

BÁO CÁO BÀI TẬP

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Tên chủ đề: Lab 2

GVHD: ThS. Đỗ Hoàng Hiên

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đại Nghĩa	21521182	21521182@gm.uit.edu.vn
2	Hoàng Gia Bảo	21521848	21521848@gm.uit.edu.vn

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

Yêu cầu 1: Sinh viên trả lời các câu hỏi bên dưới.

1.1a. Tìm hiểu về Snort? Snort cho phép chạy trên những chế độ (mode) nào?

Snort là một trong những hệ thống phát hiện xâm nhập (IDS - Intrusion Detection System) và hệ thống ngăn chặn xâm nhập (IPS - Intrusion Prevention System) phổ biến và mạnh mẽ. Nó được sử dụng để phát hiện và ngăn chặn các cuộc tấn công mạng bằng cách giám sát lưu lượng mạng và phân tích các gói tin.

Snort có thể hoạt động trong các chế độ sau:

Sniffer Mode (Chế độ Sniffer): Ở chế độ này, Snort hoạt động như một sniffer thông thường, thu thập dữ liệu từ lưu lượng mạng mà không phân tích chúng.

Packet Logger Mode (Chế độ ghi gói tin): Snort có thể ghi lại toàn bộ hoặc một phần của lưu lượng mạng vào các tập tin log để phân tích sau này.

Network Intrusion Detection Mode (Chế độ phát hiện xâm nhập mạng): Chế độ này cho phép Snort phân tích dữ liệu từ lưu lượng mạng để phát hiện các hành vi không mong muốn hoặc các cuộc tấn công mạng.

1.1b. Trình bày những tính năng chính của Snort?

Phát hiện và Ngăn chặn Xâm nhập: Snort có khả năng phát hiện và ngăn chặn các cuộc tấn công mạng thông qua việc phân tích lưu lượng mạng và so khớp với các quy tắc đã được xác định trước.

Phân tích dựa trên Quy tắc: Snort sử dụng một cơ sở dữ liệu quy tắc mạnh mẽ để phân tích các gói tin và xác định xem chúng có chứa dấu hiệu của các cuộc tấn công hay không.

Cập nhật linh hoạt: Cộng đồng người dùng Snort liên tục cung cấp các quy tắc mới và cập nhật cho Snort để bảo vệ khỏi các mối đe dọa mới.

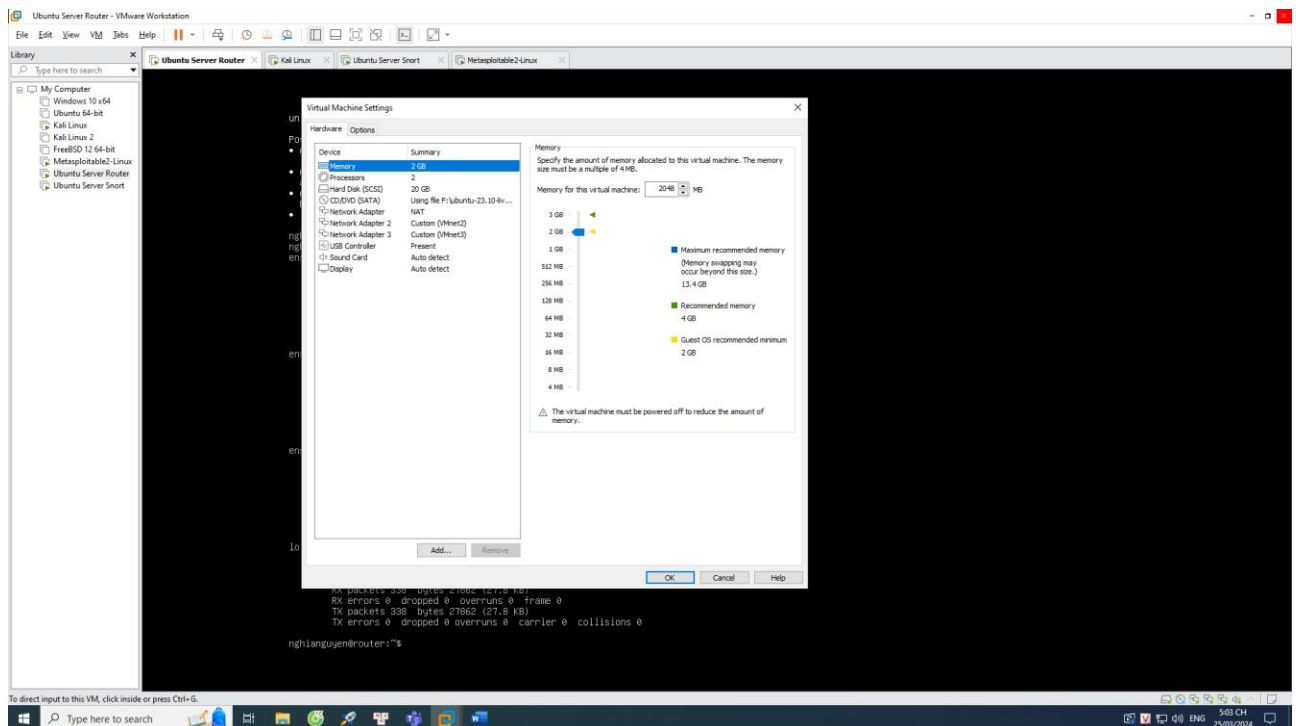
Tích hợp với hệ thống khác: Snort có thể tích hợp với các giải pháp bảo mật khác như firewall và hệ thống giám sát mạng để tăng cường khả năng bảo vệ mạng.

Hiệu suất cao và Tính linh hoạt: Snort được xây dựng để hoạt động hiệu quả trên cả mạng nhỏ và mạng lớn với khả năng tùy chỉnh linh hoạt theo nhu cầu cụ thể của môi trường mạng.

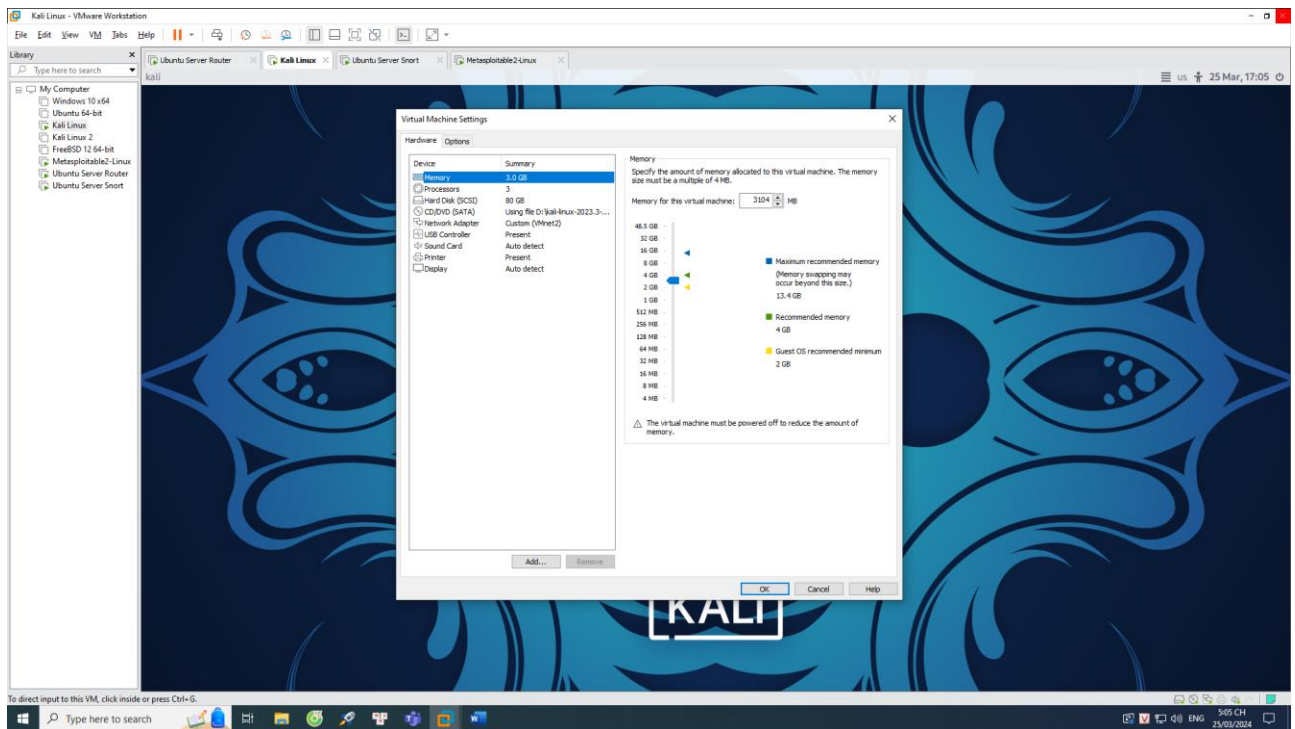
Yêu cầu 2: Sinh viên cài đặt và cấu hình Snort Inline theo các bước bên dưới. Chụp lại các hình ảnh minh chứng (chụp full màn hình) cho từng bước làm

Trước hết là em sẽ tiến hành thực hiện cấu hình 04 máy ảo theo mô hình được mô tả.

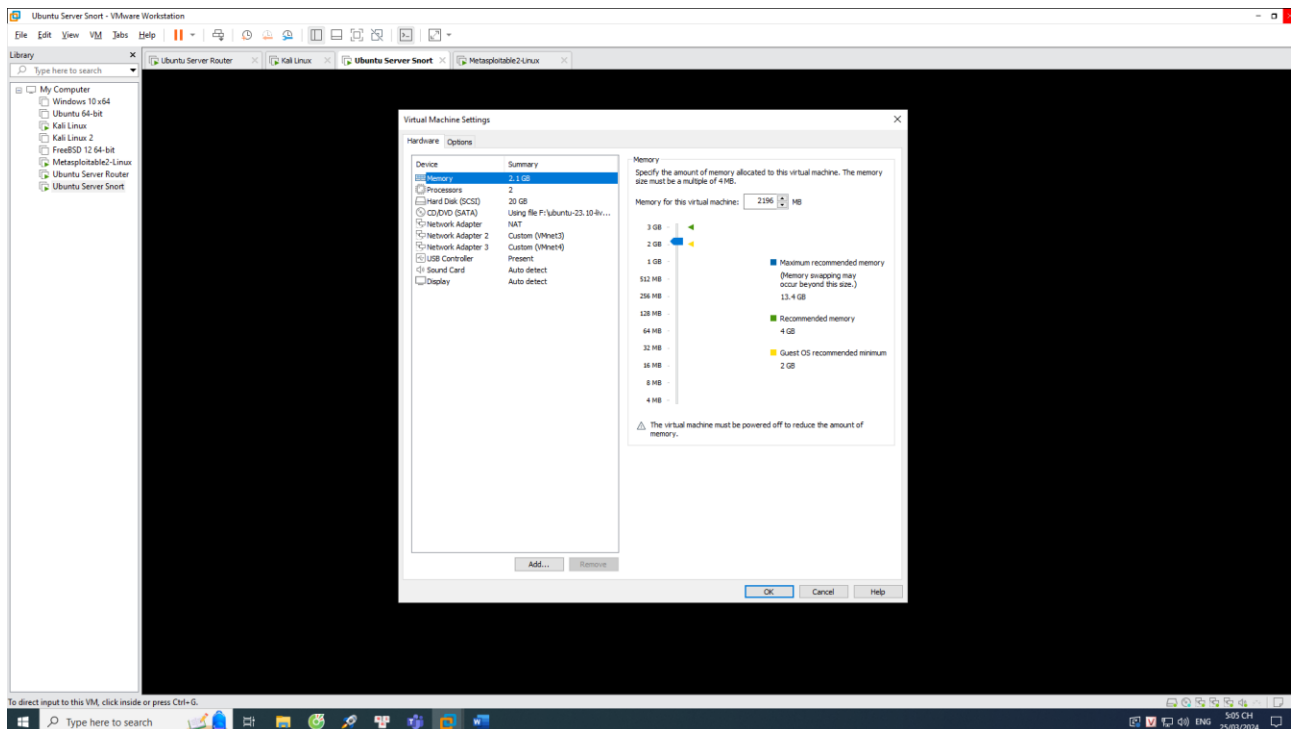
Gán card mạng cho router:



