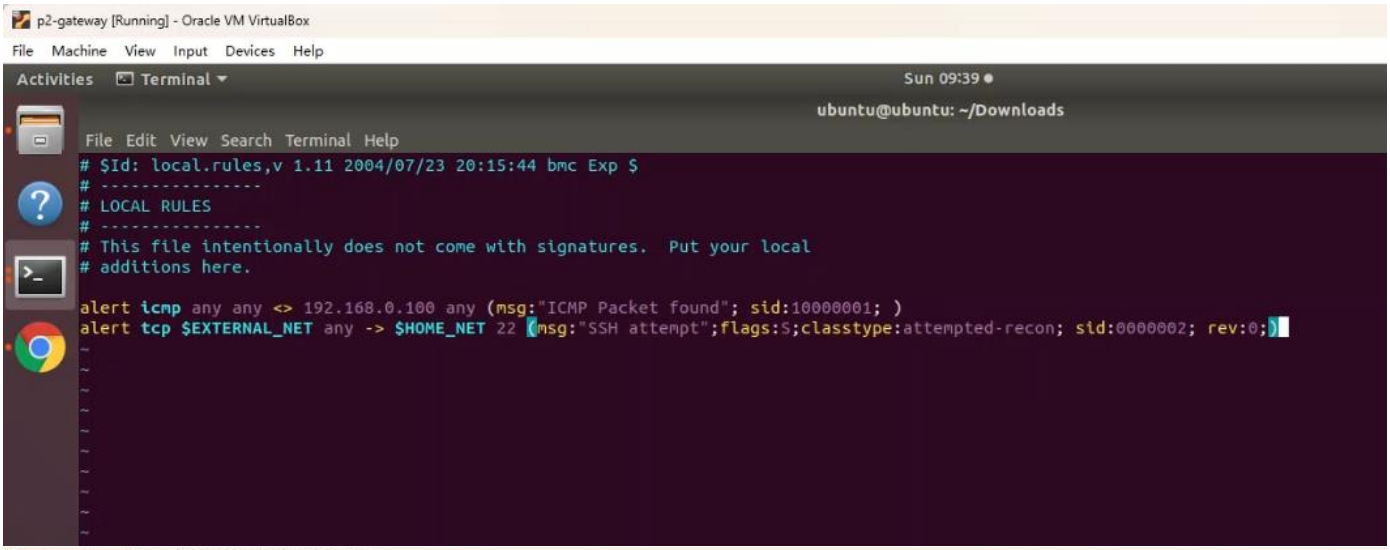
请编辑高亮部分 提交中或英文版本皆可.

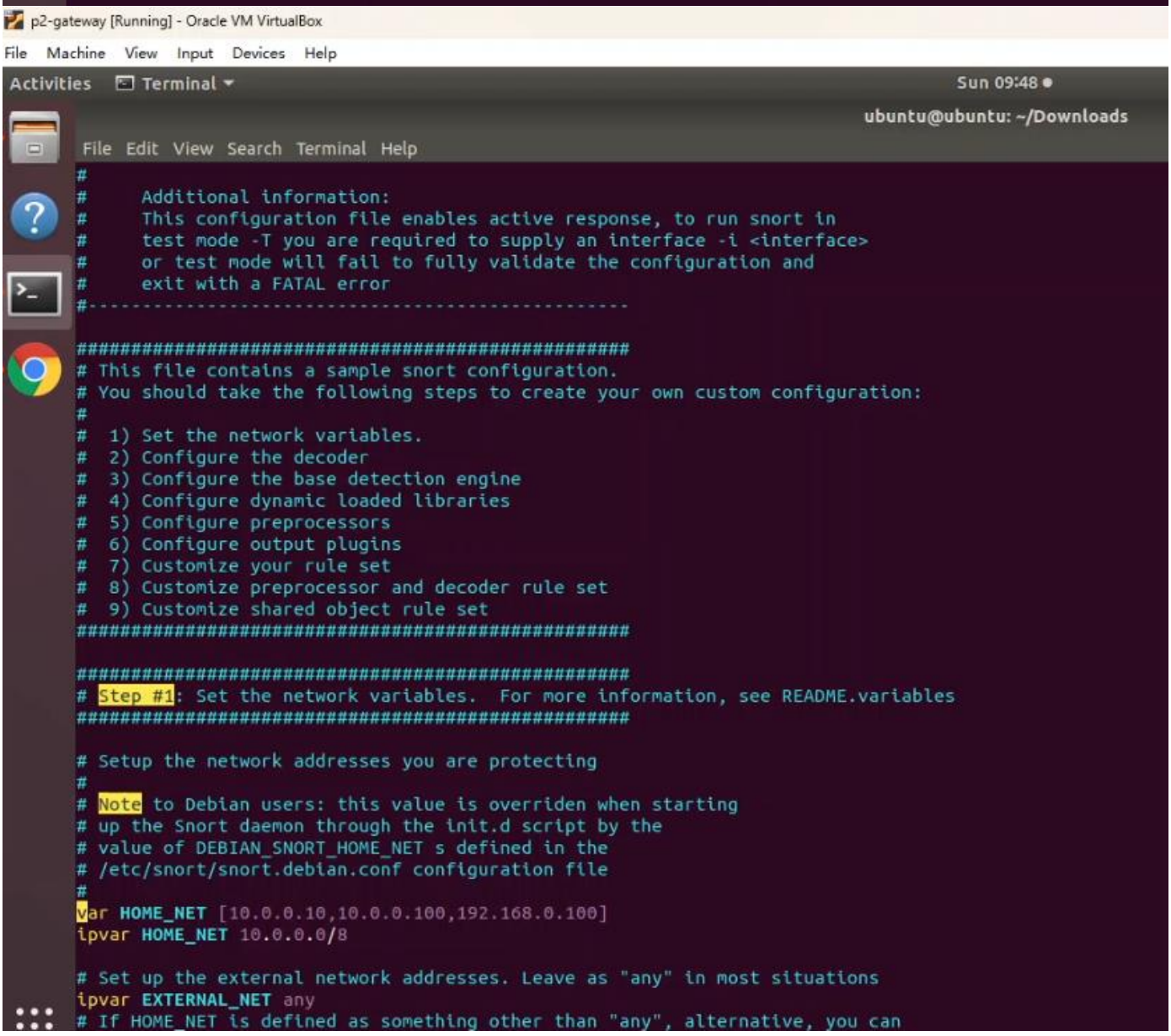




3.2 任务 3.2 用系统变量来创建和测试 snort 规则 14

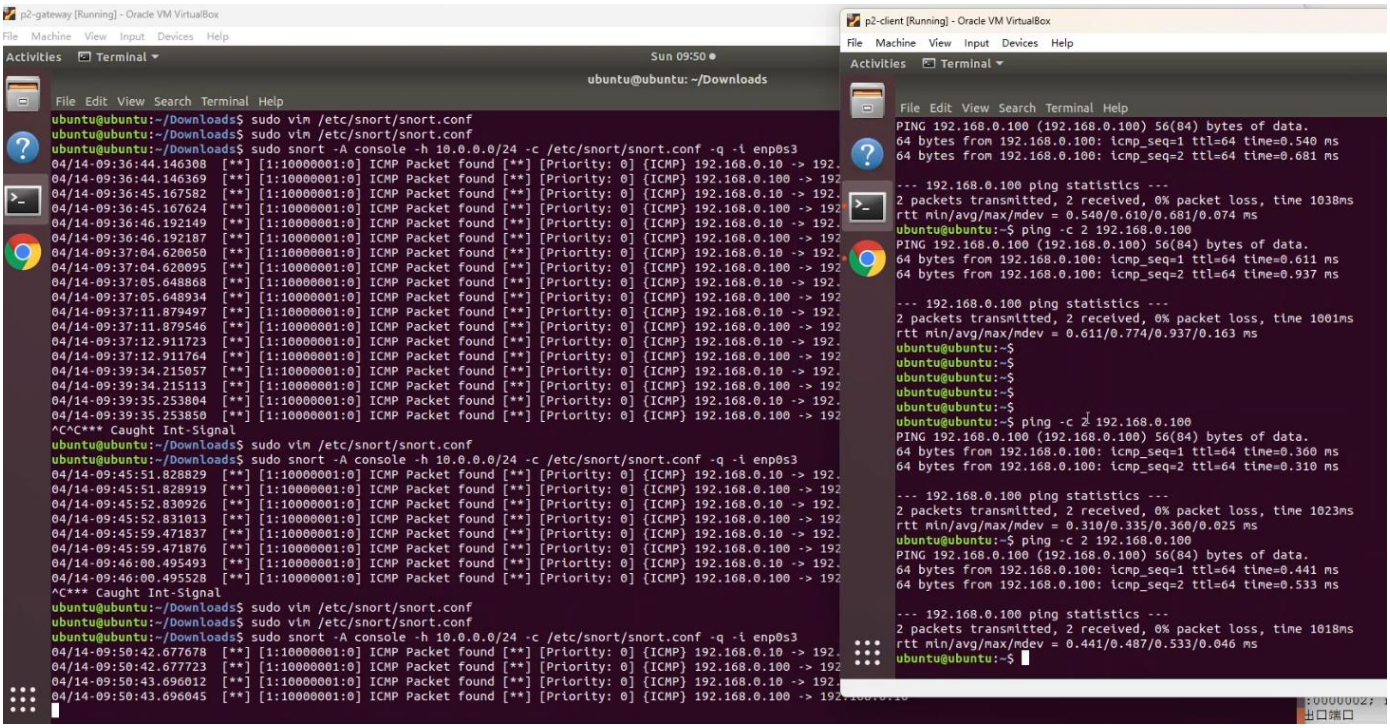
请编辑高亮部分 提交中或英文版本皆可.



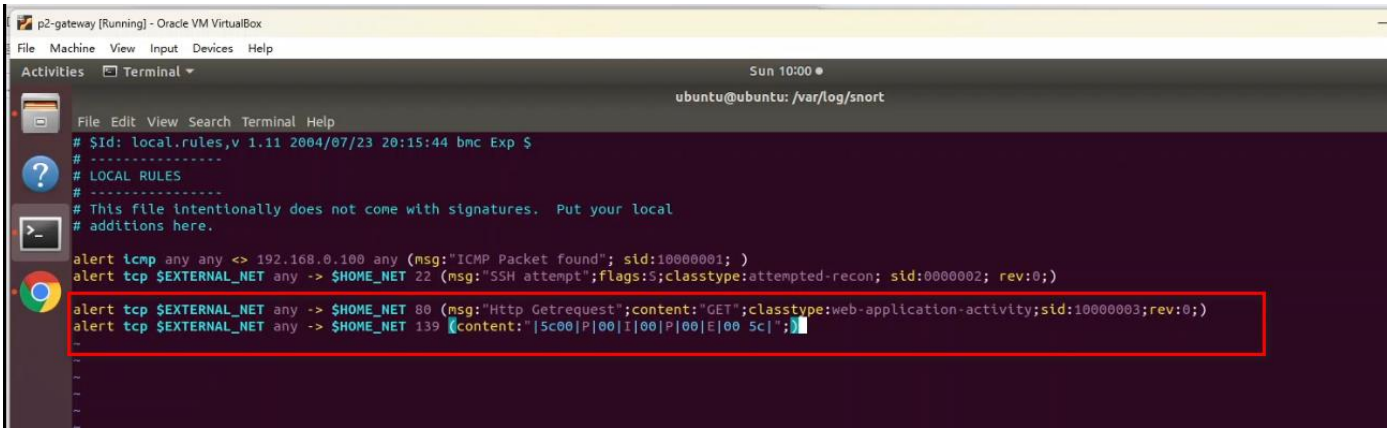


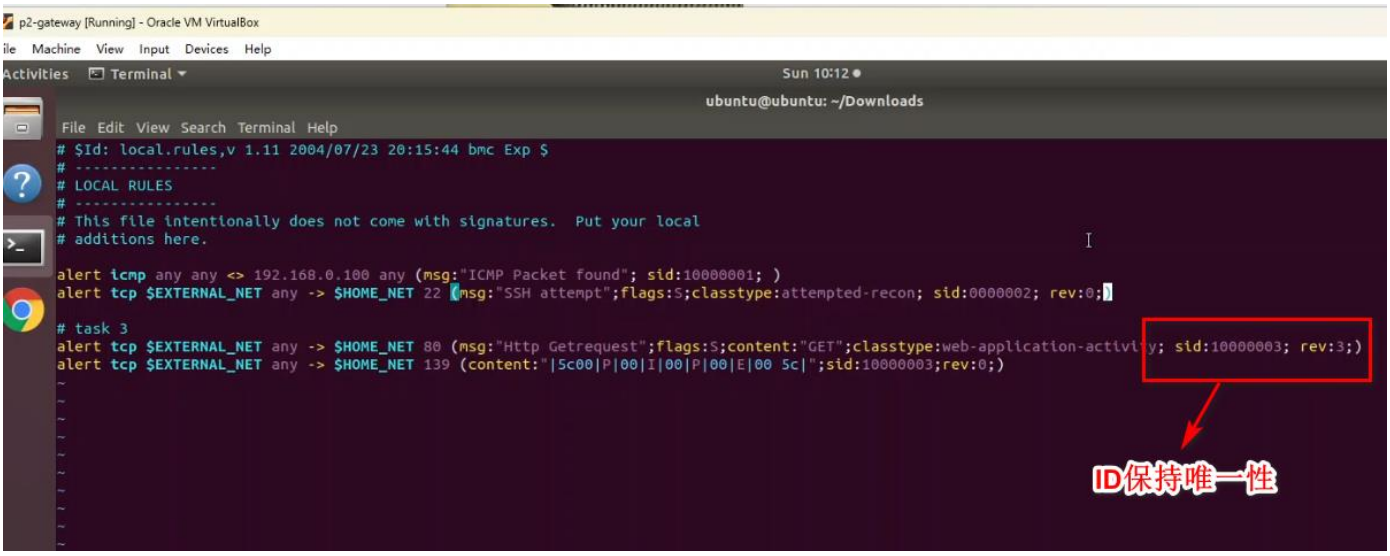
测试

请编辑高亮部分 提交中或英文版本皆可.

