

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.

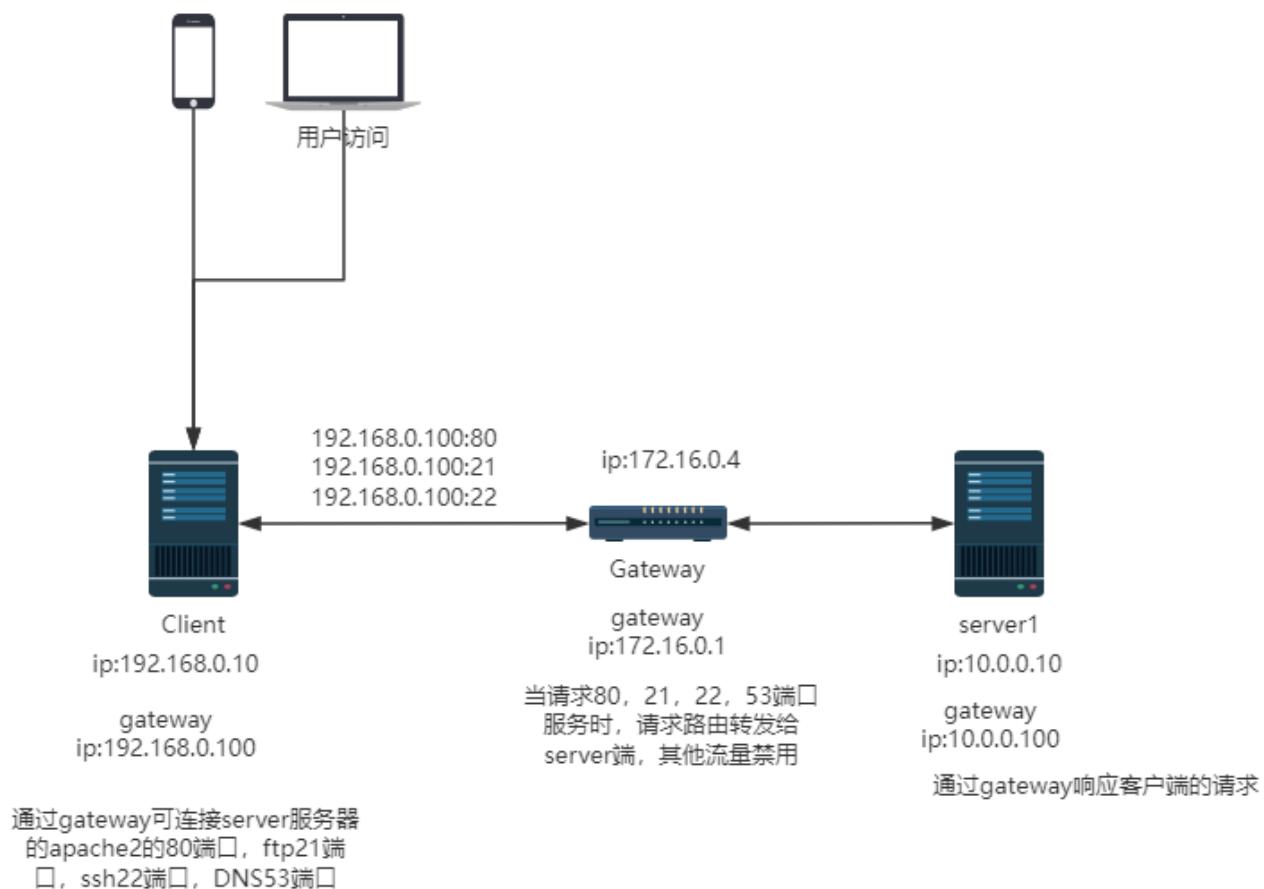
在 client 端安装 hping3，在网关部署防火墙转发请求到 server，并启动 snort 检测异常流量的实践，已完成 3 个试验。

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 diagram 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



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

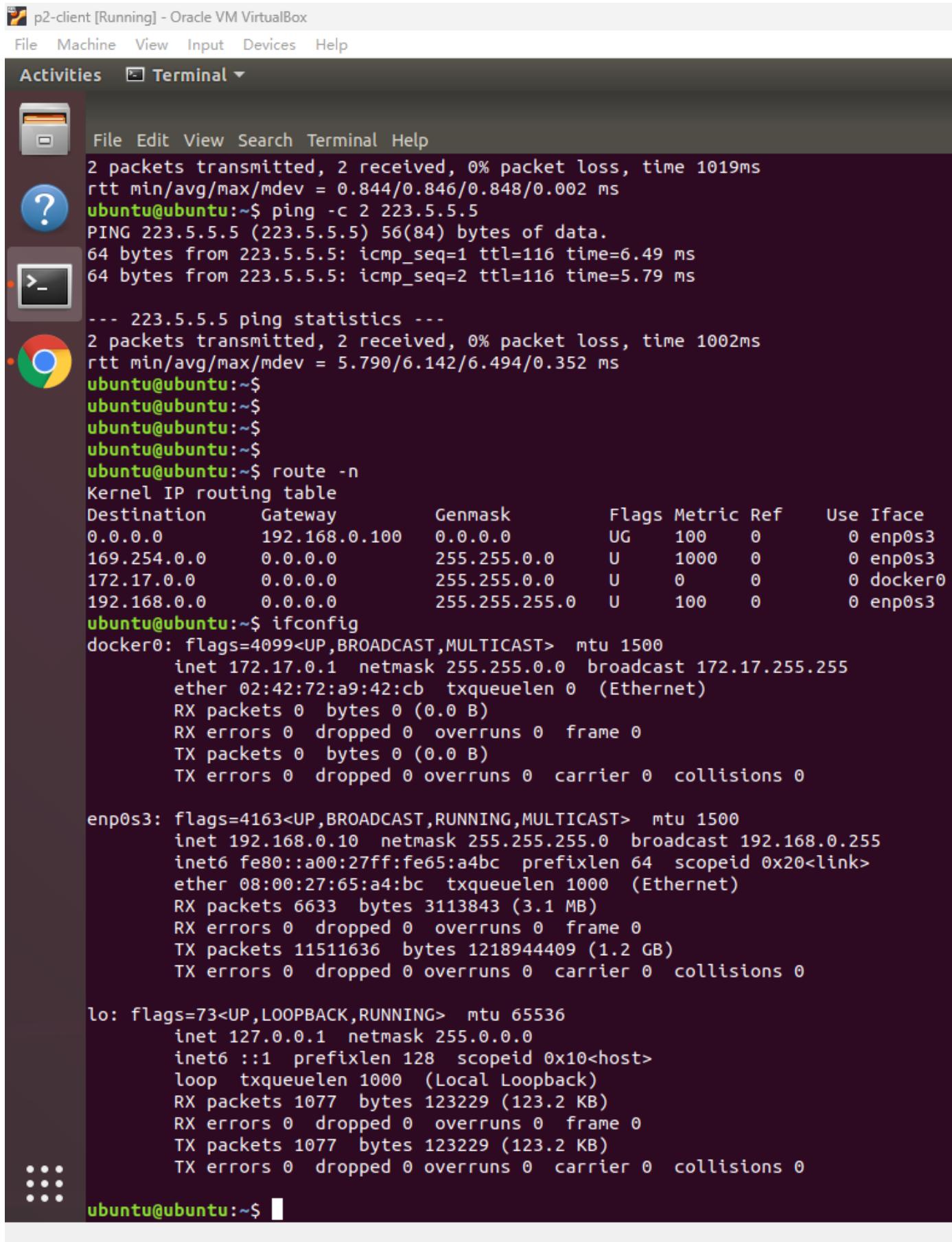
服务器端 Net 2: 10.0.0.0/8

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.



p2-client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal

```

File Edit View Search Terminal Help
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.844/0.846/0.848/0.002 ms
ubuntu@ubuntu:~$ ping -c 2 223.5.5.5
PING 223.5.5.5 (223.5.5.5) 56(84) bytes of data.
64 bytes from 223.5.5.5: icmp_seq=1 ttl=116 time=6.49 ms
64 bytes from 223.5.5.5: icmp_seq=2 ttl=116 time=5.79 ms

--- 223.5.5.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 5.790/6.142/6.494/0.352 ms
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.100   0.0.0.0       UG    100    0        0 enp0s3
169.254.0.0     0.0.0.0        255.255.0.0   U      1000   0        0 enp0s3
172.17.0.0      0.0.0.0        255.255.0.0   U      0       0        0 docker0
192.168.0.0     0.0.0.0        255.255.255.0 U      100    0        0 enp0s3
ubuntu@ubuntu:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
          inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
              ether 02:42:72:a9:42:cb  txqueuelen 0  (Ethernet)
                  RX packets 0  bytes 0 (0.0 B)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 0  bytes 0 (0.0 B)
                  TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
          inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
          inet6 fe80::a00:27ff:fe65:a4bc  prefixlen 64  scopeid 0x20<link>
              ether 08:00:27:65:a4:bc  txqueuelen 1000  (Ethernet)
                  RX packets 6633  bytes 3113843 (3.1 MB)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 11511636  bytes 1218944409 (1.2 GB)
                  TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

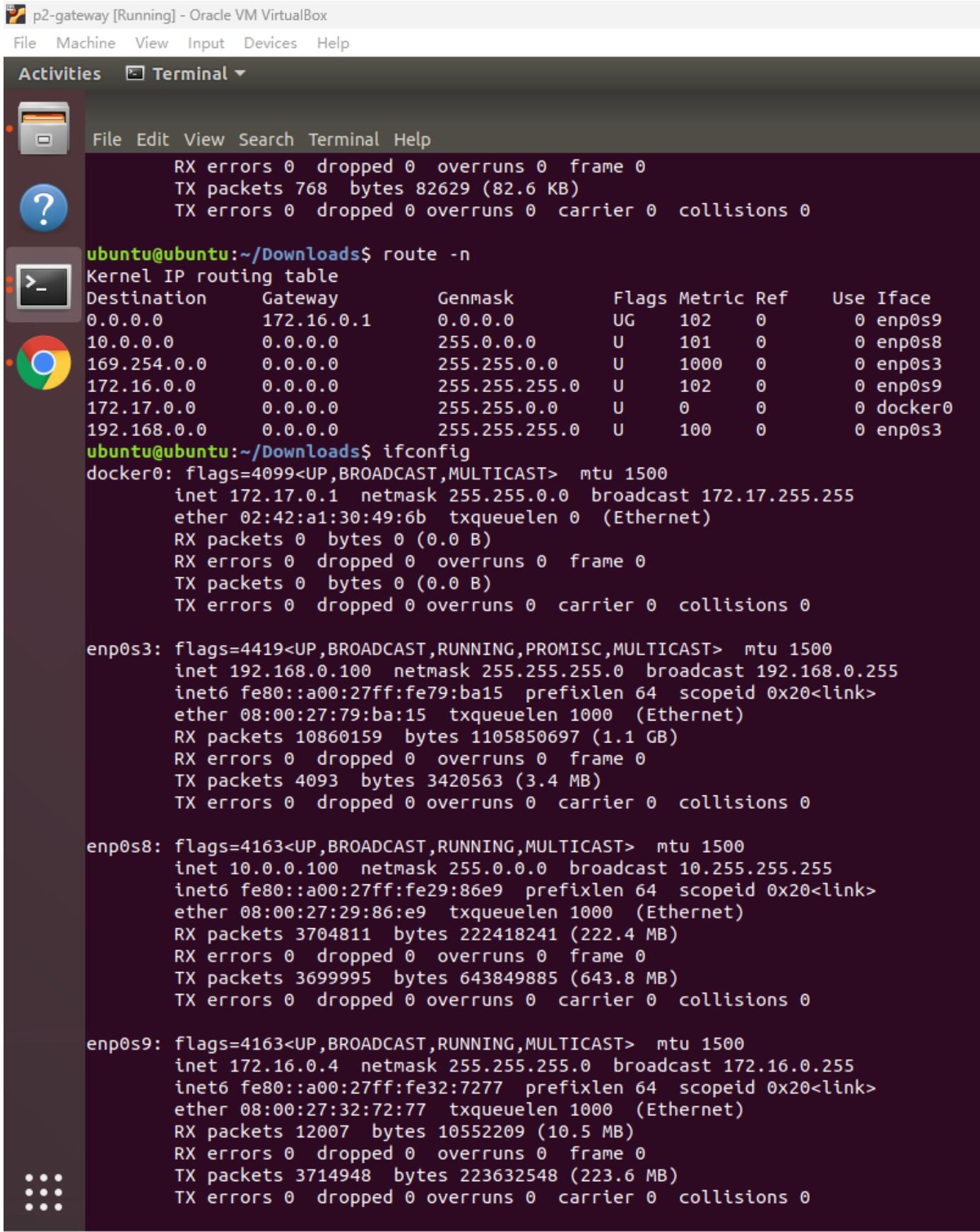
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
          inet 127.0.0.1  netmask 255.0.0.0
          inet6 ::1  prefixlen 128  scopeid 0x10<host>
              loop  txqueuelen 1000  (Local Loopback)
                  RX packets 1077  bytes 123229 (123.2 KB)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 1077  bytes 123229 (123.2 KB)
                  TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

ubuntu@ubuntu:~$ 
```

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.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "p2-gateway [Running] - Oracle VM VirtualBox". The window contains the following command-line output:

```

RX errors 0 dropped 0 overruns 0 frame 0
TX packets 768 bytes 82629 (82.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu:~/Downloads$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         172.16.0.1   0.0.0.0       UG    102    0        0 enp0s9
10.0.0.0        0.0.0.0      255.0.0.0     U      101    0        0 enp0s8
169.254.0.0     0.0.0.0      255.255.0.0   U      1000   0        0 enp0s3
172.16.0.0      0.0.0.0      255.255.255.0 U      102    0        0 enp0s9
172.17.0.0      0.0.0.0      255.255.0.0   U      0      0        0 docker0
192.168.0.0     0.0.0.0      255.255.255.0 U      100    0        0 enp0s3

ubuntu@ubuntu:~/Downloads$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
            ether 02:42:a1:30:49:6b txqueuelen 0 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s3: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
      inet 192.168.0.100 netmask 255.255.255.0 broadcast 192.168.0.255
            inet6 fe80::a00:27ff:fe79:ba15 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:79:ba:15 txqueuelen 1000 (Ethernet)
            RX packets 10860159 bytes 1105850697 (1.1 GB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4093 bytes 3420563 (3.4 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.0.100 netmask 255.0.0.0 broadcast 10.255.255.255
            inet6 fe80::a00:27ff:fe29:86e9 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:29:86:e9 txqueuelen 1000 (Ethernet)
            RX packets 3704811 bytes 222418241 (222.4 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 3699995 bytes 643849885 (643.8 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 172.16.0.4 netmask 255.255.255.0 broadcast 172.16.0.255
            inet6 fe80::a00:27ff:fe32:7277 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:32:72:77 txqueuelen 1000 (Ethernet)
            RX packets 12007 bytes 10552209 (10.5 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 3714948 bytes 223632548 (223.6 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

服务端 ifconfig 和 route -n

请编辑高亮部分 提交中或英文版本皆可.

p2-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal

```

File Edit View Search Terminal Help
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.410/0.524/0.639/0.116 ms
ubuntu@ubuntu:~$ ping -c 2 223.5.5.5
PING 223.5.5.5 (223.5.5.5) 56(84) bytes of data.
64 bytes from 223.5.5.5: icmp_seq=1 ttl=116 time=6.80 ms
64 bytes from 223.5.5.5: icmp_seq=2 ttl=116 time=5.49 ms

--- 223.5.5.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 5.496/6.152/6.808/0.656 ms
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ route -n
Kernel IP routing table
Destination      Gateway        Genmask        Flags Metric Ref    Use Iface
0.0.0.0          10.0.0.100   0.0.0.0       UG    100    0        0 enp0s3
10.0.0.0         0.0.0.0      255.0.0.0     U      100    0        0 enp0s3
169.254.0.0      0.0.0.0      255.255.0.0   U      1000   0        0 enp0s3
172.17.0.0       0.0.0.0      255.255.0.0   U      0       0        0 docker0
ubuntu@ubuntu:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
              ether 02:42:16:04:65:55 txqueuelen 0 (Ethernet)
                  RX packets 0 bytes 0 (0.0 B)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 0 bytes 0 (0.0 B)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.0.10 netmask 255.0.0.0 broadcast 10.255.255.255
      inet6 fe80::a00:27ff:fe1c:7dd3 prefixlen 64 scopeid 0x20<link>
              ether 08:00:27:1c:7d:d3 txqueuelen 1000 (Ethernet)
                  RX packets 3701129 bytes 644316525 (644.3 MB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 3719763 bytes 223596305 (223.5 MB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

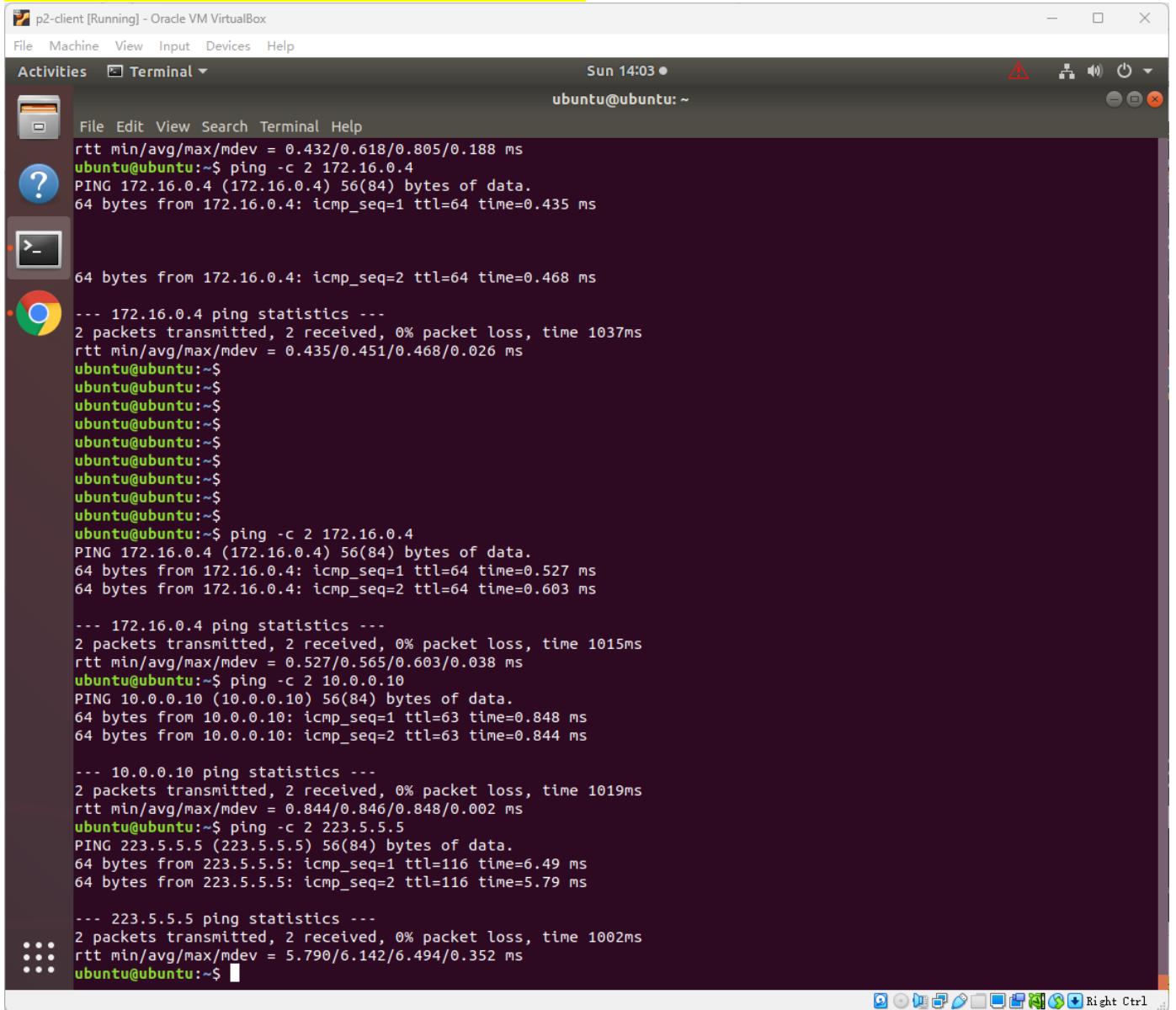
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
              loop txqueuelen 1000 (Local Loopback)
                  RX packets 653 bytes 91951 (91.9 KB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 653 bytes 91951 (91.9 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu:~$ 
```

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



