

BÁO CÁO THỰC HÀNH

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

Tên chủ đề: Triển khai Snort Inline

GVHD: Trương Thị Hoàng Hảo

Nhóm: 07

1. THÔNG TIN CHUNG:

Lớp: NT204.P21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Khánh Linh	22520769	22520769@gm.uit.edu.vn
2	Nguyễn Phúc Nhi	22521041	22521041@gm.uit.edu.vn
3	Phạm Thị Cẩm Tiên	22521473	22521473@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	100%	2 – 3
2	Yêu cầu 2	100%	3 – 15
3	Yêu cầu 3	100%	15 – 20

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

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. 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 hệ thống phát hiện xâm nhập mã nguồn mở và là một hệ thống ngăn chặn xâm nhập mạnh mẽ, được phát triển bởi Martin Roesch và hiện thuộc quản lý của Cisco. Nó được sử dụng để giám sát và phát hiện các hoạt động xâm nhập vào mạng máy tính. Snort có khả năng phân tích lưu lượng mạng theo thời gian thực để phát hiện các cuộc tấn công, quét cổng, phần mềm độc hại và nhiều mối đe dọa khác.
- Snort cho phép chạy trên các chế độ sau:
 - o **Sniffer mode:** Ở chế độ này, Snort sẽ đọc các gói tin mạng đang đi qua giao diện mạng và hiển thị chúng trên bảng điều khiển theo thời gian thực.
 - o **Packet logger mode:** Ở chế độ này, Snort sẽ lưu toàn bộ các gói tin vào thư mục để phân tích.
 - o **Network Intrusion Detection System Mode:** Ở chế độ này, Snort sẽ theo dõi lưu lượng mạng và phân tích lưu lượng đó. Sau đó nó sẽ xác định các mẫu hoặc dấu hiệu của các cuộc tấn công dựa trên định nghĩa của người dùng; và thực hiện cảnh báo hoặc ngăn chặn.
 - o **Inline mode:** Ở chế độ này, Snort sẽ hoạt động như một hệ thống ngăn chặn xâm nhập (IPS), nghĩa là nó có khả năng ngăn chặn các gói tin độc hại trước khi chúng xâm nhập được vào mạng nội bộ.

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

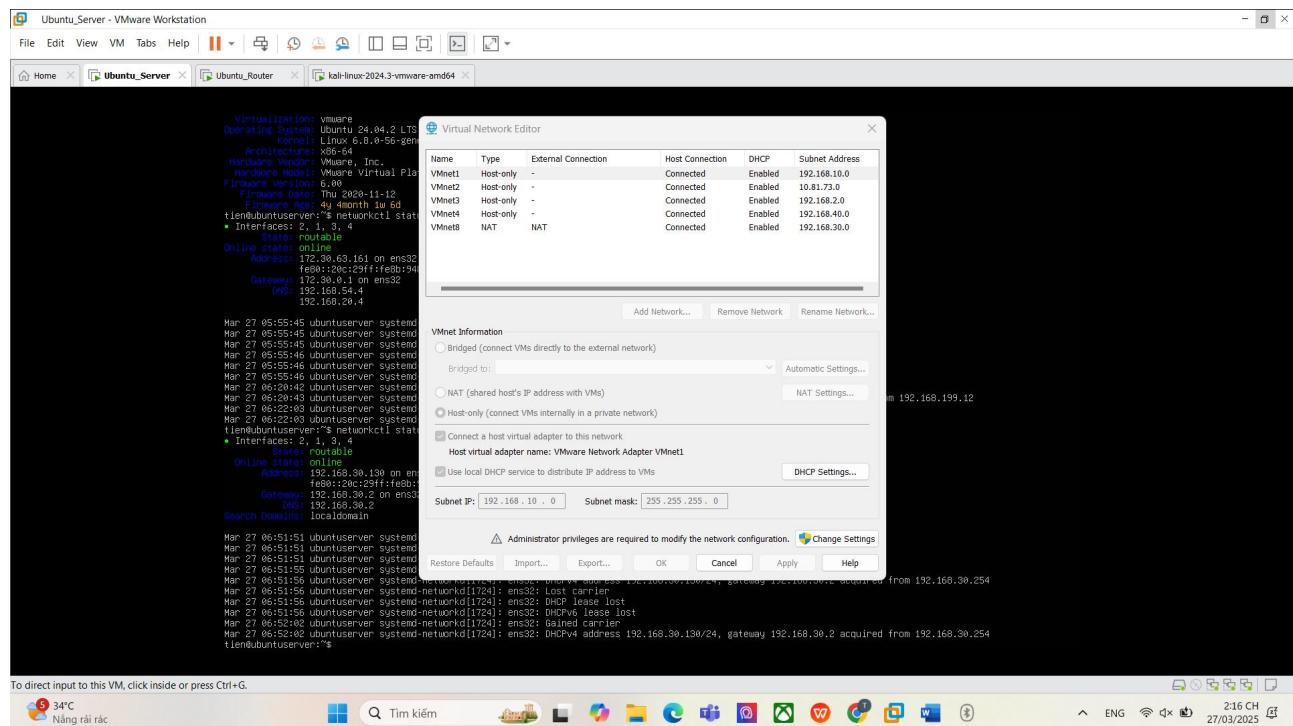
- Chế độ hoạt động linh hoạt: Snort có thể hoạt động ở nhiều chế độ khác nhau.
- Hệ thống quy tắc mạnh mẽ:
 - o Phát hiện dựa trên chữ ký (Signature-Based Detection): So sánh lưu lượng mạng với một tập hợp các quy tắc có sẵn để xác định các mối đe dọa.
 - o Phát hiện dựa trên hành vi (Anomaly-Based Detection): Phát hiện lưu lượng bất thường bằng cách so sánh với hành vi bình thường của mạng.
 - o Quy tắc linh hoạt: Có thể tạo quy tắc tùy chỉnh để phát hiện các cuộc tấn công cụ thể.
- Phát hiện và bảo vệ chống lại nhiều loại tấn công: Port scanning, DoS/DDoS, Exploit, SQL Injection, Cross-Site Scripting, buffer overflow,...
- Hỗ trợ nhiều cơ chế lấy gói tin
- Chế độ Inline giúp ngăn chặn xâm nhập
- Ghi log và tạo báo cáo chi tiết:
 - o Snort có thể lưu lại nhật ký của các gói tin đáng ngờ
 - o Snort có hỗ trợ nhiều định dạng log
- Khả năng mở rộng và tích hợp với các công cụ khác (SIEM, Snorby, BASE, Sguil,...)

- Phát hiện xâm nhập: Snort có khả năng phát hiện các hoạt động xâm nhập vào mạng máy tính thông qua phân tích gói tin mạng đi vào và đi ra khỏi mạng. Sử dụng các rule dựa trên signature hoặc hành vi để nhận diện các cuộc tấn công. Khi phát hiện tấn công Snort sẽ cảnh báo cho quản trị viên bằng cách ghi log, hiển thị thông báo trên giao diện người dùng hoặc ngăn chặn tấn công nếu được cấu hình trong chế độ IPS.

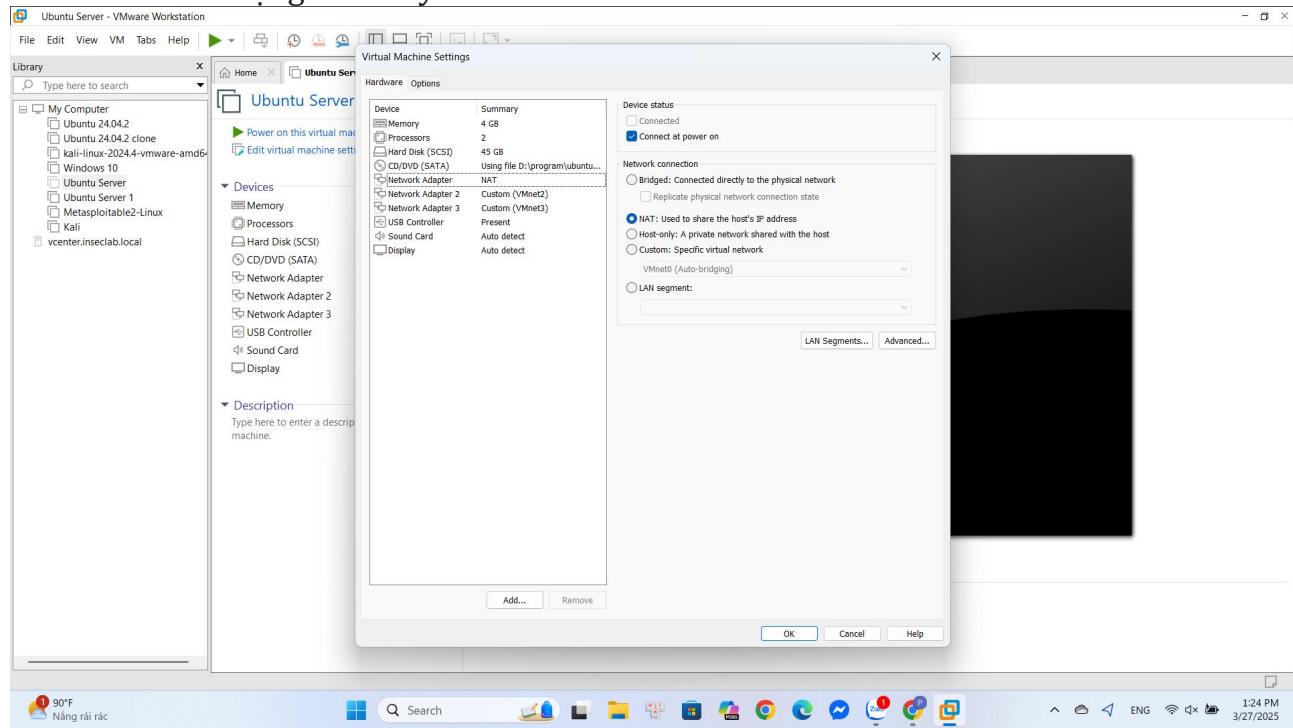
2. Yêu cầu 2: Sinh viên cài đặt và cấu hình Snort Inline theo các bước bên dưới. Chụp lại các hình ảnh minh chứng (chụp full màn hình) cho từng bước làm.