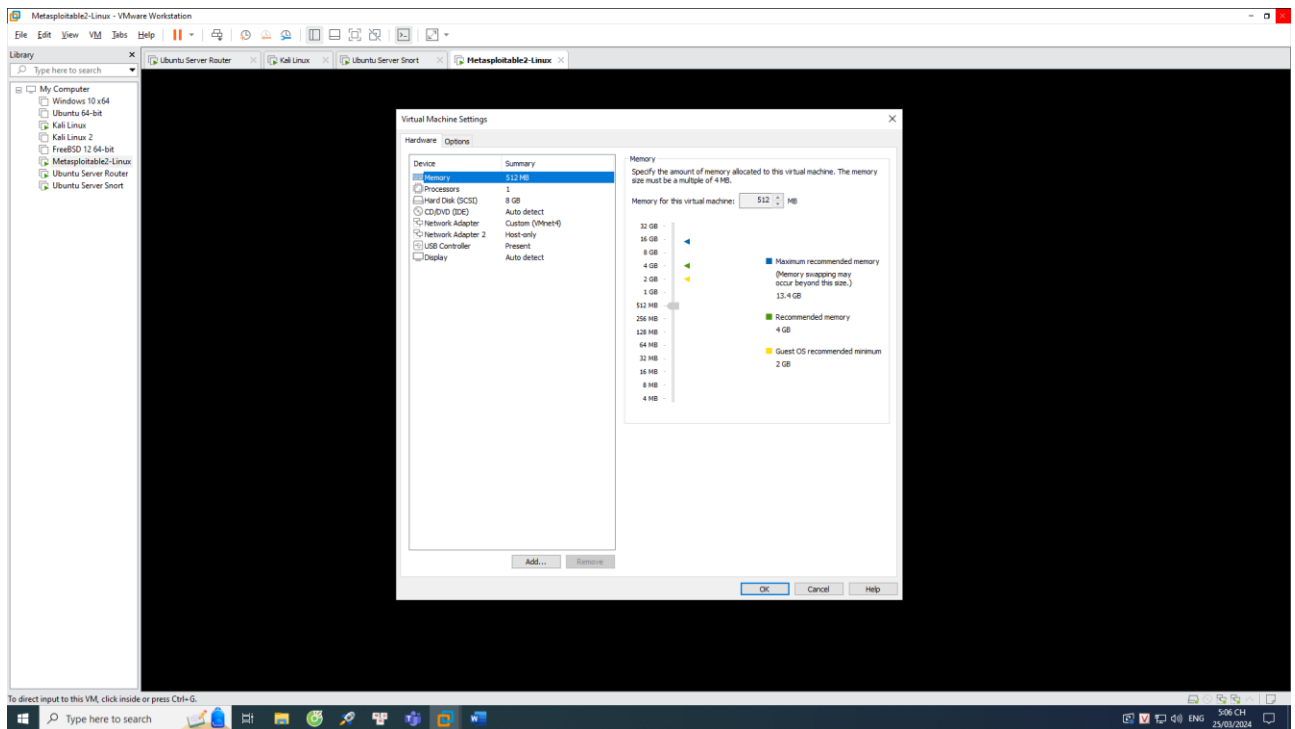
Gán card mạng cho máy kali:



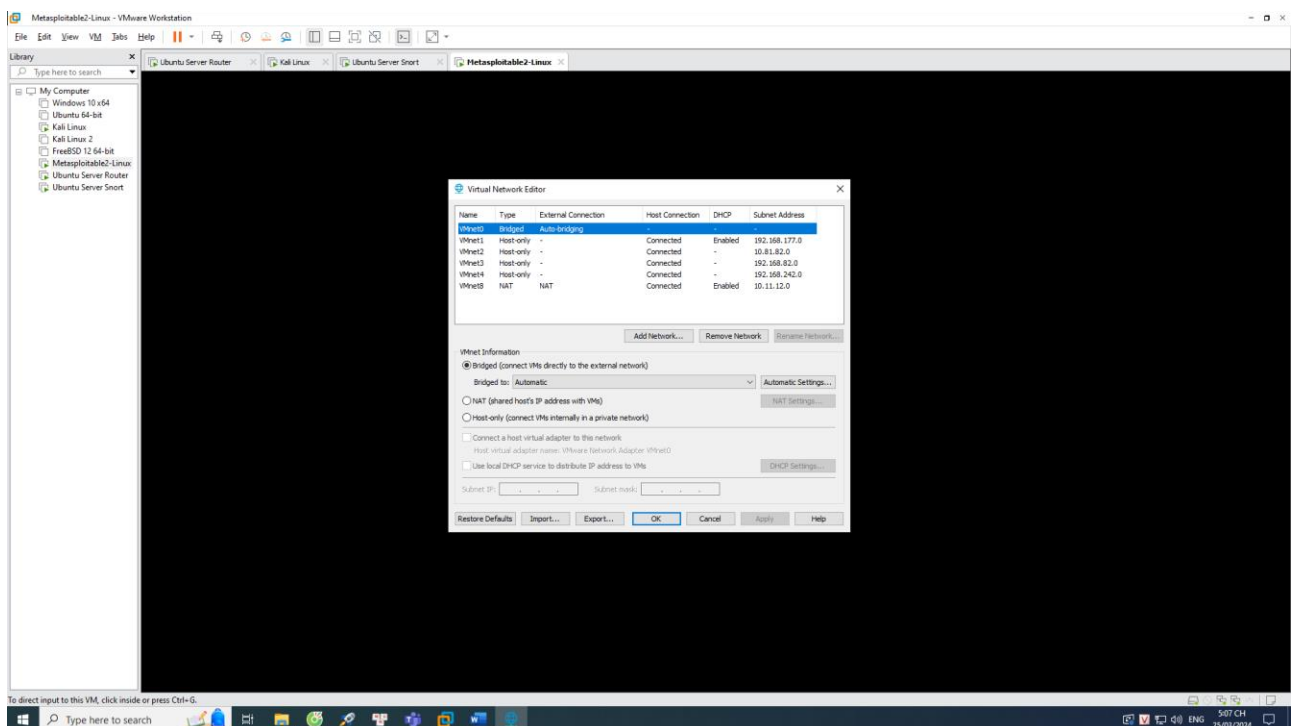
Gán card mạng cho máy Snort:



Gán card mạng cho máy victim:

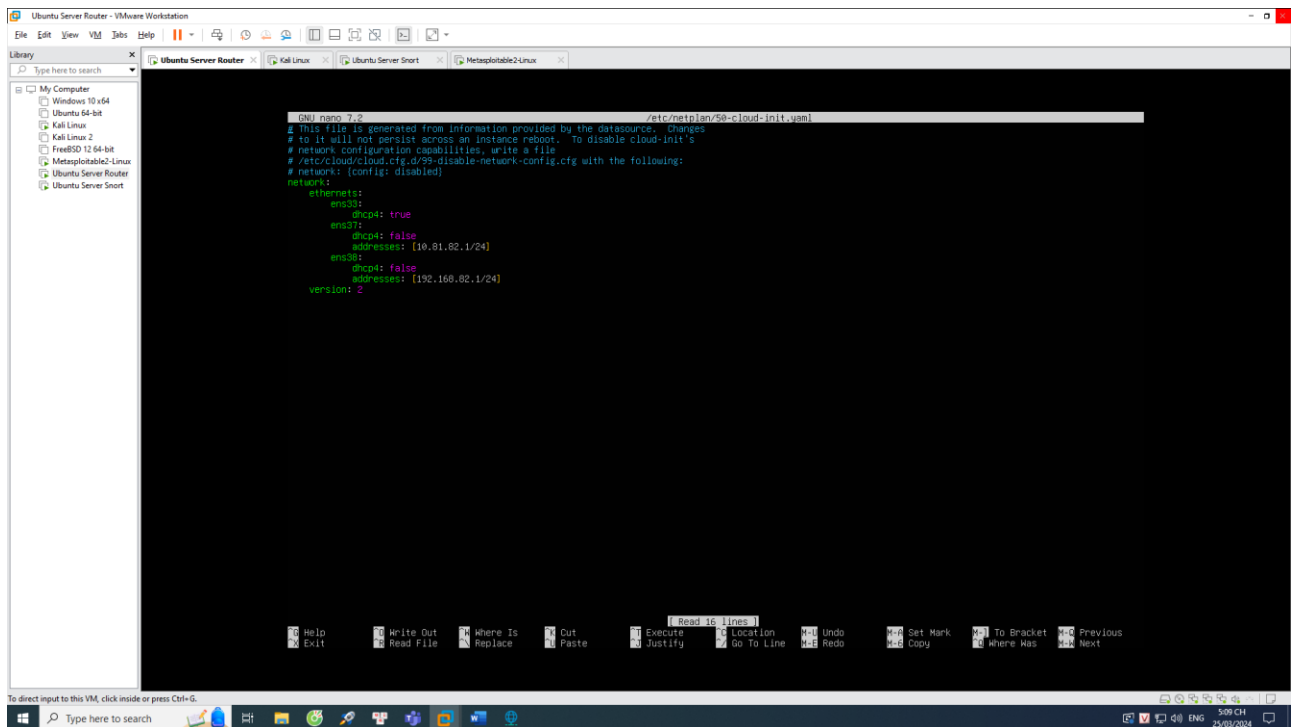


Tiếp theo là em sẽ kiểm tra card VMnet8 (NAT) đã tồn tại và được bật DHCP và cấu hình địa chỉ mạng cho các VMnet khác:

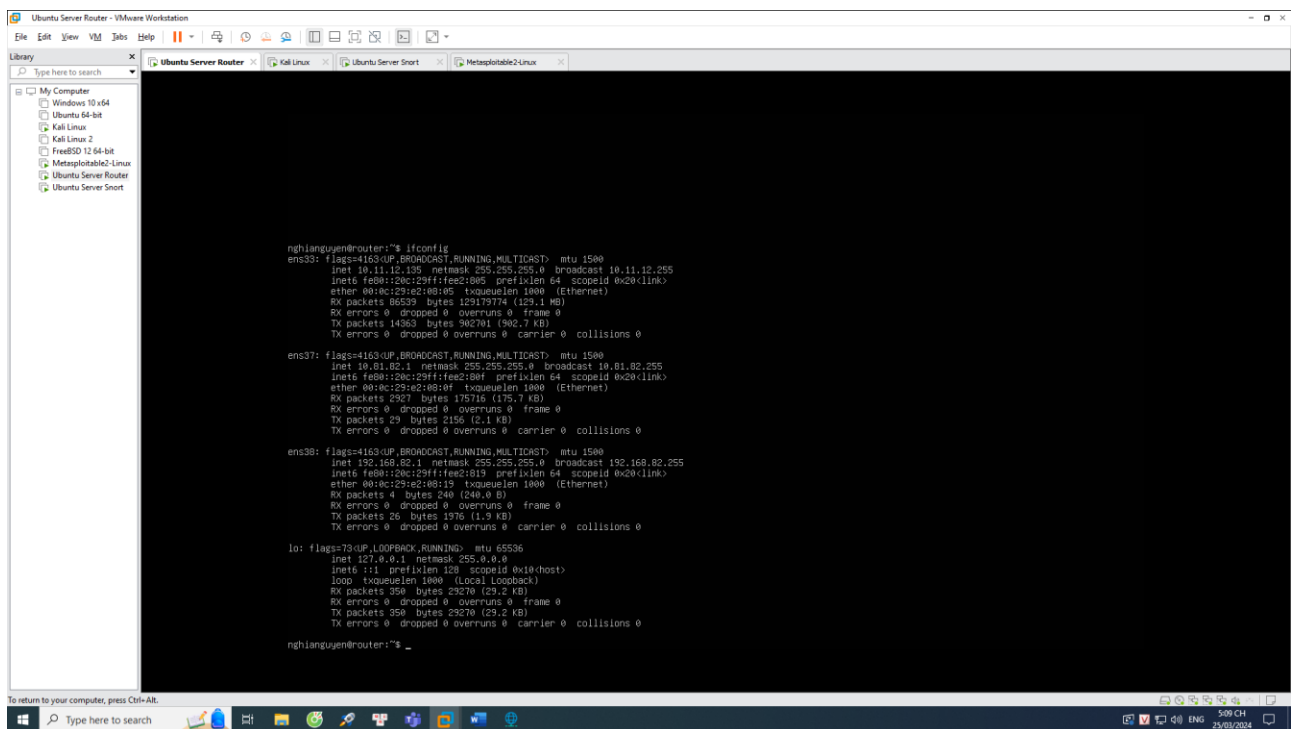


Sau khi đã gán card mạng xong, em tiến hành thay đổi địa chỉ ip cho các máy.

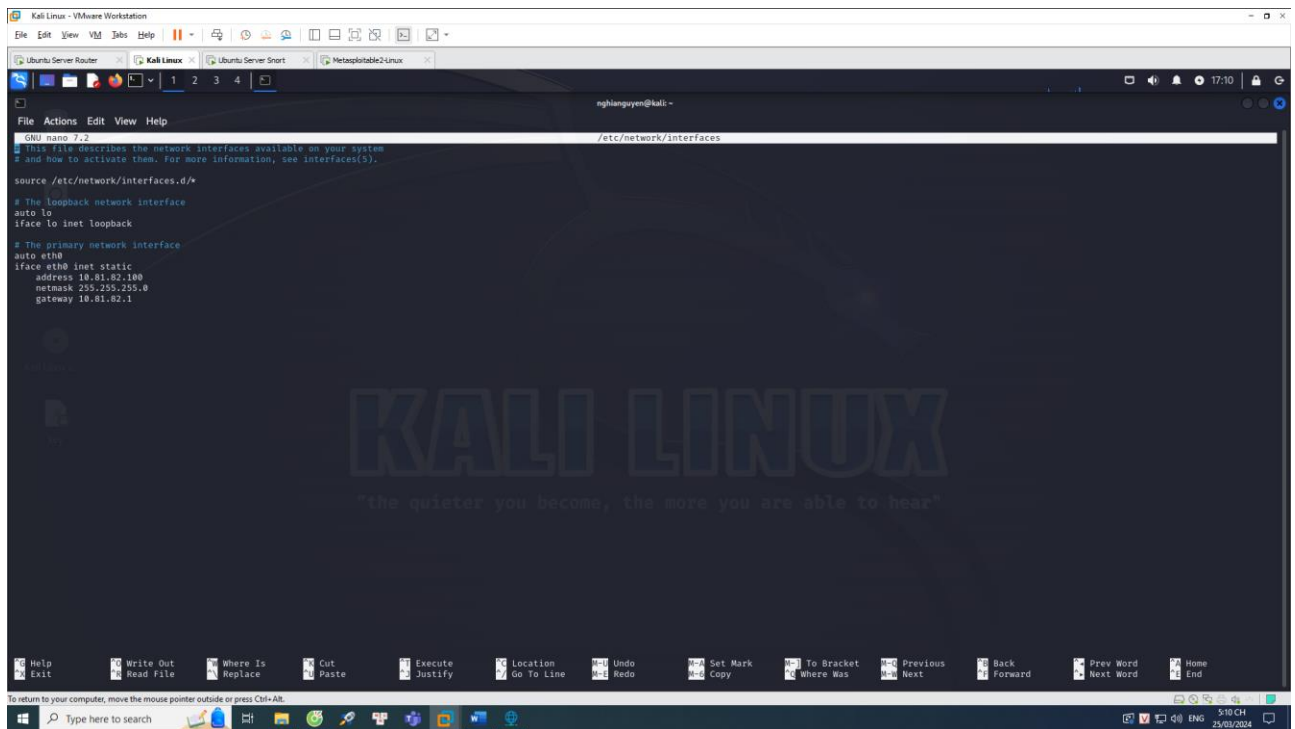
Đối với máy router:



Kết quả:



Đối với máy kali:



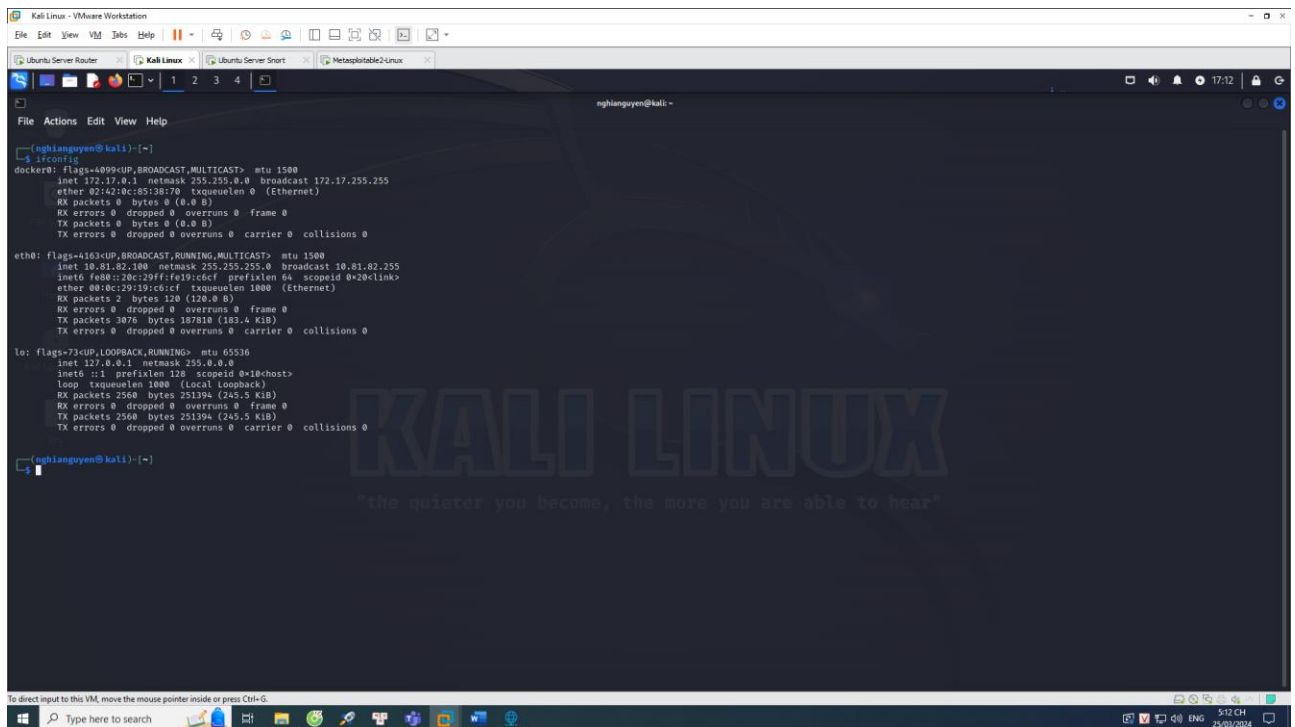
```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 10.81.82.100
    netmask 255.255.255.0
    gateway 10.81.82.1
```

Kết quả:

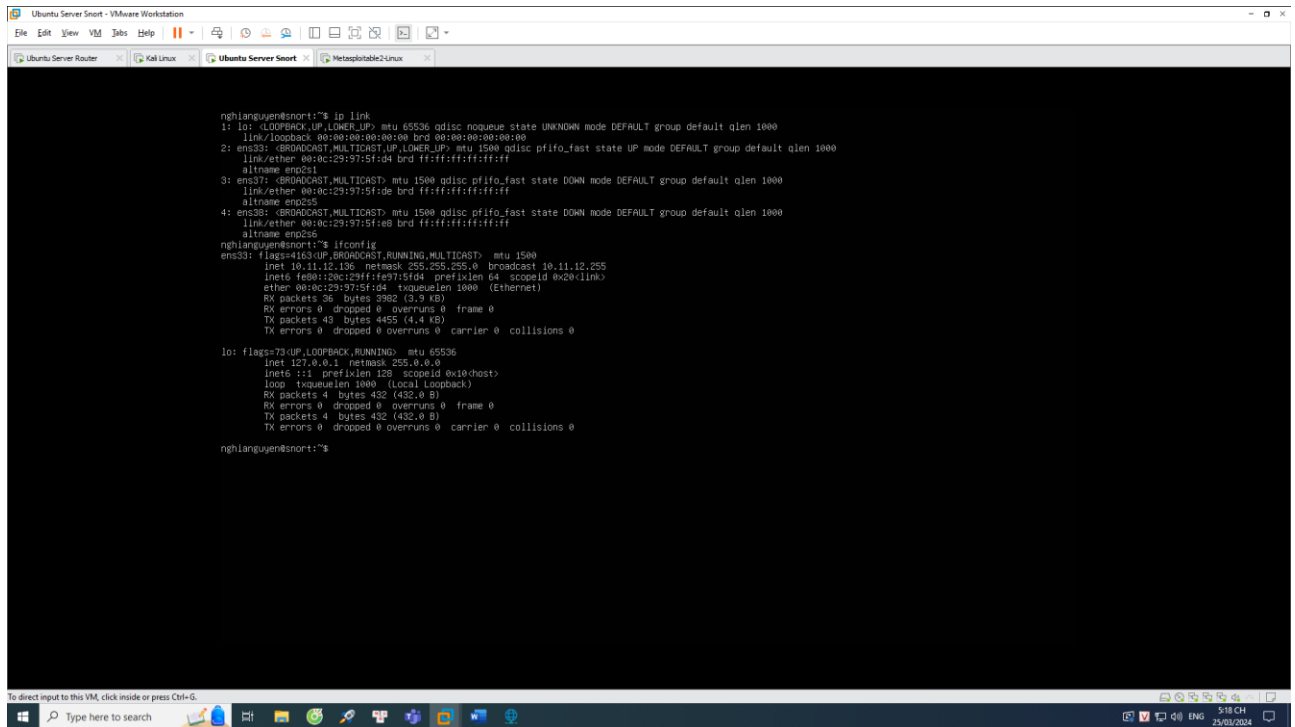


```
(nghianguyen@kali)~$ ifconfig
docker0: flags=4095<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:0c:85:38:70 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.81.82.100 netmask 255.255.255.0 broadcast 10.81.82.255
    inet6 fe80::20c:29ff:fe19:1c6d prefixlen 64 scopeid 0<link>
    ether 00:0c:29:19:1c6d:fc txqueuelen 1000 (Ethernet)
    RX packets 2 bytes 120 (120.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3076 bytes 187810 (183.4 KiB)
    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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2560 bytes 251394 (245.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2560 bytes 251394 (245.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

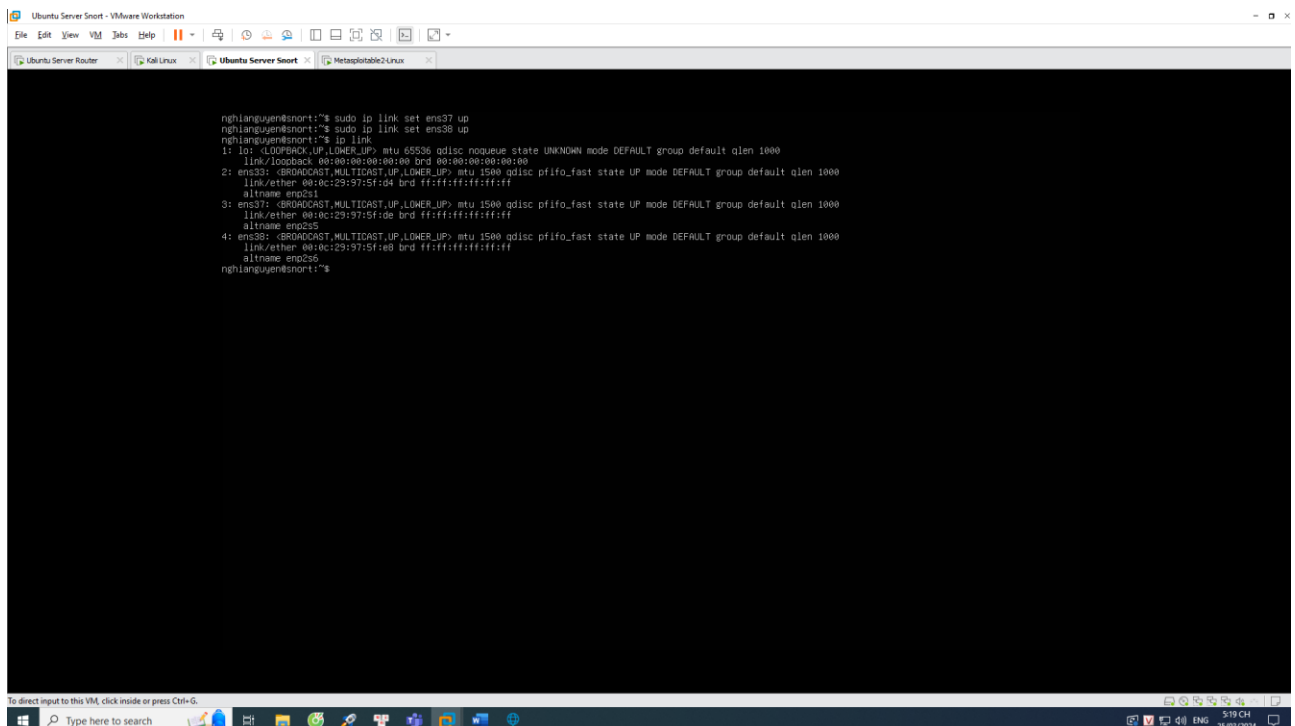
Đối với máy Snort, thông tin interfaces như sau:



```
nghianguyen@snort:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:97:5f:d4 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
3: ens37: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:97:5f:de brd ff:ff:ff:ff:ff:ff
    altname enp2s5
4: ens38: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:97:5f:e8 brd ff:ff:ff:ff:ff:ff
    altname enp2s6
nghianguyen@snort:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.11.12.136 netmask 255.255.255.0 broadcast 10.11.12.255
    inet6 fe80::120c:29ff:fe97:5fd4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:97:5f:d4 txqueuelen 1000 (Ethernet)
    RX packets 36 bytes 3960 (3.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 4455 (4.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

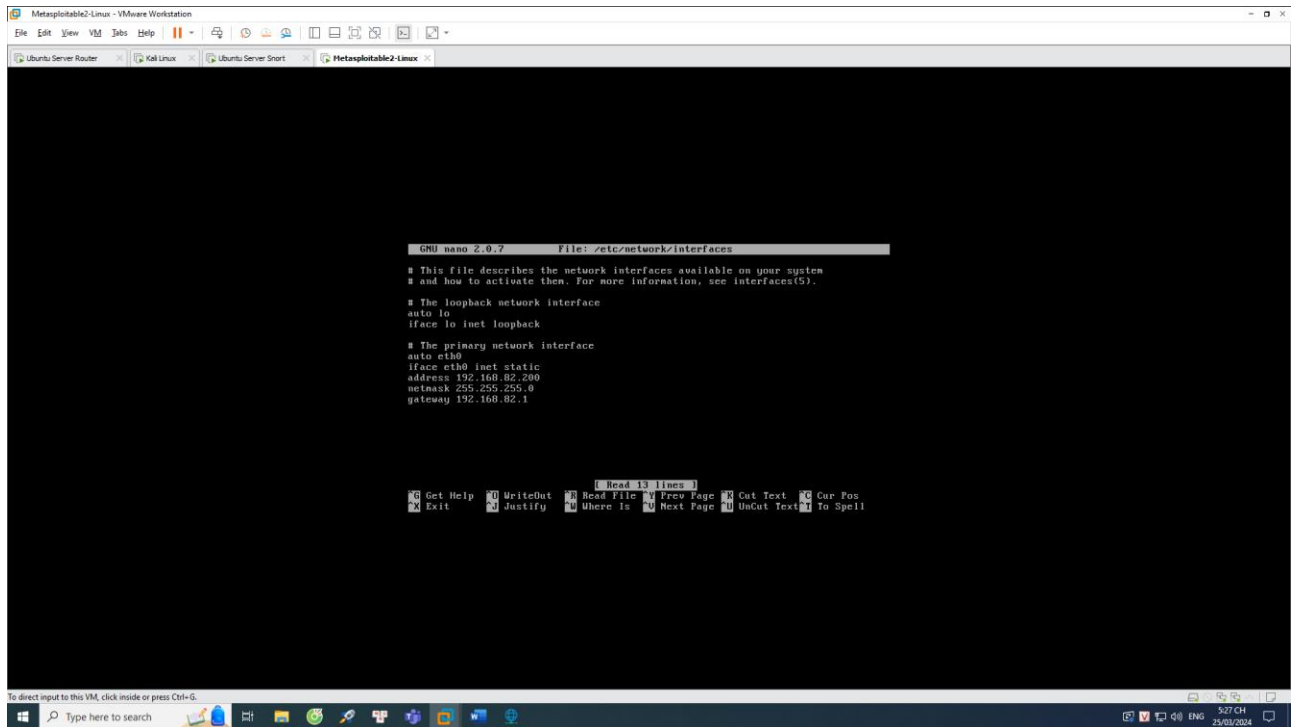
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 432 (432.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 432 (432.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
nghianguyen@snort:~$
```

Bởi vì trạng thái của ens37 và 38 đang down, nên em sẽ đổi trạng thái cho chúng thành up:



```
nghianguyen@snort:~$ sudo ip link set ens37 up
nghianguyen@snort:~$ sudo ip link set ens38 up
nghianguyen@snort:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:97:5f:d4 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:97:5f:de brd ff:ff:ff:ff:ff:ff
    altname enp2s5
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:97:5f:e8 brd ff:ff:ff:ff:ff:ff
    altname enp2s6
nghianguyen@snort:~$
```

Đổi với máy victim:

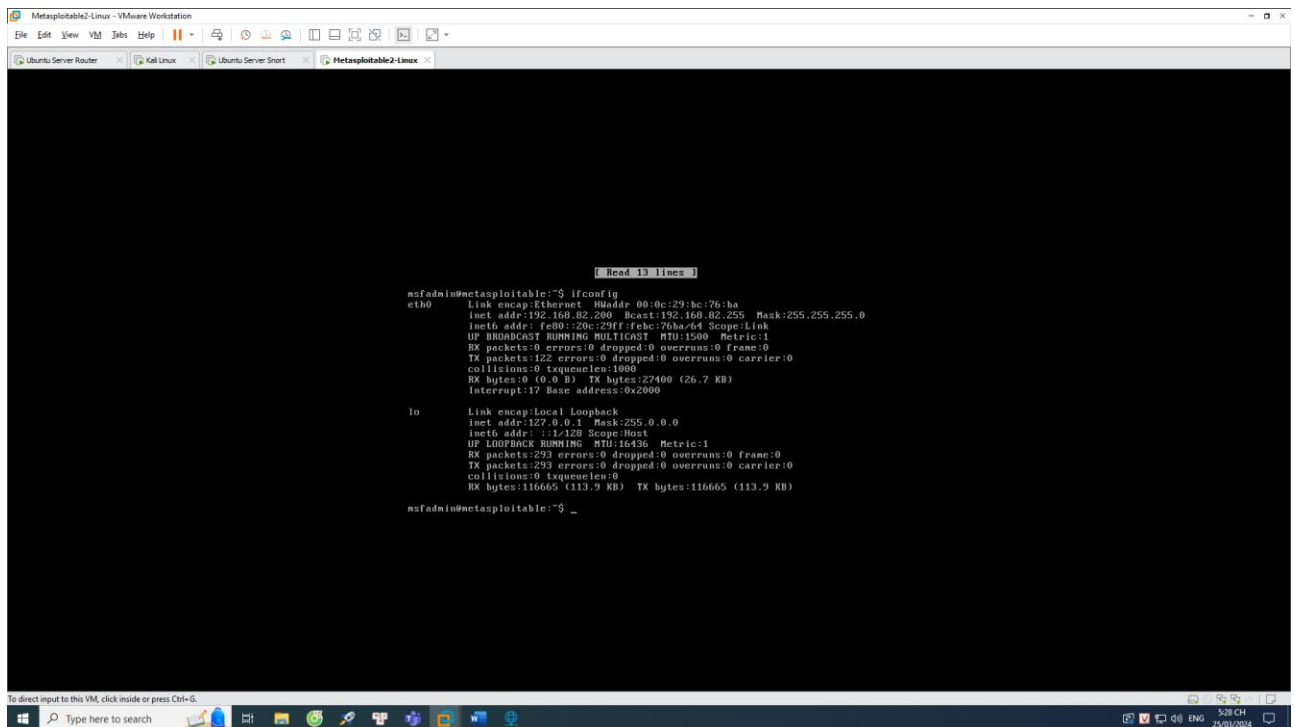