```

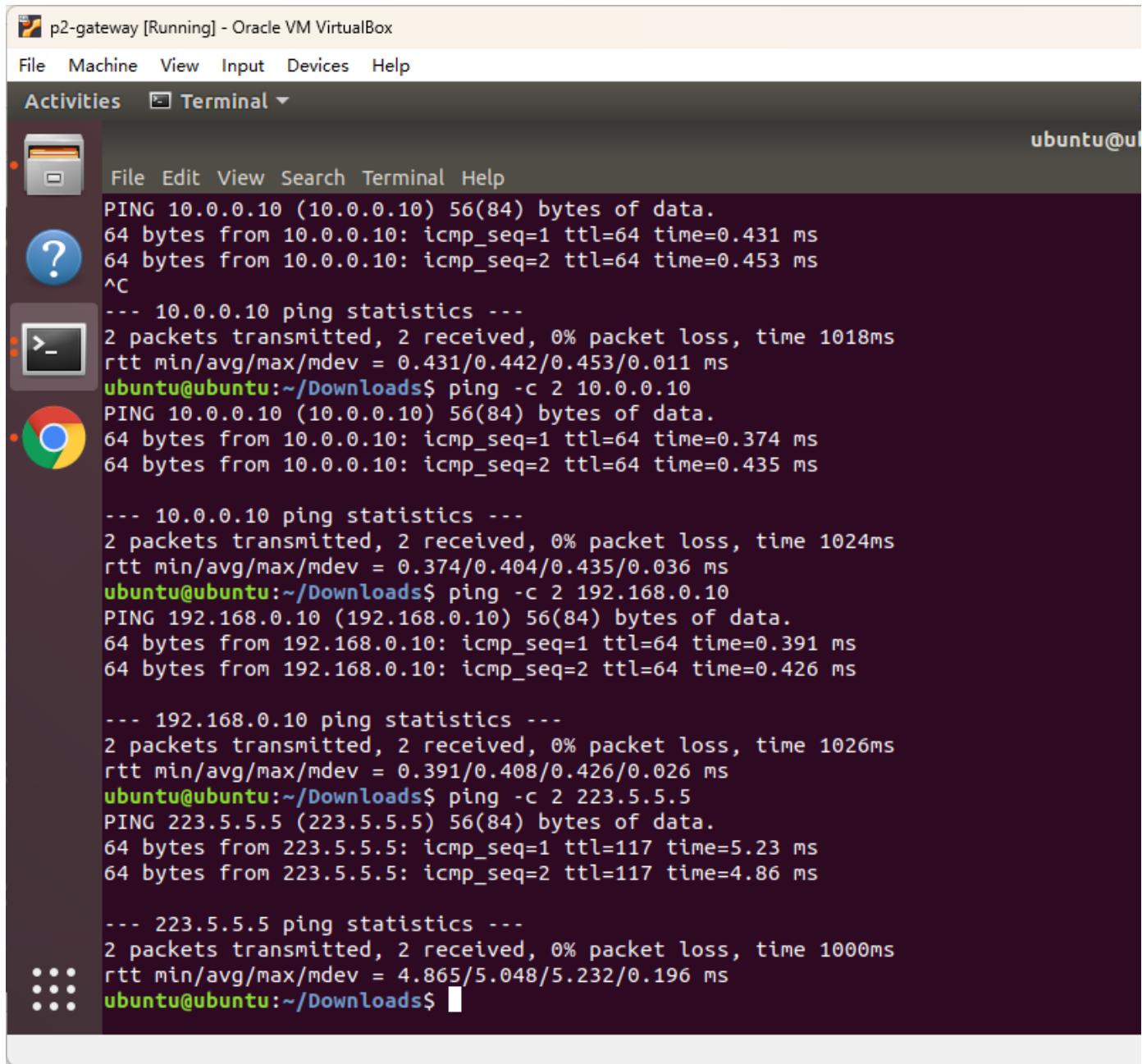
p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 14:03 ●
ubuntu@ubuntu: ~

File Edit View Search Terminal Help
rtt min/avg/max/mdev = 0.432/0.618/0.805/0.188 ms
ubuntu@ubuntu:~$ ping -c 2 172.16.0.4
PING 172.16.0.4 (172.16.0.4) 56(84) bytes of data.
64 bytes from 172.16.0.4: icmp_seq=1 ttl=64 time=0.435 ms
64 bytes from 172.16.0.4: icmp_seq=2 ttl=64 time=0.468 ms
--- 172.16.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1037ms
rtt min/avg/max/mdev = 0.435/0.451/0.468/0.026 ms
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ ping -c 2 172.16.0.4
PING 172.16.0.4 (172.16.0.4) 56(84) bytes of data.
64 bytes from 172.16.0.4: icmp_seq=1 ttl=64 time=0.527 ms
64 bytes from 172.16.0.4: icmp_seq=2 ttl=64 time=0.603 ms
--- 172.16.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 0.527/0.565/0.603/0.038 ms
ubuntu@ubuntu:~$ ping -c 2 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=63 time=0.848 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=63 time=0.844 ms
--- 10.0.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.844/0.846/0.848/0.002 ms
ubuntu@ubuntu:~$ ping -c 2 223.5.5.5
PING 223.5.5.5 (223.5.5.5) 56(84) bytes of data.
64 bytes from 223.5.5.5: icmp_seq=1 ttl=116 time=6.49 ms
64 bytes from 223.5.5.5: icmp_seq=2 ttl=116 time=5.79 ms
--- 223.5.5.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 5.790/6.142/6.494/0.352 ms
ubuntu@ubuntu:~$ 

```

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.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "p2-gateway [Running] - Oracle VM VirtualBox". The terminal content displays several ping commands being run from an Ubuntu 12.04 LTS system. The user is pinging three different IP addresses: 10.0.0.10, 192.168.0.10, and 223.5.5.5. Each ping command shows two successful packets sent with 0% loss and provides detailed statistics for each ping attempt.

```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal ▾
ubuntu@ultra: ~$ ping -c 2 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=0.431 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=0.453 ms
^C
--- 10.0.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.431/0.442/0.453/0.011 ms
ubuntu@ubuntu:~/Downloads$ ping -c 2 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=0.374 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=64 time=0.435 ms

--- 192.168.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1024ms
rtt min/avg/max/mdev = 0.374/0.404/0.435/0.036 ms
ubuntu@ubuntu:~/Downloads$ ping -c 2 223.5.5.5
PING 223.5.5.5 (223.5.5.5) 56(84) bytes of data.
64 bytes from 223.5.5.5: icmp_seq=1 ttl=117 time=5.23 ms
64 bytes from 223.5.5.5: icmp_seq=2 ttl=117 time=4.86 ms

--- 223.5.5.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 4.865/5.048/5.232/0.196 ms
ubuntu@ubuntu:~/Downloads$ █

```

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。

```

p2-server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 14:08 ●
ubuntu@ubuntu: ~
File Edit View Terminal Help
--- 10.0.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.044/0.077/0.111/0.034 ms
ubuntu@ubuntu:~$ ping -c 2 223.5.5.5
PING 223.5.5.5 (223.5.5.5) 56(84) bytes of data.
64 bytes from 223.5.5.5: icmp_seq=1 ttl=116 time=6.66 ms
64 bytes from 223.5.5.5: icmp_seq=2 ttl=116 time=6.10 ms

--- 223.5.5.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 6.100/6.382/6.665/0.293 ms
ubuntu@ubuntu:~$ ping -c 2 172.16.0.4
PING 172.16.0.4 (172.16.0.4) 56(84) bytes of data.
64 bytes from 172.16.0.4: icmp_seq=1 ttl=64 time=0.665 ms
64 bytes from 172.16.0.4: icmp_seq=2 ttl=64 time=0.460 ms

--- 172.16.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1016ms
rtt min/avg/max/mdev = 0.460/0.562/0.665/0.105 ms
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ ping -c 2 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=63 time=0.807 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=63 time=1.04 ms

--- 192.168.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.807/0.926/1.045/0.119 ms
ubuntu@ubuntu:~$ ping -c 2 172.16.0.4
PING 172.16.0.4 (172.16.0.4) 56(84) bytes of data.
64 bytes from 172.16.0.4: icmp_seq=1 ttl=64 time=0.639 ms
64 bytes from 172.16.0.4: icmp_seq=2 ttl=64 time=0.410 ms

--- 172.16.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.410/0.524/0.639/0.116 ms
ubuntu@ubuntu:~$ ping -c 2 223.5.5.5
PING 223.5.5.5 (223.5.5.5) 56(84) bytes of data.
64 bytes from 223.5.5.5: icmp_seq=1 ttl=116 time=6.80 ms
64 bytes from 223.5.5.5: icmp_seq=2 ttl=116 time=5.49 ms

--- 223.5.5.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 5.496/6.152/6.808/0.656 ms
ubuntu@ubuntu:~$ 
```

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.

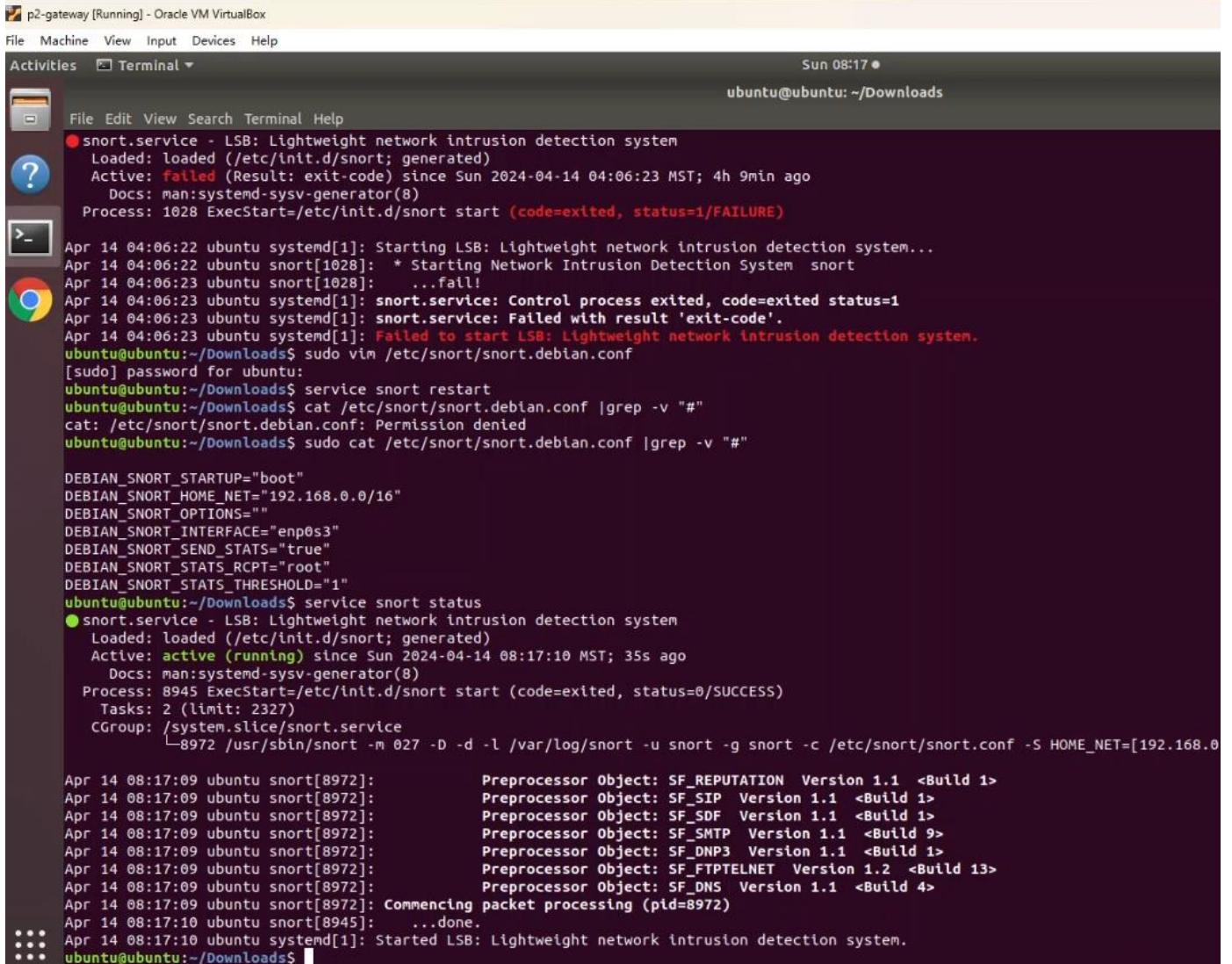
在网关上完成如下任务

1. 任务 1 Snort 的基础知识和准备工作 4

1.1 Snort 的组件 4

1.2 实验室环境的准备工作 6

2. 任务 2：运行 Snort 7



```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 08:17 ●
ubuntu@ubuntu: ~/Downloads

File Edit View Search Terminal Help
● snort.service - LSB: Lightweight network intrusion detection system
  Loaded: loaded (/etc/init.d/snort; generated)
  Active: failed (Result: exit-code) since Sun 2024-04-14 04:06:23 MST; 4h 9min ago
    Docs: man:systemd-sysv-generator(8)
   Process: 1028 ExecStart=/etc/init.d/snort start (code=exited, status=1/FAILURE)

Apr 14 04:06:22 ubuntu systemd[1]: Starting LSB: Lightweight network intrusion detection system...
Apr 14 04:06:22 ubuntu snort[1028]: * Starting Network Intrusion Detection System snort
Apr 14 04:06:23 ubuntu snort[1028]: ...fail!
Apr 14 04:06:23 ubuntu systemd[1]: snort.service: Control process exited, code=exited status=1
Apr 14 04:06:23 ubuntu systemd[1]: snort.service: Failed with result 'exit-code'.
Apr 14 04:06:23 ubuntu systemd[1]: Failed to start LSB: Lightweight network intrusion detection system.
ubuntu@ubuntu:~/Downloads$ sudo vim /etc/snort/snort.debian.conf
[sudo] password for ubuntu:
ubuntu@ubuntu:~/Downloads$ service snort restart
ubuntu@ubuntu:~/Downloads$ cat /etc/snort/snort.debian.conf |grep -v "#"
cat: /etc/snort/snort.debian.conf: Permission denied
ubuntu@ubuntu:~/Downloads$ sudo cat /etc/snort/snort.debian.conf |grep -v "#"

DEBIAN_SNORT_STARTUP="boot"
DEBIAN_SNORT_HOME_NET="192.168.0.0/16"
DEBIAN_SNORT_OPTIONS=""
DEBIAN_SNORT_INTERFACE="enp0s3"
DEBIAN_SNORT_SEND_STATS="true"
DEBIAN_SNORT_STATS_RCPT="root"
DEBIAN_SNORT_STATS_THRESHOLD="1"
ubuntu@ubuntu:~/Downloads$ service snort status
● snort.service - LSB: Lightweight network intrusion detection system
  Loaded: loaded (/etc/init.d/snort; generated)
  Active: active (running) since Sun 2024-04-14 08:17:10 MST; 35s ago
    Docs: man:systemd-sysv-generator(8)
   Process: 8945 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
     Tasks: 2 (limit: 2327)
    CGroup: /system.slice/snort.service
           └─8972 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort -c /etc/snort/snort.conf -S HOME_NET=[192.168.0

Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Apr 14 08:17:09 ubuntu snort[8972]: Commencing packet processing (pid=8972)
Apr 14 08:17:10 ubuntu snort[8945]: ...done.
::: Apr 14 08:17:10 ubuntu systemd[1]: Started LSB: Lightweight network intrusion detection system.
ubuntu@ubuntu:~/Downloads$ 
```

2.1 网络入侵检测系统设置 7

2.2 Snort 规则的图解 9

2.3 规则选项 (Metadata) 10

2.4 数据包嗅探器 11

请编辑高亮部分 提交中或英文版本皆可.

```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
File Edit View Search Terminal Help
127.0.1.1      ubuntu

# The following lines are desirable for IPv6 capable hosts
::1    ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.0.100 demo-and-test.com
192.168.0.100 www.demo-and-test.com
192.168.0.100 ftp.demo-and-test.com
192.168.0.100 ssh.demo-and-test.com

123.150.76.218 qq.com
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ 
ubuntu@ubuntu:~/Downloads$ sudo snort -v
Running in packet dump mode

     --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

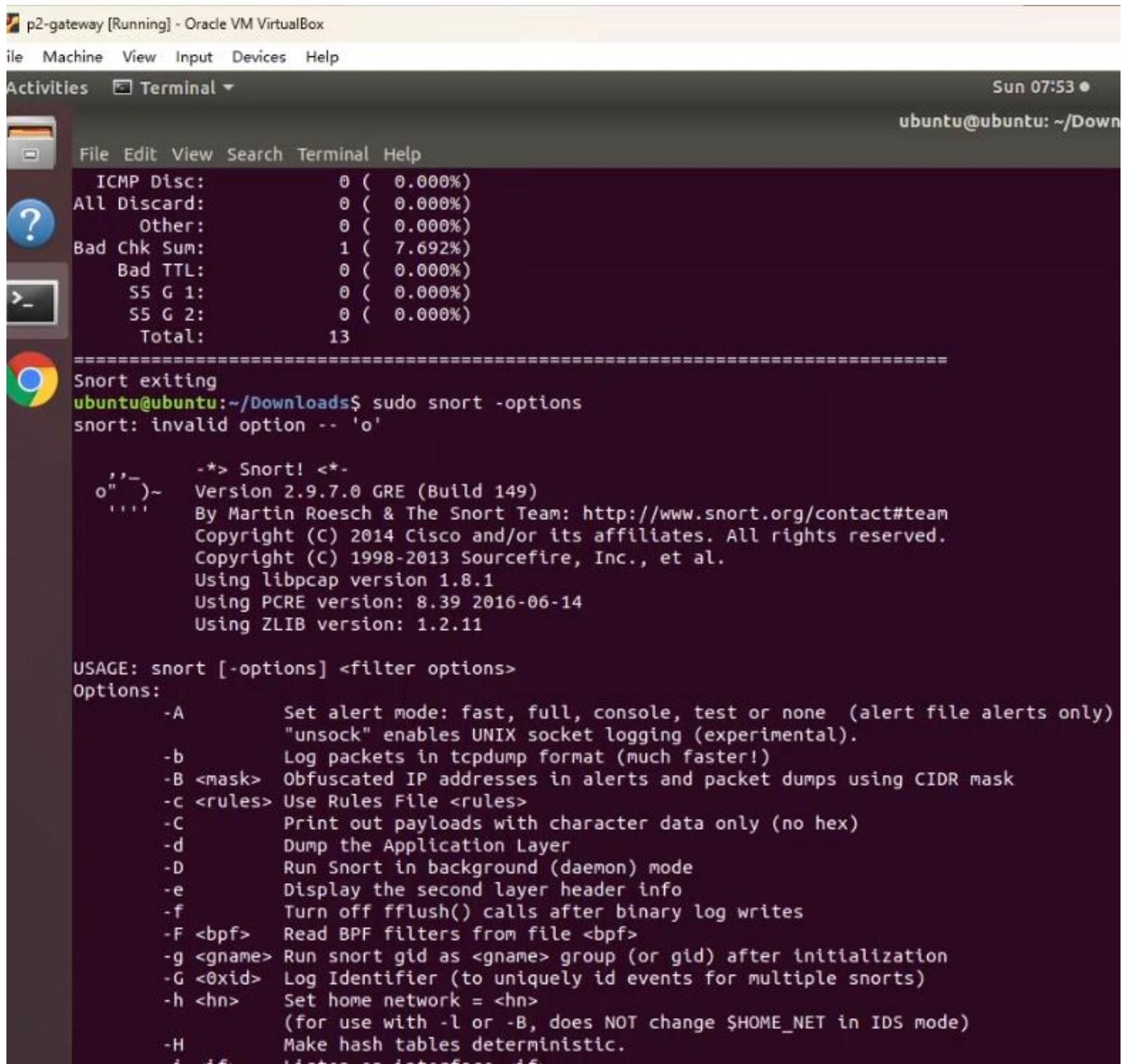
     --== Initialization Complete ==--

     --> Snort! <--
o",")~ Version 2.9.7.0 GRE (Build 149)
     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
     Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
     Copyright (C) 1998-2013 Sourcefire, Inc., et al.
     Using libpcap version 1.8.1
     Using PCRE version: 8.39 2016-06-14
     Using ZLIB version: 1.2.11

::: Commencing packet processing (pid=8581)

```

请编辑高亮部分 提交中或英文版本皆可。



```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:53
ubuntu@ubuntu: ~/Downloads

File Edit View Search Terminal Help
ICMP Disc: 0 ( 0.000%)
All Discard: 0 ( 0.000%)
    Other: 0 ( 0.000%)
Bad Chk Sum: 1 ( 7.692%)
Bad TTL: 0 ( 0.000%)
S5 G 1: 0 ( 0.000%)
S5 G 2: 0 ( 0.000%)
Total: 13
=====
Snort exiting
ubuntu@ubuntu:~/Downloads$ sudo snort -options
snort: invalid option -- 'o'

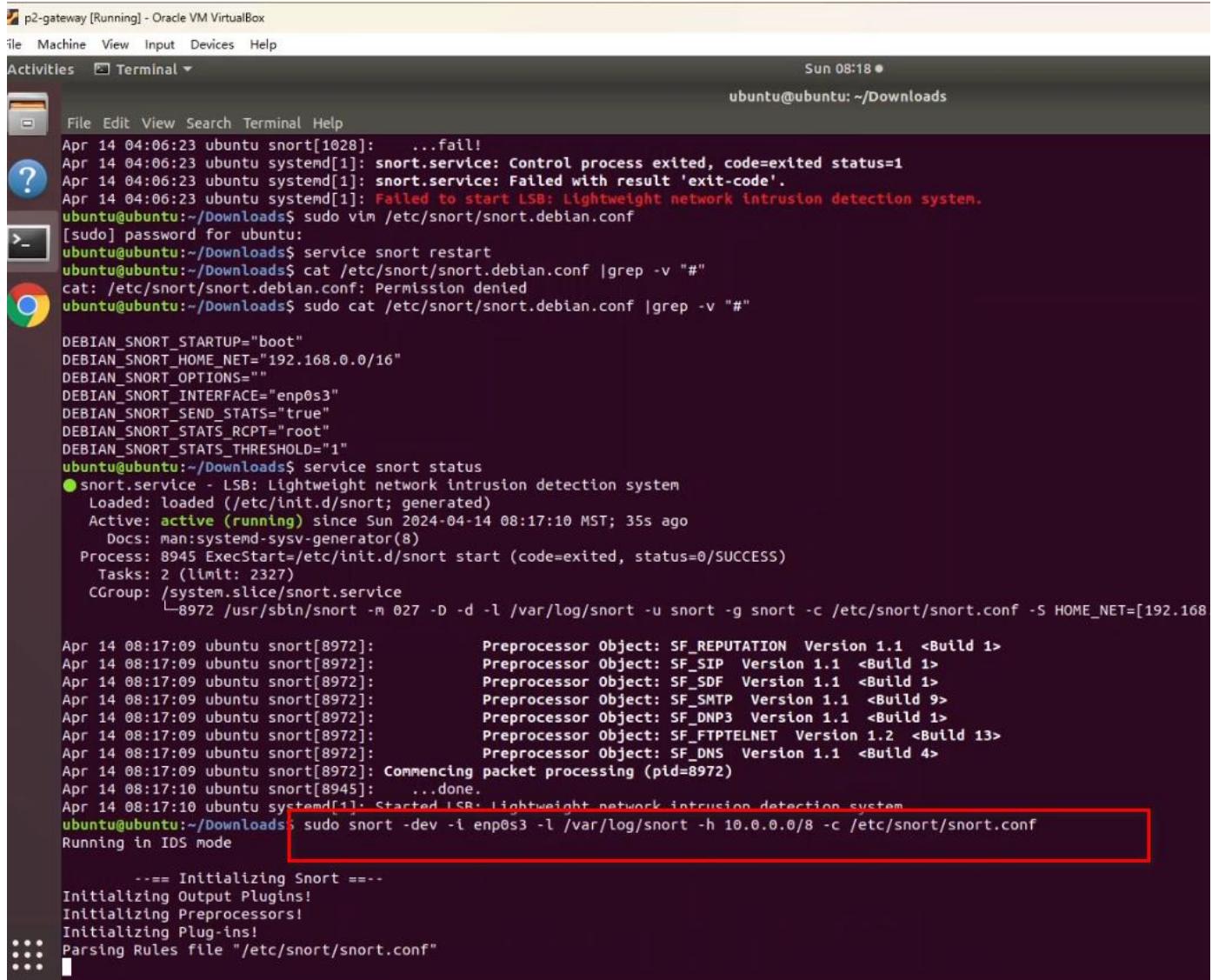
      -*> Snort! <*-
o"")~ Version 2.9.7.0 GRE (Build 149)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.8.1
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