2.1a. Cấu hình mạng cho các máy theo mô hình

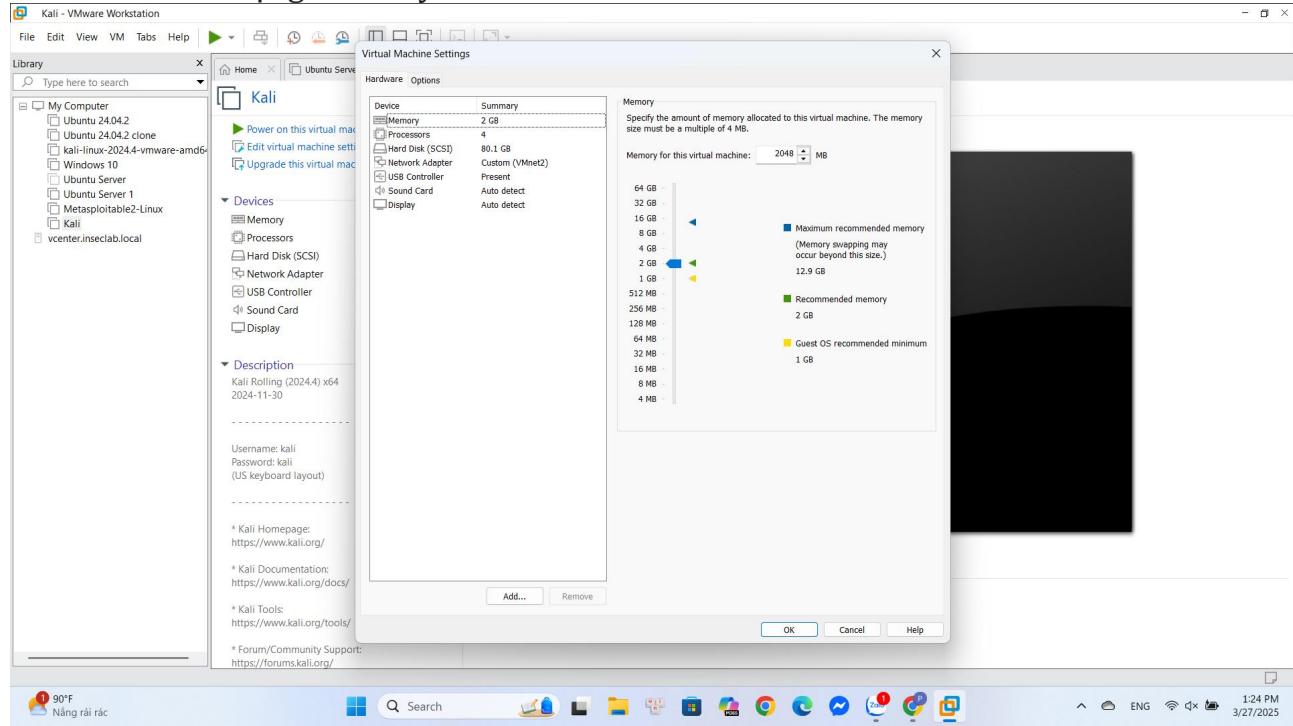
- Kiểm tra card VMnet8 (NAT) đã tồn tại và được bật DHCP. Thêm các card mạng



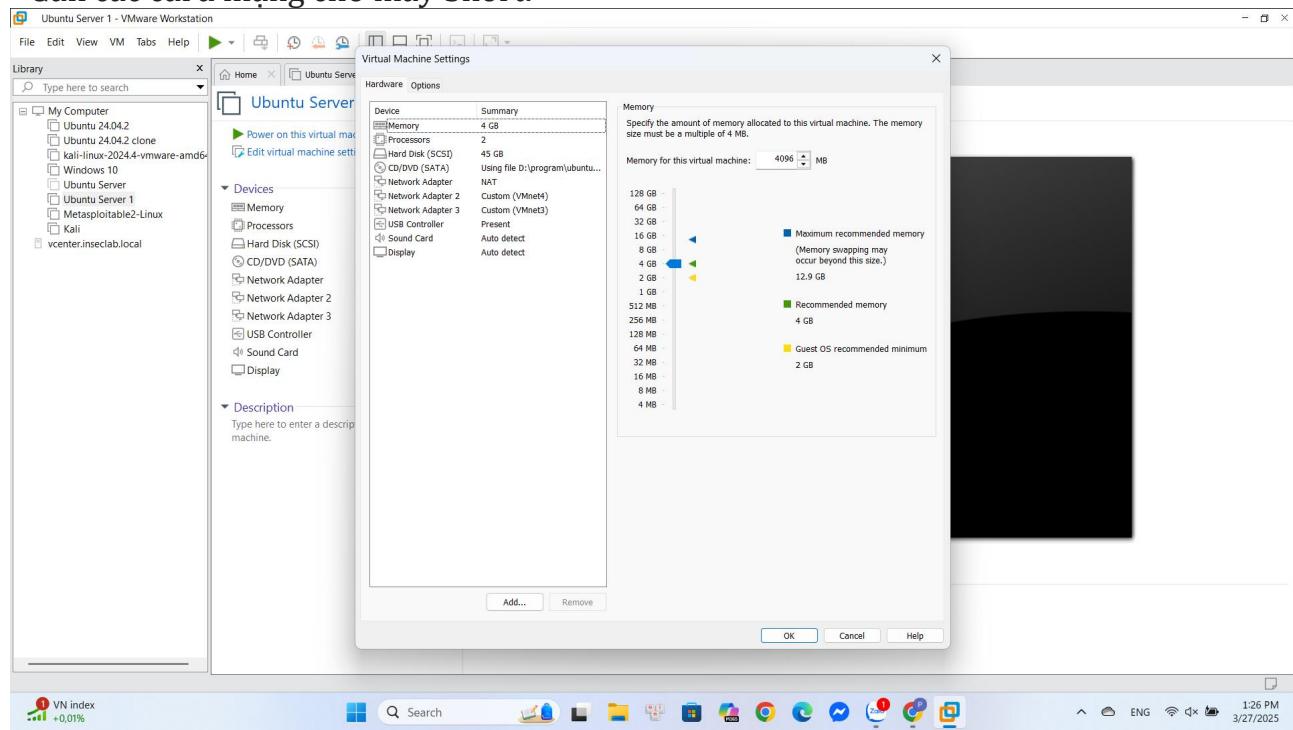
- Gán các card mạng cho máy Router.