```
GNU nano 2.0.7 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.82.200
netmask 255.255.255.0
gateway 192.168.82.1
```

Kết quả:

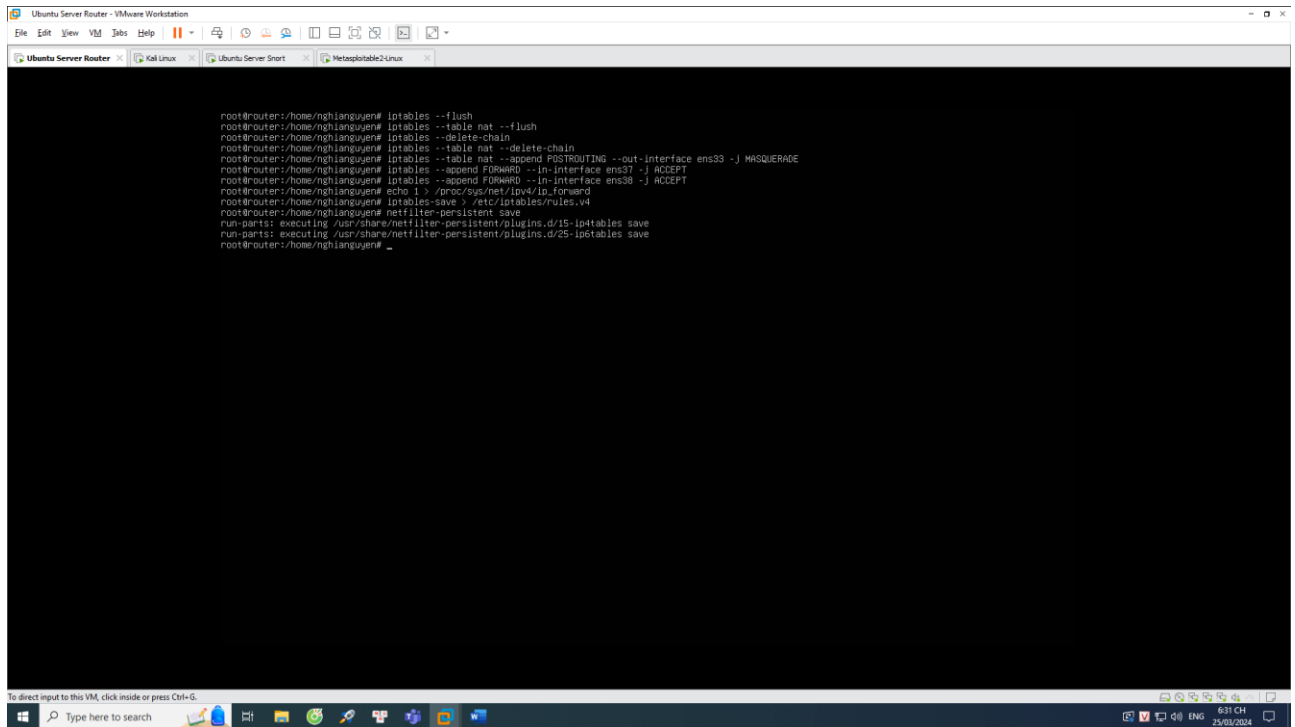


```
msfadmin@metasploit2:~$ ifconfig
eth0:
Link encap:Ethernet HWaddr 00:0c:29:3c:76:ba
inet addr:192.168.82.200 Bcast:192.168.82.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe3c:76ba/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:27400 (26.7 KB)
Interrupt:17 Base address:0x2000

lo:
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:293 errors:0 dropped:0 overruns:0 frame:0
TX packets:293 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:116665 (113.9 KB) TX bytes:116665 (113.9 KB)

msfadmin@metasploit2:~$ _
```

Cài đặt địa chỉ ip cho các interfaces, các máy đã xong, em tiến hành thực hiện việc cấu hình NAT Outbound cho máy router:

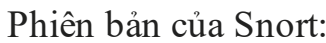


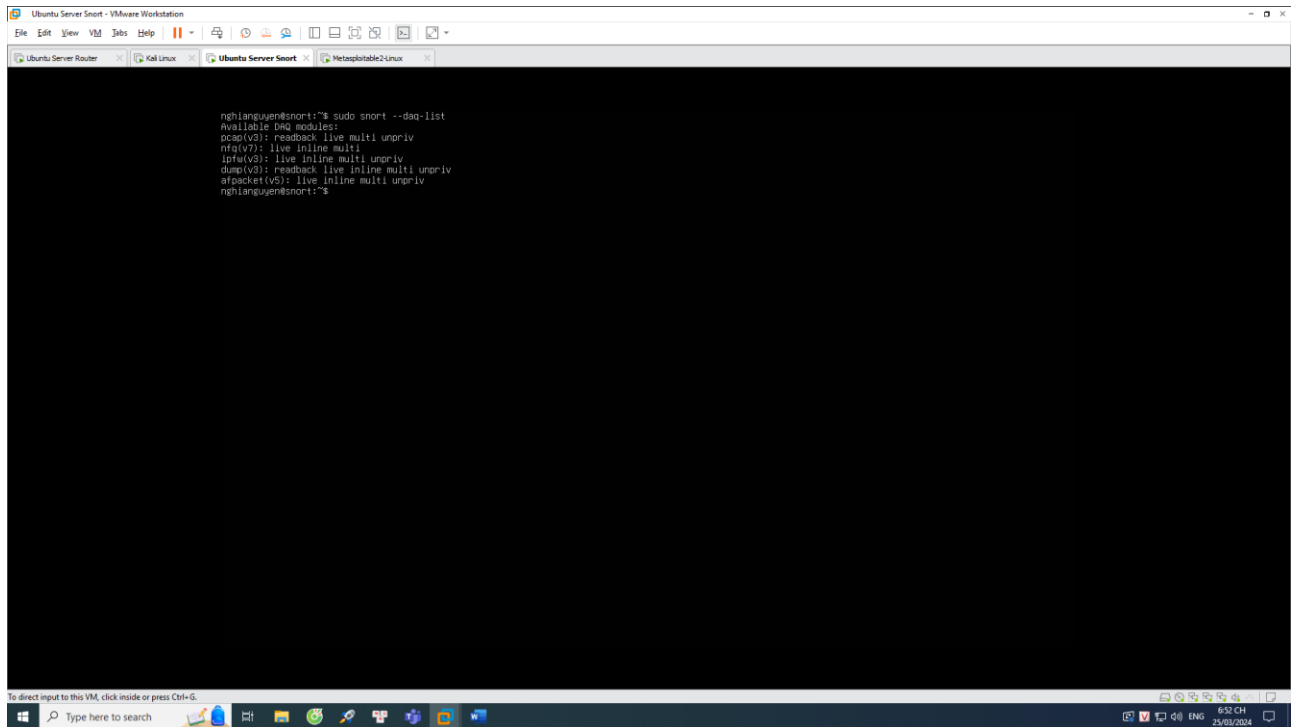
```
root@router:/home/nghianguyen# iptables --flush
root@router:/home/nghianguyen# iptables --table nat --flush
root@router:/home/nghianguyen# iptables --delete-chain
root@router:/home/nghianguyen# iptables --table nat --delete-chain
root@router:/home/nghianguyen# iptables --table nat --append POSTROUTING --out-interface ens33 -j MASQUERADE
root@router:/home/nghianguyen# iptables --append FORWARD --in-interface ens37 -j ACCEPT
root@router:/home/nghianguyen# iptables --append FORWARD --in-interface ens38 -j ACCEPT
root@router:/home/nghianguyen# echo 1 > /proc/sys/net/ipv4/ip_forward
root@router:/home/nghianguyen# iptables-save > /etc/iptables/rules.v4
root@router:/home/nghianguyen# netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
root@router:/home/nghianguyen#
```

Để các quy tắc có thể được lưu qua các lần khởi động thì em lưu chúng vào một tệp và thiết lập một quy trình để áp dụng chúng khi hệ thống khởi động. Thông qua việc cài đặt iptables-persistent và sử dụng câu lệnh “sudo iptables-save > /etc/iptables/rules.v4”, “sudo netfilter-persistent save”.

Sau khi cấu hình NAT Outbound xong, em tiếp tục tiến hành cài đặt và cấu hình Snort.

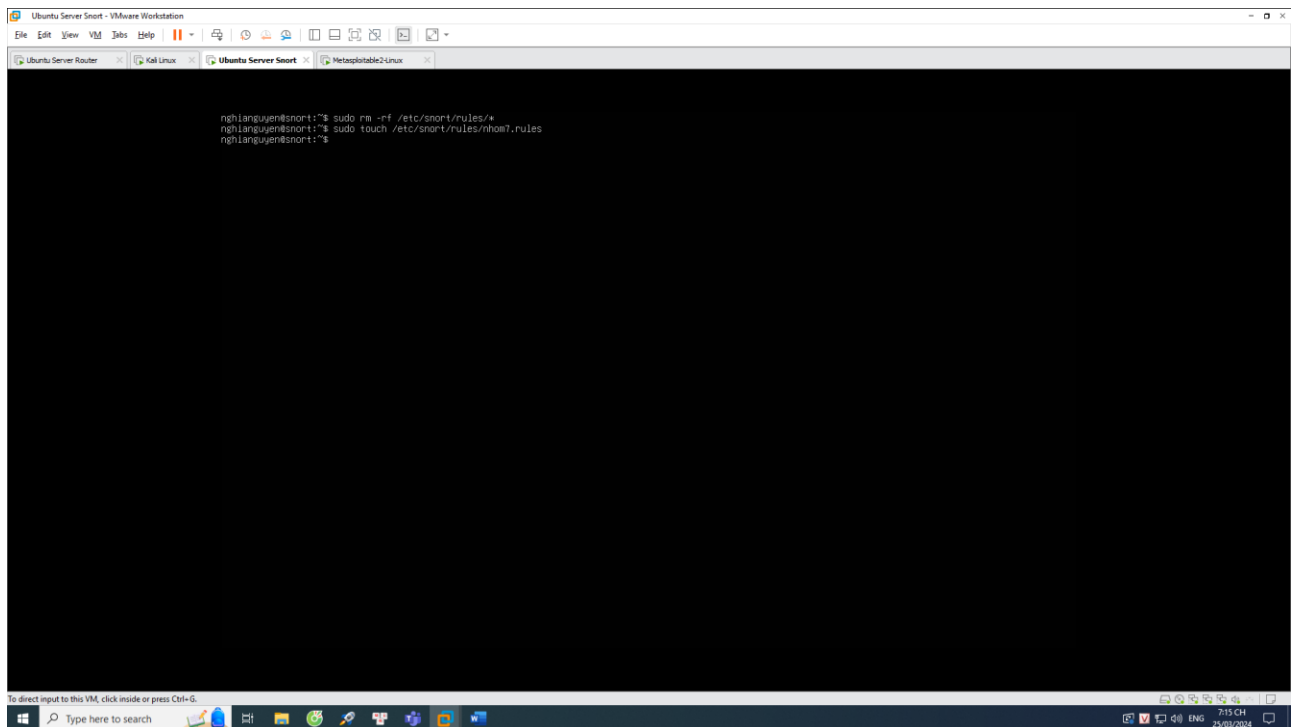
Cài đặt Snort từ công cụ APT:





```
nghianguyen@snort:~$ sudo snort --daq-list
Available DAQ modules:
pcap(v3): readback live multi unpriv
nq(v7): live inline multi
ipfu(v3): live inline multi unpriv
dump(v3): readback live inline multi unpriv
afpacket(v5): live inline multi unpriv
nghianguyen@snort:~$
```

Xóa tất cả các file rule mặc định của Snort và tạo file rule của nhóm định nghĩa:



```
nghianguyen@snort:~$ sudo rm -rf /etc/snort/rules/*
nghianguyen@snort:~$ sudo touch /etc/snort/rules/nhom7.rules
nghianguyen@snort:~$
```

Tạo file cấu hình snort của nhóm tại /etc/snort/nhom7-snort.conf với nội dung sau:

```

GNU nano 2.10 /etc/snort/nhom7-snort.conf
config daq: afpacket
config daq_mode: inline
include /etc/snort/rules/nhom7.rules

```

Kiểm tra file cấu hình snort:

```

-----[Rule Port Counts]-----
|  src  |  tcp  |  udp  |  icmp  |  ip  |
|-----|-----|-----|-----|-----|
|  dst  |  0    |  0    |  0    |  0    |
|  any  |  0    |  0    |  0    |  0    |
|  nc   |  0    |  0    |  0    |  0    |
|  sd   |  0    |  0    |  0    |  0    |
|-----|-----|-----|-----|-----|

-----[Detection-filter-config]-----
| memory-cap : 1048576 bytes
-----[Detection-filter-rules]-----
| none
-----[Rate-filter-config]-----
| memory-cap : 1048576 bytes
-----[Rate-filter-rules]-----
| none
-----[Event-filter-config]-----
| memory-cap : 1048576 bytes
-----[Event-filter-global]-----
| none
-----[Event-filter-local]-----
| none
-----[Suppression]-----
| none

Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
afpacket DAQ configured to inline.
Acquiring network traffic from "ens37:ens38".
Decoding Ethernet

--- Initialization Complete ---

--o Snort! <-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.13

Snort successfully validated the configuration!
Snort exiting
nghlanguyen@snort:~$

```

Chạy snort trong mode inline:

```

[Rule Port Counts]-----
|  tcp  udp  icmp  ip  |
|  src  0    0    0    0  |
|  dst  0    0    0    0  |
|  any  0    0    0    0  |
|  rc   0    0    0    0  |
|  ssg  0    0    0    0  |
|-----|

[detection-filter-config]-----
| memory-cap : 1048576 bytes |
|-----|
| none |
|-----|

[rate-filter-config]-----
| memory-cap : 1048576 bytes |
|-----|
| none |
|-----|

[event-filter-config]-----
| memory-cap : 1048576 bytes |
|-----|
| none |
|-----|
| none |
|-----|
| none |
|-----|

Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations
afpacket OAD configured to inline.
Acquiring network traffic from "ens3:ens38".
Reload thread starting...
Reload thread started, thread 0x7b4b687d76c0 (2415)

--== Initialization Complete ==--

o''~
...~
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2015 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PDRE version: 0.39 2016-06-14
Using ZLIB version: 1.2.15

Commencing packet processing (pid=2406)
Decoding Ethernet
-
  
```

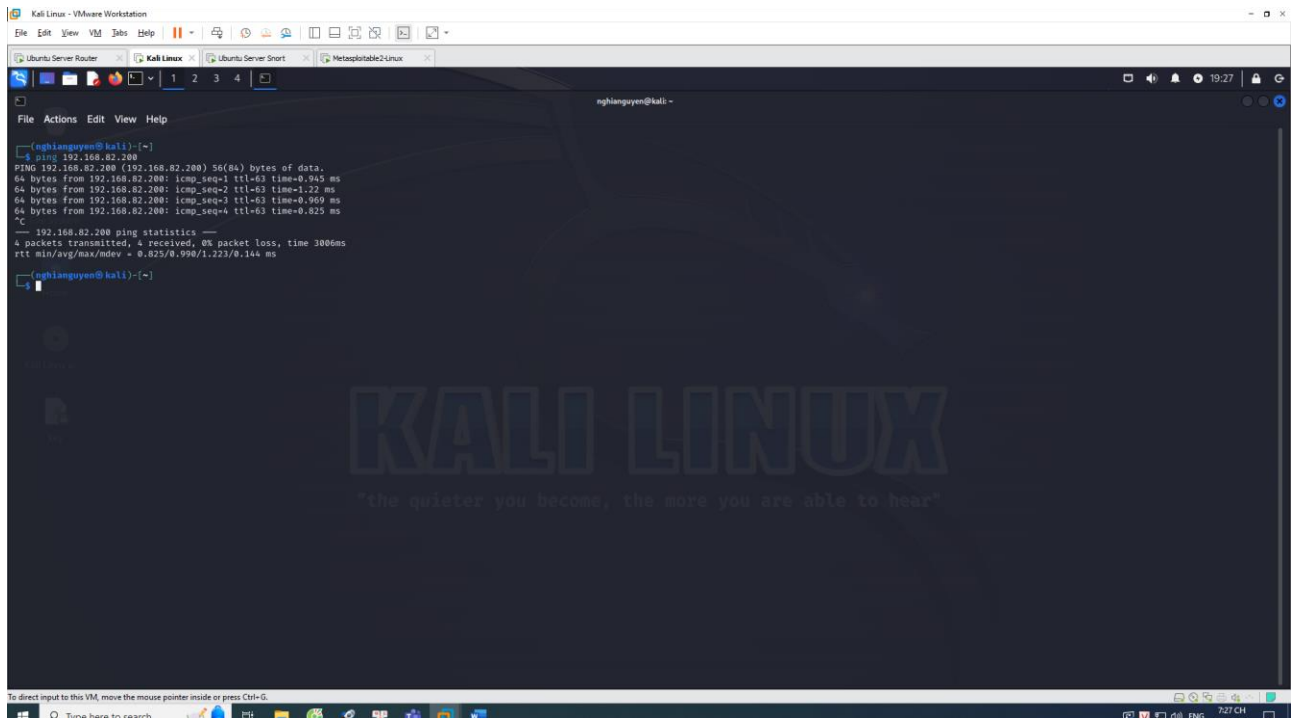
Khi đã chạy thành công, em thực hiện việc ping các máy đến nhau.

Máy Kali ping google.com:

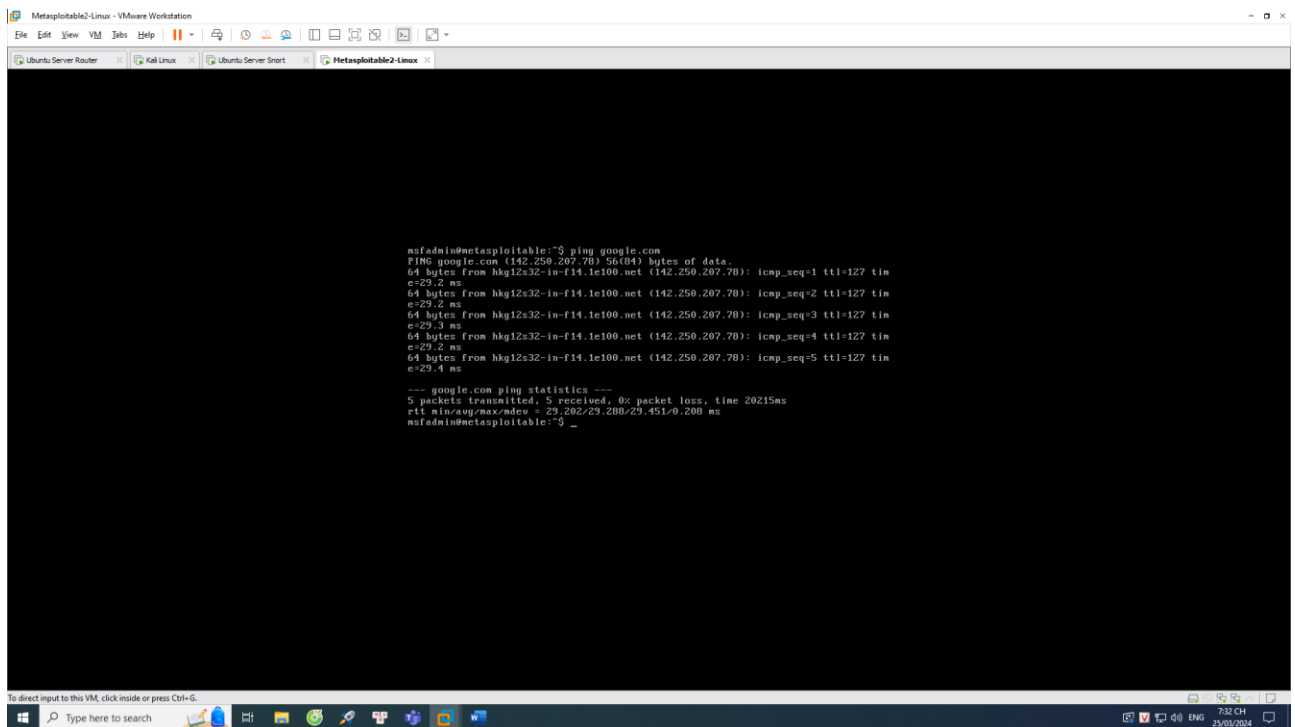
```