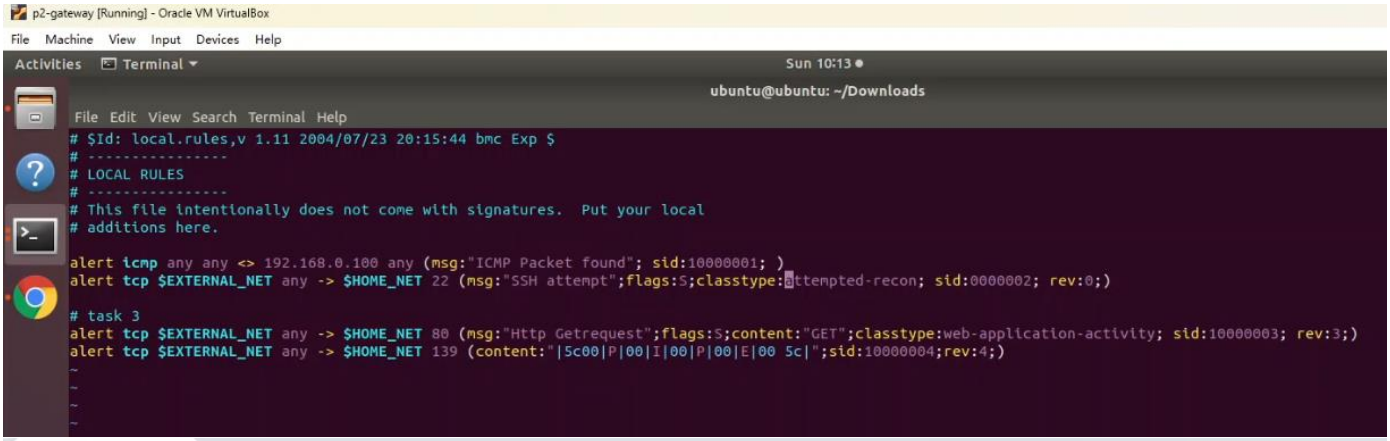


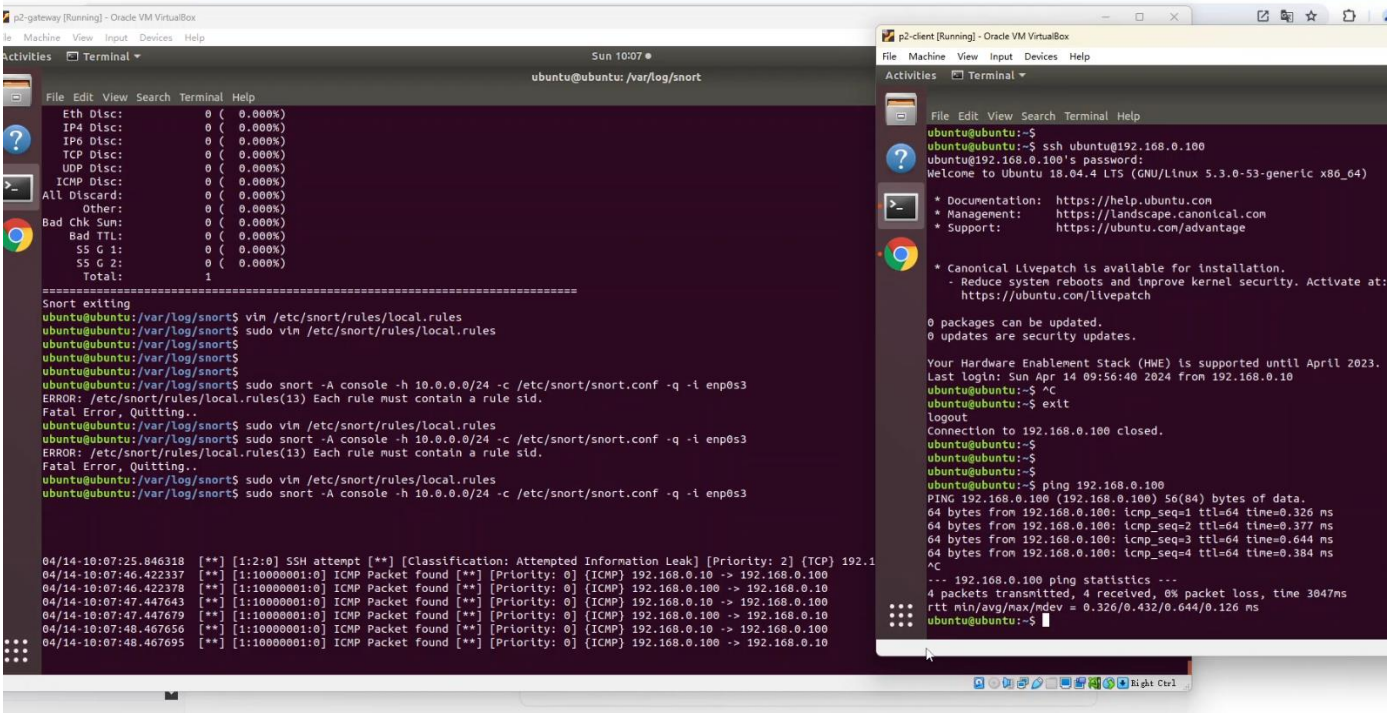
3.3 任务 3.3 用载荷规则选项来创建和测试 snort 规则 15



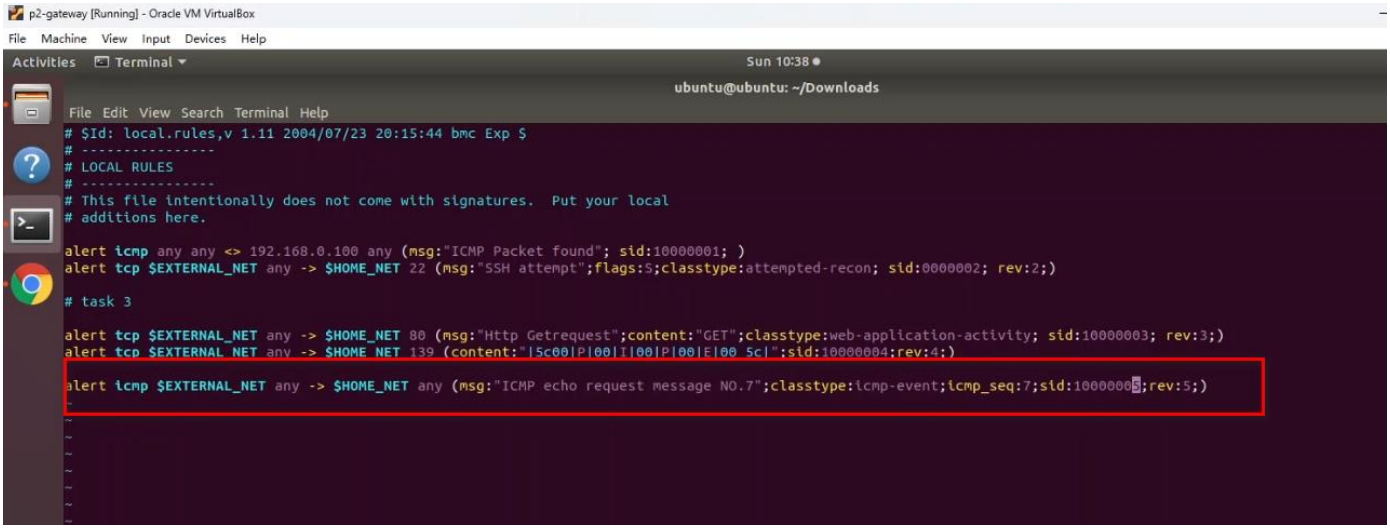


请编辑高亮部分 提交中或英文版本皆可.

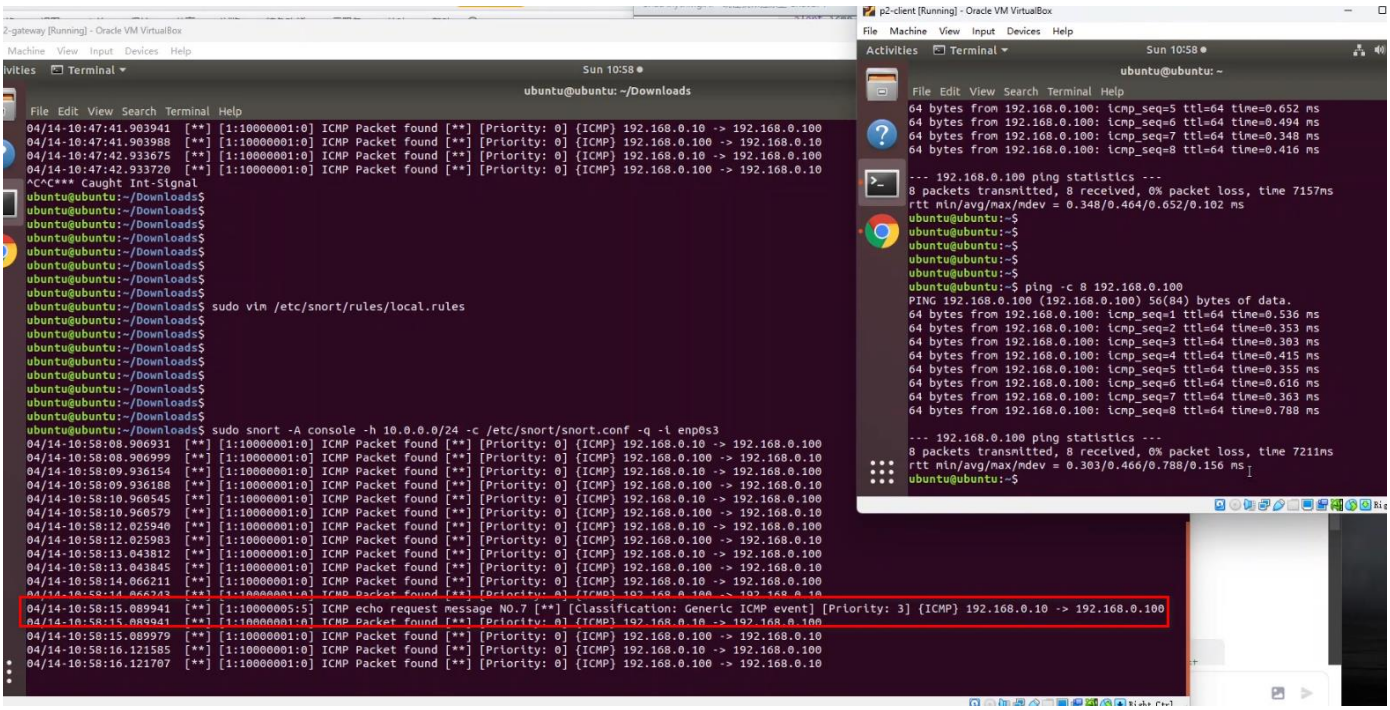


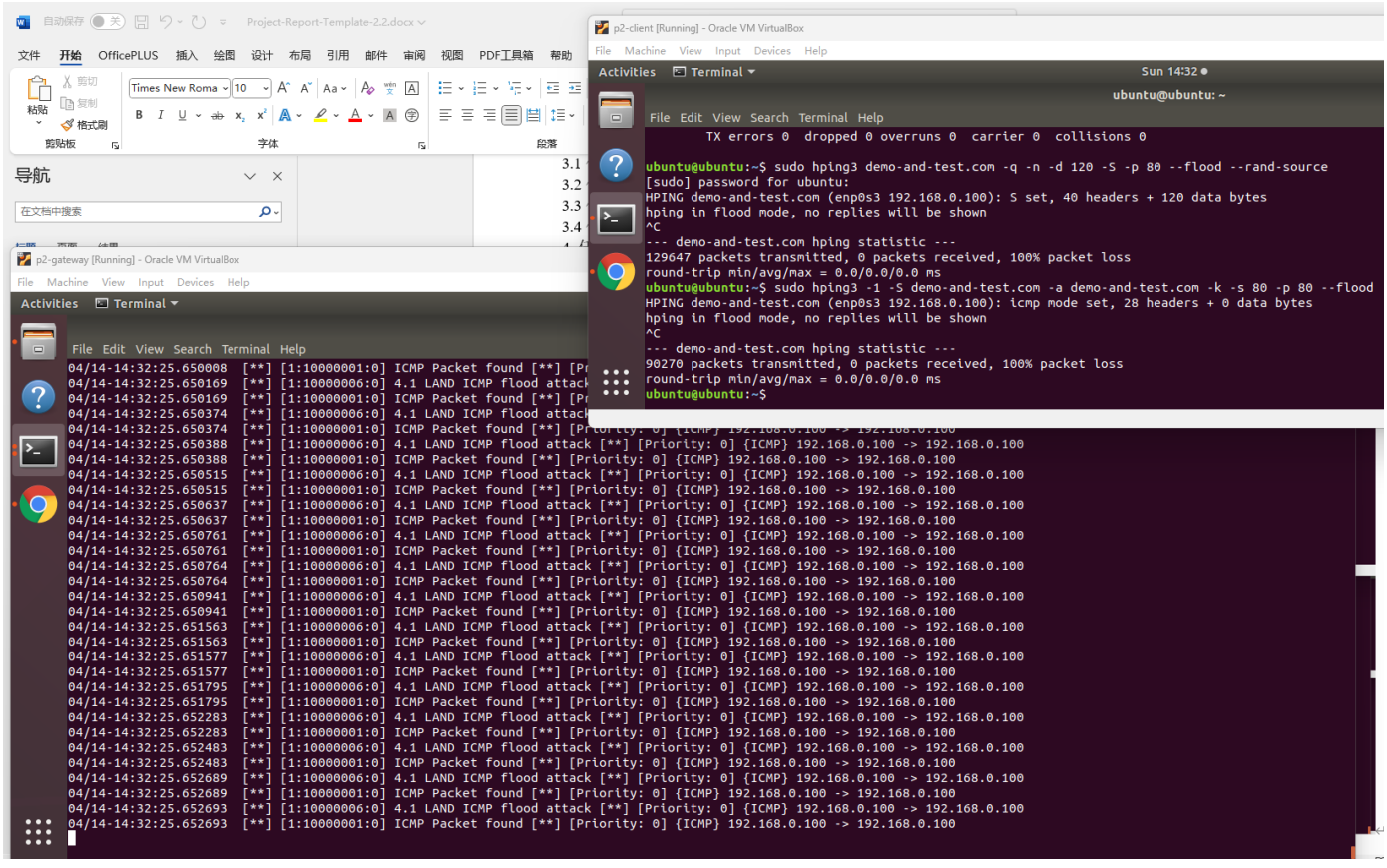


3.4 任务 3.4 用非载荷规则选项来创建和测试 snort 规则 16

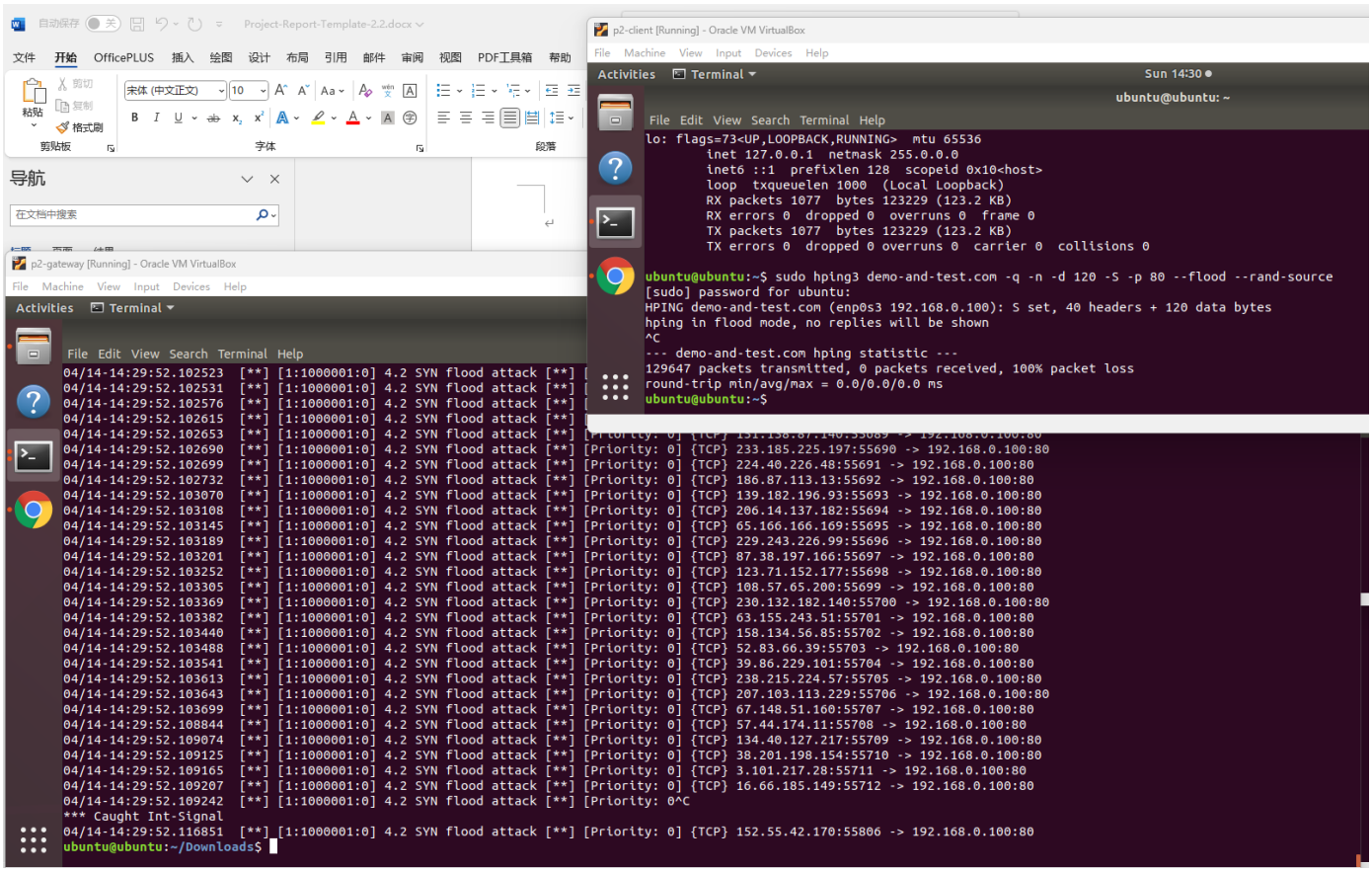


请编辑高亮部分 提交中或英文版本皆可.

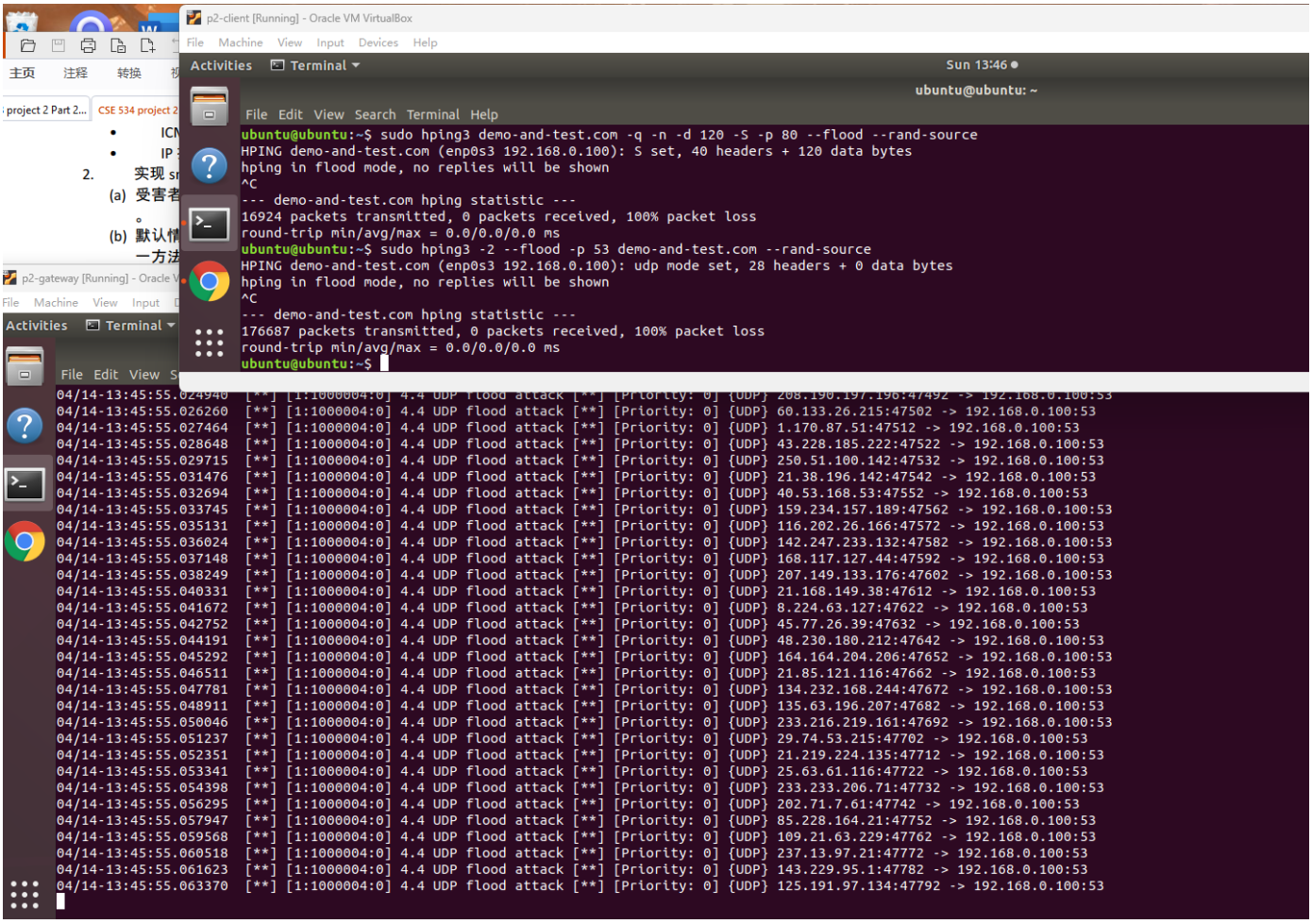




请编辑高亮部分 提交中或英文版本皆可.