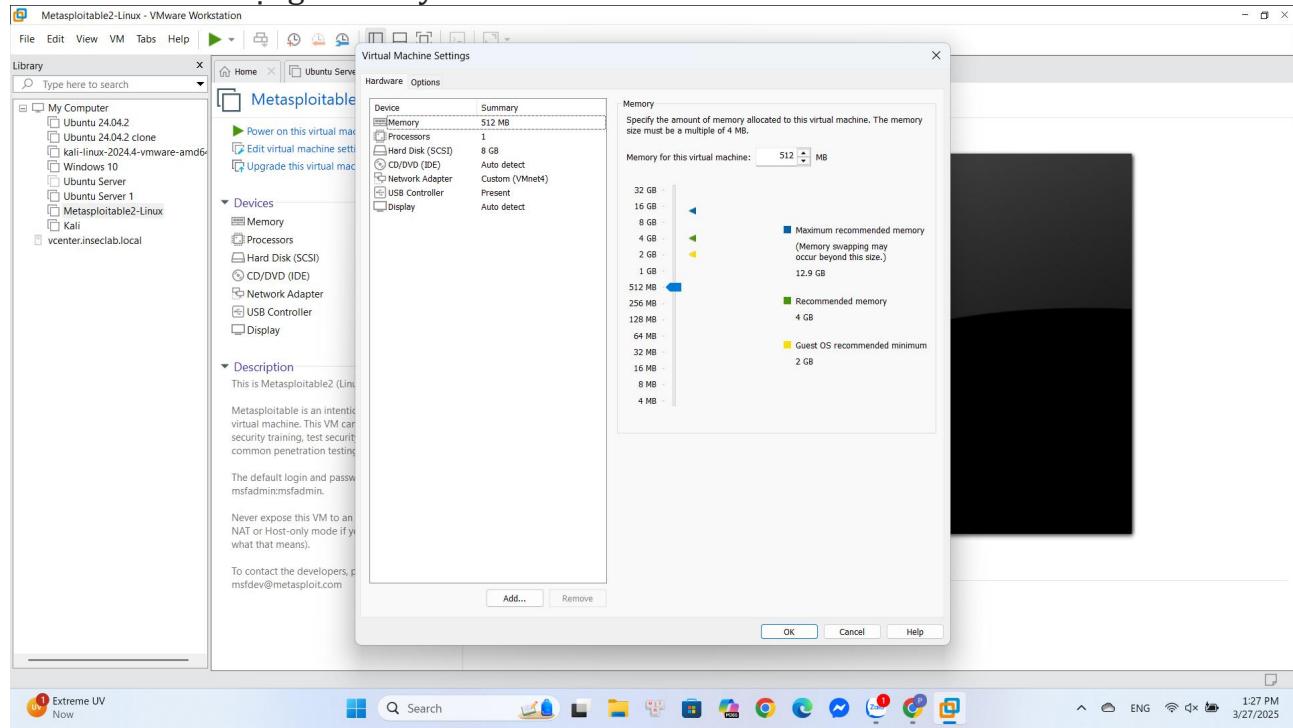
- Gán các card mạng cho máy Kali



- Gán các card mạng cho máy Snort.

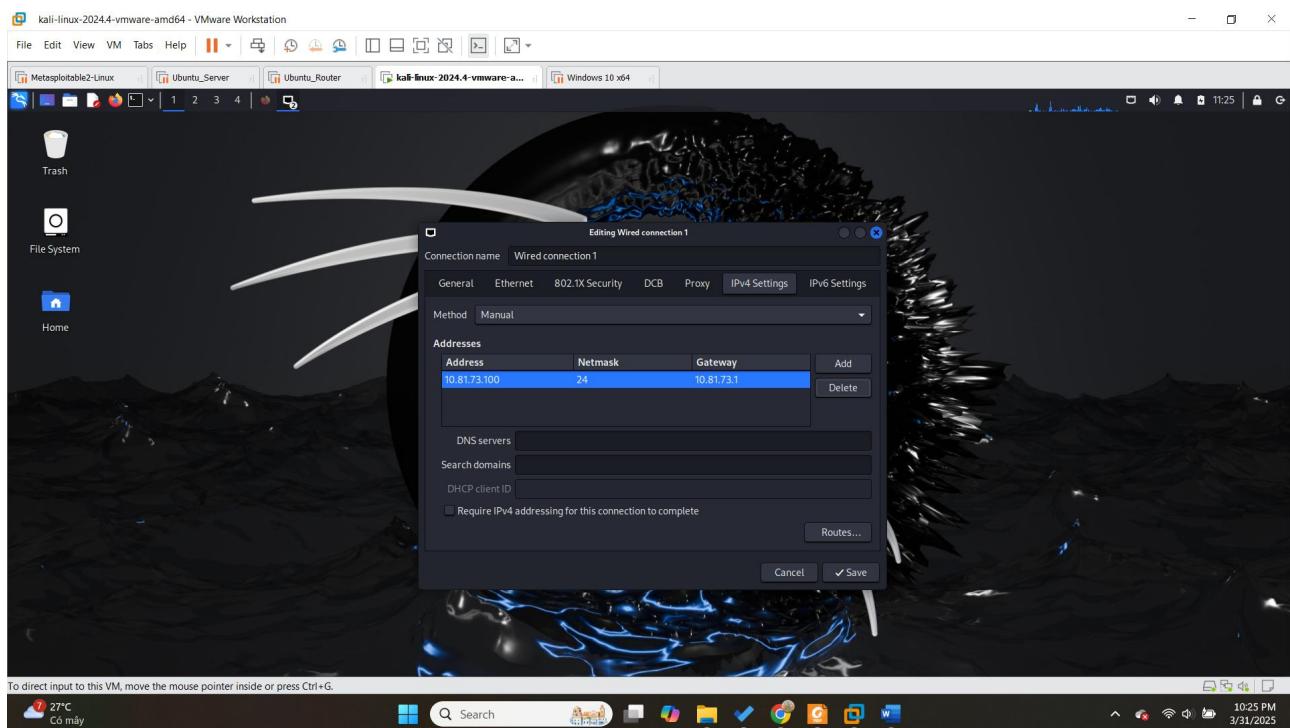


- Gán các card mạng cho máy Victim.



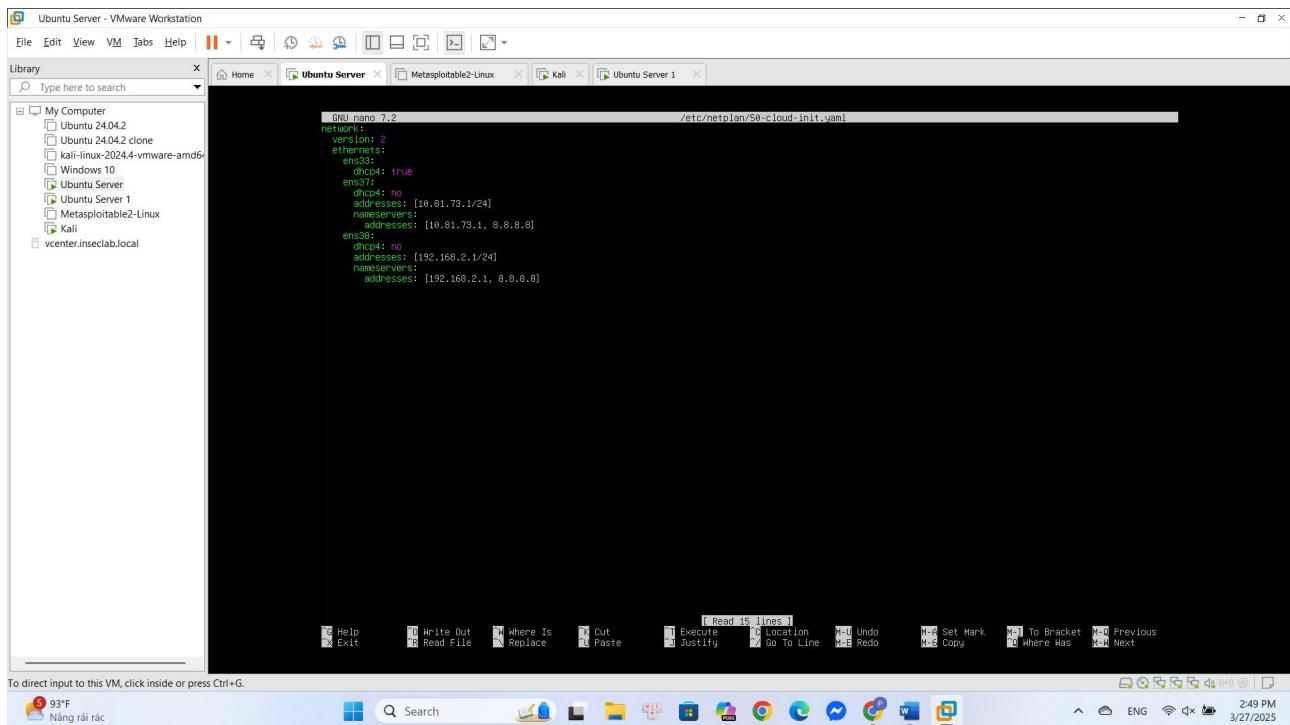
2.1b. Cấu hình địa chỉ IP cho các máy

- Máy Attacker (Kali linux)



- Máy Router (Ubuntu Server)