USAGE: snort [-options] <filter options>
Options:
  -A      Set alert mode: fast, full, console, test or none (alert file alerts only)
          "unsock" enables UNIX socket logging (experimental).
  -b      Log packets in tcpdump format (much faster!)
  -B <mask> Obfuscate IP addresses in alerts and packet dumps using CIDR mask
  -c <rules> Use Rules File <rules>
  -C      Print out payloads with character data only (no hex)
  -d      Dump the Application Layer
  -D      Run Snort in background (daemon) mode
  -e      Display the second layer header info
  -f      Turn off fflush() calls after binary log writes
  -F <bpf> Read BPF filters from file <bpf>
  -g <gname> Run snort gid as <gname> group (or gid) after initialization
  -G <0xid> Log Identifier (to uniquely id events for multiple snorts)
  -h <hn>  Set home network = <hn>
          (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
  -H      Make hash tables deterministic.
  -i <if> Listen on interface <if>

```

2.5 数据包记录器 11

请编辑高亮部分 提交中或英文版本皆可.



The screenshot shows a terminal window titled "p2-gateway [Running] - Oracle VM VirtualBox". The window has a dark theme with light-colored text. The terminal is running on an Ubuntu system, indicated by the prompt "ubuntu@ubuntu: ~/Downloads". The log output is as follows:

```

File Edit View Search Terminal Help
Apr 14 04:06:23 ubuntu snort[1028]: ...fail!
Apr 14 04:06:23 ubuntu systemd[1]: snort.service: Control process exited, code=exited status=1
Apr 14 04:06:23 ubuntu systemd[1]: snort.service: Failed with result 'exit-code'.
Apr 14 04:06:23 ubuntu systemd[1]: Failed to start LSB: Lightweight network intrusion detection system.
ubuntu@ubuntu:~/Downloads$ sudo vim /etc/snort/snort.debian.conf
[sudo] password for ubuntu:
ubuntu@ubuntu:~/Downloads$ service snort restart
ubuntu@ubuntu:~/Downloads$ cat /etc/snort/snort.debian.conf |grep -v "#"
cat: /etc/snort/snort.debian.conf: Permission denied
ubuntu@ubuntu:~/Downloads$ sudo cat /etc/snort/snort.debian.conf |grep -v "#"

DEBIAN_SNORT_STARTUP="boot"
DEBIAN_SNORT_HOME_NET="192.168.0.0/16"
DEBIAN_SNORT_OPTIONS=""
DEBIAN_SNORT_INTERFACE="enp0s3"
DEBIAN_SNORT_SEND_STATS="true"
DEBIAN_SNORT_STATS_RCPT="root"
DEBIAN_SNORT_STATS_THRESHOLD="1"
ubuntu@ubuntu:~/Downloads$ service snort status
● snort.service - LSB: Lightweight network intrusion detection system
  Loaded: loaded (/etc/init.d/snort; generated)
  Active: active (running) since Sun 2024-04-14 08:17:10 MST; 35s ago
    Docs: man:systemd-sysv-generator(8)
  Process: 8945 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 2327)
   CGroup: /system.slice/snort.service
           └─8972 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort -c /etc/snort/snort.conf -S HOME_NET=[192.168.0.0/16]

Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Apr 14 08:17:09 ubuntu snort[8972]:          Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Apr 14 08:17:09 ubuntu snort[8972]: Commencing packet processing (pid=8972)
Apr 14 08:17:10 ubuntu snort[8945]: ...done.
Apr 14 08:17:10 ubuntu systemd[1]: Started LSB: Lightweight network intrusion detection system
ubuntu@ubuntu:~/Downloads$ sudo snort -dev -i enp0s3 -l /var/log/snort -h 10.0.0.0/8 -c /etc/snort/snort.conf
Running in IDS mode

--= Initializing Snort =--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"

```

A red rectangular box highlights the command "ubuntu@ubuntu:~/Downloads\$ sudo snort -dev -i enp0s3 -l /var/log/snort -h 10.0.0.0/8 -c /etc/snort/snort.conf" and its output.

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。

```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 08: ubuntu@ubuntu:
File Edit View Search Terminal Help
Sessions ignored: 1
Detection disabled: 0
=====
SIP Preprocessor Statistics
Total sessions: 0
=====
Snort exiting
ubuntu@ubuntu:~/Downloads$ sudo snort -l /tmp/snort.log -b
Running in packet logging mode

    --- Initializing Snort ---
Initializing Output Plugins!
ERROR: Stat check on log dir failed: No such file or directory.
Fatal Error, Quitting..
ubuntu@ubuntu:~/Downloads$ sudo snort -l /tmp/snort -b
Running in packet logging mode

    --- Initializing Snort ---
Initializing Output Plugins!
ERROR: Stat check on log dir failed: No such file or directory.
Fatal Error, Quitting..
ubuntu@ubuntu:~/Downloads$ sudo snort -l /tmp/ -b
Running in packet logging mode

    --- Initializing Snort ---
Initializing Output Plugins!
Log directory = /tmp/
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

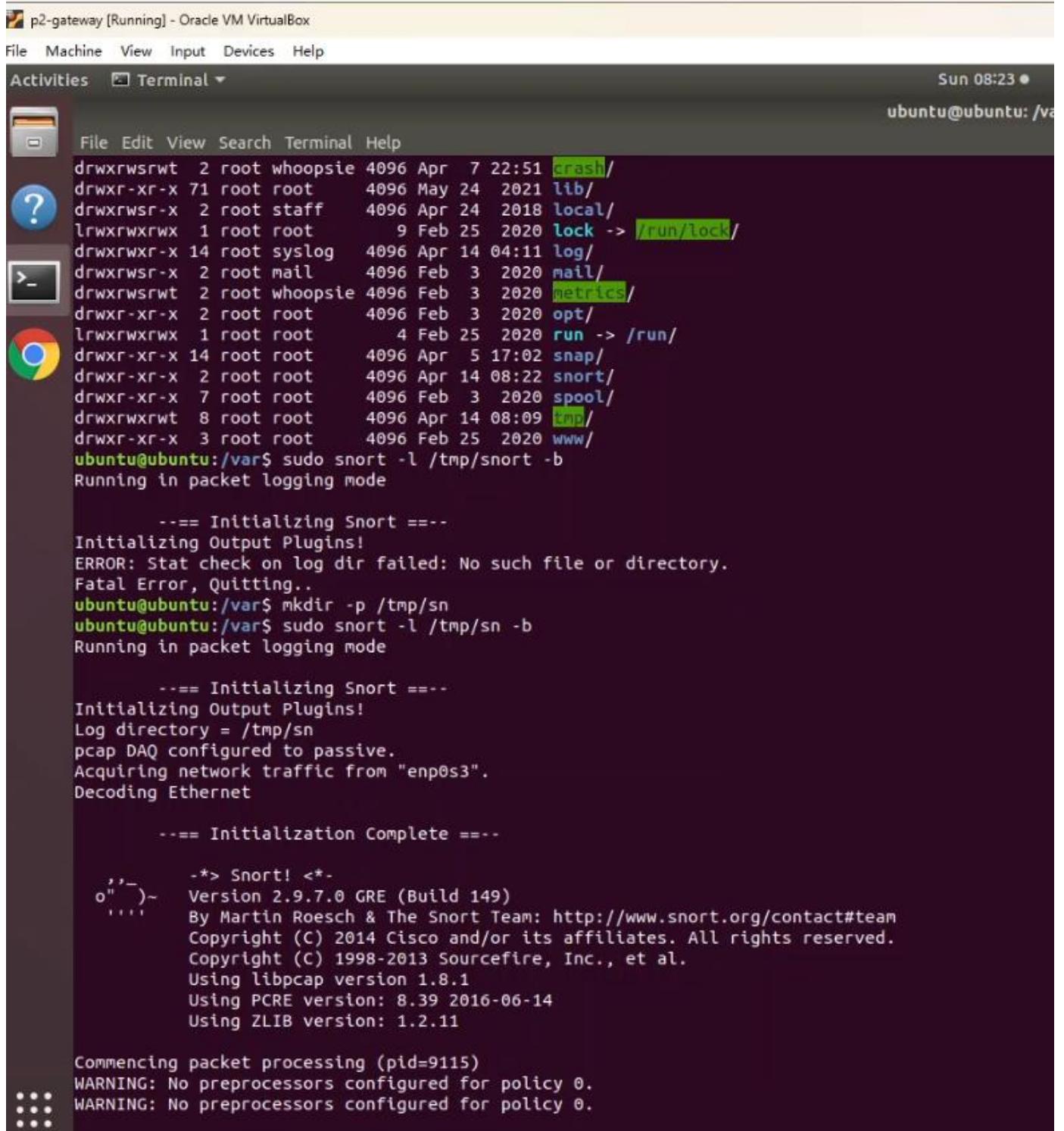
    --- Initialization Complete ---

o'''-  -*> Snort! <*-'
      Version 2.9.7.0 GRE (Build 149)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.8.1
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

Commencing packet processing (pid=9081)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.

```

请编辑高亮部分 提交中或英文版本皆可。



The screenshot shows a terminal window titled "p2-gateway [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```

File Machine View Input Devices Help
Activities Terminal Sun 08:23 ●
ubuntu@ubuntu: /var

File Edit View Search Terminal Help
drwxrwsrwt 2 root whoopsie 4096 Apr  7 22:51 crash/
drwxr-xr-x 71 root root    4096 May 24  2021 lib/
drwxrwsr-x 2 root staff   4096 Apr 24  2018 local/
lrwxrwxrwx  1 root root    9 Feb 25  2020 lock -> /run/lock/
drwxrwxr-x 14 root syslog  4096 Apr 14 04:11 log/
drwxrwsr-x 2 root mail    4096 Feb  3  2020 mail/
drwxrwsrwt 2 root whoopsie 4096 Feb  3  2020 metrics/
drwxr-xr-x 2 root root   4096 Feb  3  2020 opt/
lrwxrwxrwx  1 root root    4 Feb 25  2020 run -> /run/
drwxr-xr-x 14 root root   4096 Apr  5 17:02 snap/
drwxr-xr-x 2 root root   4096 Apr 14 08:22 snort/
drwxr-xr-x 7 root root   4096 Feb  3  2020 spool/
drwxrwsrwt 8 root root   4096 Apr 14 08:09 tmp/
drwxr-xr-x 3 root root   4096 Feb 25  2020 www/
ubuntu@ubuntu:/var$ sudo snort -l /tmp/snort -b
Running in packet logging mode

     === Initializing Snort ===
Initializing Output Plugins!
ERROR: Stat check on log dir failed: No such file or directory.
Fatal Error, Quitting..
ubuntu@ubuntu:/var$ mkdir -p /tmp/sn
ubuntu@ubuntu:/var$ sudo snort -l /tmp/sn -b
Running in packet logging mode

     === Initializing Snort ===
Initializing Output Plugins!
Log directory = /tmp/sn
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

     === Initialization Complete ===

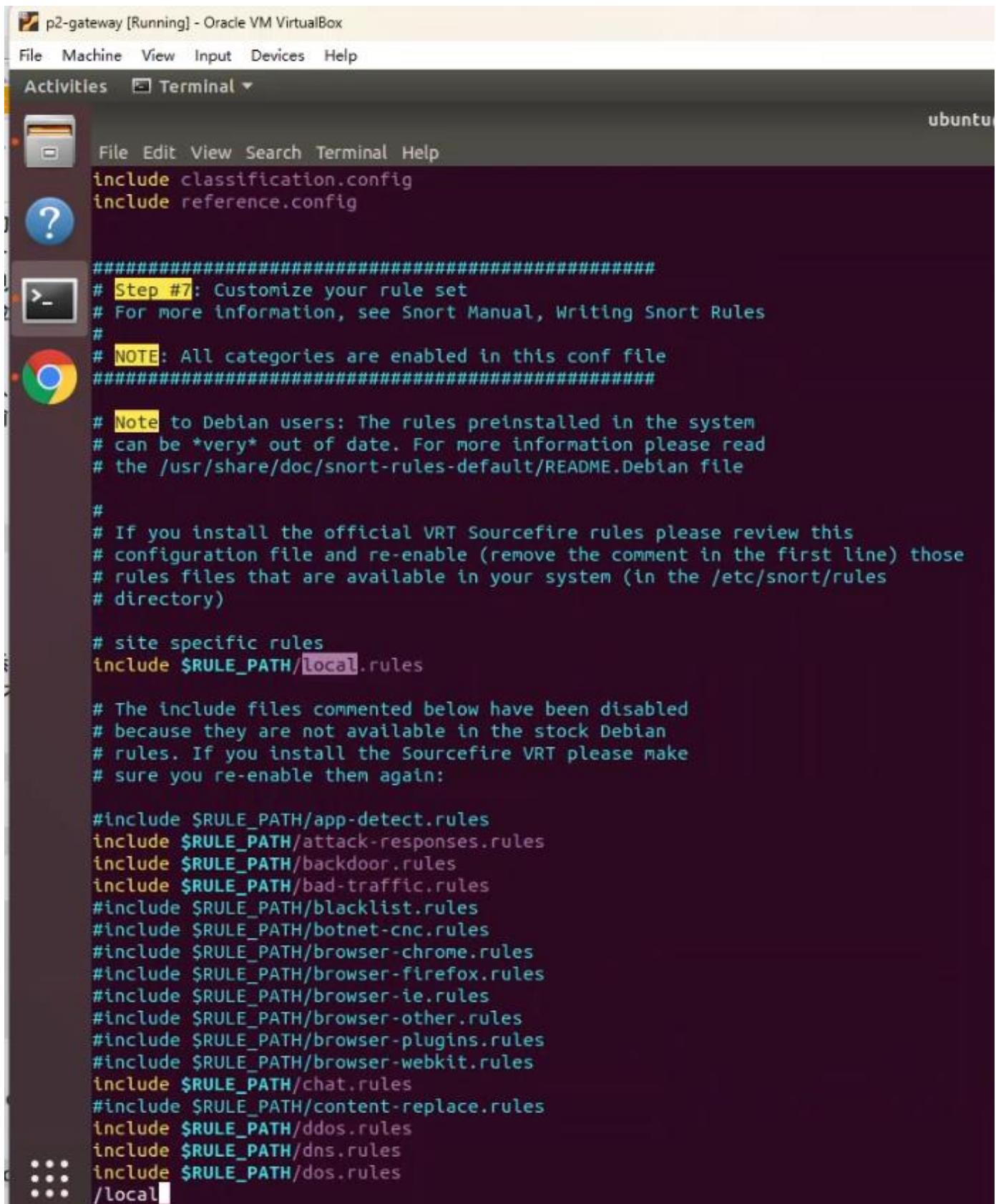
      -> Snort! <-
,,- )~ Version 2.9.7.0 GRE (Build 149)
     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
     Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
     Copyright (C) 1998-2013 Sourcefire, Inc., et al.
     Using libpcap version 1.8.1
     Using PCRE version: 8.39 2016-06-14
     Using ZLIB version: 1.2.11

Commencing packet processing (pid=9115)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.

```

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.



```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal ▾
ubuntu
File Edit View Search Terminal Help
include classification.config
include reference.config

#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

# Note to Debian users: The rules preinstalled in the system
# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

#
# If you install the official VRT Sourcefire rules please review this
# configuration file and re-enable (remove the comment in the first line) those
# rules files that are available in your system (in the /etc/snort/rules
# directory)

# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
/local

```

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。

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help Activities Terminal
File Edit View Search Terminal Help
4/14/09:32:29.583944 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
4/14/09:32:29.583981 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
4/14/09:32:30.584597 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
4/14/09:32:30.584594 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
4/14/09:32:31.584591 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
4/14/09:32:32.587011 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
4/14/09:32:37.586755 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:37.586792 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:37.586794 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:33.592533 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:33.592613 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:34.598871 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:34.598869 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:35.631789 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:35.631822 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:36.591822 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:36.591822 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:36.591867 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:37.586169 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:32:37.587451 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:33:02.289803 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:33:05.327985 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:33:08.368384 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:33:09.487947 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
4/14/09:33:12.528253 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100
^C*** Caught Int-Signal

ubuntu@ubuntu: ~Downloads\$ sudo vim /etc/snort/snort.conf

ubuntu@ubuntu: ~Downloads\$ sudo vim /etc/snort/snort.conf

ubuntu@ubuntu: ~Downloads\$ sudo snort -A console -h 10.0.0.24 -c /etc/snort/snort.conf -q -l enp0s3

04/14/09:36:44.146308 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
04/14/09:36:44.146369 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:45.167582 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:45.167624 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:46.192149 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:46.192187 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.100

^C*** Caught Int-Signal

ubuntu@ubuntu: ~Downloads\$ sudo vim /etc/snort/snort.conf

ubuntu@ubuntu: ~Downloads\$ sudo vim /etc/snort/snort.conf

ubuntu@ubuntu: ~Downloads\$ sudo snort -A console -h 10.0.0.24 -c /etc/snort/snort.conf -q -l enp0s3

04/14/09:36:44.146308 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
04/14/09:36:44.146369 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:45.167582 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:45.167624 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:46.192149 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:36:46.192187 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:37:04.620950 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
04/14/09:37:04.620995 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:37:05.648861 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
04/14/09:37:05.648934 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.100 -> 192.168.0.10
04/14/09:37:11.879497 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
04/14/09:37:11.879497 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
04/14/09:37:12.911723 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
04/14/09:37:12.911764 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.0.10 -> 192.168.0.100
^C*** Caught Int-Signal

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help Activities Terminal
File Edit View Search Terminal Help
64 bytes from 192.168.0.100: icmp_seq=17 ttl=64 time=0.300 ms
64 bytes from 192.168.0.100: icmp_seq=18 ttl=64 time=0.723 ms
64 bytes from 192.168.0.100: icmp_seq=19 ttl=64 time=0.500 ms
64 bytes from 192.168.0.100: icmp_seq=20 ttl=64 time=1.76 ms
64 bytes from 192.168.0.100: icmp_seq=21 ttl=64 time=0.903 ms
64 bytes from 192.168.0.100: icmp_seq=22 ttl=64 time=0.577 ms
64 bytes from 192.168.0.100: icmp_seq=23 ttl=64 time=0.896 ms
64 bytes from 192.168.0.100: icmp_seq=24 ttl=64 time=0.343 ms
64 bytes from 192.168.0.100: icmp_seq=25 ttl=64 time=0.333 ms
64 bytes from 192.168.0.100: icmp_seq=26 ttl=64 time=0.421 ms
^C--- 192.168.0.100 ping statistics ---
26 packets transmitted, 26 received, 0% packet loss, time 25235ms
rtt min/avg/max/mdev = 0.300/1.647/27.306/5.142 ms
ubuntu@ubuntu:~\$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.415 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.527 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.367 ms
^C--- 192.168.0.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.367/0.436/0.527/0.069 ms
ubuntu@ubuntu:~\$
ipvar HOME_NET 10.0.0.0/8 % 桌面网段
ipvar EXTERNAL_NET !\$HOME_NET

NOT")

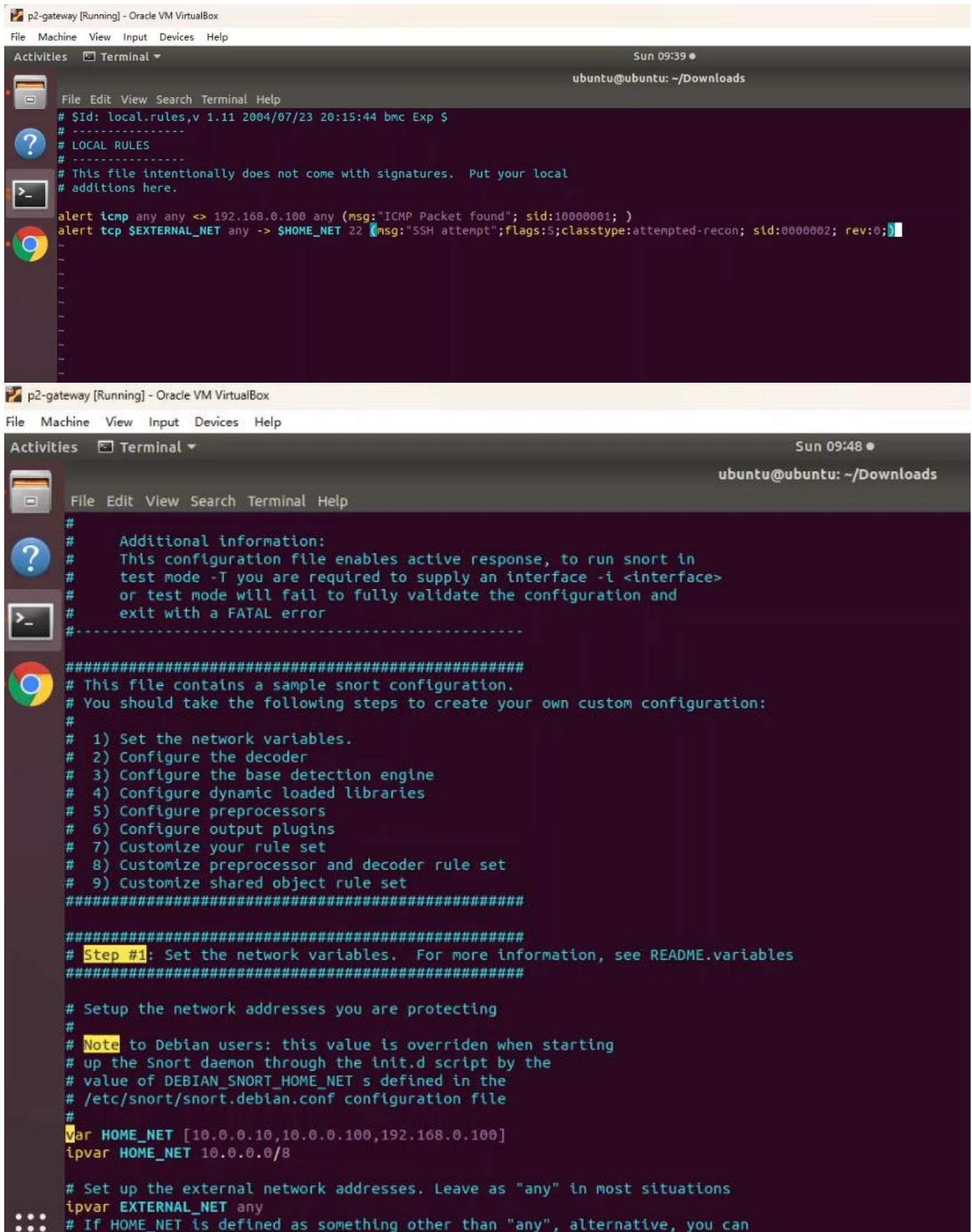
例如

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help Activities Terminal
File Edit View Search Terminal Help
Sun 09:37 *