请编辑高亮部分 提交中或英文版本皆可.



4.5 任务 4.5 端口扫描的部署与检测 19

总结：涉及的命令如下

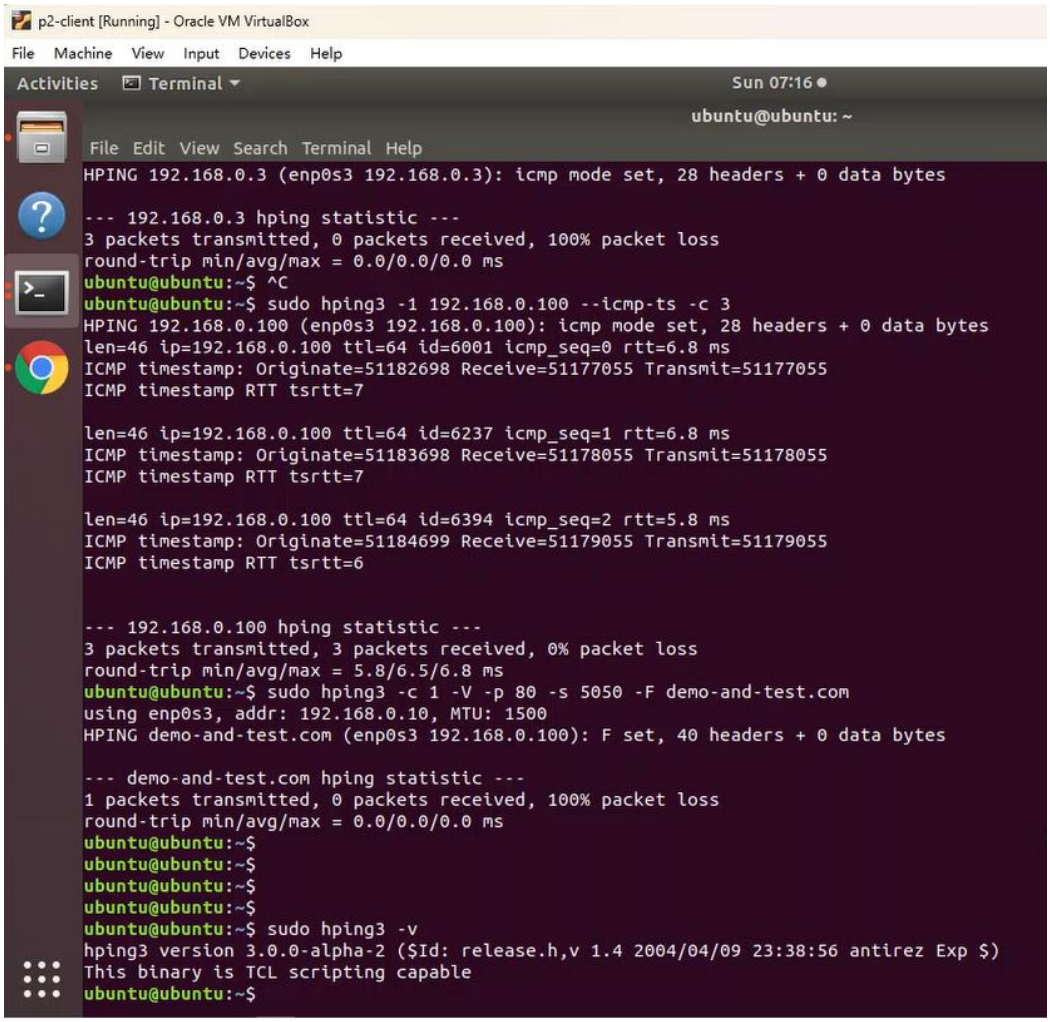
```
1.  service snort status
2.
3.  sudo vim /etc/snort/snort.debian.conf
4.
5.  sudo snort -dev -i enp0s3 -l /var/log/snort -h 10.0.0.0/8 -c /etc/snort/snort.conf
6.
7.  action protocol source port -> destination port (options)
8.
9.  sudo snort -l /var/log/snort
10.
11. sudo snort -A console -c /etc/snort/snort.conf
12.
13. sudo snort -l /tmp/sn -b
14. sudo snort [-d|e] -r /tmp/sn/snort.log.1713108188 [tcp|udp|icmp]
15. true cmd: sudo snort -d -r /tmp/sn/snort.log.1713108188 tcp
16. true cmd: sudo snort -e -r /tmp/sn/snort.log.1713108188 udp
17.
18. sudo file /var/log/snort/snort.log
19. true cmd: sudo file /tmp/sn/snort.log.1713108188
20.
21. sudo snort -c /etc/snort/snort.conf -l /var/log/snort -h 10.0.0.0/8 -s
22.
23. 任务 3：创建并测试 Snort 规则
24.
```

请编辑高亮部分 提交中或英文版本皆可.

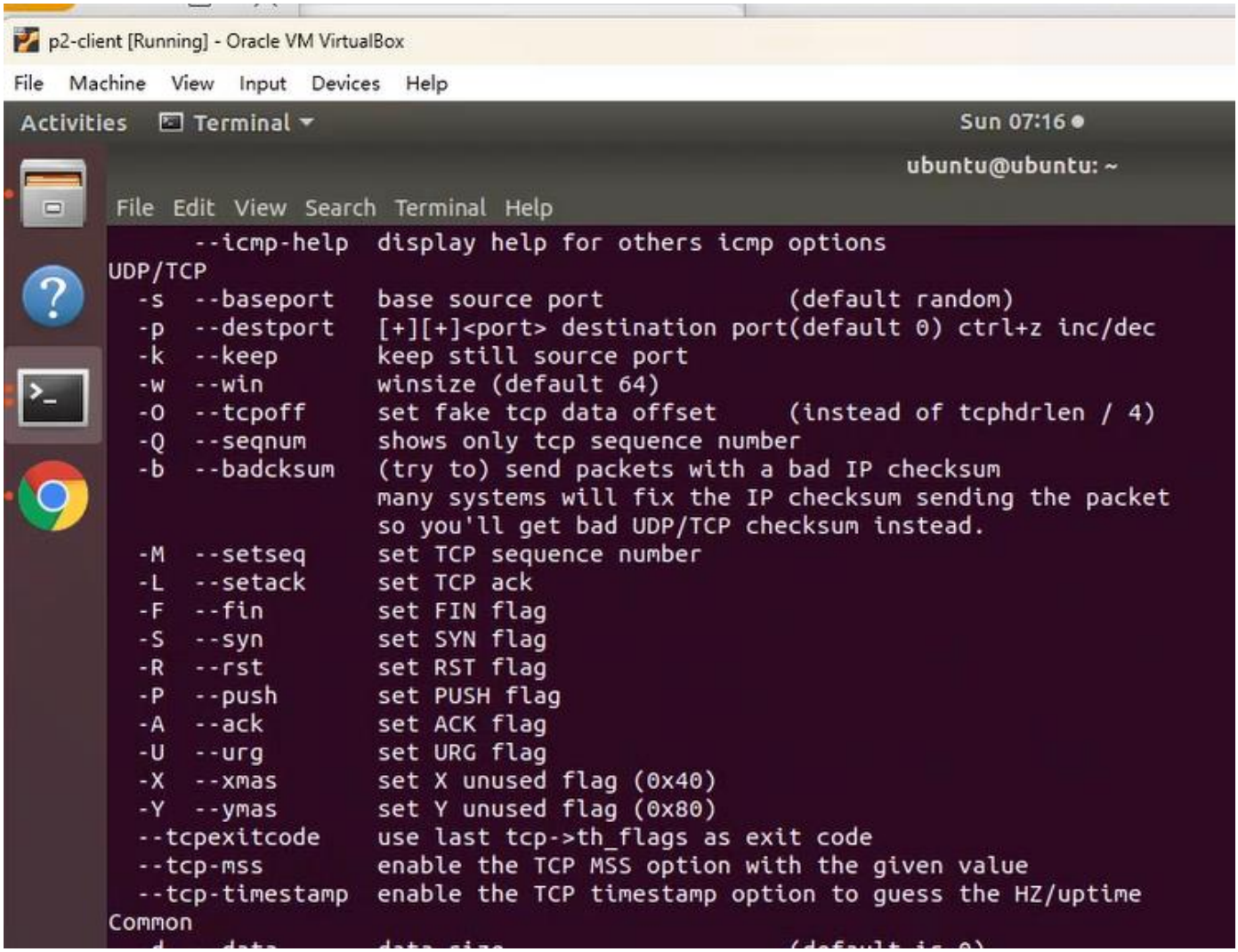
```
cd /etc/snort/
sudo cp snort.conf snort.backup.conf
bak cmd: sudo cp snort.backup.conf snort.conf
sudo vim /etc/snort/snort.conf
sudo sed -i ’s/include \$RULE_PATH/#include \$RULE_PATH/’ /etc/snort/snort.conf
true cmd: sudo sed -
i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf
sudo vim  /etc/snort/rules/local.rules

alert icmp any any <> 192.168.0.100 any (msg:"ICMP Packet found"; sid:10000001; )

sudo snort -A console -c /etc/snort/snort.conf -q -i enp0s3

3.2 任务 3.2 用系统变量来创建和测试 snort 规则

sudo vim /etc/snort/snort.conf

ipvar HOME_NET 10.0.0.0/8 % 将服务器端网络设置为 HOME_NET
ipvar EXTERNAL_NET !$HOME_NET

sudo snort -A console -h 10.0.0.0/24 -c /etc/snort/snort.conf -q -i enp0s3

vim /etc/snort/rules/local.rules

alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SSH attempt";flags:S;classtype:attempted
-recon; sid:0000002; rev:0;)
sudo snort -c /etc/snort/snort.conf -l /var/log/snort -b -q -i enp0s8 % 在本示例中，
enp0s8 是防火墙后面的出口端口


sudo snort -d -r /var/log/snort/snort.log.1713113771 tcp

任务 3.3 用载荷规则选项来创建和测试 snort 规则

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Http Getrequest";content:"GET";classtype
:web-application-activity;sid:10000003;rev:0;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (content:"|5c00|P|00|I|00|P|00|E|00 5c|";sid:
10000004;rev:1;)

$ curl 10.0.0.10 % 你可以直接访问 IP 地址并运行：curl http://10.0.0.10

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP echo request message NO.7";classt
ype:icmp-event;icmp_seq:7;sid:10000004;rev:0;)

ping -c 8 192.168.0.10


test4:
sudo vim /etc/s-nort/snort.conf
sudo vim /etc/snort/rules/local.rules
sudo vim /etc/sysctl.conf

$ sudo echo 0 >/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts % 启用对广播请求的临时响应
$ sudo sysctl net.ipv4.icmp_echo_ignore_broadcasts 0

sudo vim /etc/sysctl
net.ipv4.icmp_echo_ignore_broadcasts=0 % 你可能需要重新启动节点
```

在客户端上完成如下任务

请编辑高亮部分 提交中或英文版本皆可.

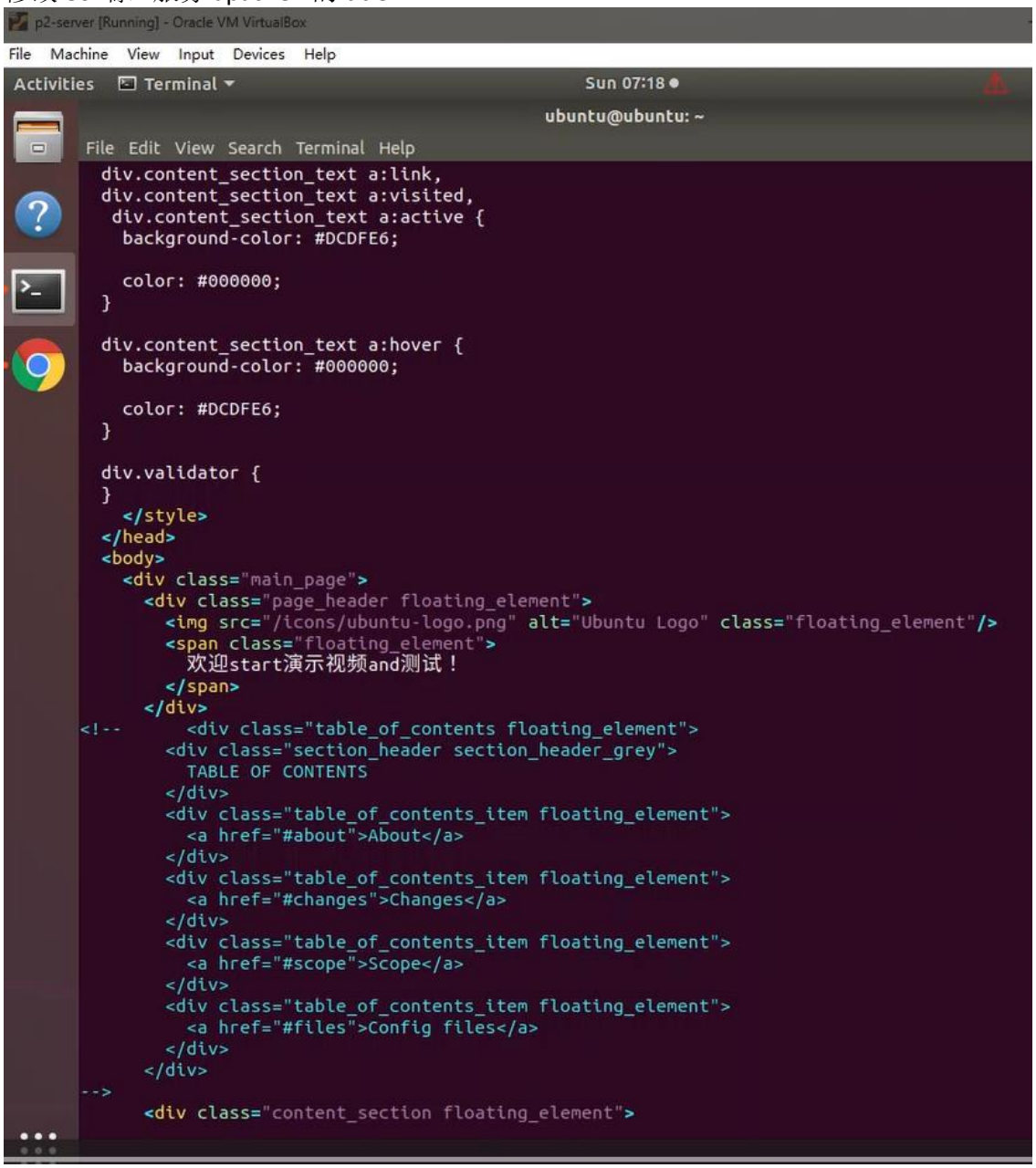


请编辑高亮部分 提交中或英文版本皆可.



请编辑高亮部分 提交中或英文版本皆可.