- Dùng lệnh **sudo nano /etc/netplan/50-cloud-init.yaml** để mở file và chỉnh sửa như hình:



```

phucnhii@22521041:~$ sudo netplan apply
phucnhii@22521041:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host loopback
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: ens3: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:44:08:08 brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.1/24 brd 192.168.0.255 metric 100
            brd 192.168.0.255
            valid_lft 1792sec preferred_lft 1792sec
            inet6 fe80::20c:29ff:fe44:0808/64 scope link
                valid_lft forever preferred_lft forever
4: ens38: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:44:08:02 brd ff:ff:ff:ff:ff:ff
        altname enp2s0
        altname enp2
        inet 10.81.73.1/24 brd 10.81.73.255 metric 100
            brd 10.81.73.255
            valid_lft forever preferred_lft forever
            inet6 fe80::20c:29ff:fe44:0802/64 scope link
                valid_lft forever preferred_lft forever
4: ens38: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:44:08:02 brd ff:ff:ff:ff:ff:ff
        altname enp2s0
        altname enp2
        inet 10.81.73.1/24 brd 10.81.73.255 metric 100
            brd 10.81.73.255
            valid_lft forever preferred_lft forever
            inet6 fe80::20c:29ff:fe44:0802/64 scope link
                valid_lft forever preferred_lft forever
4: ens38: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:44:08:02 brd ff:ff:ff:ff:ff:ff
        altname enp2s0
        altname enp2
        inet 10.81.73.1/24 brd 10.81.73.255 metric 100
            brd 10.81.73.255
            valid_lft forever preferred_lft forever
            inet6 fe80::20c:29ff:fe44:0802/64 scope link
                valid_lft forever preferred_lft forever
4: ens38: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:44:08:02 brd ff:ff:ff:ff:ff:ff
        altname enp2s0
        altname enp2
        inet 10.81.73.1/24 brd 10.81.73.255 metric 100
            brd 10.81.73.255
            valid_lft forever preferred_lft forever
            inet6 fe80::20c:29ff:fe44:0802/64 scope link
                valid_lft forever preferred_lft forever
phucnhii@22521041:~$ 

```

To direct input to this VM, click inside or press Ctrl+G.

- Máy Snort

```

Mar 27 05:55:45 ubuntuserver systemd-networkd[1724]: Enumeration completed
Mar 27 05:55:45 ubuntuserver systemd[1]: Started systemd-networkd.service - Network Configuration.
Mar 27 05:55:46 ubuntuserver systemd-networkd[1724]: ens32: Configuring with /run/systemd/network/10-netplan-ens32.network.
Mar 27 05:55:46 ubuntuserver systemd-networkd[1724]: ens32: Link UP
Mar 27 05:55:46 ubuntuserver systemd-networkd[1724]: ens32: Gained carrier
Mar 27 06:20:42 ubuntuserver systemd-networkd[1724]: ens32: Gained IPv6LL
Mar 27 06:20:43 ubuntuserver systemd-networkd[1724]: ens32: DHCPv4 address 172.30.63.161/16, gateway 172.30.6.1 acquired from 192.168.199.12
Mar 27 06:22:03 ubuntuserver systemd-networkd[1724]: eth0: Interface name change detected, renamed to ens3.
Mar 27 06:22:03 ubuntuserver systemd-networkd[1724]: eth0: Interface name change detected, renamed to ens3.
tien@ubuntuserver:~$ 
* Interfaces: 2, 1, 3, 4
  • Interface: 2, 1, 3, 4
    Online State: routable
    Online State: onlink
    Address: 192.168.30.130 on ens32
      fe80::20c:29ff:fe48:948d on ens32
    Gateway: 192.168.30.2 on ens32
    DNS: 192.168.30.2
    Search Domains: localdomain
    Search Domains: localdomain
Mar 27 06:51:51 ubuntuserver systemd-networkd[1724]: ens32: Lost carrier
Mar 27 06:51:51 ubuntuserver systemd-networkd[1724]: ens32: DHCP lease lost
Mar 27 06:51:51 ubuntuserver systemd-networkd[1724]: ens32: Gained carrier
Mar 27 06:51:55 ubuntuserver systemd-networkd[1724]: ens32: Gained carrier
Mar 27 06:51:56 ubuntuserver systemd-networkd[1724]: ens32: DHCPv4 address 192.168.30.130/24, gateway 192.168.30.2 acquired from 192.168.30.254
Mar 27 06:51:56 ubuntuserver systemd-networkd[1724]: ens32: Lost carrier
Mar 27 06:51:56 ubuntuserver systemd-networkd[1724]: ens32: DHCP lease lost
Mar 27 06:51:56 ubuntuserver systemd-networkd[1724]: ens32: Gained carrier
Mar 27 06:52:02 ubuntuserver systemd-networkd[1724]: ens32: DHCPv4 address 192.168.30.130/24, gateway 192.168.30.2 acquired from 192.168.30.254
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host loopback
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: ens3: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:80:94:97 brd ff:ff:ff:ff:ff:ff
        altname enp2s0
        altname enp2
        inet 192.168.30.130/24 brd 192.168.30.255 metric 100
            brd 192.168.30.255
            valid_lft 999sec preferred_lft 999sec
            inet6 fe80::20c:29ff:fe80:9497/64 scope link
                valid_lft forever preferred_lft forever
4: ens38: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 00:0c:29:80:94:97 brd ff:ff:ff:ff:ff:ff
        altname enp2s0
        altname enp2
        inet 192.168.30.130/24 brd 192.168.30.255 metric 100
            brd 192.168.30.255
            valid_lft forever preferred_lft forever
            inet6 fe80::20c:29ff:fe80:9497/64 scope link
                valid_lft forever preferred_lft forever
tien@ubuntuserver:~$ sudo nano /etc/network/interfaces

```

To direct input to this VM, click inside or press Ctrl+G.

- Máy Victim

- Dùng lệnh **sudo nano /etc/network/interfaces**



Metasploitable2-Linux - VMware Workstation

File Edit View VM Tabs Help | |

Metasploitable2-Linux

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 dhcp
    address 192.168.2.200
    netmask 255.255.255.0
    gateway 192.168.2.1
```

[Wrote 14 lines]

Get Help WriteOut Read File Prev Page Cut Text Cur Pos Exit Justify Where is Next Page UnCut Text To Spell

To direct input to this VM, click inside or press Ctrl+G.

Install Tools Remind Me Later Never Remind Me

Click in the virtual screen | VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

34°C Nắng nhiều nơi

Tim kiếm

257 CH 27/03/2025

Metasploitable2-Linux - VMware Workstation

File Edit View VM Tabs Help | |

Home kali-linux-2024.3-vmware-smd64 Ubuntu_Server Ubuntu_Router Metasploitable2-Linux

nsfadmin@metasploitable:~\$ ip add
1: lo <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
 link/loopback brd 00:00:00:00:00:00 state UNKNOWN
 inet 127.0.0.1/8 brd 127.0.0.1 scope host
 valid_lft forever preferred_lft forever
2: eth0 <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
 link/ether 00:29:10:0e:51 brd ff:ff:ff:ff:ff:ff
 inet 192.168.2.206/24 brd 192.168.2.255 scope global eth0
 valid_lft forever preferred_lft forever
 inet6 fe80::20c:29ff:fe84:c51/64 scope link
 valid_lft forever preferred_lft forever
nsfadmin@metasploitable:~\$

To direct input to this VM, click inside or press Ctrl+G.

28°C Có rác

Tim kiếm

VIE TL 944 CH 02/04/2025

2.1c. Cấu hình NAT outbound cho máy router

2.1d. Cài đặt và cấu hình Snort

- Cài đặt Snort từ công cụ APT. Sau khi cài đặt thành công, kiểm tra phiên bản Snort.

Ubuntu Server 1 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer

- Ubuntu 24.04.2
- Ubuntu 24.04.2 clone
- kali-linux-2024-vmware-amd64
- Windows 10
- Ubuntu Server
- Ubuntu Server 1
- Metasploitable2-Linux
- Kali

vccenter.insecelab.local

```
Setting up libnet-sleazy-perl-amd64 (1.94-1build4) ...
Setting up libnet-HTTP-Perl (6.06-1) ...
Setting up libnet-HTTP-SSL (0.2.5-1) ...
Setting up libndm2hf4 (0.8.7-5.1build3) ...
Setting up libnode-HTTP-perl (6.23-1) ...
Setting up libnmap-ncat (5.2.1+2am064 (2.0.6-8+git20231229.c525ccb+dfsg-1) ...
Setting up libnmap-ncat (5.2.1+2am064 (2.0.6-8+git20231229.c525ccb+dfsg-1) ...
Setting up libnmap-parser-perl-amd64 (3.81-1build3) ...
Setting up snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Setting up libio-socket-ssl-perl (2.065-1) ...
Setting up libio-socket-ip-perl (0.26-1) ...
Setting up liblhttp-former-perl (6.11-1) ...
Setting up liblhttp-negotiate-perl (6.01-2) ...
Setting up snort (2.9.20-0+deb11u1ubuntu1) ...
Snort configuration interface default not set, using 'ens3'
Setting up liblhttp-cookies-perl (6.11-1) ...
Setting up liblhttp-tree-perl (5.07-3) ...
Setting up liblhttp-format-perl (2.16-2) ...
Setting up libnet-smtp-simple-perl (1.04-2) ...
Setting up liblhttp-perl (6.16-1) ...
Setting up liblhttp-daemon-perl (6.16-1) ...
Setting up liblhttp-perl (6.75-1) ...
Setting up oinkmaster (2.0-4.2) ...
Setting up liblhttp-HTTP-Client-perl (6.13-1) ...
Processing triggers for libc-bin (2.39-1ubuntu0.4) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
phuchnhi@0225210411:~$ snort --version