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help Activities Terminal
File Edit View Search Terminal Help
64 bytes from 192.168.0.100: icmp_seq=20 ttl=64 time=1.76 ms
64 bytes from 192.168.0.100: icmp_seq=21 ttl=64 time=0.993 ms
64 bytes from 192.168.0.100: icmp_seq=22 ttl=64 time=0.577 ms
64 bytes from 192.168.0.100: icmp_seq=23 ttl=64 time=0.896 ms
64 bytes from 192.168.0.100: icmp_seq=24 ttl=64 time=0.343 ms
64 bytes from 192.168.0.100: icmp_seq=25 ttl=64 time=0.333 ms
64 bytes from 192.168.0.100: icmp_seq=26 ttl=64 time=0.421 ms
^C--- 192.168.0.100 ping statistics ---
26 packets transmitted, 26 received, 0% packet loss, time 25235ms
rtt min/avg/max/mdev = 0.300/1.647/27.306/5.142 ms
ubuntu@ubuntu:~\$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.415 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.527 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.367 ms
^C--- 192.168.0.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.367/0.436/0.527/0.069 ms
ubuntu@ubuntu:~\$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.859 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.859 ms
^C--- 192.168.0.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1028ms
rtt min/avg/max/mdev = 0.578/0.718/0.859/0.143 ms
ubuntu@ubuntu:~\$ ping -c 2 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.525 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.414 ms
^C--- 192.168.0.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.414/0.469/0.525/0.059 ms
ubuntu@ubuntu:~\$

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。



```
# $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:0;)

#-----#
# Additional information:
# This configuration file enables active response, to run snort in
# test mode -T you are required to supply an interface -i <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#-----#
##### This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
#
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
var HOME_NET [10.0.0.10,10.0.0.100,192.168.0.100]
ipvar HOME_NET 10.0.0.0/8

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
::: # If HOME_NET is defined as something other than "any", alternative, you can
```

测试

请编辑高亮部分 提交中或英文版本皆可。

```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
ubuntu@ubuntu: ~/Downloads
Sun 09:50 •
ubuntu@ubuntu:~/Downloads$ sudo vim /etc/snort/snort.conf
ubuntu@ubuntu:~/Downloads$ sudo snort -A console -h 10.0.0.24 -c /etc/snort/snort.conf -q -i enp0s3
04/14-09:36:44.146308 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.100
04/14-09:36:44.146369 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
04/14-09:36:45.167582 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:36:45.167624 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:36:46.192149 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:37:04.620695 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:37:05.648868 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:37:05.648934 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.100
04/14-09:37:11.879497 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.100
04/14-09:37:11.879546 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
04/14-09:37:12.911723 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:37:12.911764 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
04/14-09:39:34.215057 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:39:34.215113 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
04/14-09:39:35.253804 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:39:35.253861 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
^C*** Caught Int-Signal
ubuntu@ubuntu:~/Downloads$ sudo vim /etc/snort/snort.conf
ubuntu@ubuntu:~/Downloads$ sudo snort -A console -h 10.0.0.24 -c /etc/snort/snort.conf -q -i enp0s3
04/14-09:45:51.828829 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:45:51.828919 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
04/14-09:45:52.830926 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:45:52.831013 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
04/14-09:45:59.471837 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:45:59.471876 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
04/14-09:46:00.495493 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:46:00.495528 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10
^C*** Caught Int-Signal
ubuntu@ubuntu:~/Downloads$ sudo vim /etc/snort/snort.conf
ubuntu@ubuntu:~/Downloads$ sudo snort -A console -h 10.0.0.24 -c /etc/snort/snort.conf -q -i enp0s3
04/14-09:50:42.677678 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:50:43.696612 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.10 -> 192.168.0.10
04/14-09:50:43.696645 [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] [ICMP] 192.168.0.100 -> 192.168.0.10

```

3.3 任务 3.3 用载荷规则选项来创建和测试 snort 规则 15

```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
ubuntu@ubuntu: /var/log/snort
Sun 10:00 •
ubuntu@ubuntu: /var/log/snort
# $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:0;)

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:10000003;rev:0;)

```

```

p2-gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
ubuntu@ubuntu: ~/Downloads
Sun 10:12 •
ubuntu@ubuntu: ~/Downloads
# $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:0;)

# task 3
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Http Getrequest";flags:S;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:10000003;rev:0;)

```

ID保持唯一性

请编辑高亮部分 提交中或英文版本皆可。

The screenshot displays three terminal windows from a Linux desktop environment:

- Top Terminal:** Shows the contents of the file `/etc/snort/rules/local.rules`. It includes several Snort rules, notably for ICMP and TCP traffic, and ends with a task definition.
- Middle Terminal:** Shows the output of the command `snort -A console -h 10.0.0.0/24 -c /etc/snort/snort.conf -q -i enp0s3`. It shows a series of errors indicating that each rule must contain a rule std. The session ends with a fatal error and quitting.
- Bottom Terminal:** Shows the output of the command `sudo snort -A console -h 10.0.0.0/24 -c /etc/snort/snort.conf -q -i enp0s3`. It shows a series of ICMP packets being processed, including an SSH attempt and a ping response. The output concludes with a ping statistics summary.

3.4 任务 3.4 用非载荷规则选项来创建和测试 snort 规则 16

The screenshot shows a terminal window with the following content:

```
# $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;)

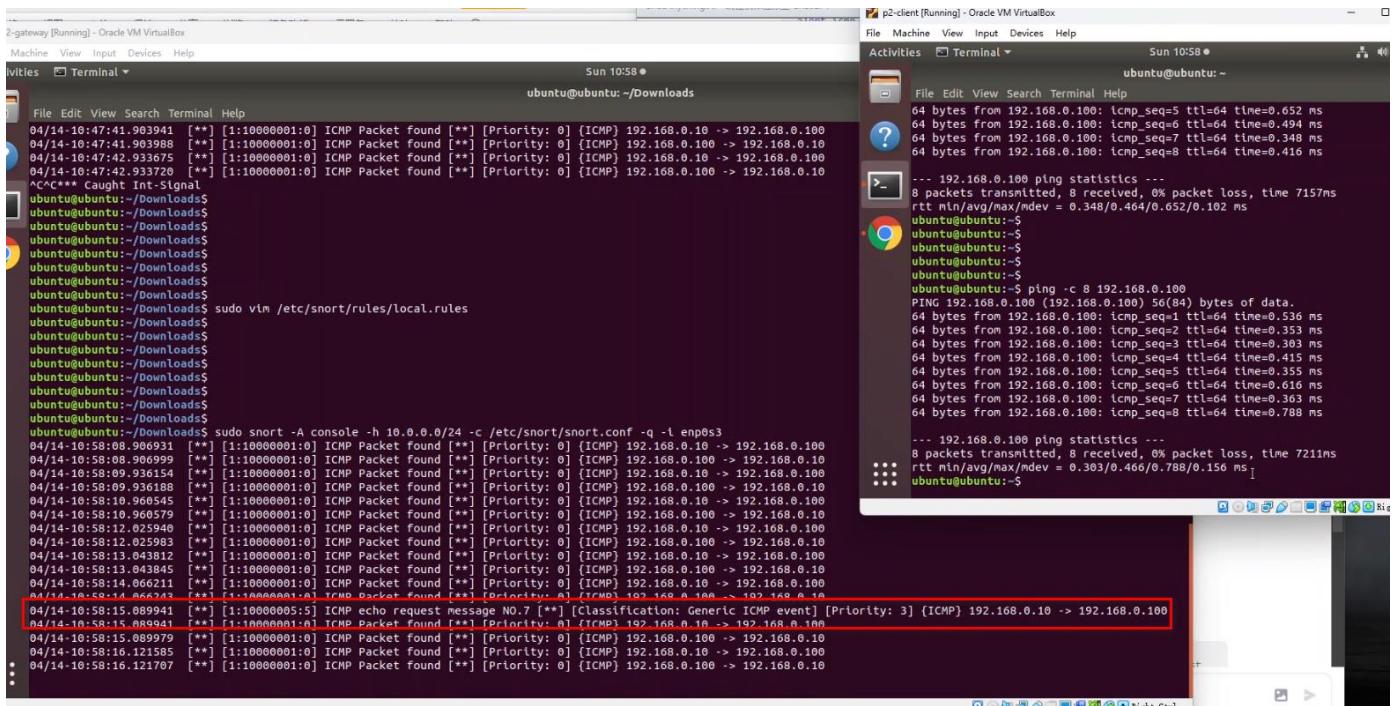
# task 3

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;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP echo request message NO.7";classtype:icmp-event;icmp_seq:7;sid:10000005;rev:5;)
```

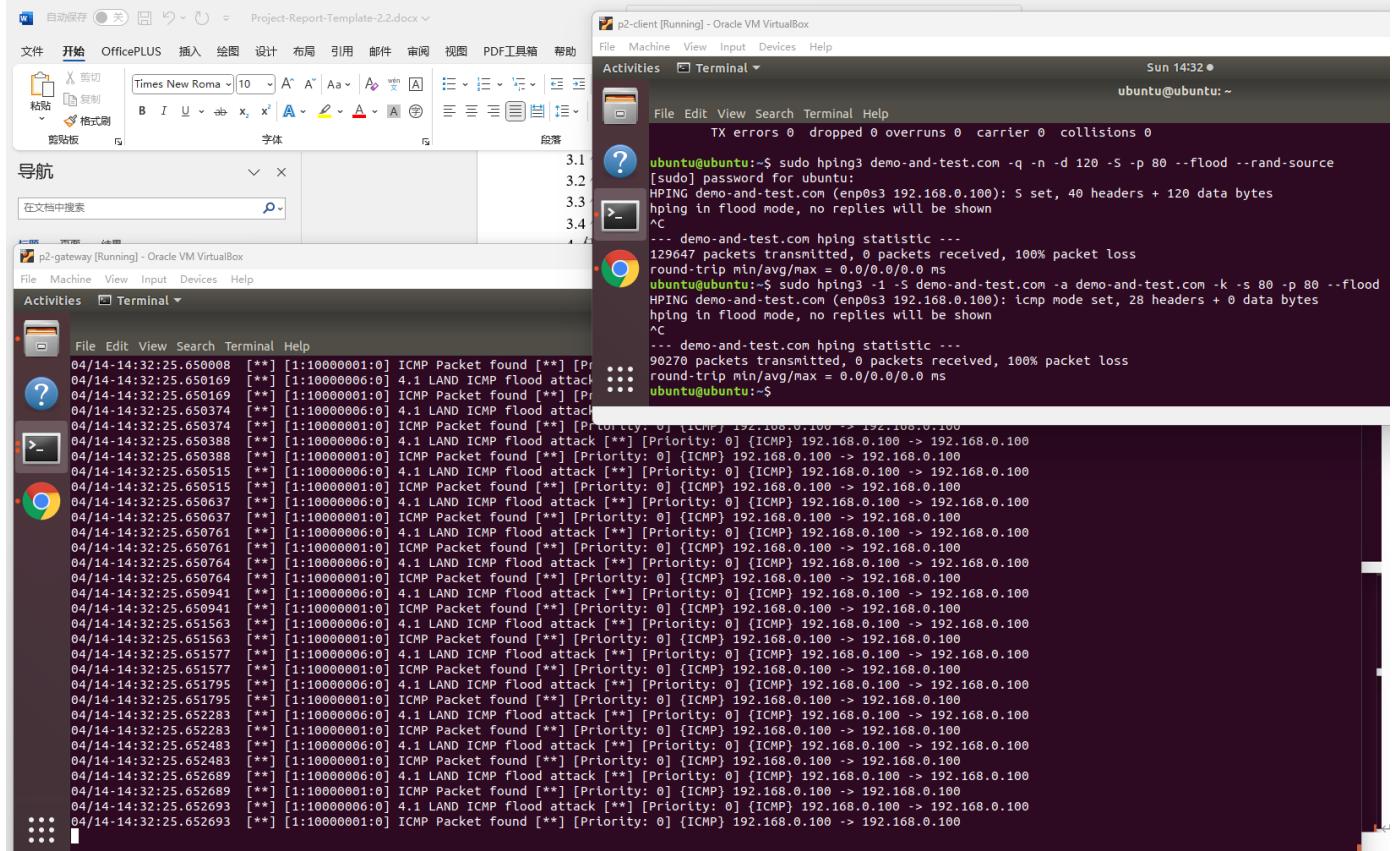
A portion of the last rule is highlighted with a red box, specifically the content part: `(msg:"ICMP echo request message NO.7";classtype:icmp-event;icmp_seq:7;sid:10000005;rev:5;)`.