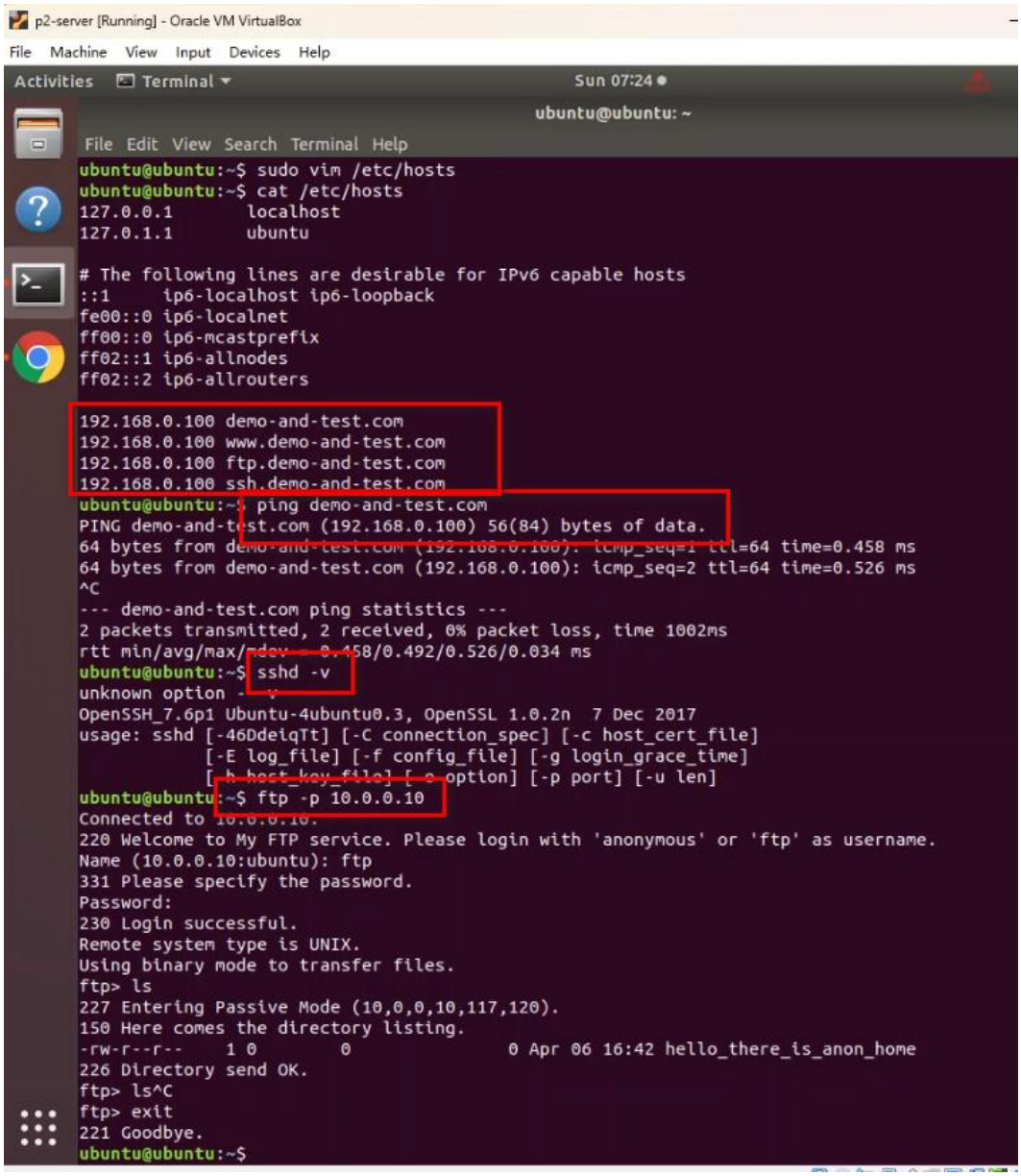
修改 80 端口服务 apache2 的 title



请编辑高亮部分 提交中或英文版本皆可.

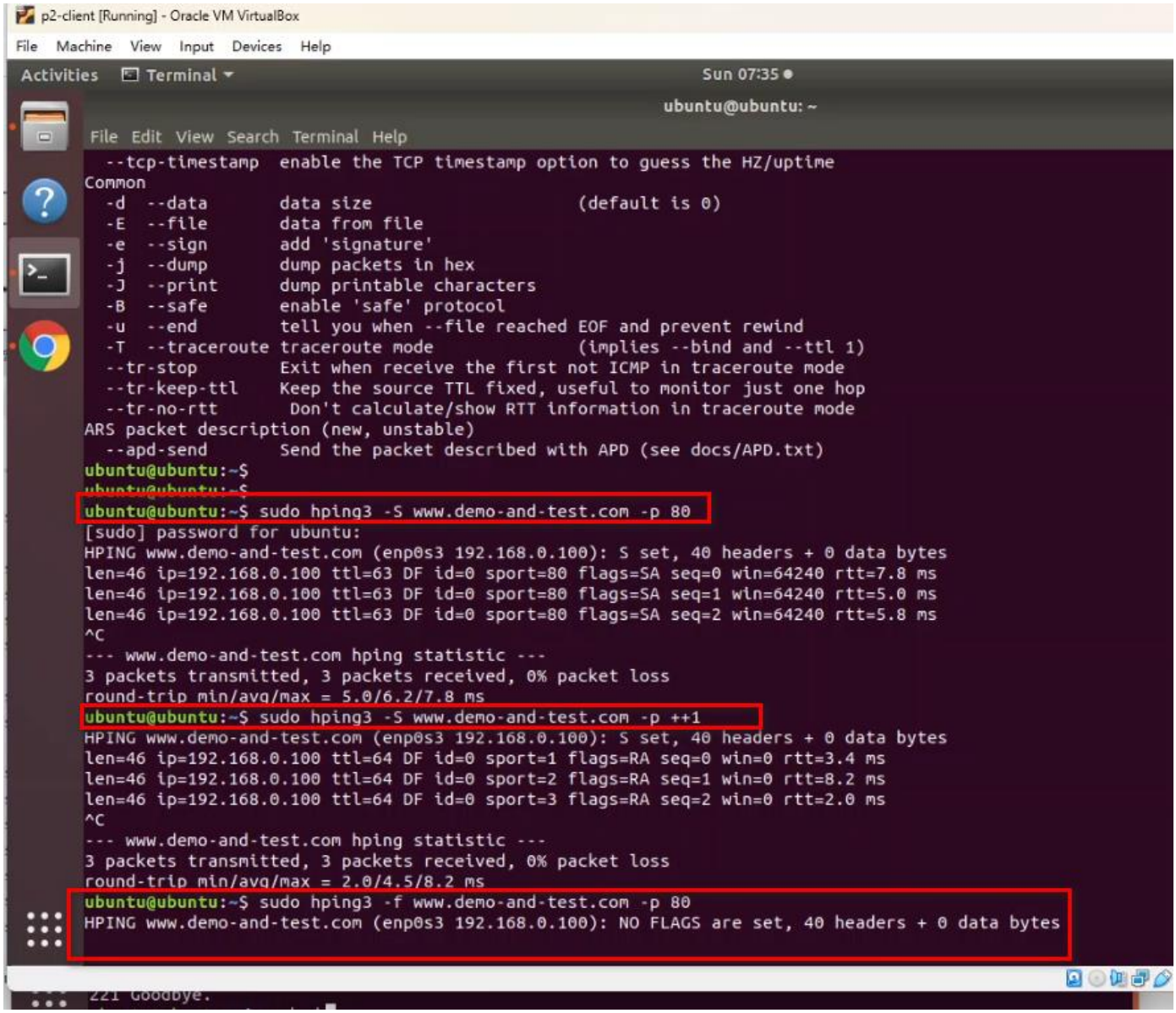
ftp 服务器的配置，启用被动端口

请编辑高亮部分 提交中或英文版本皆可.



2.2 使用 hping3 生成 TCP 测试流量 10

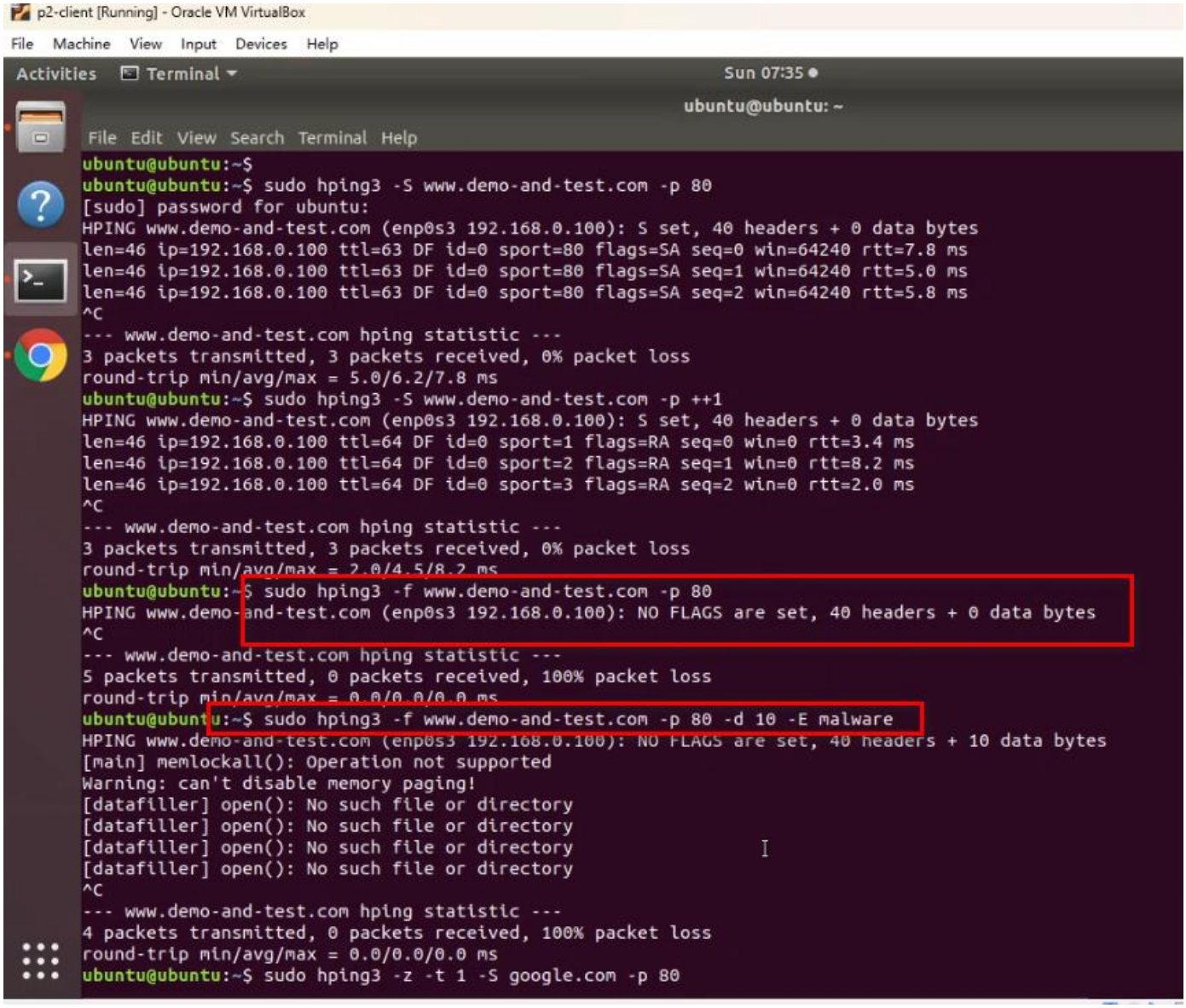
请编辑高亮部分 提交中或英文版本皆可.



2.3 使用 hping3 发送分片数据包 10

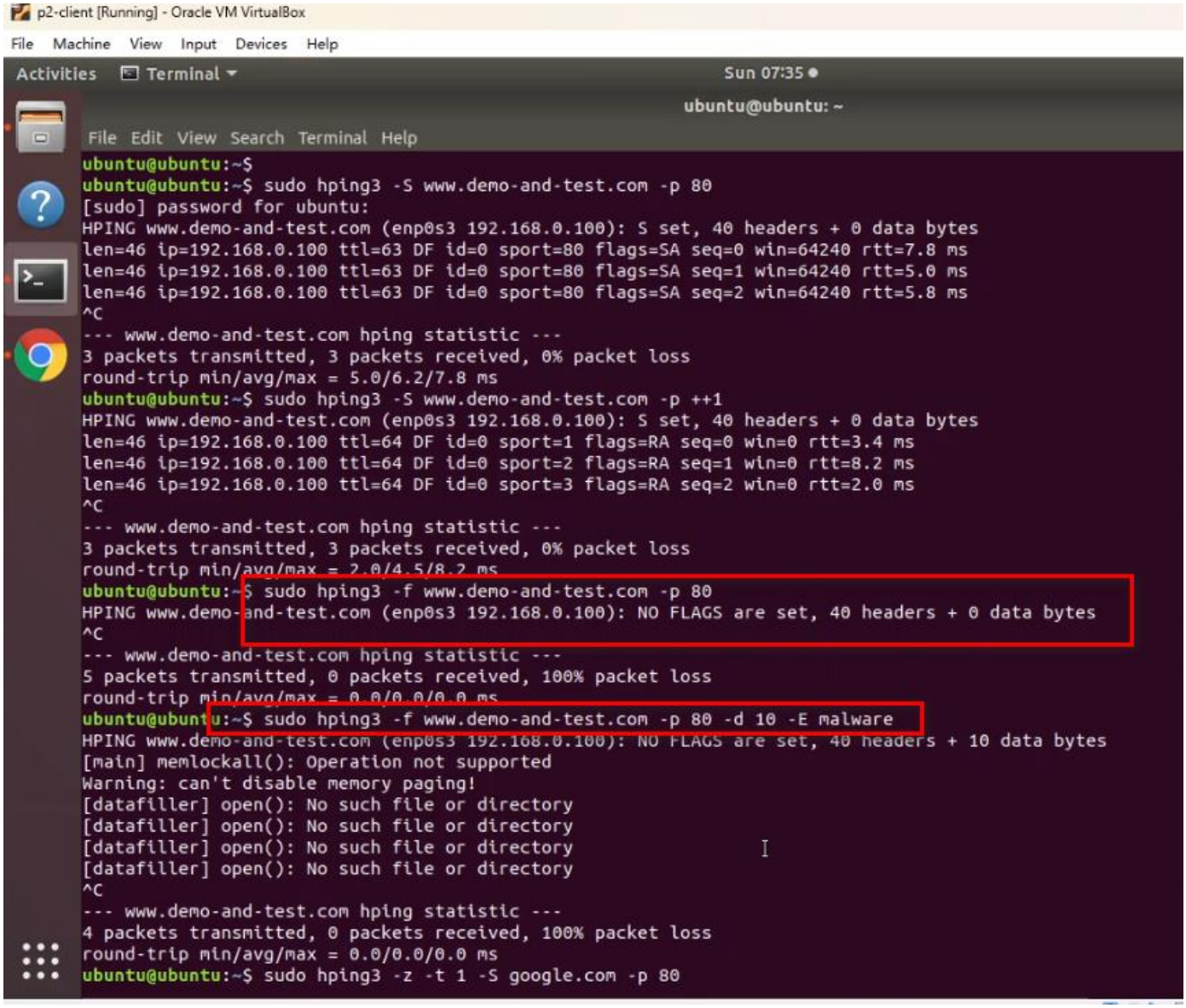
执行这条命令失败了

请编辑高亮部分 提交中或英文版本皆可.



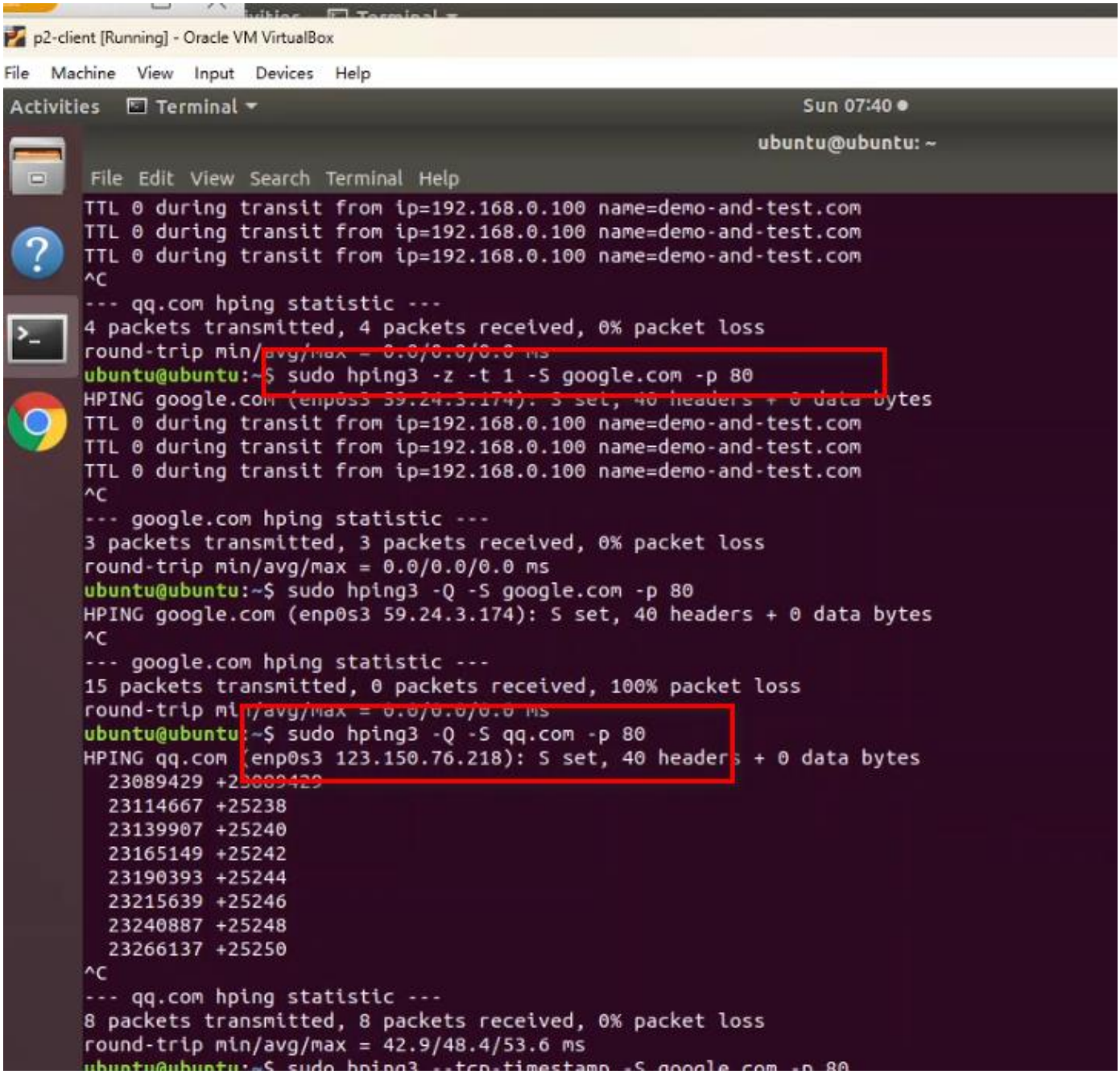
2.4 使用 hping3 发送数据 11

请编辑高亮部分 提交中或英文版本皆可.