--> Snort! <-
o...: Version 2.9.29 GRe (Build 82)
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2014 Sourcefire, Inc., et al.
Using libpcap version 1.18.4 (with TPACKET_V3)
Using PCRE version 8.37 2016-06-14
Using ZLIB version: 1.3

phuchnhi@0225210411:~$ _
```

To direct input to this VM, click inside or press Ctrl+G.

1 90°F Nắng rải rác

Search

1 ENG 3/27/2025

- Kiểm tra afpacket DAQ đã phải được cài đặt để sử dụng được mode inline.

```
phucnhil0225210411:$ sudo snort --daq-list
Available DNFQ modules:
pcap(v7): live inline multi unpriv
ntq(v7): live inline multi
ipfw(v3): live inline multi unpriv
dump(v3): readback live inline multi unpriv
af_packet(v5): live inline multi unpriv
phucnhil0225210411:$ -
```

- Xóa tất cả các file rule mặc định của Snort. Tạo file rule của nhóm định nghĩa.

```
include /etc/snort/rules/nhom7.rules
```



```
server@UbuntuServer:/etc/snort/rules$ sudo rm -rf *
server@UbuntuServer:/etc/snort/rules$ ls
server@UbuntuServer:/etc/snort/rules$ sudo touch /etc/snort/rules/nhom7.rules
server@UbuntuServer:/etc/snort/rules$
```

- Tạo file cấu hình snort của nhóm tại /etc/snort/nhom7-snort.conf với nội dung như bên dưới để bật mode inline.

```

GNU nano 7.2
config daq: tpacket
config daq_mode: inline
include /etc/snort/rules/nhom7.rules

```

- Kiểm tra file cấu hình snort bằng lệnh sau:

`sudo snort -T -c /etc/snort/nhom7-snort.conf -Q -i ens37:ens38`

- Lưu ý: ens37 và ens38 là cặp interface sử dụng cho mode inline.

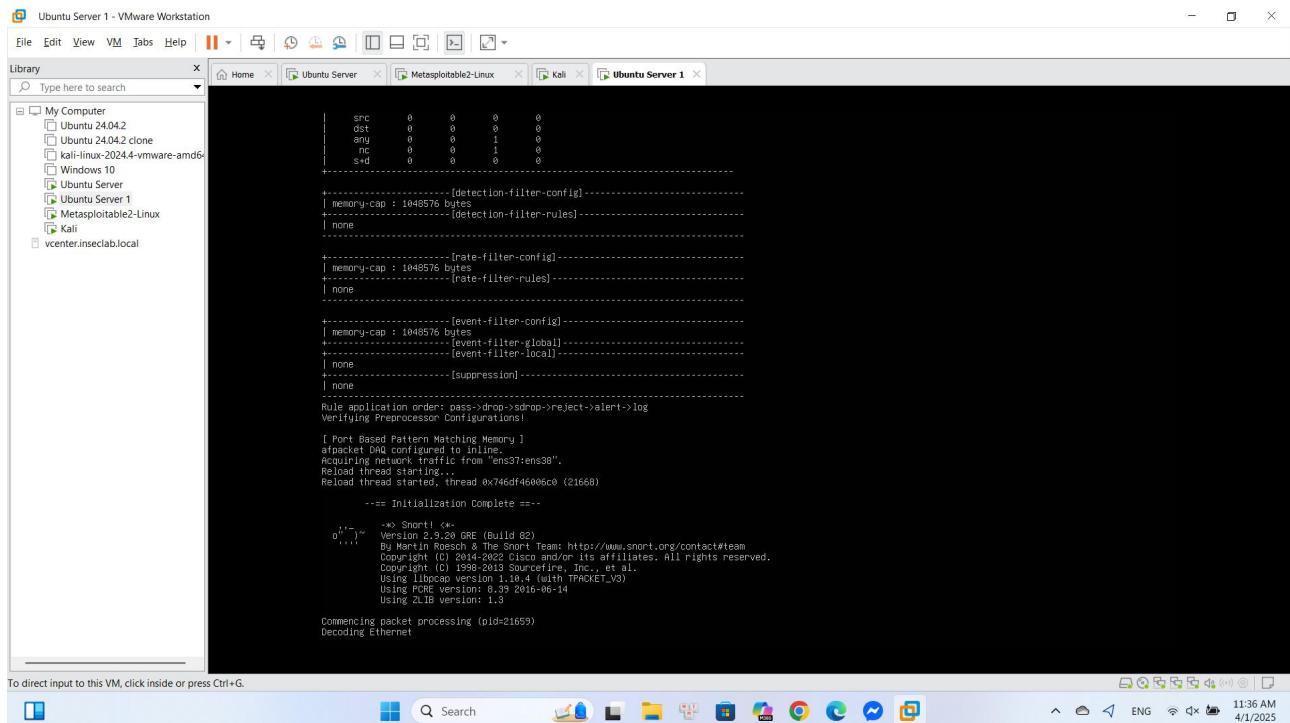
```