请编辑高亮部分 提交中或英文版本皆可。



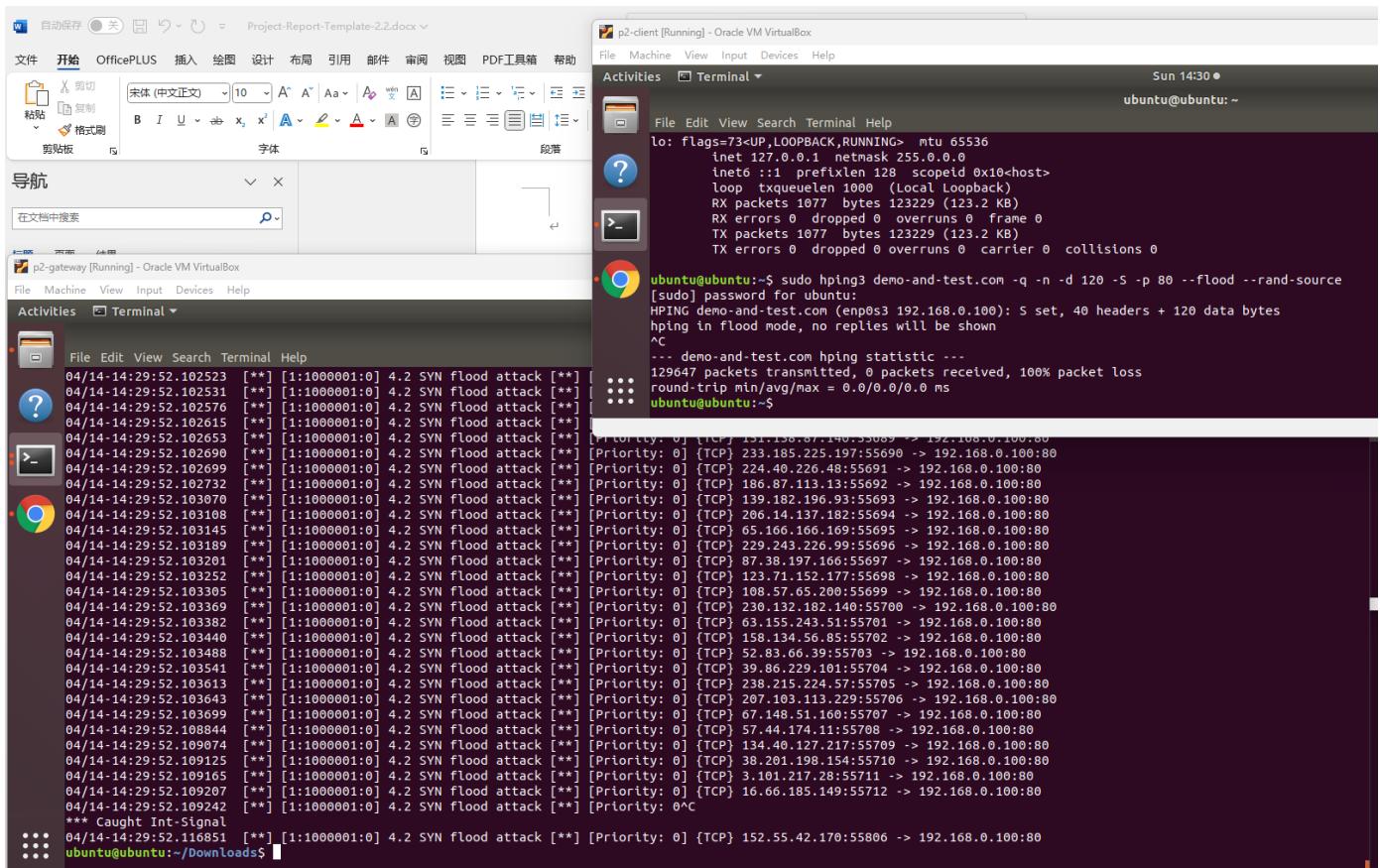
4. 任务 4：实验室要求 16

4.1 任务 4.1 Land 攻击部署和检测 17



4.2 任务 4.2 洪水攻击的部署和检测 18

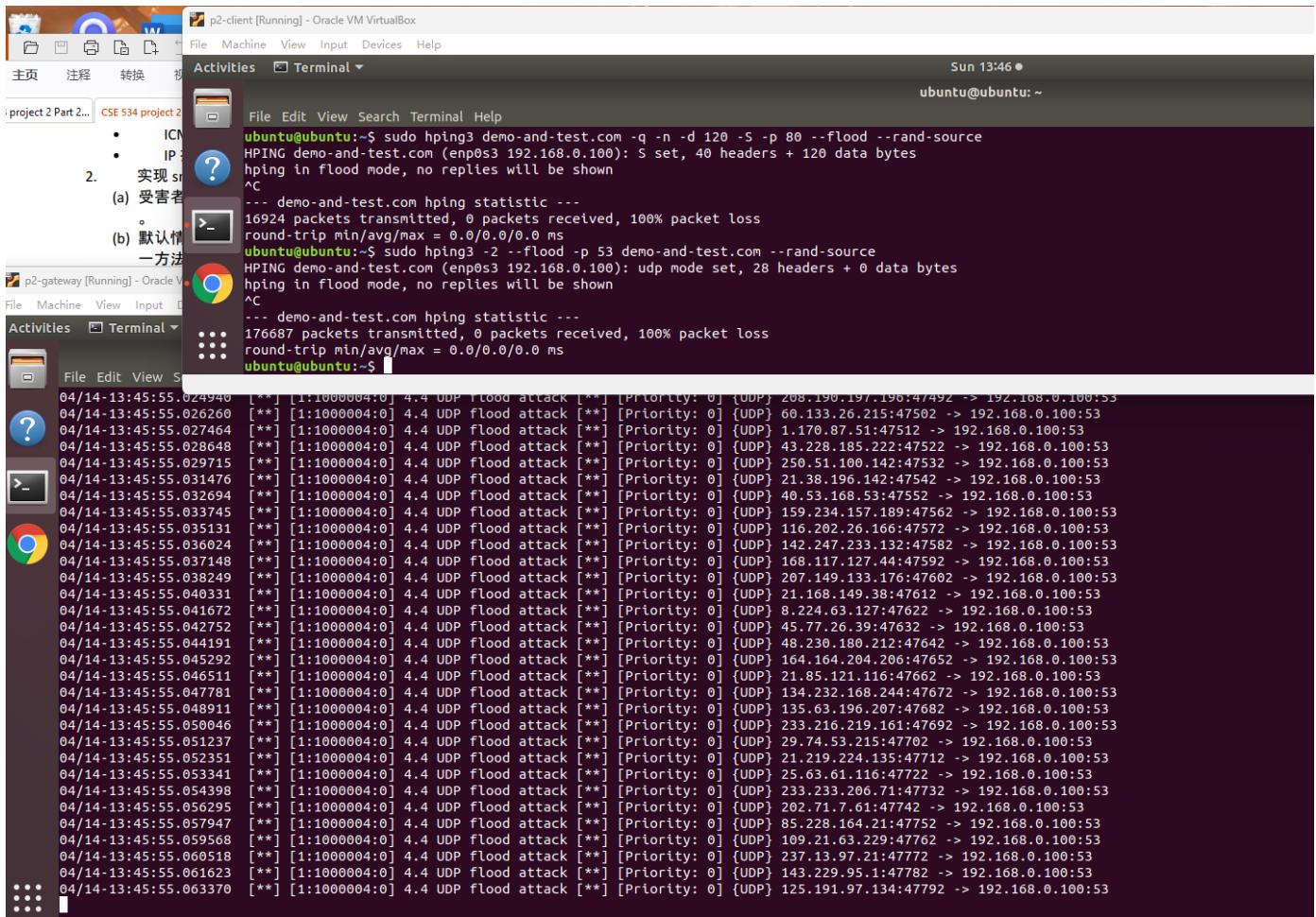
请编辑高亮部分 提交中或英文版本皆可。



4.3 任务 4.3 Smurf 攻击的部署和检测 18

4.4 任务 4.4 UDP 洪水攻击的部署和检测 19

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.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。

```

25. cd /etc/snort/
26. sudo cp snort.conf snort.backup.conf
27. bak cmd: sudo cp snort.backup.conf snort.conf
28. sudo vim /etc/snort/snort.conf
29. sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf
30. true cmd: sudo sed -
   i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf
31. sudo vim /etc/snort/rules/local.rules
32.
33. alert icmp any any <> 192.168.0.100 any (msg:"ICMP Packet found"; sid:10000001; )
34.
35. sudo snort -A console -c /etc/snort/snort.conf -q -i enp0s3
36.
37. 3.2 任务 3.2 用系统变量来创建和测试 snort 规则
38.
39. sudo vim /etc/snort/snort.conf
40.
41. ipvar HOME_NET 10.0.0.0/8 % 将服务器端网络设置为 HOME_NET
42. ipvar EXTERNAL_NET !$HOME_NET
43.
44. sudo snort -A console -h 10.0.0.0/24 -c /etc/snort/snort.conf -q -i enp0s3
45.
46. vim /etc/snort/rules/local.rules
47.
48. alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SSH attempt";flags:S;classtype:attempted-recon; sid:000002; rev:0;)
49. 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
50.
51.
52. sudo snort -d -r /var/log/snort/snort.log.1713113771 tcp
53.
54. 任务 3.3 用载荷规则选项来创建和测试 snort 规则
55.
56. alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Http Getrequest";content:"GET";classtype:web-application-activity;sid:10000003;rev:0;)
57. alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (content:"|5c00|P|00|I|00|P|00|E|00 5c|";sid:10000004;rev:1;)
58.
59. $ curl 10.0.0.10 % 你可以直接访问 IP 地址并运行: curl http://10.0.0.10
60.
61. alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP echo request message NO.7";classtype:icmp-event;icmp_seq:7;sid:10000004;rev:0;)
62.
63. ping -c 8 192.168.0.10
64.
65.
66. test4:
67. sudo vim /etc/snort/snort.conf
68. sudo vim /etc/snort/rules/local.rules
69. sudo vim /etc/sysctl.conf
70.
71. $ sudo echo 0 >/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts % 启用对广播请求的临时响应
72. $ sudo sysctl net.ipv4.icmp_echo_ignore_broadcasts 0
73.
74. sudo vim /etc/sysctl
75. net.ipv4.icmp_echo_ignore_broadcasts=0 % 你可能需要重新启动节点

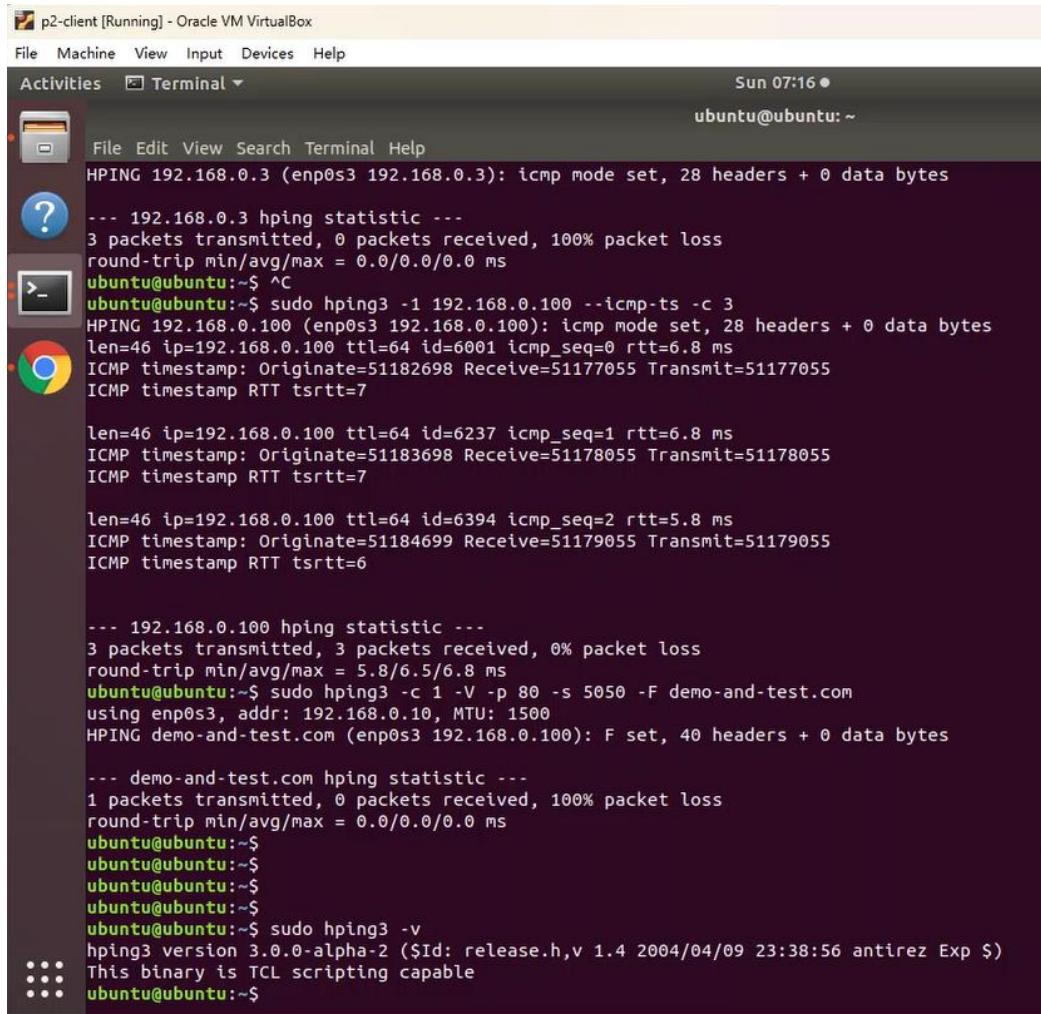
```

在客户端上完成如下任务

2. 使用 hping3 测试网络 8

2.1 测试已安装的软件和服务 8

请编辑高亮部分 提交中或英文版本皆可.



```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:16 ●
ubuntu@ubuntu:~>

File Edit View Search Terminal Help
HPING 192.168.0.3 (enp0s3 192.168.0.3): icmp mode set, 28 headers + 0 data bytes
--- 192.168.0.3 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ ^C
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.100 --icmp-ts -c 3
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=6001 icmp_seq=0 rtt=6.8 ms
ICMP timestamp: Originate=51182698 Receive=51177055 Transmit=51177055
ICMP timestamp RTT tsrtt=7

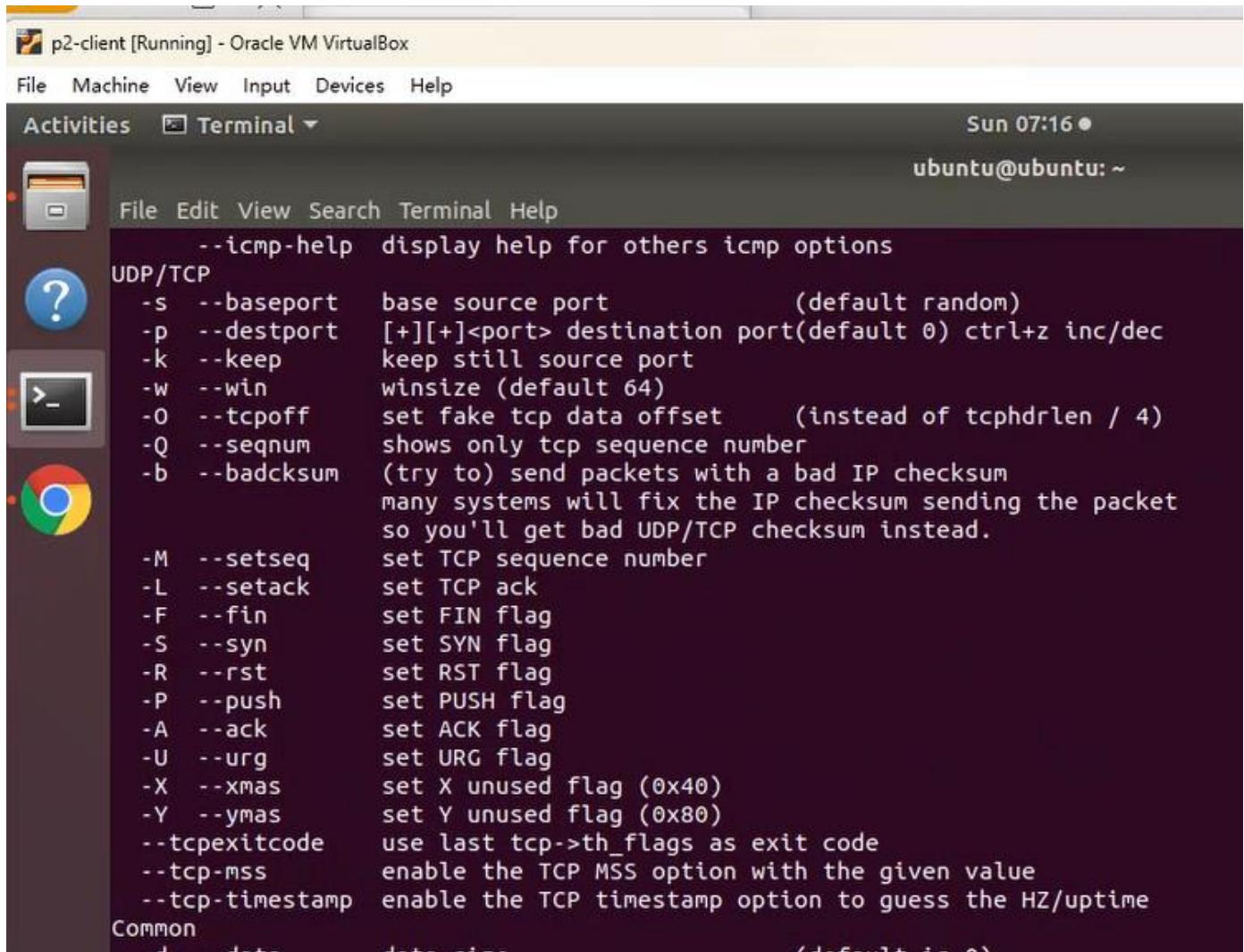
len=46 ip=192.168.0.100 ttl=64 id=6237 icmp_seq=1 rtt=6.8 ms
ICMP timestamp: Originate=51183698 Receive=51178055 Transmit=51178055
ICMP timestamp RTT tsrtt=7

len=46 ip=192.168.0.100 ttl=64 id=6394 icmp_seq=2 rtt=5.8 ms
ICMP timestamp: Originate=51184699 Receive=51179055 Transmit=51179055
ICMP timestamp RTT tsrtt=6

--- 192.168.0.100 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.8/6.5/6.8 ms
ubuntu@ubuntu:~$ sudo hping3 -c 1 -V -p 80 -s 5050 -F demo-and-test.com
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING demo-and-test.com (enp0s3 192.168.0.100): F set, 40 headers + 0 data bytes

--- demo-and-test.com hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ sudo hping3 -v
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable
ubuntu@ubuntu:~$
```

请编辑高亮部分 提交中或英文版本皆可.

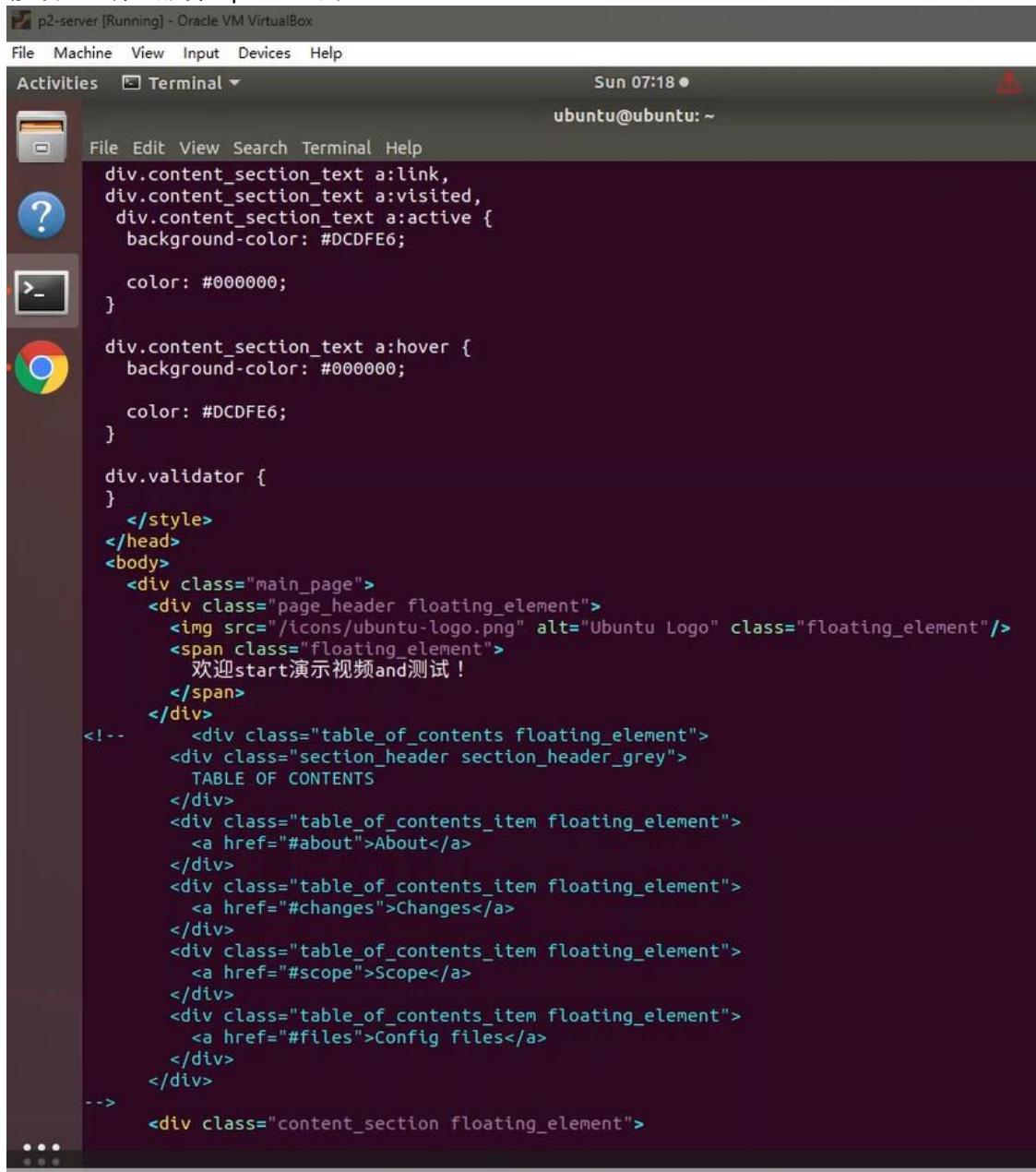


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "p2-client [Running] - Oracle VM VirtualBox". The terminal shows a command-line interface for setting network flags. The user has entered the command "tcpdump -c 100 -w /tmp/packets.pcap >> /tmp/packets.pcap" followed by a series of flags. The flags are color-coded: red for common flags (-s, -l, -t, -A, -U, -X, -Y), blue for UDP/TCP specific flags (-s, -p, -k, -w, -O, -Q, -b, -M, -L, -F, -S, -R, -P, -A, -U, -X, -Y, --tcpexitcode, --tcp-mss, --tcp-timestamp), and green for common flags (-d). The terminal window also displays the date and time (Sun 07:16) and the user's session information (ubuntu@ubuntu: ~).

```
--icmp-help  display help for others icmp options
UDP/TCP
-s  --baseport  base source port          (default random)
-p  --destport  [+][+<port> destination port(default 0) ctrl+z inc/dec
-k  --keep      keep still source port
-w  --win       winsize (default 64)
-O  --tcpoff    set fake tcp data offset   (instead of tcphdrlen / 4)
-Q  --seqnum    shows only tcp sequence number
-b  --badcksum  (try to) send packets with a bad IP checksum
               many systems will fix the IP checksum sending the packet
               so you'll get bad UDP/TCP checksum instead.
-M  --setseq    set TCP sequence number
-L  --setack    set TCP ack
-F  --fin       set FIN flag
-S  --syn       set SYN flag
-R  --rst       set RST flag
-P  --push     set PUSH flag
-A  --ack      set ACK flag
-U  --urg      set URG flag
-X  --xmas    set X unused flag (0x40)
-Y  --ymas    set Y unused flag (0x80)
--tcpexitcode use last tcp->th_flags as exit code
--tcp-mss    enable the TCP MSS option with the given value
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d  --data     data size
               (default is 0)
```

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



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window has a dark background and contains the following code:

```
File Machine View Input Devices Help
Activities Terminal Sun 07:18 ●
ubuntu@ubuntu: ~
File Edit View Search Terminal Help
div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

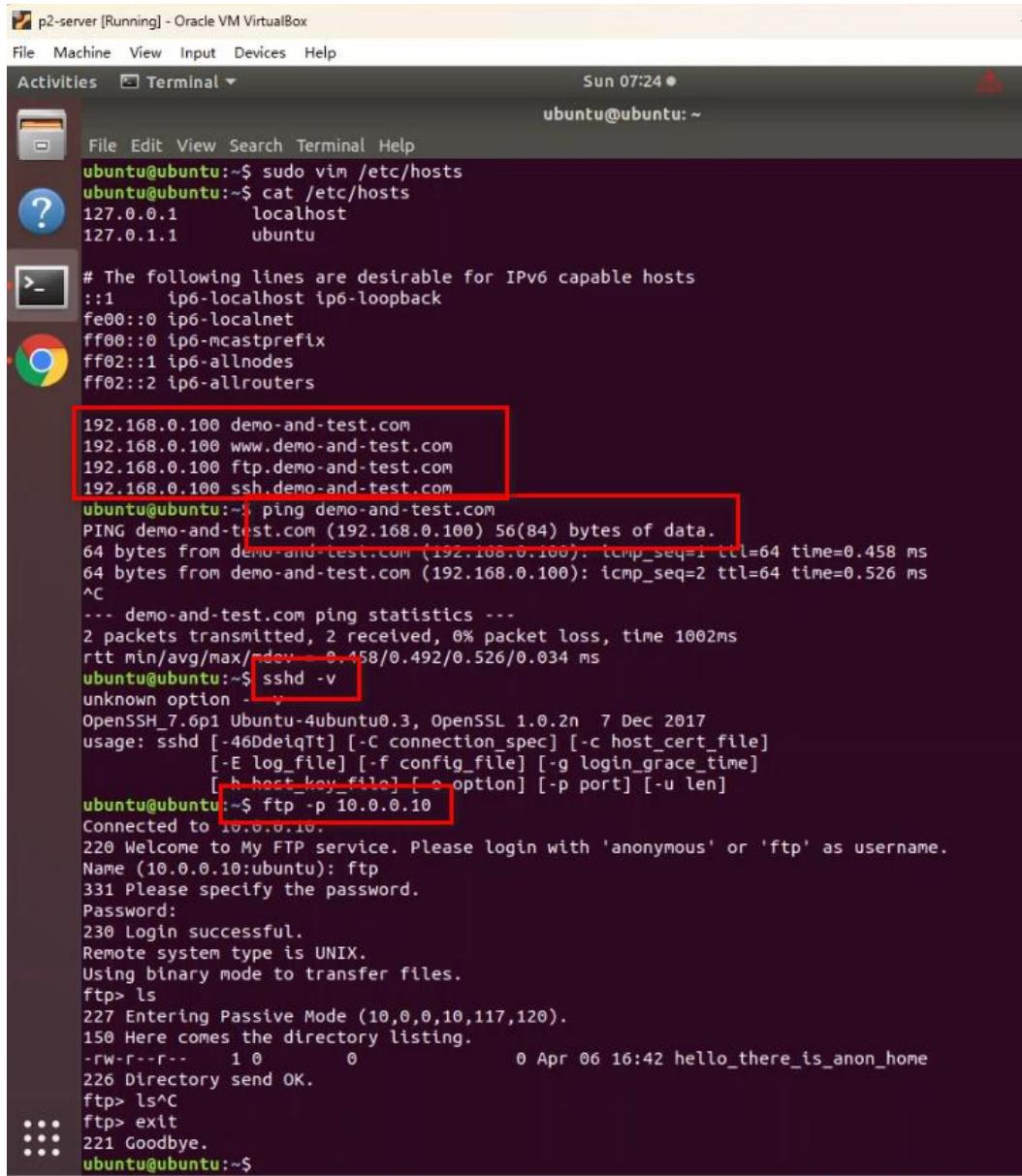
<span class="floating_element">
    欢迎start演示视频and测试 !
</span>
</div>
<!--
    <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
            TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
            <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
            <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
            <a href="#scope">Scope</a>
        </div>
        <div class="table_of_contents_item floating_element">
            <a href="#files">Config files</a>
        </div>
    </div>
-->
<div class="content_section floating_element">
```

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.