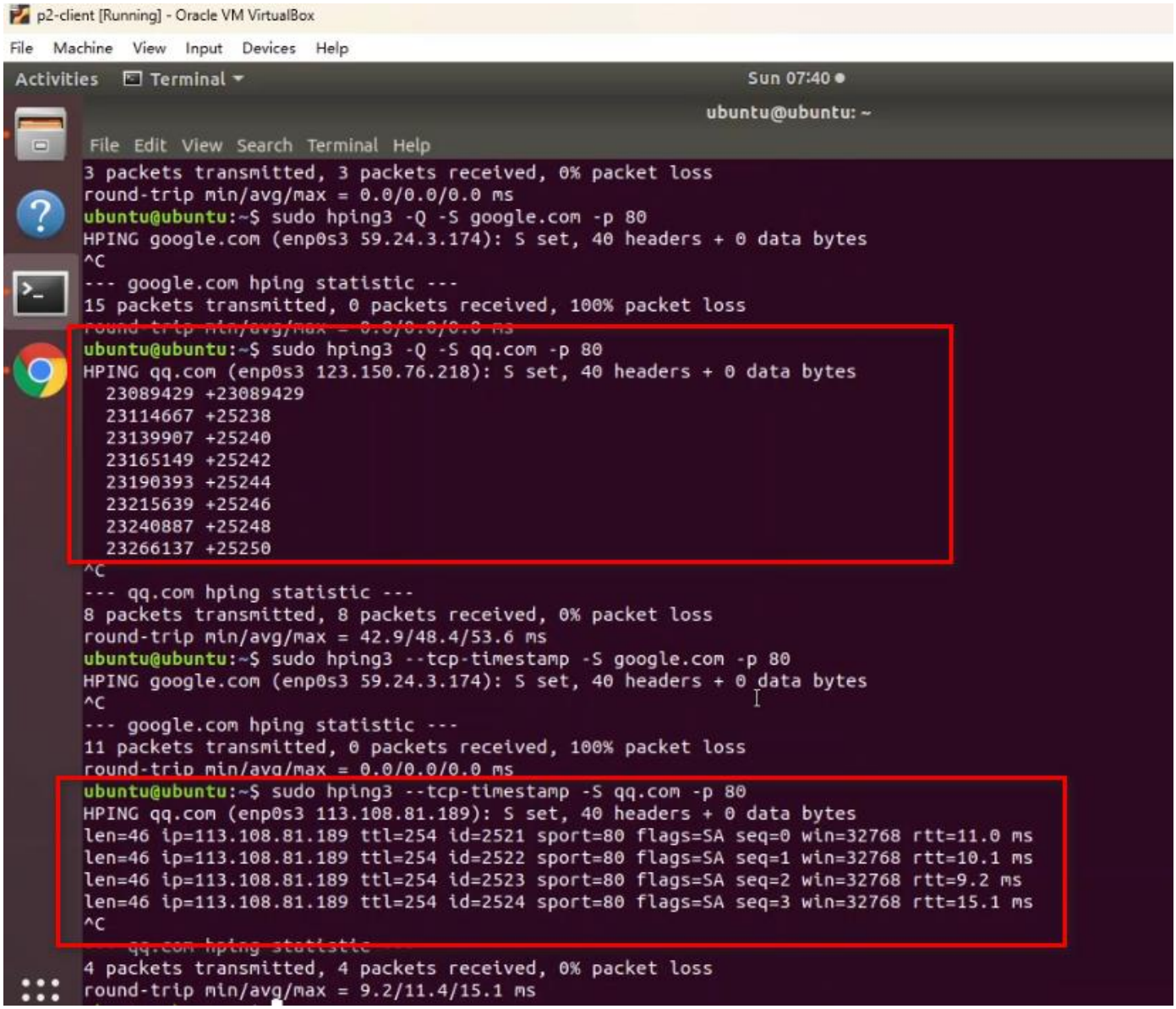
2.5 使用 hping3 进行网络诊断 11

请编辑高亮部分 提交中或英文版本皆可.



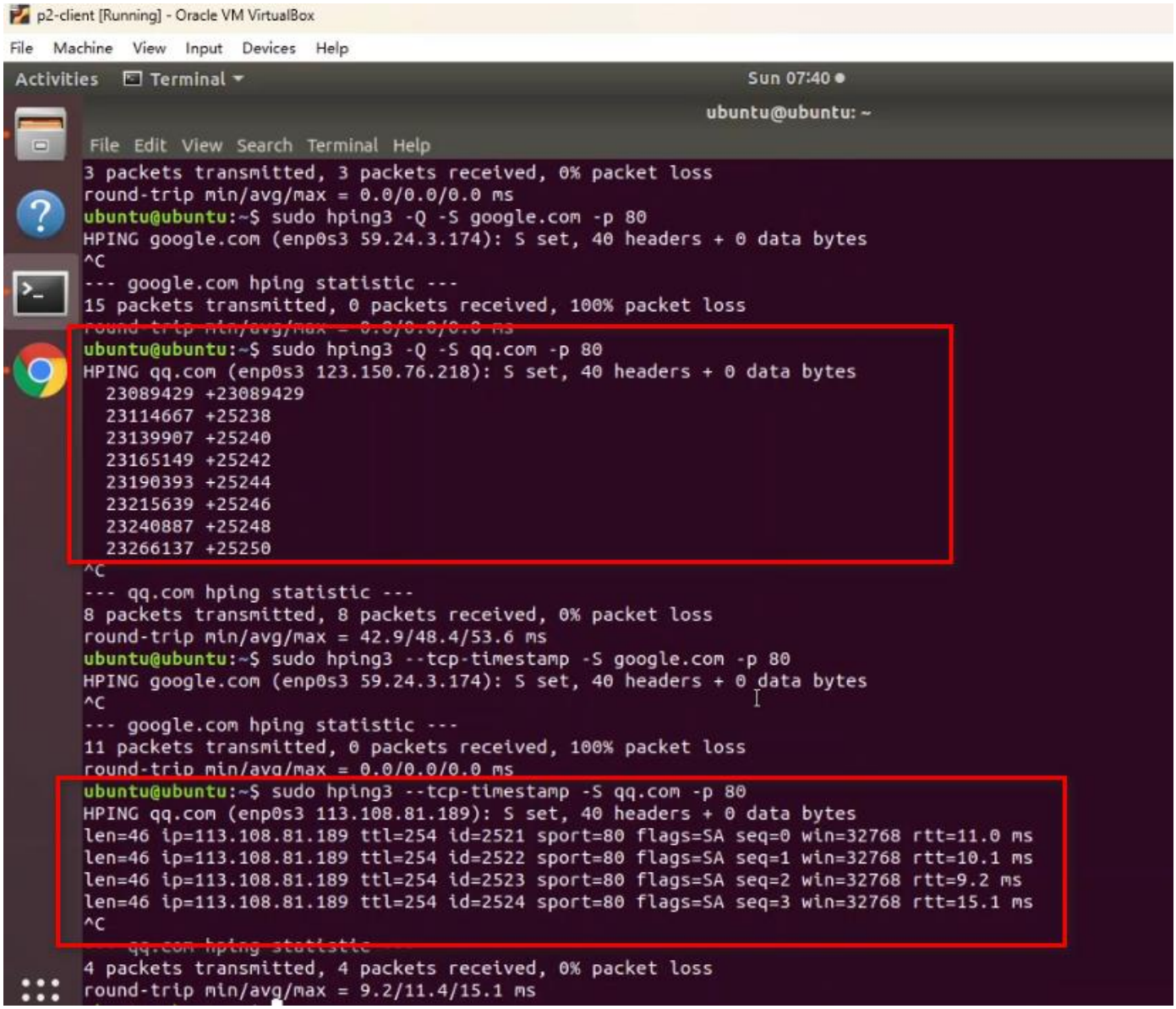
2.6 使用 hping3 预测序列号 12

请编辑高亮部分 提交中或英文版本皆可.

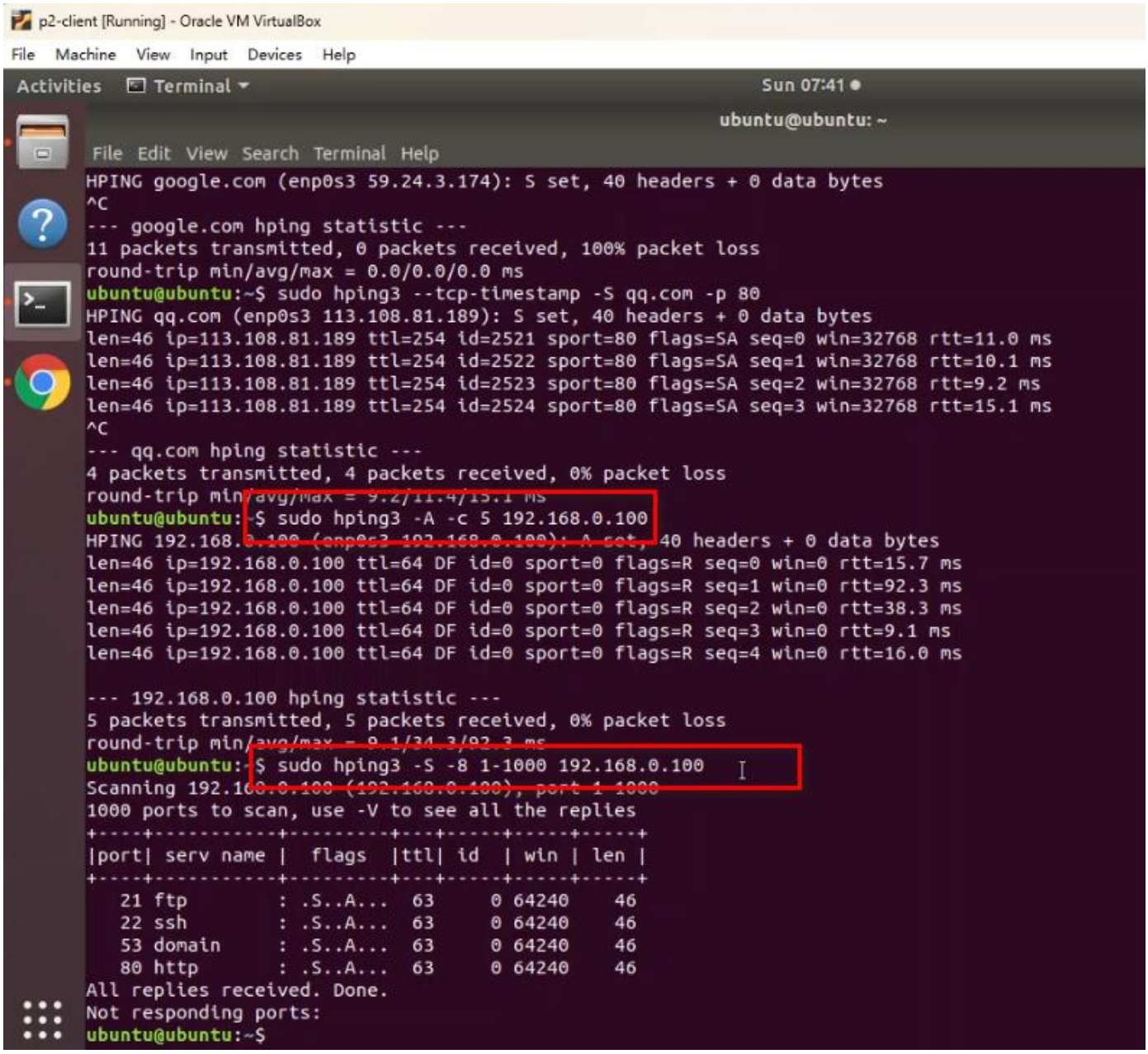


2.7 使用 hping3 测试服务器的正常运行时间 12

请编辑高亮部分 提交中或英文版本皆可.

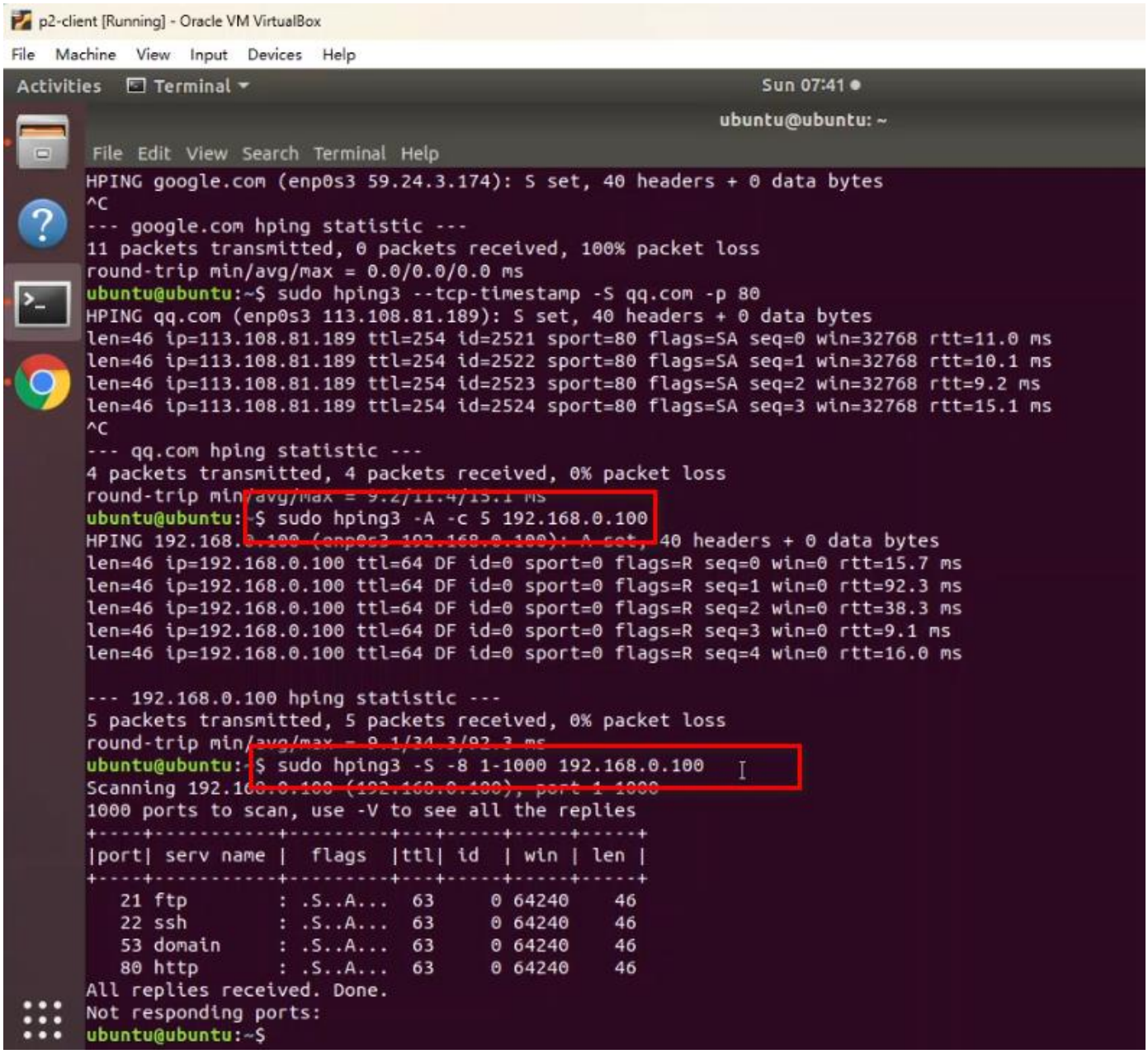


请编辑高亮部分 提交中或英文版本皆可.