dst 0 0 0 0
any 0 0 0 0
src 0 0 0 0
s+d 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]
+-----[event-filter-local]
| none
+-----[suppression]
| none
Rule application order: pass->drop->reject->alert->log
Verifying Preprocessor Configurations!
MaxRSS at the end of rules:29440
af_packet DAQ configured to inline.
Auditting network traffic from "ens37:ens38".
Decoding Ethernet
--- Initialization Complete ---
-> Snort! <-
Version 2.9.20 GRe (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 1998-2010 Sourcefire, Inc., et al.
Copyright (C) 1998-2010 Cisco and/or its affiliates. All rights reserved.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
Total snort Fixed Memory Cost = MaxRSS:29568
Snort successfully validated the configuration!
Snort exiting
server@ubuntu-server:/etc/snort#

```

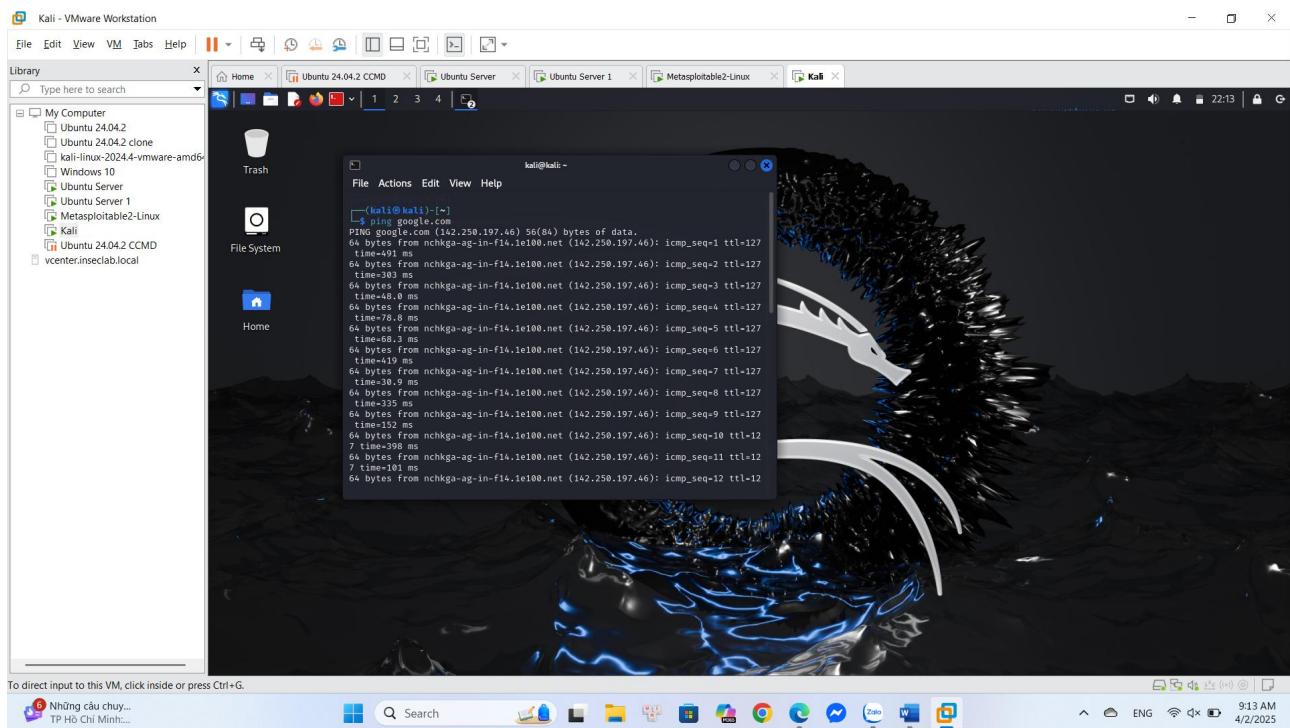
- Chạy snort trong mode inline với dòng lệnh sau:

`sudo snort -c /etc/snort/nhom7-snort.conf -Q -i ens37:ens38`

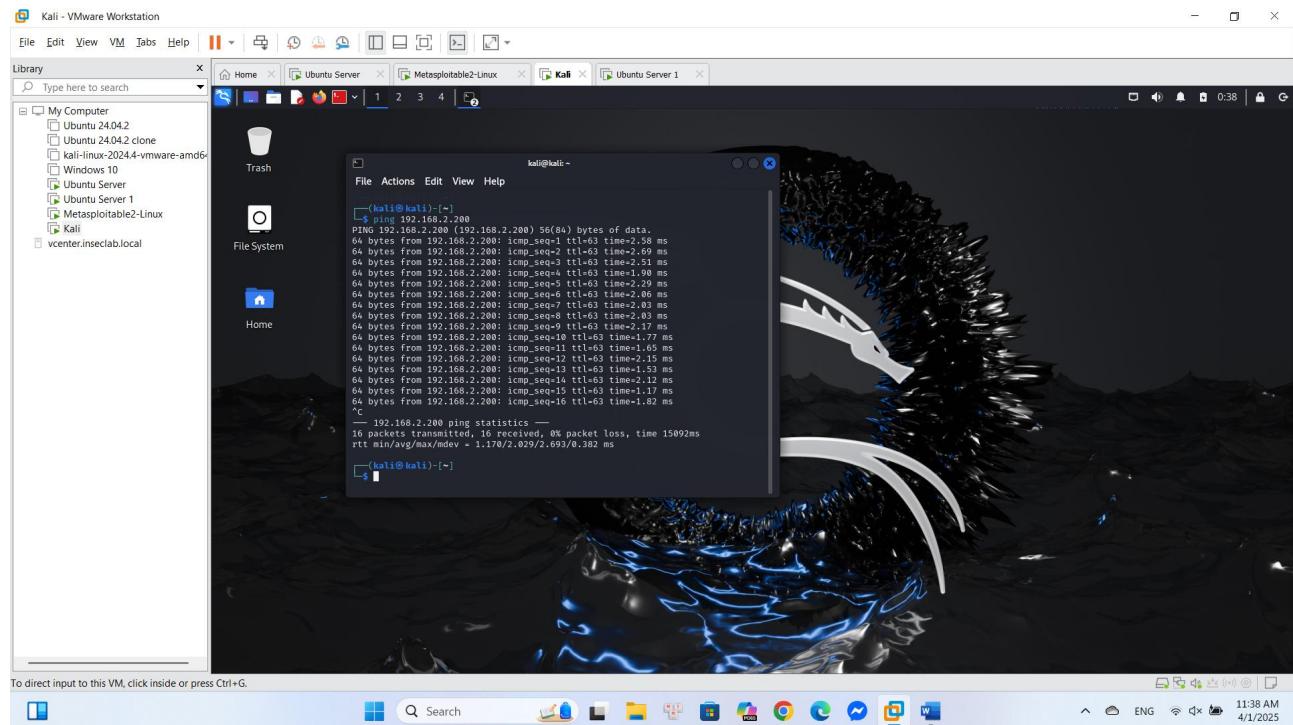


- Sau khi chạy thành công, kiểm tra kết nối của các máy.

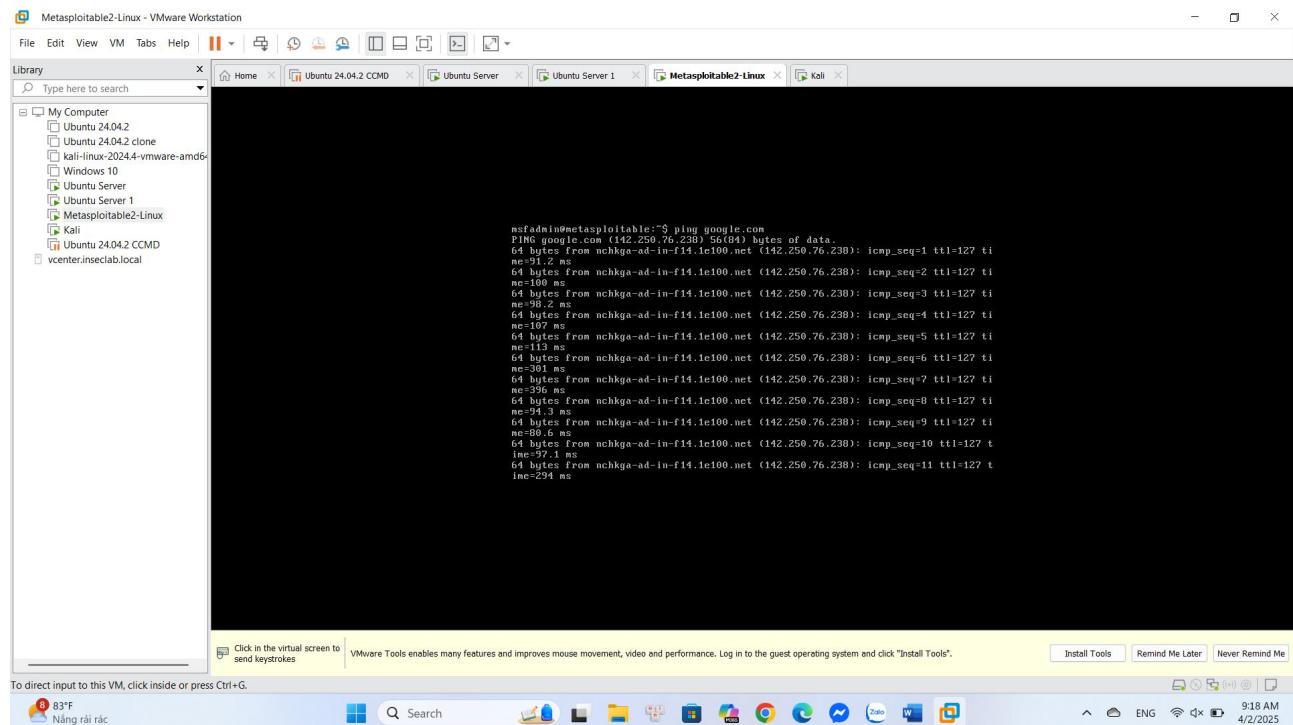
- Máy Kali ping google.com



- Máy Kali ping máy Victim

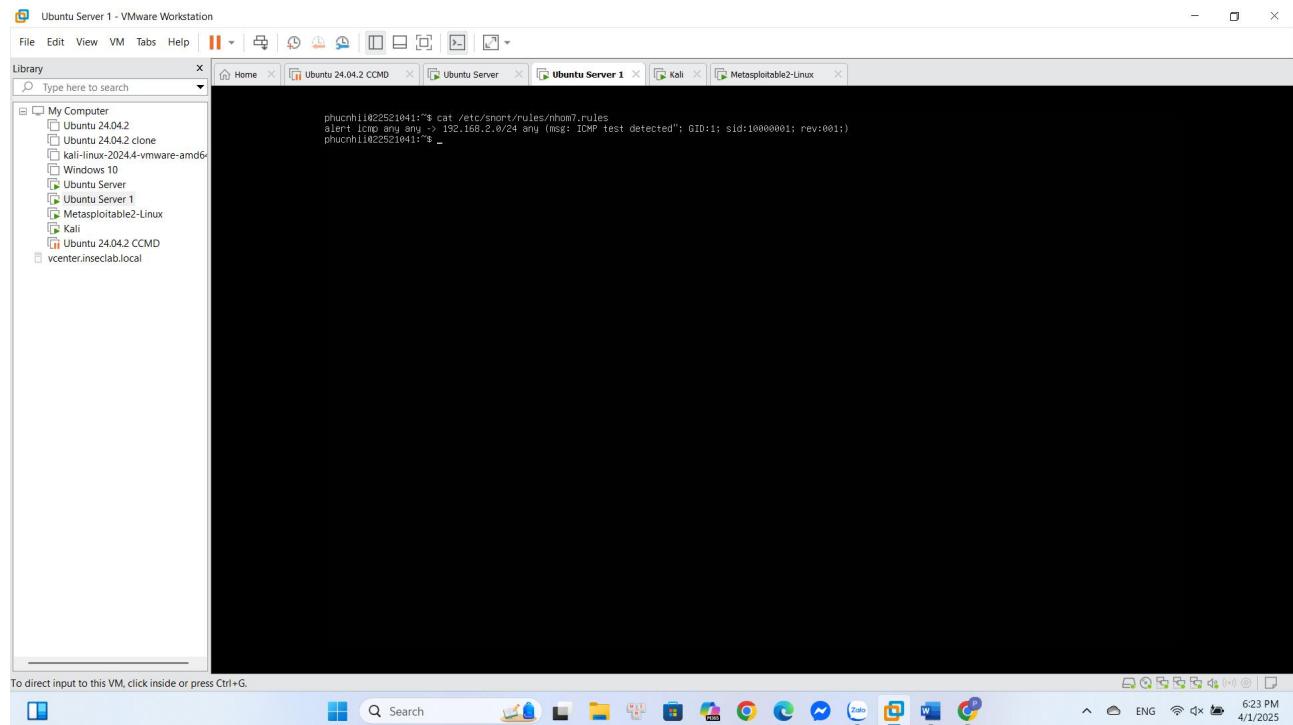


- Máy Victim ping google.com



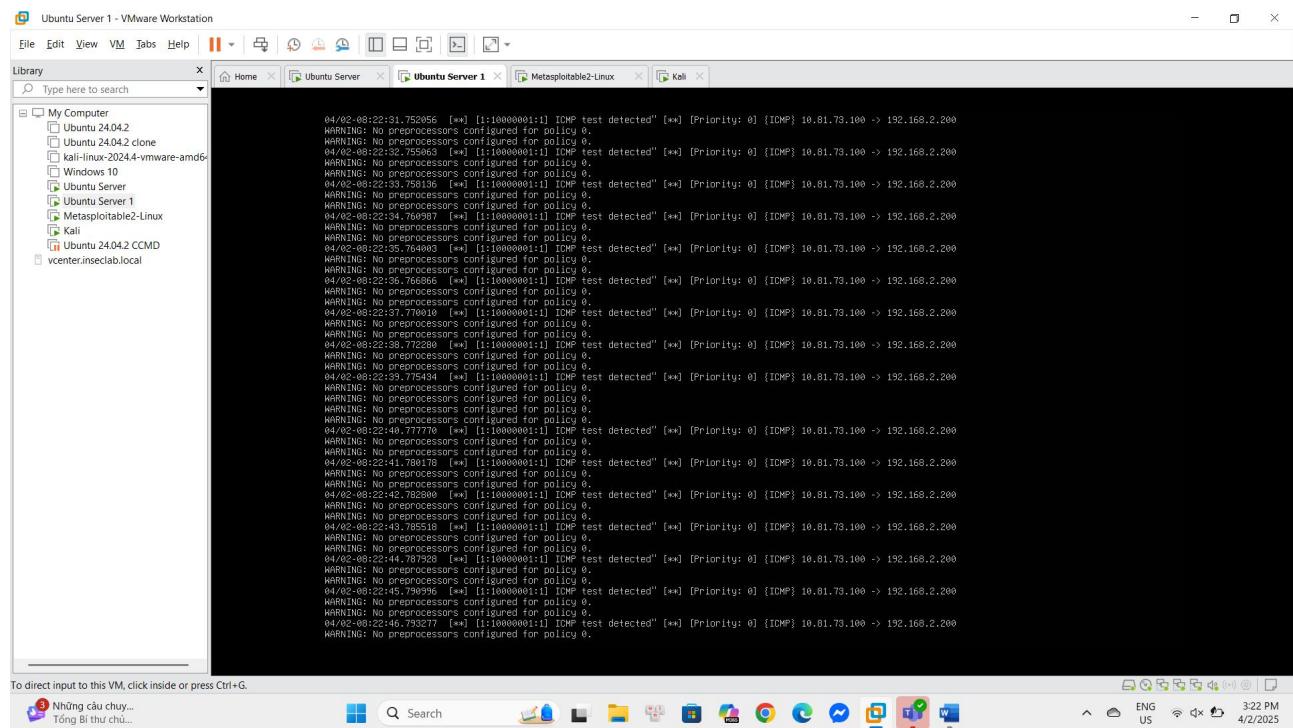
2.1e. Viết rule cho Snort

- Viết rule phát hiện gói ICMP gửi đến lớp mạng 192.168.2.0/24 trong file /etc/snort/rules/nhom7.rules như sau:



- Kiểm tra log của snort trên console và /var/log/snort/alert

- Trên console



- Trên /var/log/snort/alert