The screenshot shows a terminal window titled "p2-server [Running] - Oracle VM VirtualBox". The terminal displays the following session:

```

File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo vim /etc/hosts
ubuntu@ubuntu:~$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      ubuntu

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.0.100 demo-and-test.com
192.168.0.100 www.demo-and-test.com
192.168.0.100 ftp.demo-and-test.com
192.168.0.100 ssh.demo-and-test.com
ubuntu@ubuntu:~$ ping demo-and-test.com
PING demo-and-test.com (192.168.0.100) 56(84) bytes of data.
64 bytes from demo-and-test.com (192.168.0.100): icmp_seq=1 ttl=64 time=0.458 ms
64 bytes from demo-and-test.com (192.168.0.100): icmp_seq=2 ttl=64 time=0.526 ms
^C
--- demo-and-test.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev 0.458/0.492/0.526/0.034 ms
ubuntu@ubuntu:~$ sshd -v
unknown option -v
OpenSSH_7.6p1 Ubuntu-4ubuntu0.3, OpenSSL 1.0.2n 7 Dec 2017
usage: sshd [-46DdeiqTt] [-c connection_spec] [-c host_cert_file]
           [-E log_file] [-f config_file] [-g login_grace_time]
           [-h host_key_file] [-o option] [-p port] [-u len]
ubuntu@ubuntu:~$ ftp -p 10.0.0.10
Connected to 10.0.0.10.
220 Welcome to My FTP service. Please login with 'anonymous' or 'ftp' as username.
Name (10.0.0.10:ubuntu): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,0,0,10,117,120).
150 Here comes the directory listing.
-rw-r--r-- 1 0          0          0 Apr 06 16:42 hello_there_is_anon_home
226 Directory send OK.
ftp> ls^C
ftp> exit
221 Goodbye.
ubuntu@ubuntu:~$
```

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。

```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:35 ●
ubuntu@ubuntu:~ File Edit View Search Terminal Help
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data      data size          (default is 0)
-E --file      data from file
-e --sign      add 'signature'
-j --dump      dump packets in hex
-J --print     dump printable characters
-B --safe      enable 'safe' protocol
-u --end       tell you when --file reached EOF and prevent rewind
-T --traceroute traceroute mode           (implies --bind and --ttl 1)
--tr-stop      Exit when receive the first not ICMP in traceroute mode
--tr-keep-ttl   Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt    Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
--apd-send     Send the packet described with APD (see docs/APD.txt)
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ sudo hping3 -S www.demo-and-test.com -p 80
[sudo] password for ubuntu:
HPING www.demo-and-test.com (enp0s3 192.168.0.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=7.8 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=5.0 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=5.8 ms
^C
--- www.demo-and-test.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.0/6.2/7.8 ms
ubuntu@ubuntu:~$ sudo hping3 -S www.demo-and-test.com -p ++1
HPING www.demo-and-test.com (enp0s3 192.168.0.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=1 flags=RA seq=0 win=0 rtt=3.4 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=2 flags=RA seq=1 win=0 rtt=8.2 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=3 flags=RA seq=2 win=0 rtt=2.0 ms
^C
--- www.demo-and-test.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.0/4.5/8.2 ms
ubuntu@ubuntu:~$ sudo hping3 -f www.demo-and-test.com -p 80
HPING www.demo-and-test.com (enp0s3 192.168.0.100): NO FLAGS are set, 40 headers + 0 data bytes
... ZZZ Goodbye.

```

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.

```

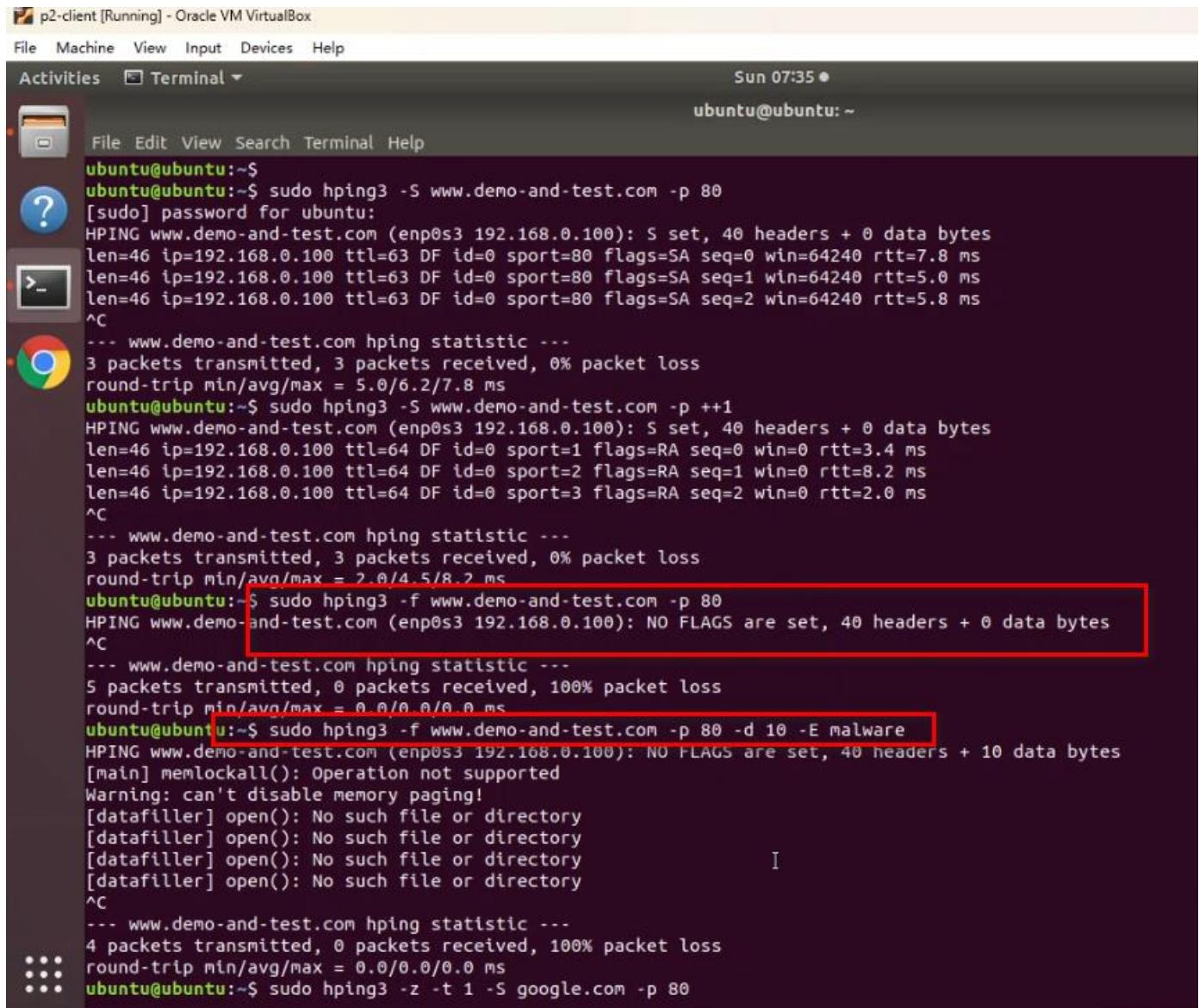
p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:35 *
ubuntu@ubuntu:~$

File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo hping3 -S www.demo-and-test.com -p 80
[sudo] password for ubuntu:
HPING www.demo-and-test.com (enp0s3 192.168.0.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=7.8 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=5.0 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=5.8 ms
^C
--- www.demo-and-test.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.0/6.2/7.8 ms
ubuntu@ubuntu:~$ sudo hping3 -S www.demo-and-test.com -p ++1
HPING www.demo-and-test.com (enp0s3 192.168.0.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=1 flags=RA seq=0 win=0 rtt=3.4 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=2 flags=RA seq=1 win=0 rtt=8.2 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=3 flags=RA seq=2 win=0 rtt=2.0 ms
^C
--- www.demo-and-test.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.0/4.5/8.2 ms
ubuntu@ubuntu:~$ sudo hping3 -f www.demo-and-test.com -p 80
HPING www.demo-and-test.com (enp0s3 192.168.0.100): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- www.demo-and-test.com hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -f www.demo-and-test.com -p 80 -d 10 -E malware
HPING www.demo-and-test.com (enp0s3 192.168.0.100): NO FLAGS are set, 40 headers + 10 data bytes
[main] memlockall(): Operation not supported
Warning: can't disable memory paging!
[datafiller] open(): No such file or directory
^C
--- www.demo-and-test.com hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -z -t 1 -S google.com -p 80

```

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.



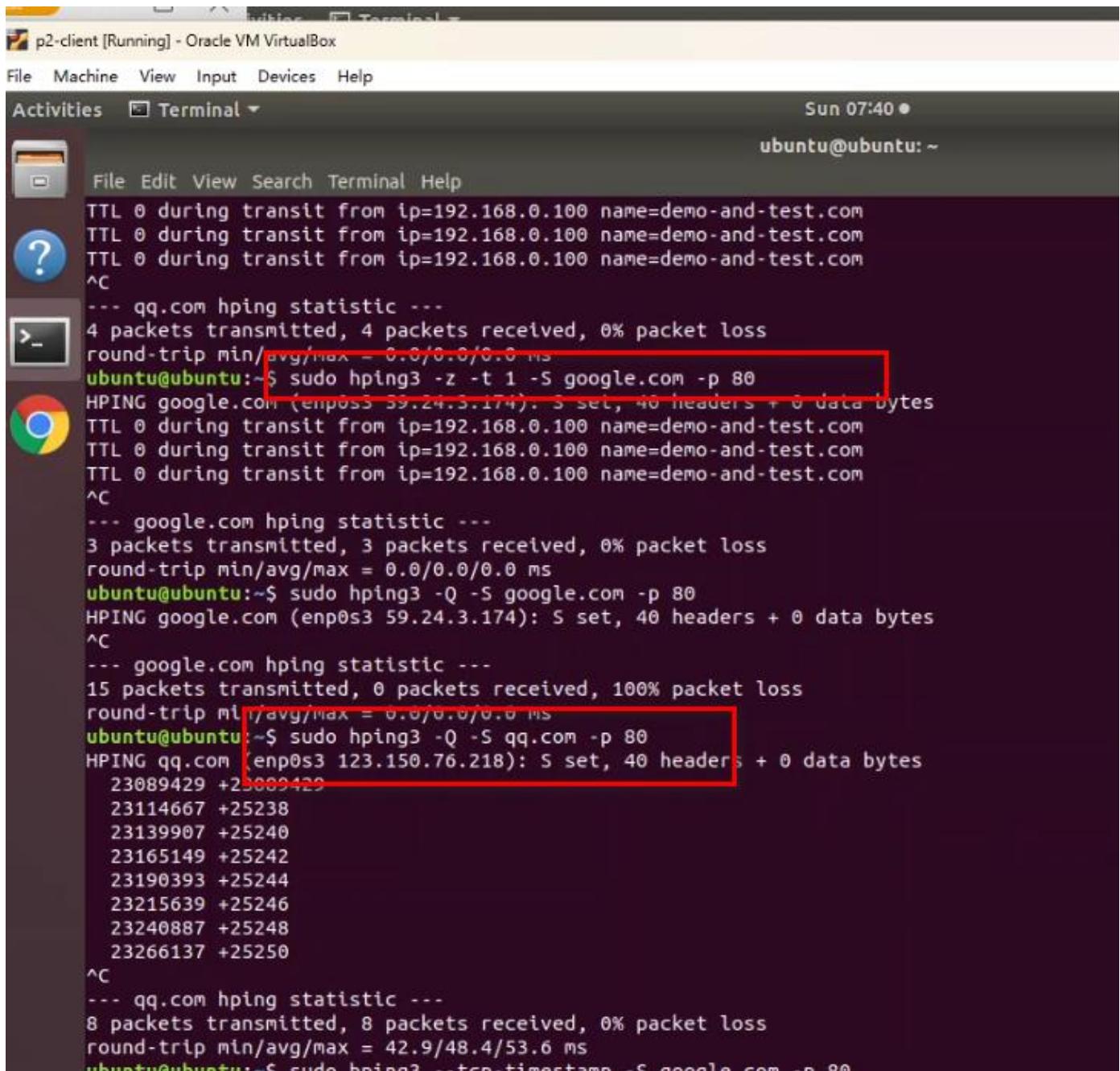
```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:35 •
ubuntu@ubuntu:~$ sudo hping3 -S www.demo-and-test.com -p 80
[sudo] password for ubuntu:
HPING www.demo-and-test.com (enp0s3 192.168.0.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=7.8 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=5.0 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=5.8 ms
^C
--- www.demo-and-test.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.0/6.2/7.8 ms
ubuntu@ubuntu:~$ sudo hping3 -S www.demo-and-test.com -p ++1
HPING www.demo-and-test.com (enp0s3 192.168.0.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=1 flags=RA seq=0 win=0 rtt=3.4 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=2 flags=RA seq=1 win=0 rtt=8.2 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=3 flags=RA seq=2 win=0 rtt=2.0 ms
^C
--- www.demo-and-test.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.0/4.5/8.2 ms
ubuntu@ubuntu:~$ sudo hping3 -f www.demo-and-test.com -p 80
HPING www.demo-and-test.com (enp0s3 192.168.0.100): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- www.demo-and-test.com hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -f www.demo-and-test.com -p 80 -d 10 -E malware
HPING www.demo-and-test.com (enp0s3 192.168.0.100): NO FLAGS are set, 40 headers + 10 data bytes
[main] memlockall(): Operation not supported
Warning: can't disable memory paging!
[datafiller] open(): No such file or directory
^C
--- www.demo-and-test.com hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -z -t 1 -S google.com -p 80

```

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。



```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:40 *
ubuntu@ubuntu: ~

File Edit View Search Terminal Help
TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
^C
--- qq.com hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -z -t 1 -S google.com -p 80
HPING google.com (enp0s3 59.24.3.174): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
^C
--- google.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -Q -S google.com -p 80
HPING google.com (enp0s3 59.24.3.174): S set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
15 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -Q -S qq.com -p 80
HPING qq.com (enp0s3 123.150.76.218): S set, 40 headers + 0 data bytes
23089429 +25089429
23114667 +25238
23139907 +25240
23165149 +25242
23190393 +25244
23215639 +25246
23240887 +25248
23266137 +25250
^C
--- qq.com hping statistic ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 42.9/48.4/53.6 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S google.com -p 80

```

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.

```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:40 ●
ubuntu@ubuntu: ~
File Edit View Search Terminal Help
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -Q -S google.com -p 80
HPING google.com (enp0s3 59.24.3.174): 5 set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
15 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -Q -S qq.com -p 80
HPING qq.com (enp0s3 123.150.76.218): 5 set, 40 headers + 0 data bytes
 23089429 +23089429
 23114667 +25238
 23139907 +25240
 23165149 +25242
 23190393 +25244
 23215639 +25246
 23240887 +25248
 23266137 +25250
^C
--- qq.com hping statistic ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 42.9/48.4/53.6 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S google.com -p 80
HPING google.com (enp0s3 59.24.3.174): 5 set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
11 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S qq.com -p 80
HPING qq.com (enp0s3 113.108.81.189): 5 set, 40 headers + 0 data bytes
len=46 ip=113.108.81.189 ttl=254 id=2521 sport=80 flags=SA seq=0 win=32768 rtt=11.0 ms
len=46 ip=113.108.81.189 ttl=254 id=2522 sport=80 flags=SA seq=1 win=32768 rtt=10.1 ms
len=46 ip=113.108.81.189 ttl=254 id=2523 sport=80 flags=SA seq=2 win=32768 rtt=9.2 ms
len=46 ip=113.108.81.189 ttl=254 id=2524 sport=80 flags=SA seq=3 win=32768 rtt=15.1 ms
^C
qq.com hping statistic
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.2/11.4/15.1 ms

```

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.

```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:40 ●
ubuntu@ubuntu: ~
File Edit View Search Terminal Help
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -Q -S google.com -p 80
HPING google.com (enp0s3 59.24.3.174): 5 set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
15 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -Q -S qq.com -p 80
HPING qq.com (enp0s3 123.150.76.218): 5 set, 40 headers + 0 data bytes
 23089429 +23089429
 23114667 +25238
 23139907 +25240
 23165149 +25242
 23190393 +25244
 23215639 +25246
 23240887 +25248
 23266137 +25250
^C
--- qq.com hping statistic ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 42.9/48.4/53.6 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S google.com -p 80
HPING google.com (enp0s3 59.24.3.174): 5 set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
11 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S qq.com -p 80
HPING qq.com (enp0s3 113.108.81.189): 5 set, 40 headers + 0 data bytes
len=46 ip=113.108.81.189 ttl=254 id=2521 sport=80 flags=SA seq=0 win=32768 rtt=11.0 ms
len=46 ip=113.108.81.189 ttl=254 id=2522 sport=80 flags=SA seq=1 win=32768 rtt=10.1 ms
len=46 ip=113.108.81.189 ttl=254 id=2523 sport=80 flags=SA seq=2 win=32768 rtt=9.2 ms
len=46 ip=113.108.81.189 ttl=254 id=2524 sport=80 flags=SA seq=3 win=32768 rtt=15.1 ms
^C
qq.com hping statistic
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.2/11.4/15.1 ms

```

3. 使用 hping3 进行侦察 12

3.1 将 ACK 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.

```

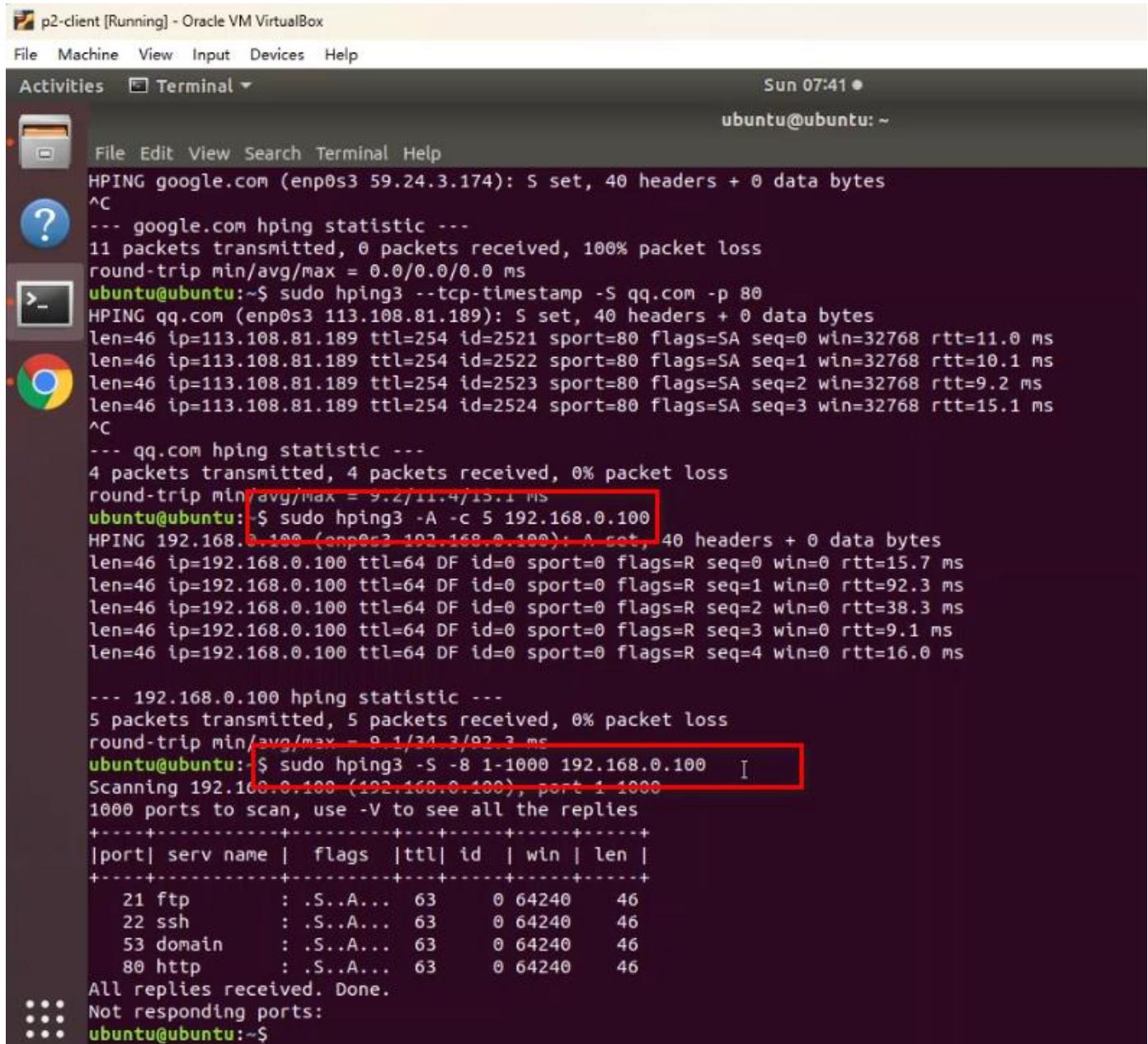
p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:41 •
ubuntu@ubuntu: ~

File Edit View Search Terminal Help
HPING google.com (enp0s3 59.24.3.174): S set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
11 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S qq.com -p 80
HPING qq.com (enp0s3 113.108.81.189): S set, 40 headers + 0 data bytes
len=46 ip=113.108.81.189 ttl=254 id=2521 sport=80 flags=SA seq=0 win=32768 rtt=11.0 ms
len=46 ip=113.108.81.189 ttl=254 id=2522 sport=80 flags=SA seq=1 win=32768 rtt=10.1 ms
len=46 ip=113.108.81.189 ttl=254 id=2523 sport=80 flags=SA seq=2 win=32768 rtt=9.2 ms
len=46 ip=113.108.81.189 ttl=254 id=2524 sport=80 flags=SA seq=3 win=32768 rtt=15.1 ms
^C
--- qq.com hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.2/11.4/15.1 ms
ubuntu@ubuntu:~$ sudo hping3 -A -c 5 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=0 win=0 rtt=15.7 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=1 win=0 rtt=92.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=2 win=0 rtt=38.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=3 win=0 rtt=9.1 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=4 win=0 rtt=16.0 ms

--- 192.168.0.100 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 9.1/24.3/92.3 ms
ubuntu@ubuntu:~$ sudo hping3 -S -8 1-1000 192.168.0.100  I
Scanning 192.168.0.100 (192.168.0.100), port 1-1000
1000 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+-----+-----+-----+
      21 ftp       : .S..A... 63      0 64240    46
      22 ssh       : .S..A... 63      0 64240    46
      53 domain   : .S..A... 63      0 64240    46
      80 http      : .S..A... 63      0 64240    46
All replies received. Done.
Not responding ports:
ubuntu@ubuntu:~$
```