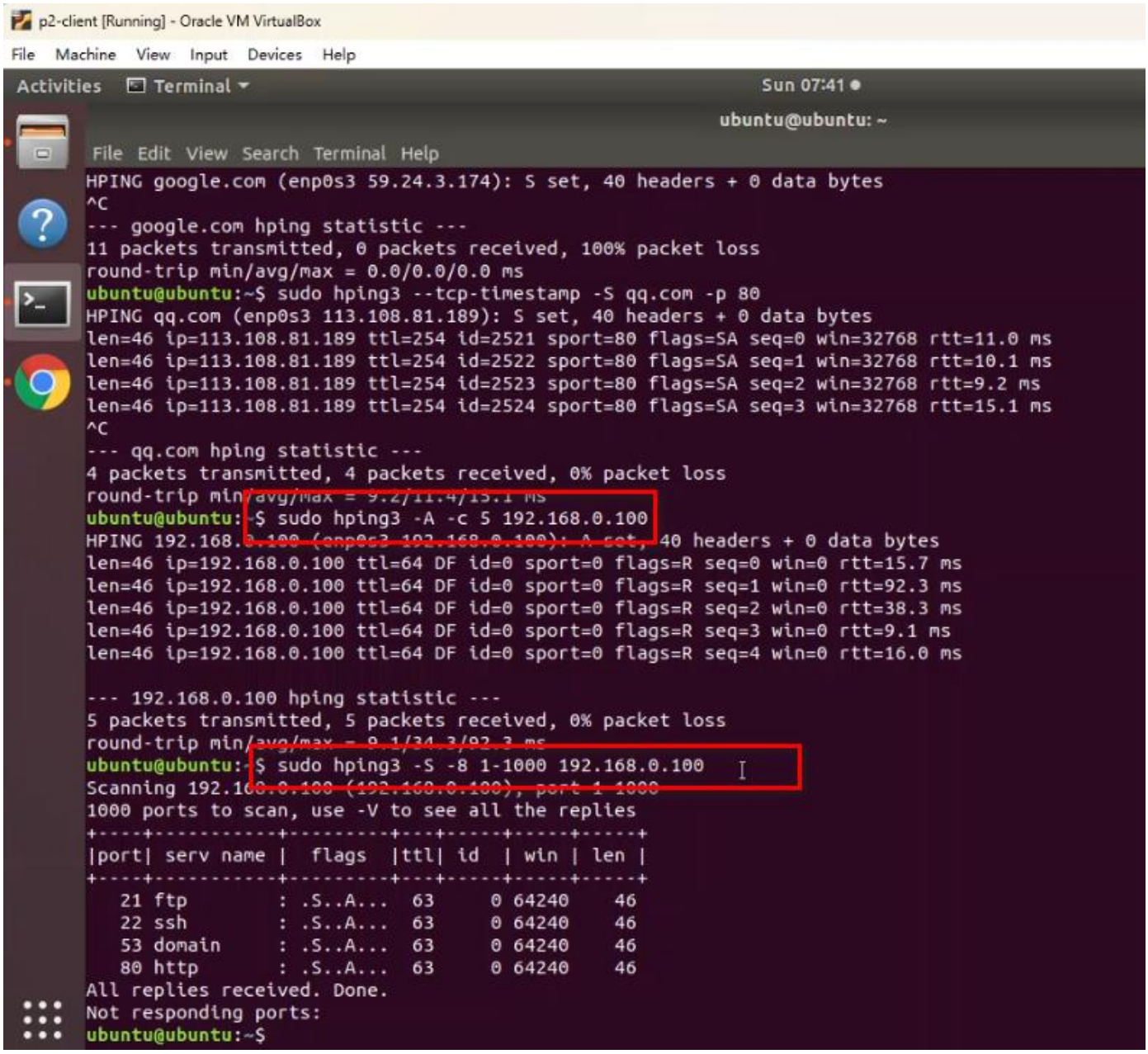


3.2 将 SYN 数据包发送到目标 13

请编辑高亮部分 提交中或英文版本皆可.

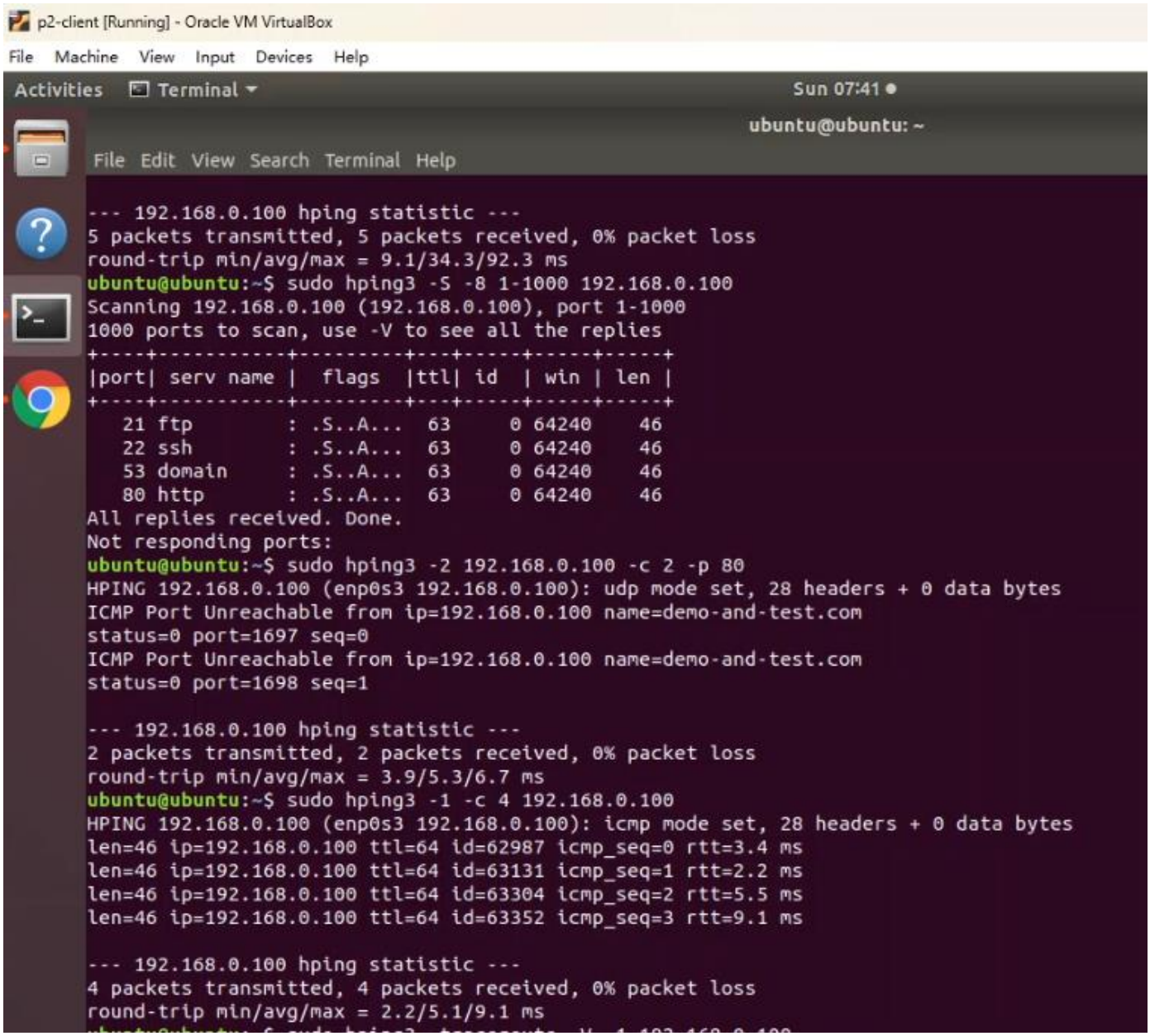


请编辑高亮部分 提交中或英文版本皆可.

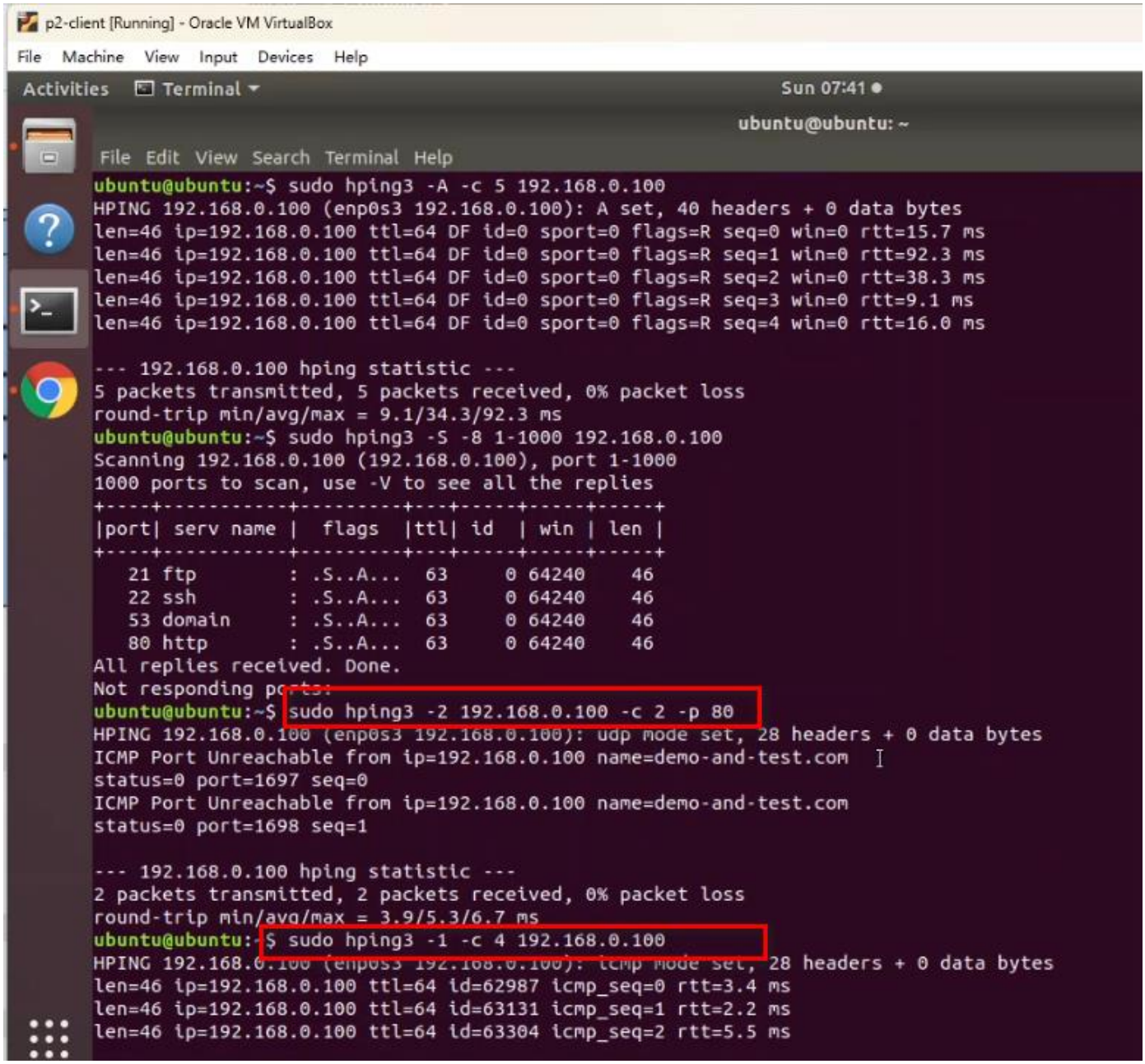


3.3 将 UDP 数据包发送到目标 14

请编辑高亮部分 提交中或英文版本皆可.

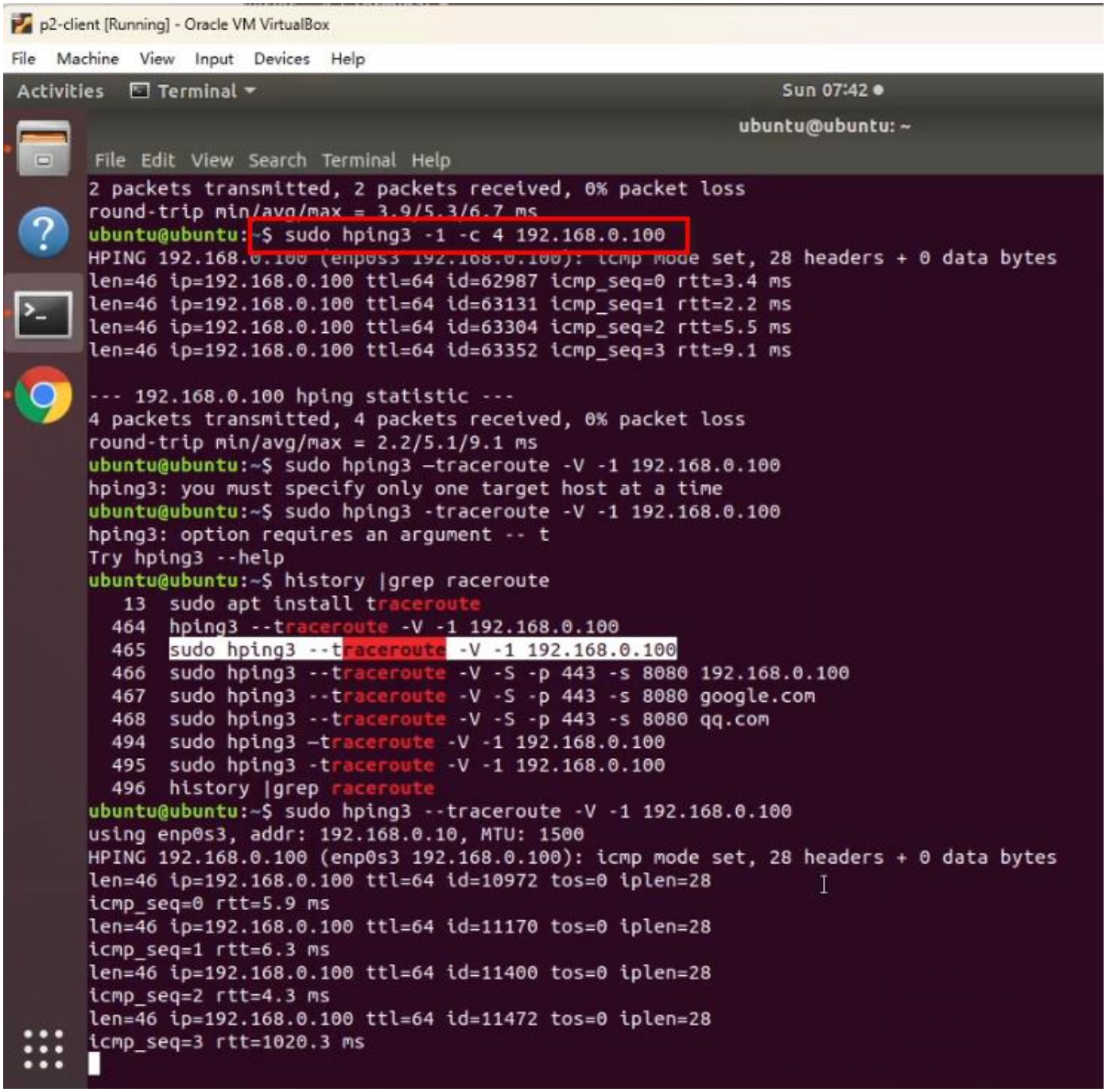


请编辑高亮部分 提交中或英文版本皆可.



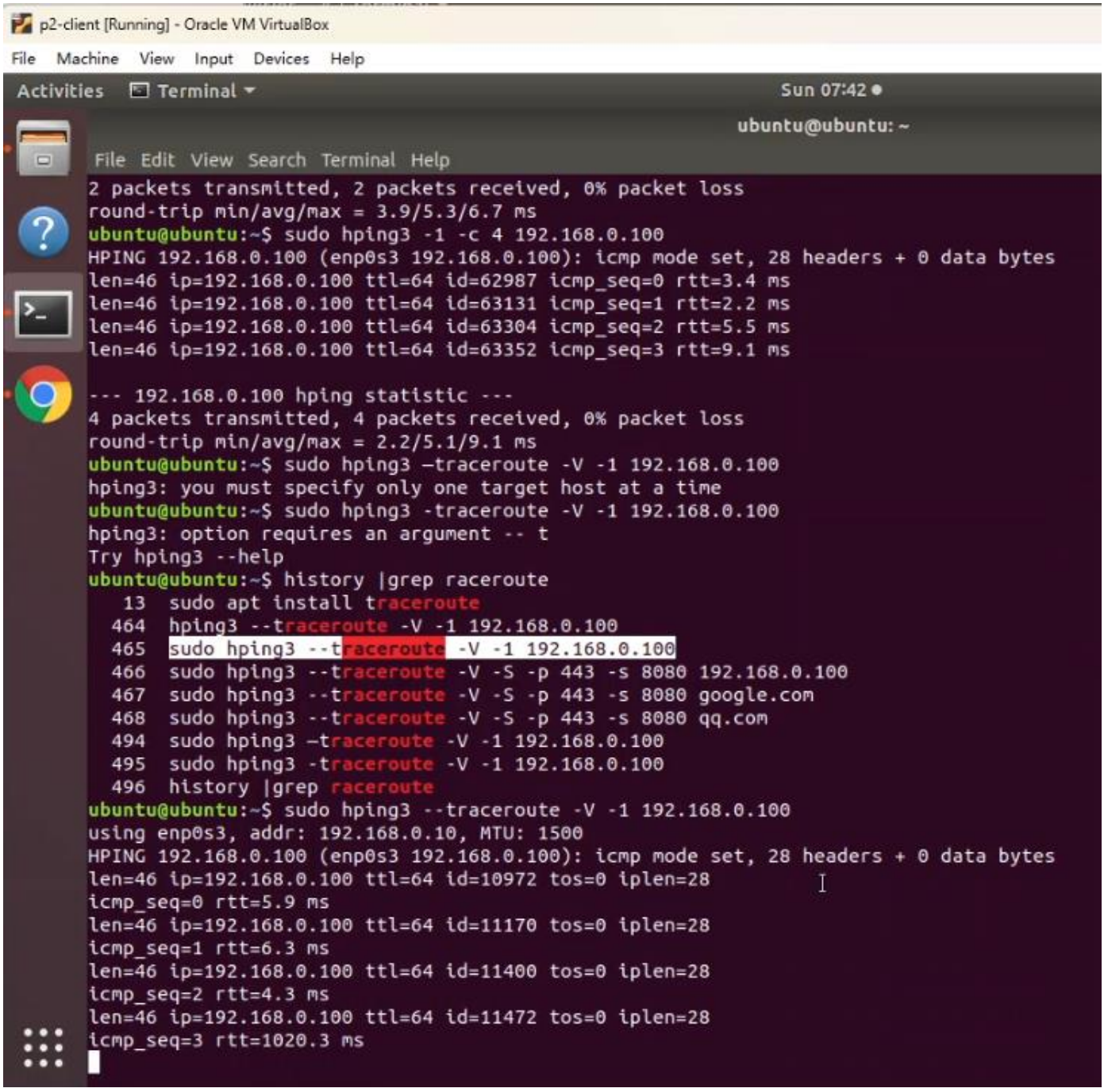
3.4 将 ping 数据包发送到目标 14

请编辑高亮部分 提交中或英文版本皆可.