```

[*] [I:10000001:1] ICMP test detected" (**)
[Priority: 0]
04/01-11:25:49.114355 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:59147 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:028259 Seq:76 ECHO

[*] [I:10000001:1] ICMP test detected" (**)
[Priority: 0]
04/01-11:25:48.114355 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:59148 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:028259 Seq:77 ECHO

[*] [I:10000001:1] ICMP test detected" (**)
[Priority: 0]
04/01-11:25:49.116477 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:59149 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:028259 Seq:78 ECHO

[*] [I:10000001:1] ICMP test detected" (**)
[Priority: 0]
04/01-11:25:50.118674 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:59164 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:028259 Seq:79 ECHO

[*] [I:10000001:1] ICMP test detected" (**)
[Priority: 0]
04/01-11:25:52.122595 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:59165 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:028259 Seq:80 ECHO

[*] [I:10000001:1] ICMP test detected" (**)
[Priority: 0]
04/01-11:25:52.122597 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:59166 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:028259 Seq:81 ECHO

[*] [I:10000001:1] ICMP test detected" (**)
[Priority: 0]
04/01-11:25:54.127052 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:59432 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:028259 Seq:82 ECHO

phuchnh1022521041:"$ _
```

3. 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

- Trước khi viết áp dụng rule #1.
- Từ 2.1e. ta có rule phát hiện gói ICMP

```

phuchnh1022521041:"$ cat /etc/snort/rules/nhom7.rules
alert icmp any any -> 192.168.2.0/25 any (msg: "ICMP test detected"; GID:1; sid:10000001; rev:001;)

phuchnh1022521041:"$ _
```

- Khởi động Snort

```

Ubuntu Server 1 - VMware Workstation
File Edit View VM Tabs Help | 
Library Type here to search
My Computer
Ubuntu 24.04.2
Ubuntu 24.04.2 clone
kali-linux-2024.4-vmware-amd64
Windows 10
Ubuntu Server
Ubuntu Server 1
Metasploitable2-Linux
Kali
Ubuntu 24.04.2 CCMD
vcenter.insecclab.local

Snort! ->
Version 2.9.20.0GE (Build 62)
Copyright (C) 2014-2022 The Snort Team; http://www.snort.org/contact#team
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with THICKET_V3)
Using Python version 3.9.16 2016-06-14
Using DB version: 1.1

Commencing packet processing (pid=24407)
Decoding Ethernet
-

```

- Ping từ Attacker tới Victim

```

File Edit View VM Tabs Help | 
Library Type here to search
My Computer
Ubuntu 24.04.2
Ubuntu 24.04.2 clone
kali-linux-2024.4-vmware-amd64
Windows 10
Ubuntu Server
Ubuntu Server 1
Metasploitable2-Linux
Kali
Ubuntu 24.04.2 CCMD
vcenter.insecclab.local