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.



```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:41 •
ubuntu@ubuntu: ~

File Edit View Search Terminal Help
HPING google.com (enp0s3 59.24.3.174): S set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
11 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S qq.com -p 80
HPING qq.com (enp0s3 113.108.81.189): S set, 40 headers + 0 data bytes
len=46 ip=113.108.81.189 ttl=254 id=2521 sport=80 flags=SA seq=0 win=32768 rtt=11.0 ms
len=46 ip=113.108.81.189 ttl=254 id=2522 sport=80 flags=SA seq=1 win=32768 rtt=10.1 ms
len=46 ip=113.108.81.189 ttl=254 id=2523 sport=80 flags=SA seq=2 win=32768 rtt=9.2 ms
len=46 ip=113.108.81.189 ttl=254 id=2524 sport=80 flags=SA seq=3 win=32768 rtt=15.1 ms
^C
--- qq.com hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.2/11.4/15.1 ms
ubuntu@ubuntu:~$ sudo hping3 -A -c 5 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=0 win=0 rtt=15.7 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=1 win=0 rtt=92.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=2 win=0 rtt=38.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=3 win=0 rtt=9.1 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=4 win=0 rtt=16.0 ms

--- 192.168.0.100 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 9.1/24.3/92.3 ms
ubuntu@ubuntu:~$ sudo hping3 -S -8 1-1000 192.168.0.100 I
Scanning 192.168.0.100 (192.168.0.100), port 1-1000
1000 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+-----+-----+-----+
      21 ftp       : .S..A... 63      0 64240    46
      22 ssh       : .S..A... 63      0 64240    46
      53 domain   : .S..A... 63      0 64240    46
      80 http     : .S..A... 63      0 64240    46
All replies received. Done.
Not responding ports:
ubuntu@ubuntu:~$
```

请编辑高亮部分 提交中或英文版本皆可.

```

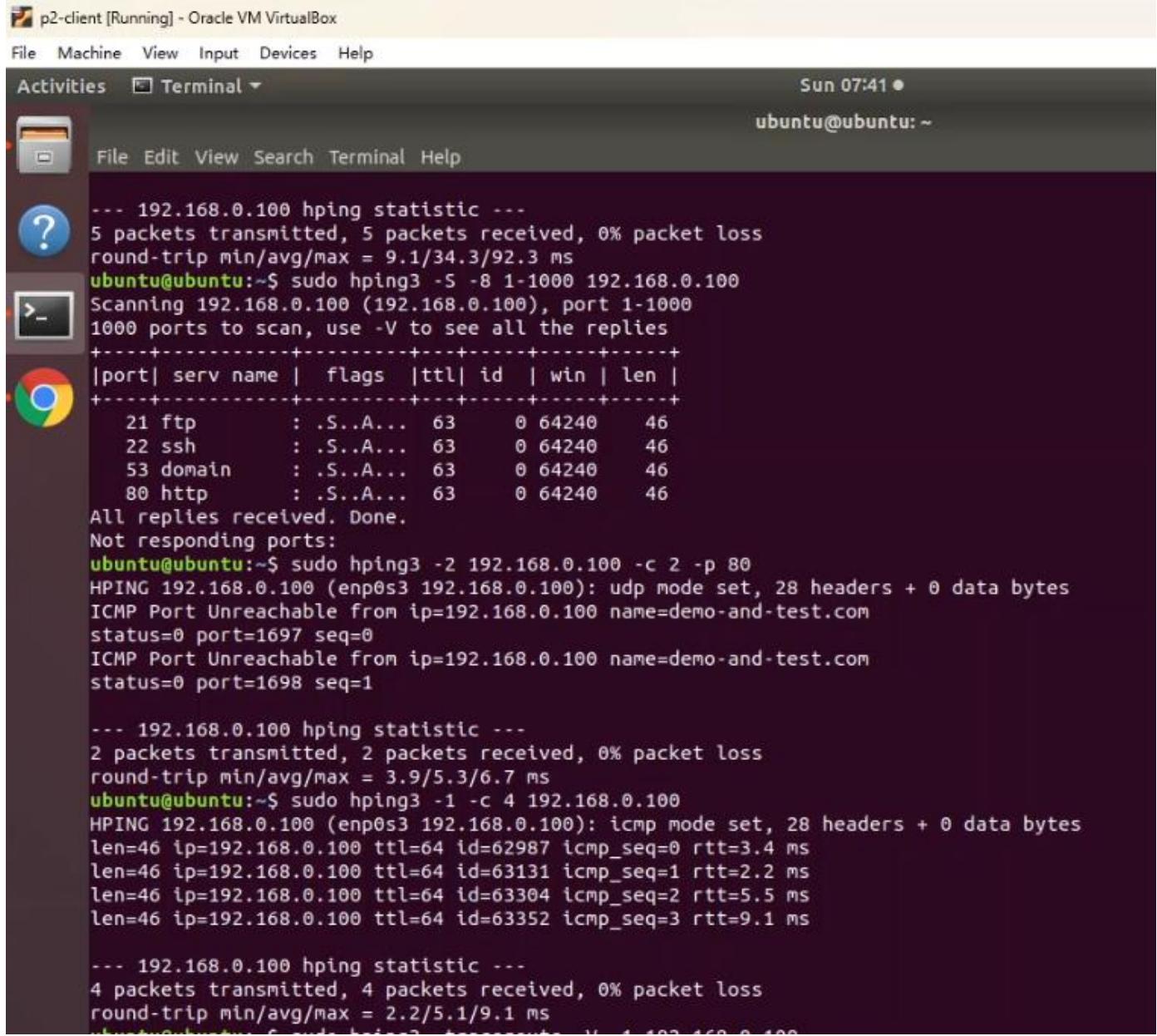
p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:41 •
ubuntu@ubuntu: ~

File Edit View Search Terminal Help
HPING google.com (enp0s3 59.24.3.174): S set, 40 headers + 0 data bytes
^C
--- google.com hping statistic ---
11 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 --tcp-timestamp -S qq.com -p 80
HPING qq.com (enp0s3 113.108.81.189): S set, 40 headers + 0 data bytes
len=46 ip=113.108.81.189 ttl=254 id=2521 sport=80 flags=SA seq=0 win=32768 rtt=11.0 ms
len=46 ip=113.108.81.189 ttl=254 id=2522 sport=80 flags=SA seq=1 win=32768 rtt=10.1 ms
len=46 ip=113.108.81.189 ttl=254 id=2523 sport=80 flags=SA seq=2 win=32768 rtt=9.2 ms
len=46 ip=113.108.81.189 ttl=254 id=2524 sport=80 flags=SA seq=3 win=32768 rtt=15.1 ms
^C
--- qq.com hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 9.2/11.4/15.1 ms
ubuntu@ubuntu:~$ sudo hping3 -A -c 5 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=0 win=0 rtt=15.7 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=1 win=0 rtt=92.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=2 win=0 rtt=38.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=3 win=0 rtt=9.1 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=4 win=0 rtt=16.0 ms

--- 192.168.0.100 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 9.1/24.3/92.3 ms
ubuntu@ubuntu:~$ sudo hping3 -S -8 1-1000 192.168.0.100  I
Scanning 192.168.0.100 (192.168.0.100), port 1-1000
1000 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+-----+-----+-----+
      21 ftp       : .S..A... 63      0 64240    46
      22 ssh       : .S..A... 63      0 64240    46
      53 domain    : .S..A... 63      0 64240    46
      80 http      : .S..A... 63      0 64240    46
All replies received. Done.
Not responding ports:
ubuntu@ubuntu:~$
```

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。



```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:41 ●
ubuntu@ubuntu: ~
File Edit View Search Terminal Help

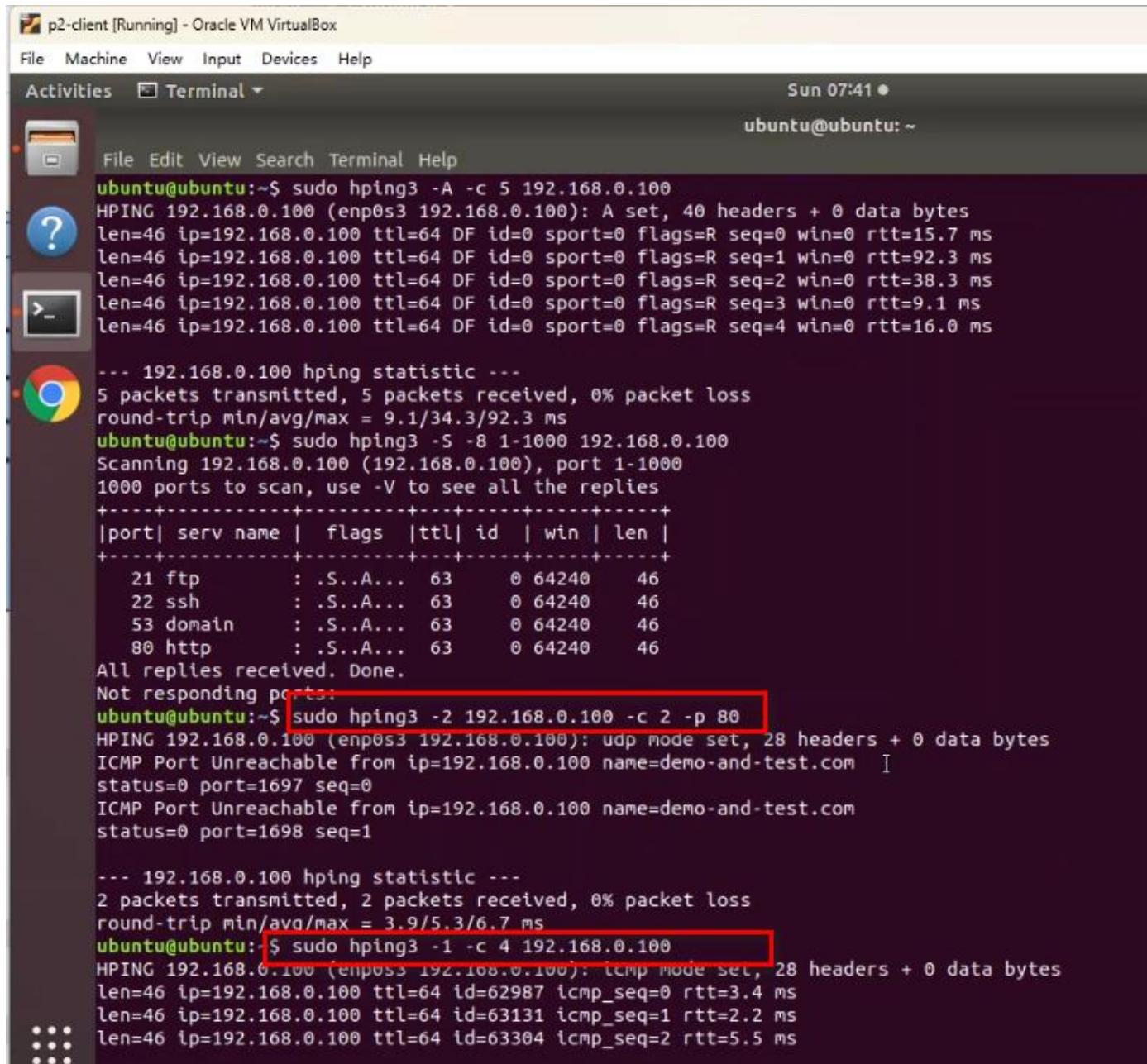
--- 192.168.0.100 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 9.1/34.3/92.3 ms
ubuntu@ubuntu:~$ sudo hping3 -S -8 1-1000 192.168.0.100
Scanning 192.168.0.100 (192.168.0.100), port 1-1000
1000 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags |ttl| id | win | len |
+-----+
 21 ftp      : .S..A... 63    0 64240   46
 22 ssh      : .S..A... 63    0 64240   46
 53 domain   : .S..A... 63    0 64240   46
 80 http     : .S..A... 63    0 64240   46
All replies received. Done.
Not responding ports:
ubuntu@ubuntu:~$ sudo hping3 -2 192.168.0.100 -c 2 -p 80
HPING 192.168.0.100 (enp0s3 192.168.0.100): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.0.100 name=demo-and-test.com
status=0 port=1697 seq=0
ICMP Port Unreachable from ip=192.168.0.100 name=demo-and-test.com
status=0 port=1698 seq=1

--- 192.168.0.100 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.9/5.3/6.7 ms
ubuntu@ubuntu:~$ sudo hping3 -1 -c 4 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=62987 icmp_seq=0 rtt=3.4 ms
len=46 ip=192.168.0.100 ttl=64 id=63131 icmp_seq=1 rtt=2.2 ms
len=46 ip=192.168.0.100 ttl=64 id=63304 icmp_seq=2 rtt=5.5 ms
len=46 ip=192.168.0.100 ttl=64 id=63352 icmp_seq=3 rtt=9.1 ms

--- 192.168.0.100 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.2/5.1/9.1 ms
ubuntu@ubuntu:~$ hping3 -1 -c 4 192.168.0.100

```

请编辑高亮部分 提交中或英文版本皆可.



```

File Machine View Input Devices Help
Activities Terminal Sun 07:41 ●
ubuntu@ubuntu:~$

File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo hping3 -A -c 5 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=0 win=0 rtt=15.7 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=1 win=0 rtt=92.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=2 win=0 rtt=38.3 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=3 win=0 rtt=9.1 ms
len=46 ip=192.168.0.100 ttl=64 DF id=0 sport=0 flags=R seq=4 win=0 rtt=16.0 ms

--- 192.168.0.100 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 9.1/34.3/92.3 ms
ubuntu@ubuntu:~$ sudo hping3 -S -8 1-1000 192.168.0.100
Scanning 192.168.0.100 (192.168.0.100), port 1-1000
1000 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags |ttl| id | win | len |
+-----+
21 ftp      : .S..A... 63    0 64240   46
22 ssh      : .S..A... 63    0 64240   46
53 domain   : .S..A... 63    0 64240   46
80 http     : .S..A... 63    0 64240   46
All replies received. Done.
Not responding ports:
ubuntu@ubuntu:~$ sudo hping3 -2 192.168.0.100 -c 2 -p 80
HPING 192.168.0.100 (enp0s3 192.168.0.100): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.0.100 name=demo-and-test.com []
status=0 port=1697 seq=0
ICMP Port Unreachable from ip=192.168.0.100 name=demo-and-test.com
status=0 port=1698 seq=1

--- 192.168.0.100 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.9/5.3/6.7 ms
ubuntu@ubuntu:~$ sudo hping3 -1 -c 4 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=62987 icmp_seq=0 rtt=3.4 ms
len=46 ip=192.168.0.100 ttl=64 id=63131 icmp_seq=1 rtt=2.2 ms
len=46 ip=192.168.0.100 ttl=64 id=63304 icmp_seq=2 rtt=5.5 ms

```

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.

```

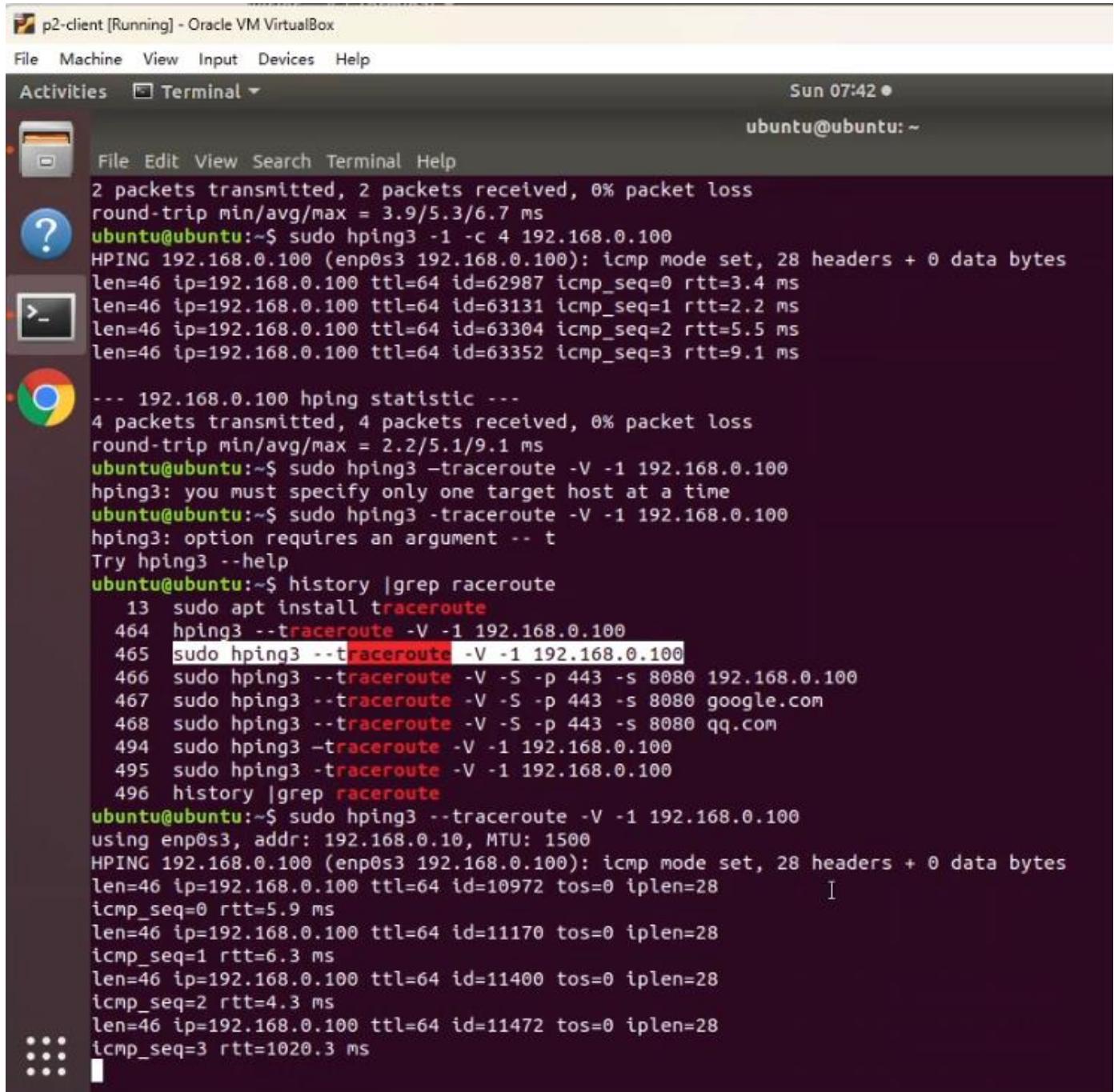
p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:42 •
ubuntu@ubuntu:~ File Edit View Search Terminal Help
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.9/5.3/6.7 ms
ubuntu@ubuntu:~$ sudo hping3 -1 -c 4 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=62987 icmp_seq=0 rtt=3.4 ms
len=46 ip=192.168.0.100 ttl=64 id=63131 icmp_seq=1 rtt=2.2 ms
len=46 ip=192.168.0.100 ttl=64 id=63304 icmp_seq=2 rtt=5.5 ms
len=46 ip=192.168.0.100 ttl=64 id=63352 icmp_seq=3 rtt=9.1 ms

--- 192.168.0.100 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.2/5.1/9.1 ms
ubuntu@ubuntu:~$ sudo hping3 -traceroute -V -1 192.168.0.100
hping3: you must specify only one target host at a time
ubuntu@ubuntu:~$ sudo hping3 -traceroute -V -1 192.168.0.100
hping3: option requires an argument -- t
Try hping3 --help
ubuntu@ubuntu:~$ history |grep traceroute
      13 sudo apt install traceroute
  464 sudo hping3 --traceroute -V -1 192.168.0.100
  465 sudo hping3 --traceroute -V -1 192.168.0.100
  466 sudo hping3 --traceroute -V -S -p 443 -s 8080 192.168.0.100
  467 sudo hping3 --traceroute -V -S -p 443 -s 8080 google.com
  468 sudo hping3 --traceroute -V -S -p 443 -s 8080 qq.com
  494 sudo hping3 -traceroute -V -1 192.168.0.100
  495 sudo hping3 -traceroute -V -1 192.168.0.100
  496 history |grep traceroute
ubuntu@ubuntu:~$ sudo hping3 -traceroute -V -1 192.168.0.100
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=10972 tos=0 iplen=28
icmp_seq=0 rtt=5.9 ms
len=46 ip=192.168.0.100 ttl=64 id=11170 tos=0 iplen=28
icmp_seq=1 rtt=6.3 ms
len=46 ip=192.168.0.100 ttl=64 id=11400 tos=0 iplen=28
icmp_seq=2 rtt=4.3 ms
len=46 ip=192.168.0.100 ttl=64 id=11472 tos=0 iplen=28
icmp_seq=3 rtt=1020.3 ms

```

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.



p2-client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Sun 07:42 ●

ubuntu@ubuntu:~

```

File Edit View Search Terminal Help
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.9/5.3/6.7 ms
ubuntu@ubuntu:~$ sudo hping3 -1 -c 4 192.168.0.100
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=62987 icmp_seq=0 rtt=3.4 ms
len=46 ip=192.168.0.100 ttl=64 id=63131 icmp_seq=1 rtt=2.2 ms
len=46 ip=192.168.0.100 ttl=64 id=63304 icmp_seq=2 rtt=5.5 ms
len=46 ip=192.168.0.100 ttl=64 id=63352 icmp_seq=3 rtt=9.1 ms

--- 192.168.0.100 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.2/5.1/9.1 ms
ubuntu@ubuntu:~$ sudo hping3 -traceroute -V -1 192.168.0.100
hping3: you must specify only one target host at a time
ubuntu@ubuntu:~$ sudo hping3 -traceroute -V -1 192.168.0.100
hping3: option requires an argument -- t
Try hping3 --help
ubuntu@ubuntu:~$ history |grep raceroute
    13 sudo apt install traceroute
  464 hping3 --traceroute -V -1 192.168.0.100
  465 sudo hping3 --traceroute -V -1 192.168.0.100
  466 sudo hping3 --traceroute -V -S -p 443 -s 8080 192.168.0.100
  467 sudo hping3 --traceroute -V -S -p 443 -s 8080 google.com
  468 sudo hping3 --traceroute -V -S -p 443 -s 8080 qq.com
  494 sudo hping3 -traceroute -V -1 192.168.0.100
  495 sudo hping3 -traceroute -V -1 192.168.0.100
  496 history |grep raceroute
ubuntu@ubuntu:~$ sudo hping3 -traceroute -V -1 192.168.0.100
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=10972 tos=0 iplen=28
icmp_seq=0 rtt=5.9 ms
len=46 ip=192.168.0.100 ttl=64 id=11170 tos=0 iplen=28
icmp_seq=1 rtt=6.3 ms
len=46 ip=192.168.0.100 ttl=64 id=11400 tos=0 iplen=28
icmp_seq=2 rtt=4.3 ms
len=46 ip=192.168.0.100 ttl=64 id=11472 tos=0 iplen=28
icmp_seq=3 rtt=1020.3 ms