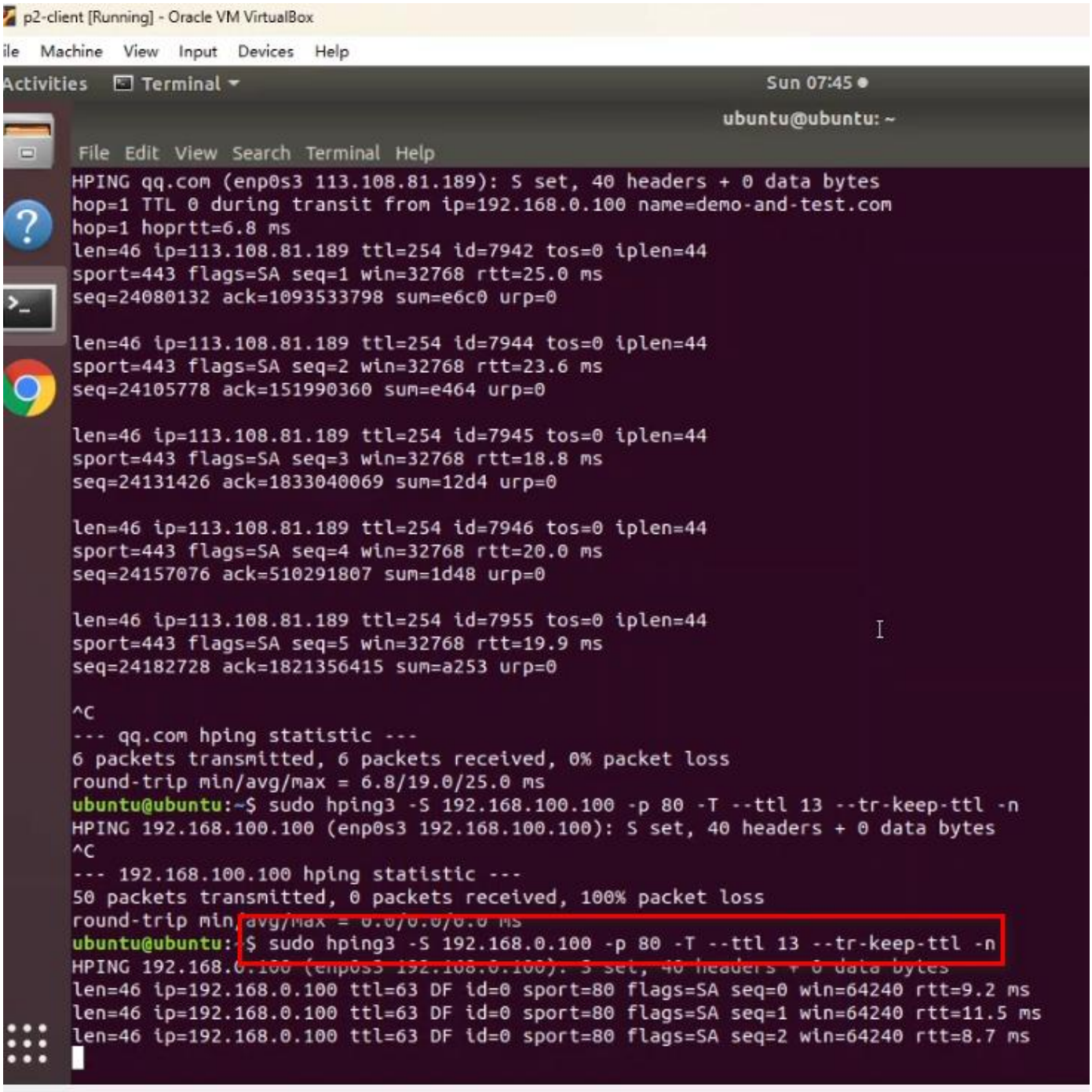


3.5 将 traceroute/ping 数据包发送到目标 14

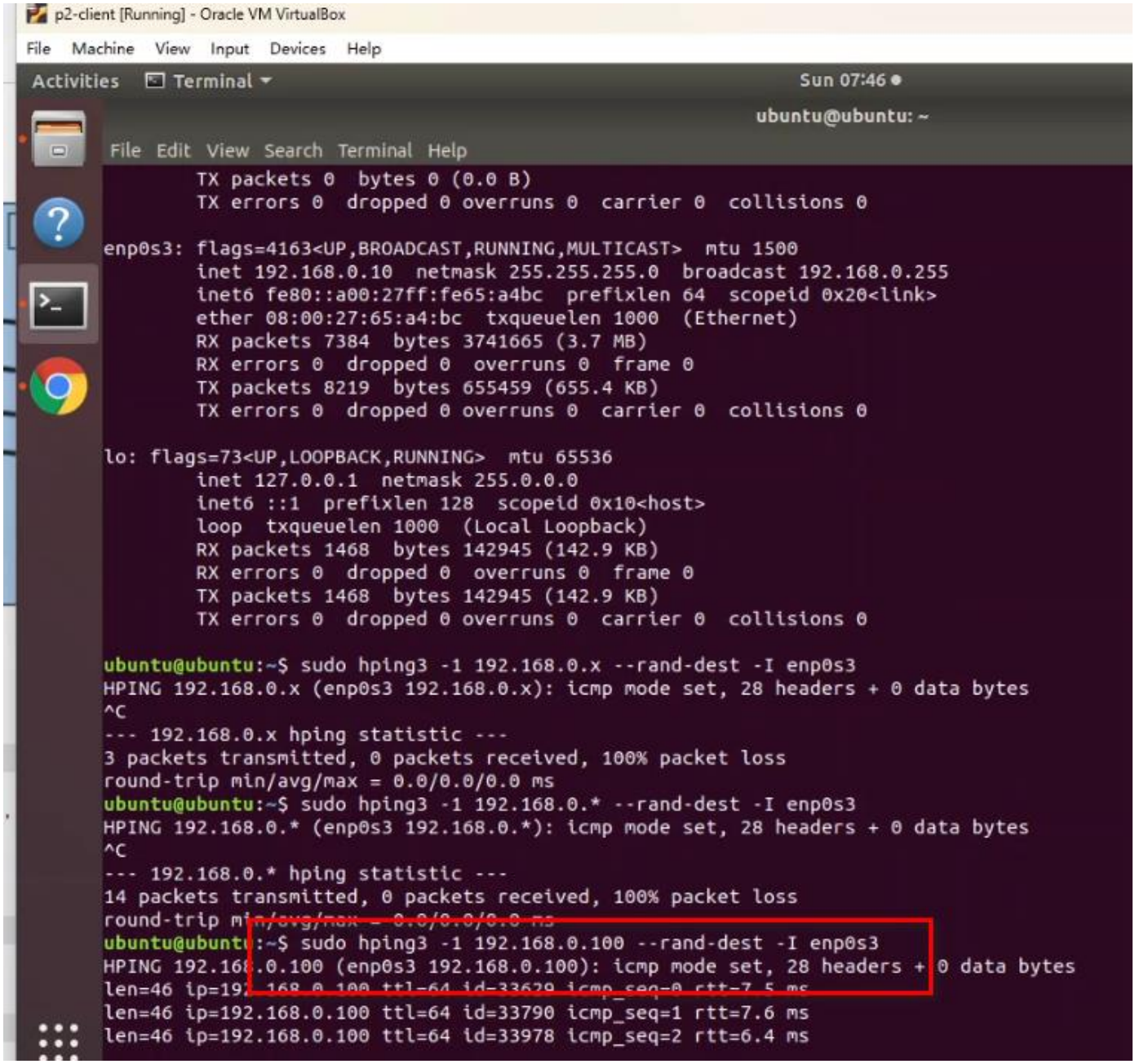
请编辑高亮部分 提交中或英文版本皆可.



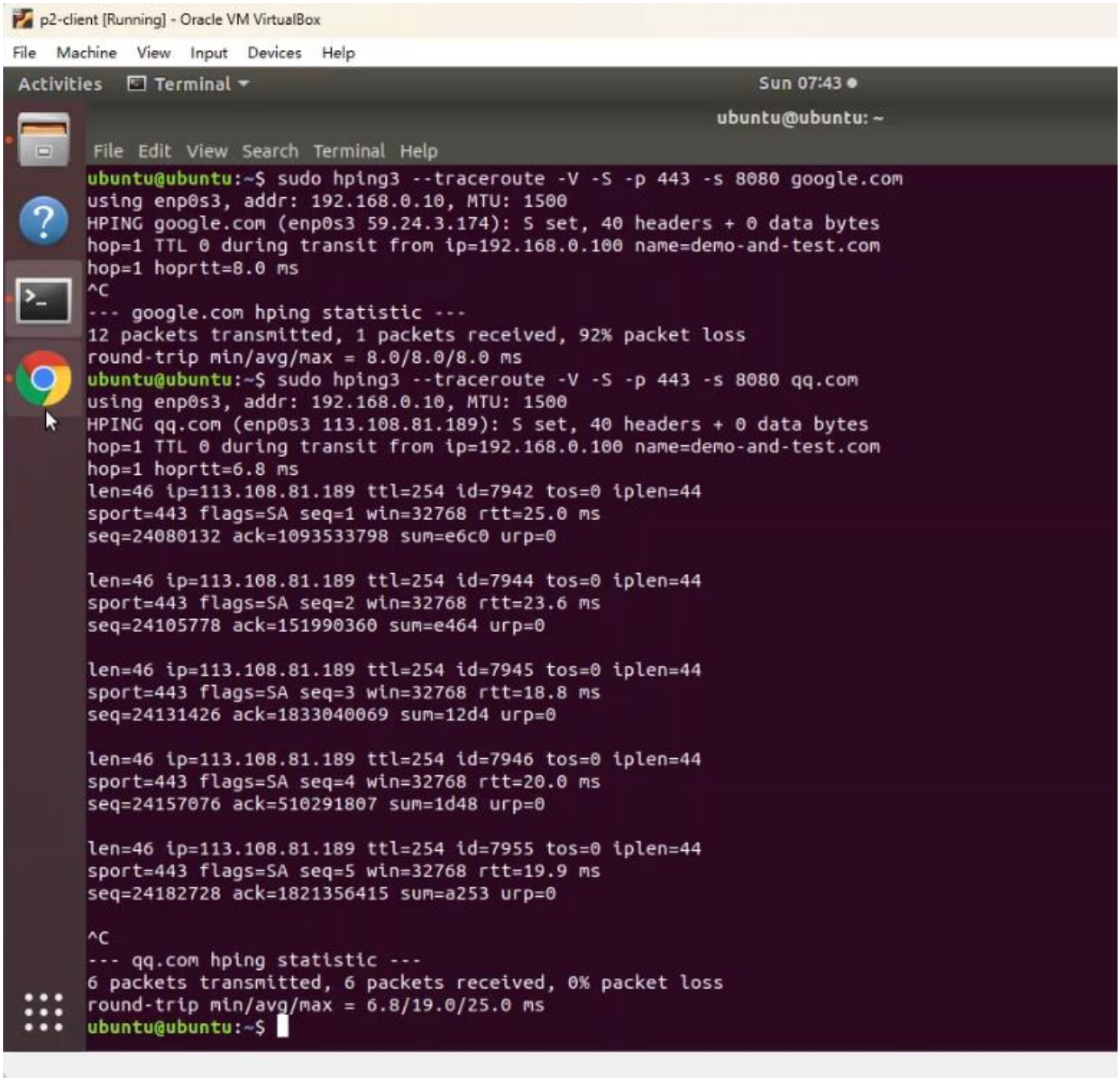
请编辑高亮部分 提交中或英文版本皆可.



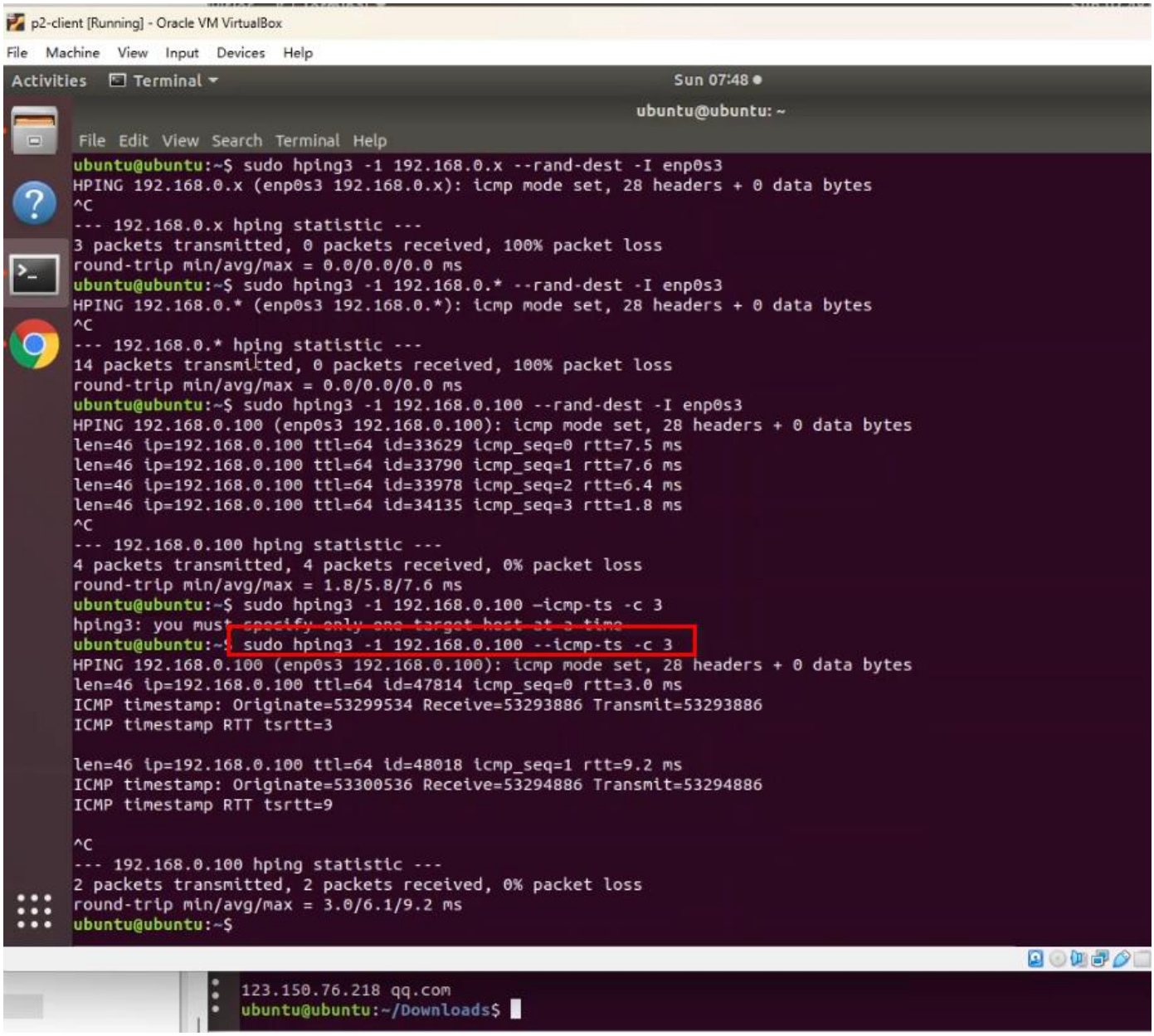
请编辑高亮部分 提交中或英文版本皆可.



请编辑高亮部分 提交中或英文版本皆可.