nghianguyen@kali: ~
[~] ping google.com
PING google.com (172.217.24.238) 56(84) bytes of data:
64 bytes from del0s05-in-f14.1e100.net (172.217.24.238): icmp_seq=1 ttl=127 time=28.9 ms
64 bytes from kul06s17-in-f238.1e100.net (172.217.24.238): icmp_seq=2 ttl=127 time=31.9 ms
64 bytes from hkg12346-in-f14.1e100.net (172.217.24.238): icmp_seq=3 ttl=127 time=34.6 ms
64 bytes from kul06s17-in-f238.1e100.net (172.217.24.238): icmp_seq=4 ttl=127 time=33.9 ms
^C
- google.com ping statistics -
4 packets transmitted, 4 received, 0% packet loss, time 301ms
rtt min/avg/max/mdev = 28.945/32.340/34.622/2.197 ms
[~]
  
```

Máy Kali ping máy Victim:

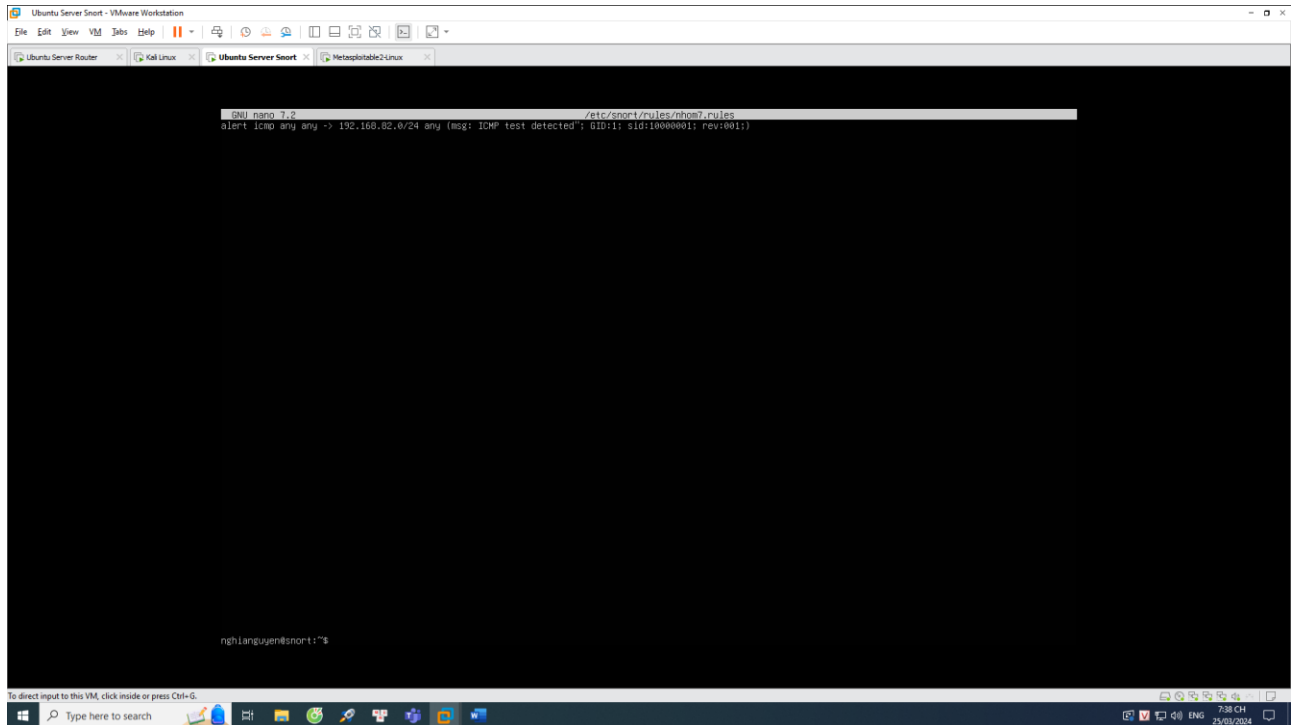


Máy Victim ping google.com:



Để mà có thể ping được tới google.com thì em đã phải chỉnh sửa một tí ở file /etc/resolv.conf, bằng cách thêm nội dung “nameserver 8.8.8.8 nameserver 8.8.4.4” để nó có thể phân giải tên miền.

Tiếp đến là em sẽ viết rule cho snort để phát hiện gói ICMP gửi đến lớp mạng 192.168.82.0/24 trong file /etc/snort/rules/nhom7.rules:

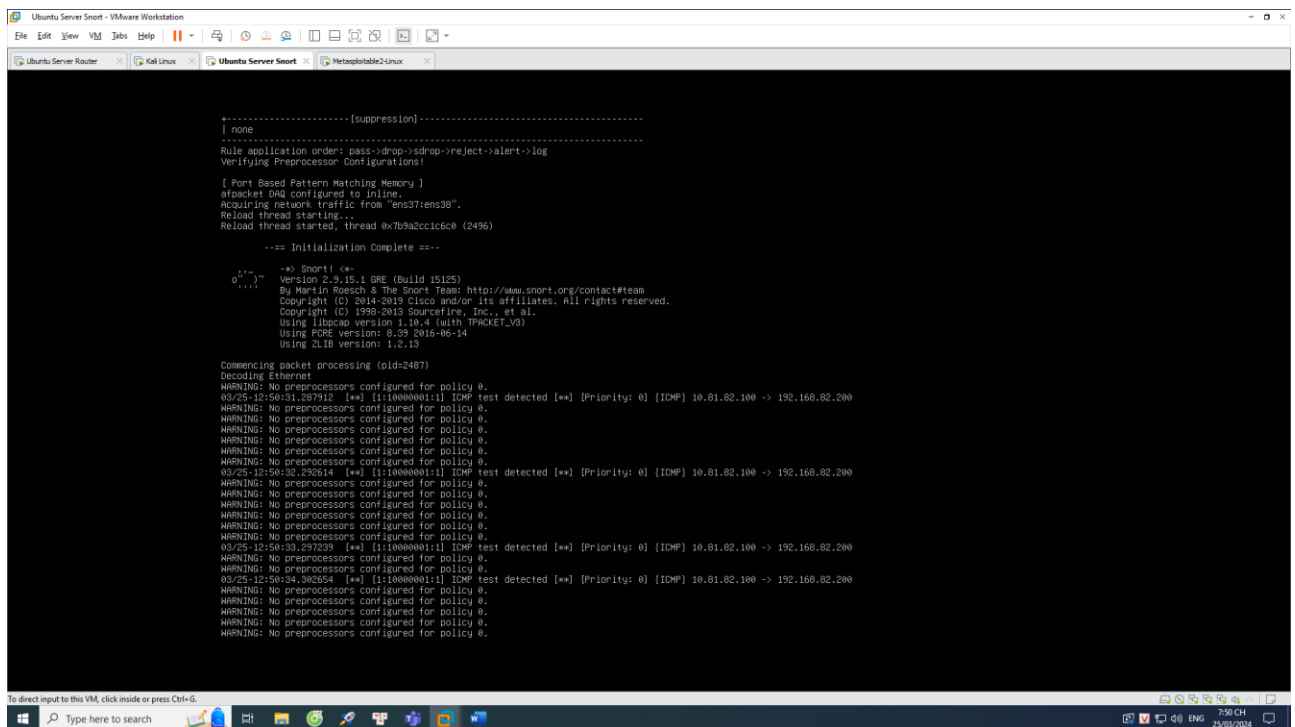


```
GNU nano 2.9.2 /etc/snort/rules/nhom7.rules
alert icmp any any -> 192.168.82.0/24 any (msg: ICMP test detected; SID:1; rev:001)

nghianguyen@snort:~$
```

Bây giờ em sẽ thử ping lại từ máy kali đến máy victim và xem alert:

Trên console:



```
+-----[suppression]-----
| none
+-----
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
a/packet IDQ configured to inline.
Acquiring network traffic from "ens37:ens38".
Reload thread starting...
Reload thread started, thread 0x7b9a2cc6c0e (2496)

--- Initialization Complete ---

--o-- Snort! <--
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V9)
Using PDRE version: 0.39 2016-06-14
Using ZLIB version: 1.2.13

Commencing packet processing (pid=2487)
Decoding Ethernet
WARNING: No preprocessors configured for policy #.
03/25-12:50:31.287912 [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] [ICMP] 10.81.82.100 -> 192.168.82.200
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
03/25-12:50:32.262614 [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] [ICMP] 10.81.82.100 -> 192.168.82.200
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
03/25-12:50:33.297229 [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] [ICMP] 10.81.82.100 -> 192.168.82.200
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
03/25-12:50:34.302654 [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] [ICMP] 10.81.82.100 -> 192.168.82.200
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
WARNING: No preprocessors configured for policy #.
```


Trong /var/log/snort/alert:

```

GNU nano 2.9.3 /var/log/snort/alert
[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:32.566994 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20146 InLen:20 OptLen:0 If
Type:8 Code:0 ID:27280 Seq:1 ECHO

[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:34.579310 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20232 InLen:20 OptLen:0 If
Type:8 Code:0 ID:27280 Seq:2 ECHO

[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:35.604326 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20356 InLen:20 OptLen:0 If
Type:8 Code:0 ID:27280 Seq:3 ECHO

[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:36.627468 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20403 InLen:20 OptLen:0 If
Type:8 Code:0 ID:27280 Seq:4 ECHO

[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:37.651763 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20502 InLen:20 OptLen:0 If
Type:8 Code:0 ID:27280 Seq:5 ECHO

[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:38.675988 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20615 InLen:20 OptLen:0 If
Type:8 Code:0 ID:27280 Seq:6 ECHO

[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:39.679398 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20659 InLen:20 OptLen:0 If
Type:8 Code:0 ID:27280 Seq:7 ECHO

[**] [1:1000000:1] ICMP test detected [**]
[Priority: 0]
00/25-12:39:40.691374 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:20677 InLen:20 OptLen:0 If

```

Yêu cầu 3: Sinh viên viết rule drop các gói ICMP đi đến máy Victim (rule #1). Sử dụng tcpdump trên máy Victim kiểm tra các trường hợp sau:

- Trước khi viết áp dụng rule #1.
- Sau khi áp dụng rule #1.

Kiểm tra alert log của Snort để xem kết quả.

Sử dụng tcpdump để kiểm tra máy victim trước khi viết rule:

```

msfadmin@metasploit> sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
00:58:29.110990 IP 10.81.82.100 > 192.168.82.200: ICMP echo request, id 62312, s
eq 1, length 64
00:58:29.110127 IP 192.168.82.200 > 10.81.82.100: ICMP echo reply, id 62312, s
eq 1, length 64
00:58:29.110349 IP 192.168.82.200.50147 > 192.168.220.2.domain: 24424+ PTR? 200.
82.168.192.in-addr.arpa. (45)
00:58:30.120863 IP 10.81.82.100 > 192.168.82.200: ICMP echo request, id 62312, s
eq 2, length 64
00:58:30.120896 IP 192.168.82.200 > 10.81.82.100: ICMP echo reply, id 62312, s
eq 2, length 64
00:58:31.125522 IP 10.81.82.100 > 192.168.82.200: ICMP echo request, id 62312, s
eq 3, length 64
00:58:31.125550 IP 192.168.82.200 > 10.81.82.100: ICMP echo reply, id 62312, s
eq 3, length 64
00:58:32.120703 IP 10.81.82.100 > 192.168.82.200: ICMP echo request, id 62312, s
eq 4, length 64
00:58:32.120815 IP 192.168.82.200 > 10.81.82.100: ICMP echo reply, id 62312, s
eq 4, length 64

```

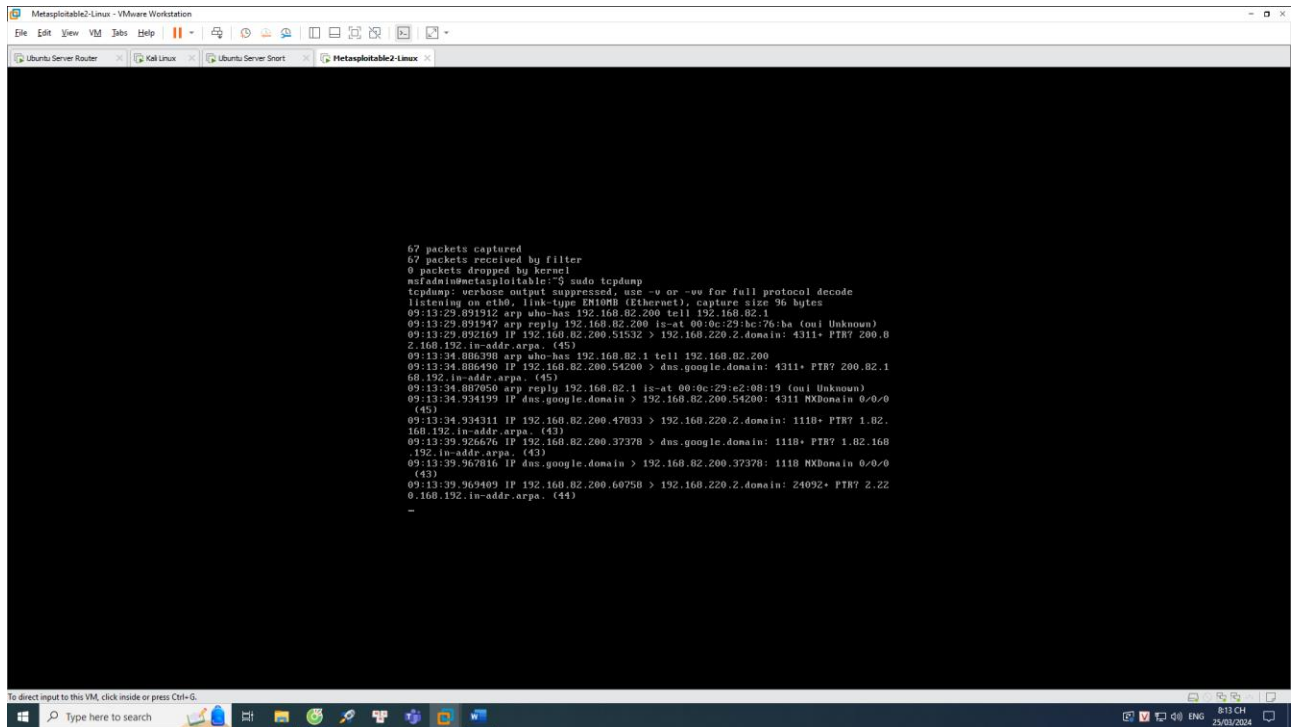
Bây giờ em sẽ tiến hành viết rule để drop các gói ICMP đi đến máy Victim, rule sẽ là “drop icmp any any -> 192.168.82.200 any (msg:"ICMP to 192.168.82.200 dropped"; itype: 8; sid:10000002; rev:001);”