```

请编辑高亮部分 提交中或英文版本皆可.

```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:45 ●
ubuntu@ubuntu: ~
File Edit View Search Terminal Help
HPING qq.com (enp0s3 113.108.81.189): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
hop=1 hoprtt=6.8 ms
len=46 ip=113.108.81.189 ttl=254 id=7942 tos=0 iplen=44
sport=443 flags=SA seq=1 win=32768 rtt=25.0 ms
seq=24080132 ack=1093533798 sum=e6c0 urp=0

len=46 ip=113.108.81.189 ttl=254 id=7944 tos=0 iplen=44
sport=443 flags=SA seq=2 win=32768 rtt=23.6 ms
seq=24105778 ack=151990360 sum=e464 urp=0

len=46 ip=113.108.81.189 ttl=254 id=7945 tos=0 iplen=44
sport=443 flags=SA seq=3 win=32768 rtt=18.8 ms
seq=24131426 ack=1833040069 sum=12d4 urp=0

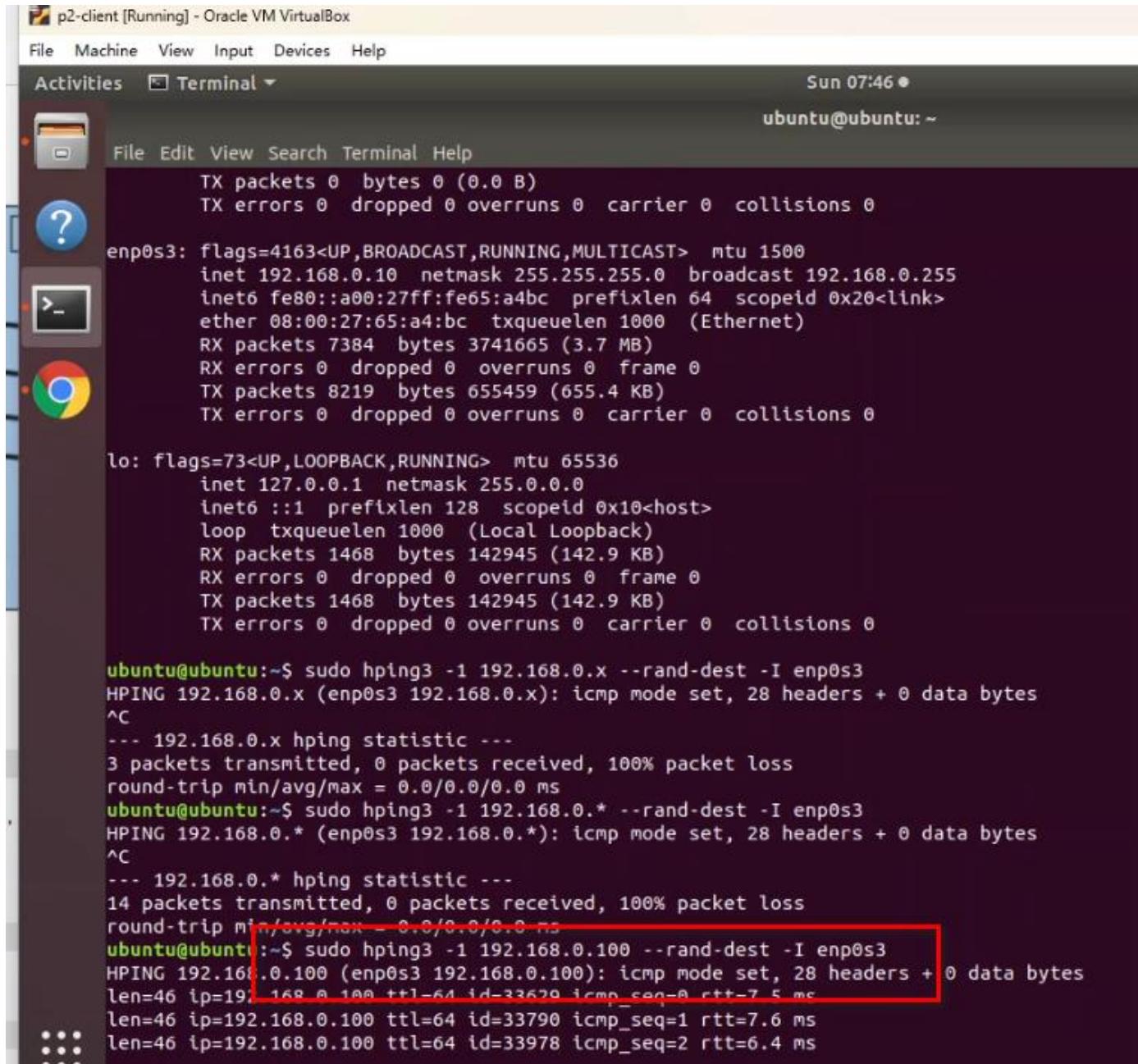
len=46 ip=113.108.81.189 ttl=254 id=7946 tos=0 iplen=44
sport=443 flags=SA seq=4 win=32768 rtt=20.0 ms
seq=24157076 ack=510291807 sum=1d48 urp=0

len=46 ip=113.108.81.189 ttl=254 id=7955 tos=0 iplen=44
sport=443 flags=SA seq=5 win=32768 rtt=19.9 ms
seq=24182728 ack=1821356415 sum=a253 urp=0

^C
--- qq.com hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 6.8/19.0/25.0 ms
ubuntu@ubuntu:~$ sudo hping3 -S 192.168.100.100 -p 80 -T --ttl 13 --tr-keep-ttl -n
HPING 192.168.100.100 (enp0s3 192.168.100.100): S set, 40 headers + 0 data bytes
^C
--- 192.168.100.100 hping statistic ---
50 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -S 192.168.0.100 -p 80 -T --ttl 13 --tr-keep-ttl -n
HPING 192.168.0.100 (enp0s3 192.168.0.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=9.2 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=11.5 ms
len=46 ip=192.168.0.100 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=8.7 ms

```

请编辑高亮部分 提交中或英文版本皆可.



The screenshot shows a terminal window titled "p2-client [Running] - Oracle VM VirtualBox". The terminal displays the following information:

```

File Machine View Input Devices Help
Activities Terminal Sun 07:46 •
ubuntu@ubuntu:~>

File Edit View Search Terminal Help
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.10 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::a00:27ff:fe65:a4bc prefixlen 64 scopeid 0x20<link>
ether 08:00:27:65:a4:bc txqueuelen 1000 (Ethernet)
RX packets 7384 bytes 3741665 (3.7 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8219 bytes 655459 (655.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 1468 bytes 142945 (142.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1468 bytes 142945 (142.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.x --rand-dest -I enp0s3
HPING 192.168.0.x (enp0s3 192.168.0.x): icmp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.x hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.* --rand-dest -I enp0s3
HPING 192.168.0.* (enp0s3 192.168.0.*): icmp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.* hping statistic ---
14 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.100 --rand-dest -I enp0s3
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=33679 icmp_seq=0 rtt=7.5 ms
len=46 ip=192.168.0.100 ttl=64 id=33790 icmp_seq=1 rtt=7.6 ms
len=46 ip=192.168.0.100 ttl=64 id=33978 icmp_seq=2 rtt=6.4 ms

```

The last command, `sudo hping3 -1 192.168.0.100 --rand-dest -I enp0s3`, is highlighted with a red box.

3.6 其他类型的端口扫描 16

请编辑高亮部分 提交中或英文版本皆可.

```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:43 ●
ubuntu@ubuntu: ~

File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo hping3 --traceroute -V -S -p 443 -s 8080 google.com
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING google.com (enp0s3 59.24.3.174): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
hop=1 hoprtt=8.0 ms
^C
--- google.com hping statistic ---
12 packets transmitted, 1 packets received, 92% packet loss
round-trip min/avg/max = 8.0/8.0/8.0 ms
ubuntu@ubuntu:~$ sudo hping3 --traceroute -V -S -p 443 -s 8080 qq.com
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING qq.com (enp0s3 113.108.81.189): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.0.100 name=demo-and-test.com
hop=1 hoprtt=6.8 ms
len=46 ip=113.108.81.189 ttl=254 id=7942 tos=0 iplen=44
sport=443 flags=SA seq=1 win=32768 rtt=25.0 ms
seq=24080132 ack=1093533798 sum=e6c0 urp=0

len=46 ip=113.108.81.189 ttl=254 id=7944 tos=0 iplen=44
sport=443 flags=SA seq=2 win=32768 rtt=23.6 ms
seq=24105778 ack=151990360 sum=e464 urp=0

len=46 ip=113.108.81.189 ttl=254 id=7945 tos=0 iplen=44
sport=443 flags=SA seq=3 win=32768 rtt=18.8 ms
seq=24131426 ack=1833040069 sum=12d4 urp=0

len=46 ip=113.108.81.189 ttl=254 id=7946 tos=0 iplen=44
sport=443 flags=SA seq=4 win=32768 rtt=20.0 ms
seq=24157076 ack=510291807 sum=id48 urp=0

len=46 ip=113.108.81.189 ttl=254 id=7955 tos=0 iplen=44
sport=443 flags=SA seq=5 win=32768 rtt=19.9 ms
seq=24182728 ack=1821356415 sum=a253 urp=0

^C
--- qq.com hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 6.8/19.0/25.0 ms
ubuntu@ubuntu:~$ █

```

请编辑高亮部分 提交中或英文版本皆可.

```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:48 •
ubuntu@ubuntu:~>

File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.x --rand-dest -I enp0s3
HPING 192.168.0.x (enp0s3 192.168.0.x): icmp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.x hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.* --rand-dest -I enp0s3
HPING 192.168.0.* (enp0s3 192.168.0.*): icmp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.* hping statistic ---
14 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.100 --rand-dest -I enp0s3
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 lp=192.168.0.100 ttl=64 id=33629 icmp_seq=0 rtt=7.5 ms
len=46 ip=192.168.0.100 ttl=64 id=33790 icmp_seq=1 rtt=7.6 ms
len=46 ip=192.168.0.100 ttl=64 id=33978 icmp_seq=2 rtt=6.4 ms
len=46 ip=192.168.0.100 ttl=64 id=34135 icmp_seq=3 rtt=1.8 ms
^C
--- 192.168.0.100 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.8/5.8/7.6 ms
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.100 -icmp-ts -c 3
hping3: you must specify only one target host at a time
ubuntu@ubuntu:~$ sudo hping3 -1 192.168.0.100 --icmp-ts -c 3
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=47814 icmp_seq=0 rtt=3.0 ms
ICMP timestamp: Originate=53299534 Receive=53294886 Transmit=53293886
ICMP timestamp RTT tsrtt=9

len=46 ip=192.168.0.100 ttl=64 id=48018 icmp_seq=1 rtt=9.2 ms
ICMP timestamp: Originate=53300536 Receive=53294886 Transmit=53294886
ICMP timestamp RTT tsrtt=9

^C
--- 192.168.0.100 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.0/6.1/9.2 ms
ubuntu@ubuntu:~$
```

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。

```

p2-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 07:49
ubuntu@ubuntu: ~

File Edit View Search Terminal Help
HPING 192.168.0.100 (enp0s3 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=64 id=47814 icmp_seq=0 rtt=3.0 ms
ICMP timestamp: Originate=53299534 Receive=53293886 Transmit=53293886
ICMP timestamp RTT tsrtt=3

len=46 ip=192.168.0.100 ttl=64 id=48018 icmp_seq=1 rtt=9.2 ms
ICMP timestamp: Originate=53300536 Receive=53294886 Transmit=53294886
ICMP timestamp RTT tsrtt=9

^C
--- 192.168.0.100 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.0/6.1/9.2 ms
ubuntu@ubuntu:~$ sudo hping3 -c 1 -V -p 80 -s 5050 -F demo-and-test.com
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING demo-and-test.com (enp0s3 192.168.0.100): F set, 40 headers + 0 data bytes

--- demo-and-test.com hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
ubuntu@ubuntu:~$ sudo hping3 -c 1 -V -p 80 -s 5050 -A demo-and-test.com
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING demo-and-test.com (enp0s3 192.168.0.100): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=63 DF id=0 tos=0 iplen=40
sport=80 flags=R seq=0 win=0 rtt=3.2 ms
seq=1312367869 ack=0 sum=e1a6 urp=0

I

--- demo-and-test.com hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.2/3.2/3.2 ms
ubuntu@ubuntu:~$ sudo hping3 -c 1 -V -p 80 -s 5050 -M 0 -UPF demo-and-test.com
using enp0s3, addr: 192.168.0.10, MTU: 1500
HPING demo-and-test.com (enp0s3 192.168.0.100): FPU set, 40 headers + 0 data bytes

--- demo-and-test.com hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

```

请编辑高亮部分 提交中或英文版本皆可。

```

File Edit View Search Terminal Help
318 sudo nmap -sT -p- 192.168.0.100
319 sudo nmap -sU -p- 192.168.0.100
426 history | grep nmap
ubuntu@ubuntu:~$ sudo nmap -sN demo-and-test.com
[sudo] password for ubuntu:
Starting Nmap 7.60 ( https://nmap.org ) at 2024-04-14 16:02 MST
Nmap scan report for demo-and-test.com (192.168.0.100)
Host is up (0.00028s latency).
Not shown: 997 closed ports
PORT      STATE          SERVICE
22/tcp    open|filtered  ssh
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
MAC Address: 08:00:27:79:BA:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.45 seconds
ubuntu@ubuntu:~$ 

```

4.1 什么是 DOS 攻击? 16

4.2 ICMP 洪水 17

4.3 Smurf 洪水攻击 18

4.4 Fraggle 洪水攻击 19

4.5 UDP 洪水攻击 19

4.6 Land 攻击 20

4.7 基于 TCP 的洪水攻击 21

 4.7.1 TCP 洪水 21

涉及的命令如下:

1. #客户端的攻击命令
2. sudo hping3 -1 -S 192.168.0.100 -a 192.168.0.100 -k -s 80 -p 80 --flood
- 3.
4. #snort 的规则 rule
5. ubuntu@ubuntu:~/Downloads\$ cat /etc/snort/rules/local.rules
6. # \$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp \$
7. # -----
8. # LOCAL RULES
9. # -----
10. # This file intentionally does not come with signatures. Put your local
11. # additions here.
- 12.
13. alert icmp any any <> 192.168.0.100 any (msg:"ICMP Packet found"; sid:10000001;)
14. alert tcp \$EXTERNAL_NET any -> \$HOME_NET 22 (msg:"SSH attempt";flags:S;classtype:attempted-recon; sid:000002; rev:2;)
- 15.
16. # 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 discoveries, 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：

```

1. #!/bin/sh
2.
3. #####
4. # 1.1. Internet ip address
5. #####
6. Internet_IP="172.16.0.4"
7. Internet_IP_RANGE="172.16.0.0/12"
8. Internet_BCAST_ADDRESS="172.31.255.255"
9. Internet_IFACE="enp0s9"
10.
11. #####
12. # 1.2 Client network configuration.
13. #####
14. Client_NET_IP="192.168.0.10"
15. Client_NET_IP_RANGE="192.168.0.0/24"
16. Client_NET_BCAST_ADDRESS="192.168.0.255"
17. Client_NET_IFACE="enp0s3"
18.
19. #####
20. # 1.3 Server Network Configuration.
21. #####
22. Server_NET_IP="10.0.0.10"
23. Server_NET_IP_RANGE="10.0.0.0/8"
24. Server_NET_BCAST_ADDRESS="10.255.255.255"
25. Server_NET_IFACE="enp0s8"
26.
27. #####
28. # Server and NAT IP aliases
29. #####
30. #
31.
32. #
33. # IP aliases for the server (server's IP address)
34. #
35. LO_IFACE="lo"
36. LO_IP="127.0.0.1"
37. WEB_IP_ADDRESS="10.0.0.10"
38. MAIL_IP_ADDRESS="10.0.0.10"
39. SSH_IP_ADDRESS="10.0.0.10"
40. DNS_IP_ADDRESS="10.0.0.10"
41. FTP_IP_ADDRESS="10.0.0.10"
42. #IP aliases for NATED services (this is the GW's ip on client network)
43. NAT_WEB_IP_ADDRESS="192.168.0.100"
44. NAT_MAIL_IP_ADDRESS="192.168.0.100"
45. NAT_SSH_IP_ADDRESS="192.168.0.100"
46. NAT_DNS_IP_ADDRESS="192.168.0.100"
47. NAT_FTP_IP_ADDRESS="192.168.0.100"
48. PASV_FTP_PORT_RANGE="30000:30099"
49.
50. #####
51. # 1.4 IPTables Configuration.
52. #####

```

请编辑高亮部分 提交中或英文版本皆可。

```

53. IPTABLES="/sbin/iptables"
54.
55. #####
56. # 2. Module loading.
57. #####
58. /sbin/depmod -a
59.
60. #
61. # flush iptables
62. #
63. # 清空现有规则
64. $IPTABLES -F
65. $IPTABLES -X
66. $IPTABLES -F -t nat
67. $IPTABLES -F -t mangle
68. $IPTABLES -F -t filter
69.
70. # Load required kernel modules
71. /sbin/modprobe ip_tables
72. /sbin/modprobe ip_conntrack
73. /sbin/modprobe iptable_filter
74. /sbin/modprobe iptable_mangle
75. /sbin/modprobe iptable_nat
76. /sbin/modprobe ipt_LOG
77. /sbin/modprobe ipt_limit
78. /sbin/modprobe ipt_state
79.
80.
81. #####
82. # 3. /proc set up.
83. #####
84. echo "1" > /proc/sys/net/ipv4/ip_forward
85. #
86.
87. #####
88. # 4. rules set up.
89. #####
90.
91. # Blacklist
92. $IPTABLES -P INPUT ACCEPT
93. $IPTABLES -P OUTPUT ACCEPT
94. $IPTABLES -P FORWARD ACCEPT
95.
96. # User-defined chains
97. $IPTABLES -I FORWARD 1 -p tcp --tcp-flags FIN FIN -j ACCEPT
98.
99. $IPTABLES -P INPUT ACCEPT $IPTABLES -P OUTPUT ACCEPT $IPTABLES -P FORWARD ACCEPT
100.
101.# 允许来自客户端的 ICMP 请求
102.$IPTABLES -A INPUT -p icmp --icmp-type echo-request -s $Client_NET_IP_RANGE -j ACCEPT
103.$IPTABLES -A OUTPUT -p icmp --icmp-type echo-reply -d $Client_NET_IP_RANGE -j ACCEPT
104.
105.#允许来自客户端的所有 ICMP 请求
106.$IPTABLES -A INPUT -p icmp -s $Client_NET_IP_RANGE -j ACCEPT $IPTABLES -A OUTPUT -p icmp -
   d $Client_NET_IP_RANGE -j ACCEPT
107.
108.# 允许转发的 ICMP 请求和回复
109.$IPTABLES -A FORWARD -p icmp -s $Client_NET_IP_RANGE -j ACCEPT
110.$IPTABLES -A FORWARD -p icmp -d $Client_NET_IP_RANGE -j ACCEPT
111.
112.#允许转发来自客户端的所有 ICMP 请求和回复
113.$IPTABLES -A FORWARD -p icmp -s $Client_NET_IP_RANGE -d $Server_NET_IP_RANGE -j ACCEPT
114.$IPTABLES -A FORWARD -p icmp -s $Server_NET_IP_RANGE -d $Client_NET_IP_RANGE -j ACCEPT
115.
```

请编辑高亮部分 提交中或英文版本皆可。

```

116.# 允许来自客户端网络的所有 TCP 流量
117.$IPTABLES -A FORWARD -p tcp -s $Client_NET_IP_RANGE -d $WEB_IP_ADDRESS -j ACCEPT
118.$IPTABLES -A FORWARD -p tcp -s $Client_NET_IP_RANGE -d $NAT_WEB_IP_ADDRESS -j ACCEPT
119.
120.$IPTABLES -A FORWARD -p tcp -s $NAT_WEB_IP_ADDRESS -d $Client_NET_IP_RANGE -j ACCEPT
121.$IPTABLES -A FORWARD -p tcp -s $WEB_IP_ADDRESS -d $Client_NET_IP_RANGE -j ACCEPT
122.
123.# 允许从客户端网络到外部的所有 TCP 回复，无论是否设置了 SYN 标志
124.$IPTABLES -A FORWARD -p tcp -s $Client_NET_IP_RANGE -d $Server_NET_IP_RANGE -j ACCEPT
125.$IPTABLES -A FORWARD -p tcp -s $Server_NET_IP_RANGE -d $Client_NET_IP_RANGE -j ACCEPT
126.
127.#
128.$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 80 -j DNAT --
    to $WEB_IP_ADDRESS
129.$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 22 -j DNAT --
    to $SSH_IP_ADDRESS
130.$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 53 -j DNAT --
    to $DNS_IP_ADDRESS
131.$IPTABLES -t nat -A PREROUTING -p tcp -d $NAT_WEB_IP_ADDRESS --dport 21 -j DNAT --
    to $FTP_IP_ADDRESS
132.
133.# 允许所有内网节点访问 Internet
134.$IPTABLES -t nat -A POSTROUTING -o $Internet_IFACE -j MASQUERADE
135.
136.
137.# 允许已建立和相关的连接
138.$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
139.$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
140.$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
141.
142.
143.# 记录所有丢弃的输入和转发包
144.$IPTABLES -A INPUT -j LOG --log-prefix "Dropped Input: "
145.$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：

```

1. # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2. #
3. # LOCAL RULES
4. #
5. # This file intentionally does not come with signatures. Put your local
6. # additions here.
7.
8. alert icmp any any <> 192.168.0.100 any (msg:"ICMP Packet found"; sid:10000001; )
9. alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SSH attempt";flags:S;classtype:attempted
   -recon; sid:0000002; rev:2;)
10.
11. # task 3
12.
13. alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Http Getrequest";content:"GET";classtype
   :web-application-activity; sid:10000003; rev:3;)
14. 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).