(kali㉿kali)-[~]
ping 192.168.2.200
PING 192.168.2.200(192.168.2.200) 56(84) bytes of data.
64 bytes from 192.168.2.200: icmp_seq=1 ttl=63 time=3.06 ms
64 bytes from 192.168.2.200: icmp_seq=2 ttl=63 time=2.66 ms
64 bytes from 192.168.2.200: icmp_seq=3 ttl=63 time=3.29 ms
64 bytes from 192.168.2.200: icmp_seq=4 ttl=63 time=1.11 ms
64 bytes from 192.168.2.200: icmp_seq=5 ttl=63 time=2.62 ms
64 bytes from 192.168.2.200: icmp_seq=6 ttl=63 time=2.40 ms
64 bytes from 192.168.2.200: icmp_seq=7 ttl=63 time=2.67 ms
64 bytes from 192.168.2.200: icmp_seq=8 ttl=63 time=1.67 ms
64 bytes from 192.168.2.200: icmp_seq=9 ttl=63 time=2.40 ms
64 bytes from 192.168.2.200: icmp_seq=10 ttl=63 time=2.03 ms
64 bytes from 192.168.2.200: icmp_seq=11 ttl=63 time=2.16 ms
64 bytes from 192.168.2.200: icmp_seq=12 ttl=63 time=2.21 ms
64 bytes from 192.168.2.200: icmp_seq=13 ttl=63 time=2.09 ms
64 bytes from 192.168.2.200: icmp_seq=14 ttl=63 time=1.94 ms
64 bytes from 192.168.2.200: icmp_seq=15 ttl=63 time=1.83 ms
64 bytes from 192.168.2.200: icmp_seq=16 ttl=63 time=1.38 ms
64 bytes from 192.168.2.200: icmp_seq=17 ttl=63 time=1.89 ms
64 bytes from 192.168.2.200: icmp_seq=18 ttl=63 time=2.36 ms
64 bytes from 192.168.2.200: icmp_seq=19 ttl=63 time=2.10 ms
64 bytes from 192.168.2.200: icmp_seq=20 ttl=63 time=2.02 ms
64 bytes from 192.168.2.200: icmp_seq=21 ttl=63 time=2.05 ms
64 bytes from 192.168.2.200: icmp_seq=22 ttl=63 time=2.14 ms
64 bytes from 192.168.2.200: icmp_seq=23 ttl=63 time=2.37 ms

```

- Kiểm tra alert log của Snort ta phát hiện ping từ Attacker

```

Ubuntu Server 1 - VMware Workstation
File Edit View VM Tabs Help | 
Library Type here to search
My Computer
Ubuntu 24.04.2
Ubuntu 24.04.2 clone
kali-linux-2024.4-vmware-amd64
Windows 10
Ubuntu Server
Ubuntu Server 1
Metasploitable2-Linux
Kali
Ubuntu 24.04.2 CCMD
vcenter.inseclab.local

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:21.718423 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:51649 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:103 ECHO

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:22.719336 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:51684 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:104 ECHO

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:23.722381 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:52003 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:105 ECHO

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:24.722759 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:52228 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:106 ECHO

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:25.725840 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:52424 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:107 ECHO

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:26.727413 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:52544 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:108 ECHO

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:27.729074 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:52778 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:109 ECHO

[*] [I:1:00000001:1] ICMP test detected" [*]
[Priority: 0]
04/01/15:12:28.730255 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:52893 ILen:20 DgmLen:84 DF
Type:8 Code:0 ID:1783 Seq:110 ECHO

phuchanh1022521041:"_

```

To direct input to this VM, click inside or press Ctrl+G.

Những câu chuyện Việt Nam và Bi... 10:12 PM 4/1/2025

• Dùng tcpdump trên máy Victim để kiểm tra: sudo tcpdump -i any icmp

```

Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help | 
Library Type here to search
My Computer
Ubuntu 24.04.2
Ubuntu 24.04.2 clone
kali-linux-2024.4-vmware-amd64
Windows 10
Ubuntu Server
Ubuntu Server 1
Metasploitable2-Linux
Kali
Ubuntu 24.04.2 CCMD
vcenter.inseclab.local

09:48:22.640037 IP 10.81.73.100 > 192.168.2.200: ICMP echo request, id 1783, seq 376, length 64
09:48:22.640075 IP 192.168.2.200 > 10.81.73.100: ICMP echo reply, id 1783, seq 3
09:48:23.641533 IP 10.81.73.100 > 192.168.2.200: ICMP echo request, id 1783, seq 377, length 64
09:48:23.641569 IP 192.168.2.200 > 10.81.73.100: ICMP echo reply, id 1783, seq 3
09:48:24.644141 IP 10.81.73.100 > 192.168.2.200: ICMP echo request, id 1783, seq 378, length 64
09:48:24.644149 IP 192.168.2.200 > 10.81.73.100: ICMP echo reply, id 1783, seq 3
09:48:25.645736 IP 10.81.73.100 > 192.168.2.200: ICMP echo request, id 1783, seq 379, length 64
09:48:25.645765 IP 192.168.2.200 > 10.81.73.100: ICMP echo reply, id 1783, seq 3
09:48:26.647644 IP 10.81.73.100 > 192.168.2.200: ICMP echo request, id 1783, seq 380, length 64
09:48:26.647750 IP 192.168.2.200 > 10.81.73.100: ICMP echo reply, id 1783, seq 3
09:48:27.649124 IP 10.81.73.100 > 192.168.2.200: ICMP echo request, id 1783, seq 381, length 64
09:48:27.649165 IP 192.168.2.200 > 10.81.73.100: ICMP echo reply, id 1783, seq 3
09:48:27.649165 IP 192.168.2.200 > 10.81.73.100: ICMP echo reply, id 1783, seq 3

```

To direct input to this VM, click inside or press Ctrl+G.

79°F Nhiều máy 10:17 PM 4/1/2025

- Viết rule#1 drop các gói ICMP đi đến máy Victim.

```
phucnh11@22521041:~$ cat /etc/snort/rules/nhom7_1.rules
drop icmp any any -> 192.168.2.200 any (msg:'Dropping all ICMP traffic to 192.168.2.200'; sid:10000001; rev:1)
```

To direct input to this VM, click inside or press Ctrl+G.

Nhiều máy

ENG Wi-Fi 10:25 PM
4/1/2025

- Chính sửa file /etc/snort/nhom7-snort.conf để áp dụng rule #1

```
phucnh11@22521041:~$ cat /etc/snort/nhom7-snort.conf
config dsrc: afaocket
config dacl_mode: inline
include /etc/snort/rules/nhom7_1.rules
phucnh11@22521041:~$
```

To direct input to this VM, click inside or press Ctrl+G.

Nhiều máy

ENG Wi-Fi 10:28 PM
4/1/2025

- Sau khi áp dụng rule #1.

- Khởi động Snort

```

Ubuntu Server 1 - VMware Workstation
File Edit View VM Tabs Help | ||| Home | Ubuntu Server | Ubuntu Server 1 | Metasploitable2-Linux | Kali |
Library Type here to search
My Computer
Ubuntu 24.04.2
Ubuntu 24.04.2 clone
kali-linux-2024.4-vmware-amd64
Windows 10
Ubuntu Server
Ubuntu Server 1
Metasploitable2-Linux
Kali
Ubuntu 24.04.2 CCMD
vcenter.insecclab.local

src 0 0 0 0
dst 0 0 1 0
any 0 0 1 0
nc 0 0 1 0
svd 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]-----
-----[event-filter-local]-----
| none
-----[suppression]-----
| none

Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[ Port Based Pattern Matching Memory ]
aPacket DNG configured to inline.
Acquiring network traffic from "ens3tens30".
Reload thread starting...
Reload thread started, thread 0x72d57c0006c0 (24488)
--- Initialization Complete ---

->> Snort! <->
0'')~ Version 2.9.20 GR (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 2014-2022 Sourcefire, Inc., Et Al.
Using libpcap version 1.16.4 (libpcap-1.16.4)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

Commencing packet processing (pid=24479)
Decoding Ethernet

```

To direct input to this VM, click inside or press Ctrl+G.

- Ping từ Attacker tới Victim ta thấy không thành công

```

Ubuntu Server 1 - VMware Workstation
File Edit View VM Tabs Help | ||| Home | Ubuntu Server | Ubuntu Server 1 | Metasploitable2-Linux | Kali |
Library Type here to search
My Computer
Ubuntu 24.04.2
Ubuntu 24.04.2 clone
kali-linux-2024.4-vmware-amd64
Windows 10
Ubuntu Server
Ubuntu Server 1
Metasploitable2-Linux
Kali
Ubuntu 24.04.2 CCMD
vcenter.insecclab.local

kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-~]$ ping 192.168.2.200
PING 192.168.2.200 (192.168.2.200) 56(84) bytes of data.

```

To direct input to this VM, click inside or press Ctrl+G.

- Dùng tcpdump trên máy Victim để kiểm tra và không thấy có gói tin nào được gửi tới

```
msfadmin@metasploitable:~$ sudo tcpdump -i any icmp
tcpdump: WARNING: Promiscuous mode not supported on the "any" device
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
0 packets captured
0 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$ _
```

- Kiểm tra alert log của Snort ta phát hiện đã chặn ping (icmp) từ Attacker

```
[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:09.306265 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:1488 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:108 ECHO

[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:09.213372 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:1488 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:109 ECHO

[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:09.206488 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:1761 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:110 ECHO

[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:09.206488 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:1761 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:111 ECHO

[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:09.208203 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:2065 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:112 ECHO

[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:09.309412 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:2195 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:113 ECHO

[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:10.332855 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:2250 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:114 ECHO

[**] [1:10000001:1] Dropping all ICMP traffic to 192.168.2.200 [**]
[Priority: 0]
04/01/15:31:10.357013 10.81.73.100 -> 192.168.2.200
ICMP TTL:63 TOS:0x0 ID:12400 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:10892 Seq:115 ECHO
```