```

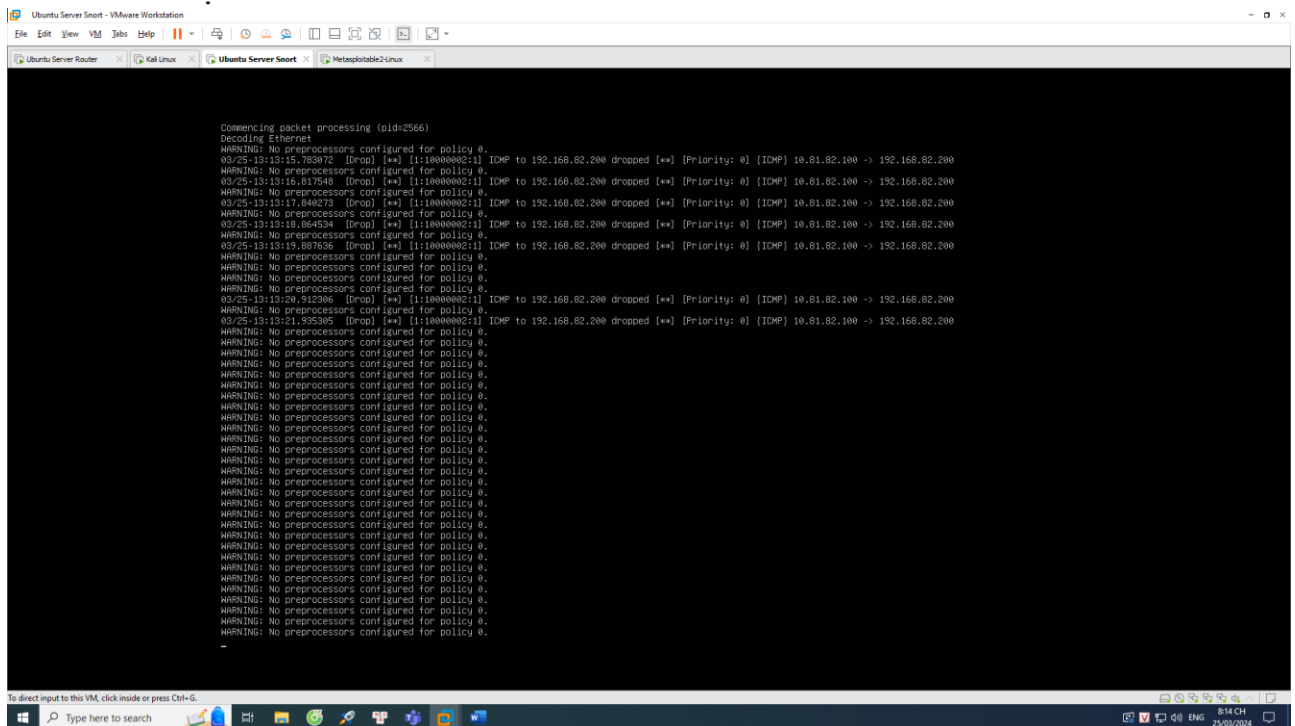
[snr] nano 7.0 /etc/snort/rules/rule7.rules
alert icmp any any -> 192.168.82.0/24 any (msg: "ICMP test detected"; sid:1; rev:001;)
drop icmp any any -> 192.168.82.200 any (msg: "ICMP to 192.168.82.200 dropped"; itype: 8; sid:10000002; rev:001;)

```

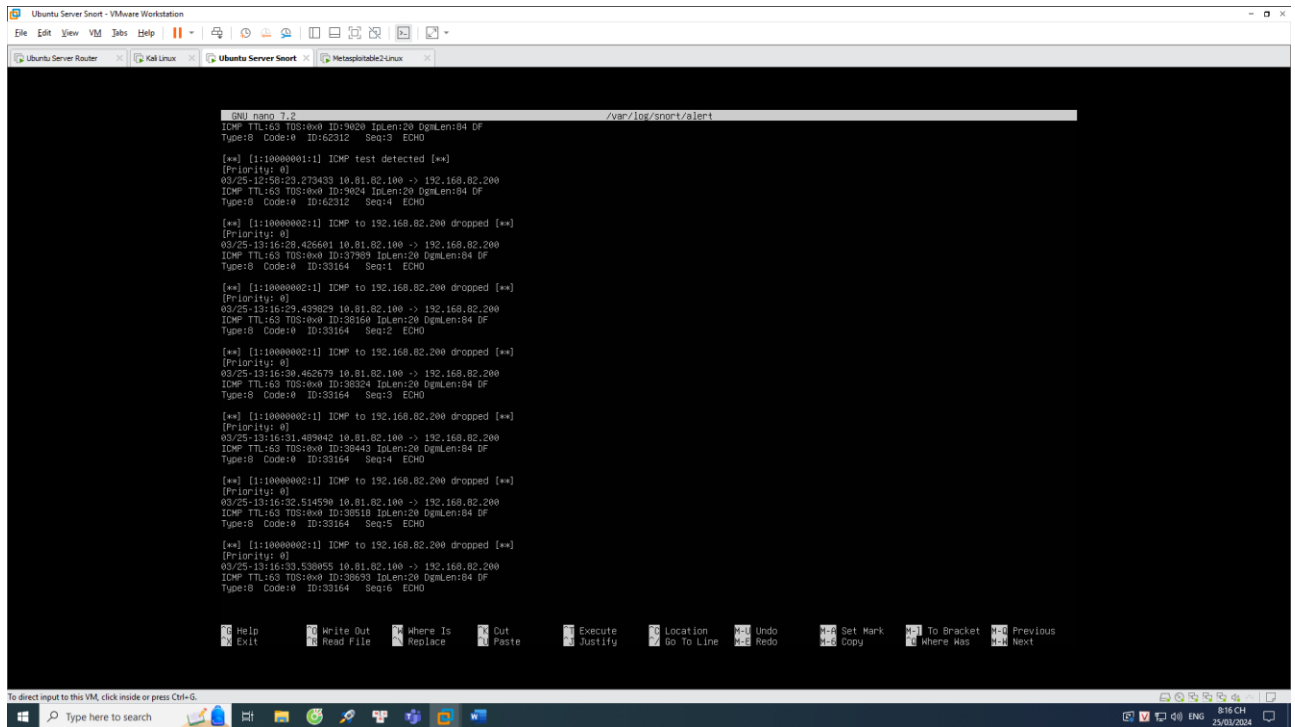
Sau khi áp dụng rule trên, em sử dụng tcpdump lại một lần nữa và dùng máy kali ping đến để kiểm tra máy victim:



Alert xuất hiện trên console:



Trong /var/log/snort/alert:



The screenshot shows a VMware Workstation interface with a terminal window titled 'Ubuntu Server Snort'. The terminal displays the output of the 'cat /var/log/snort/alert' command, showing several ICMP test packets and their corresponding responses. The logs include details such as TTL, TOS, ID, ILen, OLen, and Seq. The terminal also shows the GNU nano 2.9.2 editor interface.

```
GNU nano 2.9.2 /var/log/snort/alert
ICMP TTL:63 TOS:0x0 ID:9820 ILen:20 OLen:84 DF
Type:0 Code:0 ID:62312 Seq:3 ECHO
[**] [1:10000001:1] ICMP test detected [**]
[Priority: 0]
05/25-12:58:23.273433 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:9824 ILen:20 OLen:84 DF
Type:0 Code:0 ID:62312 Seq:4 ECHO
[**] [1:10000002:1] ICMP to 192.168.82.200 dropped [**]
[Priority: 0]
05/25-12:58:29.426601 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:37989 ILen:20 OLen:84 DF
Type:0 Code:0 ID:33164 Seq:1 ECHO
[**] [1:10000002:1] ICMP to 192.168.82.200 dropped [**]
[Priority: 0]
05/25-12:58:29.439829 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:38168 ILen:20 OLen:84 DF
Type:0 Code:0 ID:33164 Seq:2 ECHO
[**] [1:10000002:1] ICMP to 192.168.82.200 dropped [**]
[Priority: 0]
05/25-12:58:30.462679 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:38324 ILen:20 OLen:84 DF
Type:0 Code:0 ID:33164 Seq:3 ECHO
[**] [1:10000002:1] ICMP to 192.168.82.200 dropped [**]
[Priority: 0]
05/25-12:58:31.487842 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:38443 ILen:20 OLen:84 DF
Type:0 Code:0 ID:33164 Seq:4 ECHO
[**] [1:10000002:1] ICMP to 192.168.82.200 dropped [**]
[Priority: 0]
05/25-12:58:32.514590 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:38518 ILen:20 OLen:84 DF
Type:0 Code:0 ID:33164 Seq:5 ECHO
[**] [1:10000002:1] ICMP to 192.168.82.200 dropped [**]
[Priority: 0]
05/25-12:58:33.538955 10.81.82.100 -> 192.168.82.200
ICMP TTL:63 TOS:0x0 ID:38693 ILen:20 OLen:84 DF
Type:0 Code:0 ID:33164 Seq:6 ECHO
```