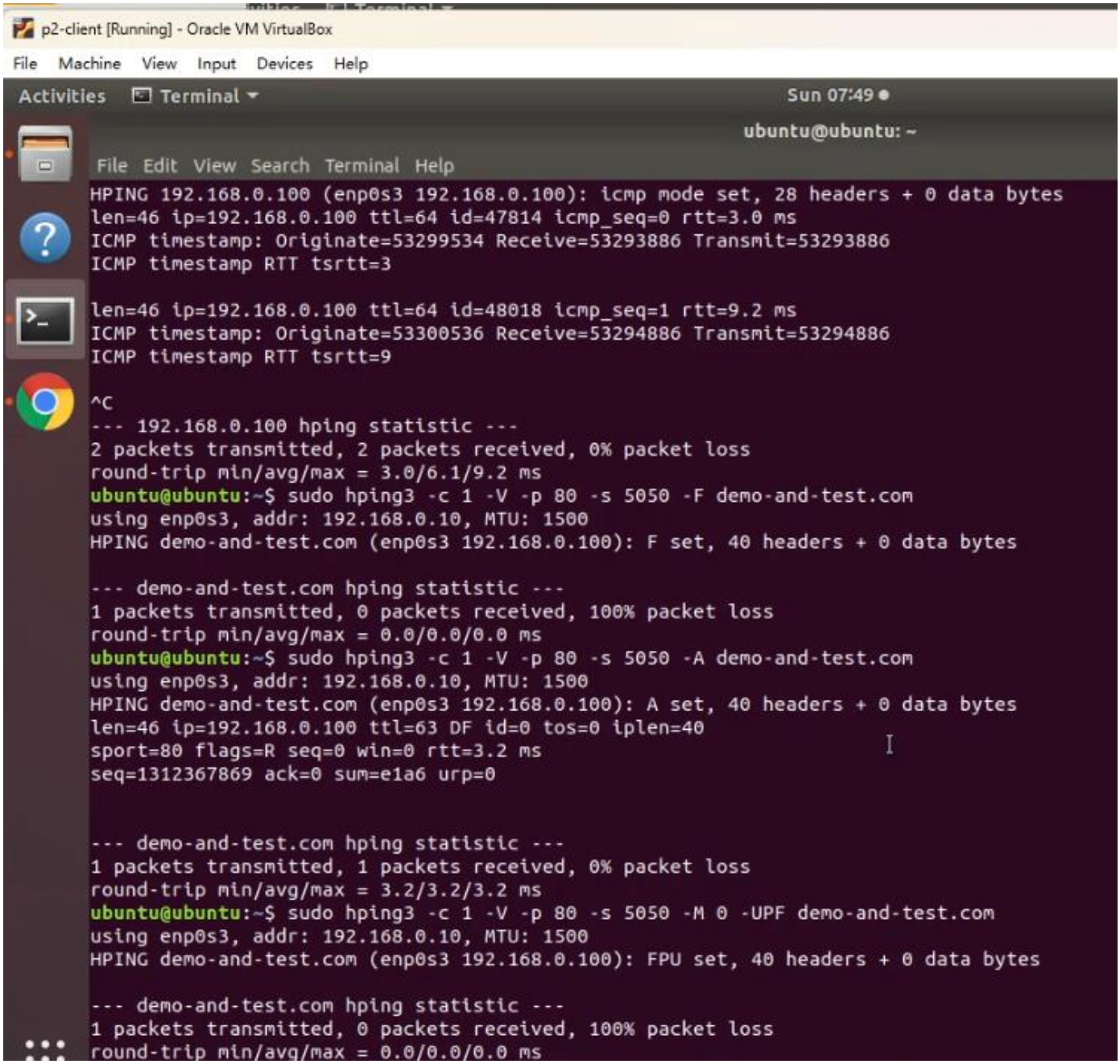


请编辑高亮部分 提交中或英文版本皆可.

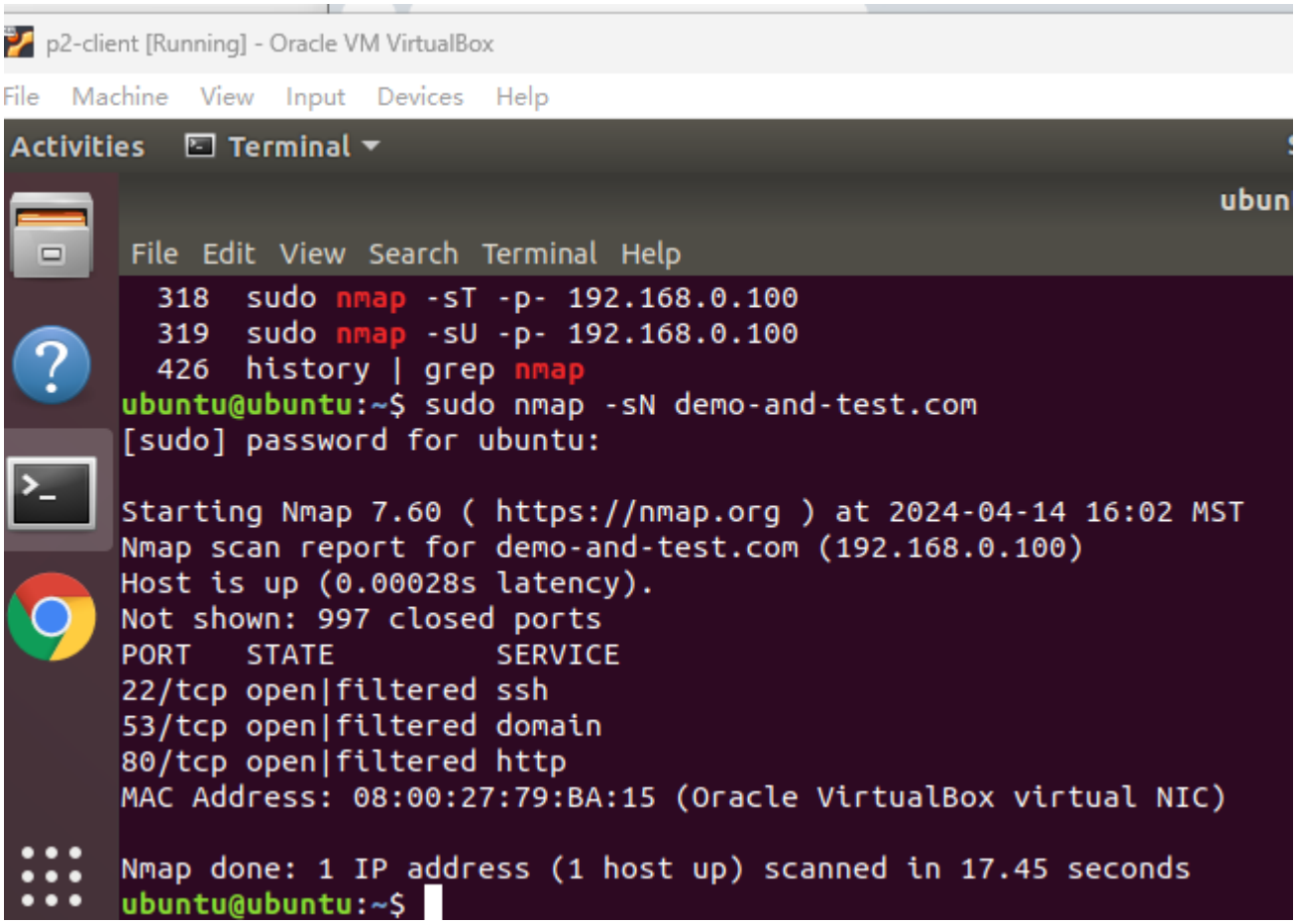


4. 使用 hping3 部署 DOS 攻击 16

请编辑高亮部分 提交中或英文版本皆可.



请编辑高亮部分 提交中或英文版本皆可.



涉及的命令如下：

```
#客户端的攻击命令
sudo hping3 -1 -S 192.168.0.100 -a 192.168.0.100 -k -s 80 -p 80 --flood

#snort 的规则 rule
ubuntu@ubuntu:~/Downloads$ cat /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp any any <> 192.168.0.100 any (msg:"ICMP Packet found"; sid:10000001; )
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SSH attempt";flags:S;classtype:attempted
-recon; sid:0000002; rev:2;)

# task 3
```

请编辑高亮部分 提交中或英文版本皆可.

```
17.
18. alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Http Getrequest";content:"GET";classtype
    :web-application-activity; sid:10000003; rev:3;)
19. alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (content:"|5c00|P|00|I|00|P|00|E|00 5c|";sid:
    10000004;rev:4;)
20.
21. alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP echo request message NO.7";classt
    ype:icmp-event;icmp_seq:7;sid:10000005;rev:5;)
22.
23. #4.1
24. alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"LAND ATTACK";flags:S;seq:0;ack:0;referen
    ce:arachnids,249;classtype:attempted-dos; sid:10000006; rev:6;)
25.
26. #new cmd
27. alert icmp any any -> 192.168.0.100 any (msg:"Possible ICMP flood attack"; itype:8; icode:
    0; detection_filter:track by_src, count 100, seconds 1; sid:10000008;)
28.
29.
30. #check
31. sudo snort -A console -c /etc/snort/snort.conf -u snort -g snort -q -i enp0s3
32.
33.
34. ########4.2
35.
36. sudo hping3 demo-and-test.com -q -n -d 120 -S -p 80 --flood --rand-source
37.
38. 第二步：编写 Snort 规则以检测 SYN 洪水攻击
39. alert tcp any any -> $HOME_NET 80 (flags: S; msg: "Possible SYN Flood"; flow: stateless; d
    etection_filter: track by_dst, count 20, seconds 60; sid:1000001;)
40.
41. # 4.4
42. sudo hping3 -2 --flood -p 53 192.168.0.100 --rand-source
43.
44.
45. alert udp any any -> $HOME_NET any (msg:"4.4 UDP flood attack"; threshold:type threshold,
    track by_dst, count 10, seconds 60; sid:1000004;)
```

V. 项目总结 CONCLUSION

描述从这个项目中吸取的教训，例如，任何有趣的发现、提示和技巧。提供关于您的项目的自我评估，并为此项目提供评论。Describe lesson learned from this project, e.g., any interesting discovers, tips, and tricks. Provide a self-assessment about your project and provide comments to this project.

需要细心的查看命令格式正不正确。

VI. 附录：文件 APPENDIX : ATTACHED FILES

提供使用的配置和开发的源文件的列表。在您的配置文件中，请注明注释。一个好的做法是在您进行更改的地方提供注释，例如：

Provide a list of used configurations and developed source files. In your configuration file, please with well-marked comments. A good practice is to provide comments where you made changes, something like:

// Your Name: comments

Your Name: comments

/*
Your Name: comments
*/

请编辑高亮部分 提交中或英文版本皆可.

注释格式取决于您使用的系统文件和程序 The comment format depends on your used system files and programs.

gateway 网关上的配置文件，包括防火墙和检查规则文件。

- 防火墙

rc.firewall

rc.firewall

文件中的配置为：

```
#!/bin/sh

####
# 1.1. Internet ip address
####
Internet_IP="172.16.0.4"
Internet_IP_RANGE="172.16.0.0/12"
Internet_BCAST_ADRESS="172.31.255.255"
Internet_IFACE="enp0s9"

####
# 1.2 Client network configuration.
####
Client_NET_IP="192.168.0.10"
Client_NET_IP_RANGE="192.168.0.0/24"
Client_NET_BCAST_ADRESS="192.168.0.255"
Client_NET_IFACE="enp0s3"

####
# 1.3 Server Network Configuration.
####
Server_NET_IP="10.0.0.10"
Server_NET_IP_RANGE="10.0.0.0/8"
Server_NET_BCAST_ADRESS="10.255.255.255"
Server_NET_IFACE="enp0s8"

####
# Server and NAT IP aliases
####
#

#
# IP aliases for the server (server's IP address)
#
LO_IFACE="lo"
LO_IP="127.0.0.1"
WEB_IP_ADDRESS="10.0.0.10"
MAIL_IP_ADDRESS="10.0.0.10"
SSH_IP_ADDRESS="10.0.0.10"
DNS_IP_ADDRESS="10.0.0.10"
FTP_IP_ADDRESS="10.0.0.10"
#IP aliases for NATed services (this is the GW's ip on client network)
NAT_WEB_IP_ADDRESS="192.168.0.100"
NAT_MAIL_IP_ADDRESS="192.168.0.100"
NAT_SSH_IP_ADDRESS="192.168.0.100"
NAT_DNS_IP_ADDRESS="192.168.0.100"
NAT_FTP_IP_ADDRESS="192.168.0.100"
PASV_FTP_PORT_RANGE="30000:30099"

####
# 1.4 IPTables Configuration.
####
```

请编辑高亮部分 提交中或英文版本皆可.

```
IPTABLES="/sbin/iptables"

####
# 2. Module loading.
####
/sbin/depmod -a

#
# flush iptables
#
# 清空现有规则
$IPTABLES -F
$IPTABLES -X
$IPTABLES -F -t nat
$IPTABLES -F -t mangle
$IPTABLES -F -t filter

# Load required kernel modules
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_limit
/sbin/modprobe ipt_state


####
# 3. /proc set up.
####
echo "1" > /proc/sys/net/ipv4/ip_forward
#


####
# 4. rules set up.
####

# Blacklist
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT

# User-defined chains
$IPTABLES -I FORWARD 1 -p tcp --tcp-flags FIN FIN -j ACCEPT

$IPTABLES -P INPUT ACCEPT $IPTABLES -P OUTPUT ACCEPT $IPTABLES -P FORWARD ACCEPT

# 允许来自客户端的 ICMP 请求
$IPTABLES -A INPUT -p icmp --icmp-type echo-request -s $Client_NET_IP_RANGE -j ACCEPT
$IPTABLES -A OUTPUT -p icmp --icmp-type echo-reply -d $Client_NET_IP_RANGE -j ACCEPT

#允许来自客户端的所有 ICMP 请求
$IPTABLES -A INPUT -p icmp -s $Client_NET_IP_RANGE -j ACCEPT $IPTABLES -A OUTPUT -p icmp -
    d $Client_NET_IP_RANGE -j ACCEPT

# 允许转发的 ICMP 请求和回复
$IPTABLES -A FORWARD -p icmp -s $Client_NET_IP_RANGE -j ACCEPT
$IPTABLES -A FORWARD -p icmp -d $Client_NET_IP_RANGE -j ACCEPT

#允许转发来自客户端的所有 ICMP 请求和回复
$IPTABLES -A FORWARD -p icmp -s $Client_NET_IP_RANGE -d $Server_NET_IP_RANGE -j ACCEPT
$IPTABLES -A FORWARD -p icmp -s $Server_NET_IP_RANGE -d $Client_NET_IP_RANGE -j ACCEPT

```

请编辑高亮部分 提交中或英文版本皆可.

```
# 允许来自客户端网络的所有 TCP 流量
$IPTABLES -A FORWARD -p tcp -s $Client_NET_IP_RANGE -d $WEB_IP_ADDRESS -j ACCEPT
$IPTABLES -A FORWARD -p tcp -s $Client_NET_IP_RANGE -d $NAT_WEB_IP_ADDRESS -j ACCEPT

$IPTABLES -A FORWARD -p tcp -s $NAT_WEB_IP_ADDRESS -d $Client_NET_IP_RANGE -j ACCEPT
$IPTABLES -A FORWARD -p tcp -s $WEB_IP_ADDRESS -d $Client_NET_IP_RANGE -j ACCEPT

# 允许从客户端网络到外部的所有 TCP 回复，无论是否设置了 SYN 标志
$IPTABLES -A FORWARD -p tcp -s $Client_NET_IP_RANGE -d $Server_NET_IP_RANGE -j ACCEPT
$IPTABLES -A FORWARD -p tcp -s $Server_NET_IP_RANGE -d $Client_NET_IP_RANGE -j ACCEPT

#
$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 80 -j DNAT --
    to $WEB_IP_ADDRESS
$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 22 -j DNAT --
    to $SSH_IP_ADDRESS
$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 53 -j DNAT --
    to $DNS_IP_ADDRESS
$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 21 -j DNAT --
    to $FTP_IP_ADDRESS

# 允许所有内网节点访问 Internet
$IPTABLES -t nat -A POSTROUTING -o $Internet_IFACE -j MASQUERADE


# 允许已建立和相关的连接
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT


# 记录所有丢弃的输入和转发包
$IPTABLES -A INPUT -j LOG --log-prefix "Dropped Input: "
$IPTABLES -A FORWARD -j LOG --log-prefix "Dropped Forward: "
```

- Snort local.rules 配置如下：

local.rules

文件中的配置为：

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp any any <> 192.168.0.100 any (msg:"ICMP Packet found"; sid:10000001; )
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SSH attempt";flags:S;classtype:attempted
    -recon; sid:0000002; rev:2;)

# task 3

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Http Getrequest";content:"GET";classtype
    :web-application-activity; sid:10000003; rev:3;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (content:"|5c00|P|00|I|00|P|00|E|00 5c|";sid:
    10000004;rev:4;)
```

请编辑高亮部分 提交中或英文版本皆可.

```
15.
16. alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP echo request message NO.7";classt
    ype:icmp-event;icmp_seq:7;sid:10000005;rev:5;)
17.
18. #task 4.1
19. alert icmp any any -> $HOME_NET any (msg:"4.1 LAND ICMP flood attack"; itype:8; icode:0; d
    etection_filter:track by_src, count 100, seconds 1; sid:10000006;)
20.
21. #task 4.2
22. alert tcp any any -> $HOME_NET 80 (flags: S; msg: "4.2 SYN flood attack"; flow: stateless;
     detection_filter: track by_dst, count 20, seconds 60; sid:1000001;)
23.
24. #task 4.4
25. alert udp any any -> $HOME_NET any (msg:"4.4 UDP flood attack"; threshold:type threshold,
    track by_dst, count 10, seconds 60; sid:1000004;)
```

VII. 参考 REFERENCES

参考是可选的，可以向阅读你的报告提供链接源以进行验证和学习。Reference is optional, but nice to have to allow others to read your report with additional linked source for validation and learning.

[1] Wireshark, available at https://www.wireshark.org/, accessed by 8/31/2018.
[2] Postel, Jon. "RFC 791: Internet protocol." (1981).