

BÁO CÁO THỰC HÀNH

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

Lab 2: Triển khai Snort inline

Lớp: NT204.P22.ANTT.2

THÀNH VIÊN THỰC HIỆN (Nhóm 10):

STT	Họ và tên	MSSV
1	Nguyễn Xuân Huy	22520568
2	Nguyễn Khang Hưng	22520515

Điểm tự đánh giá

10

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

B.1 Tìm hiểu và sử dụng Snort

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 1 hệ thống phòng chống xâm nhập (IPS) với mã nguồn mở, sử dụng 1 loạt các quy tắc để xác định được các hoạt động độc hại diễn ra trên hệ thống mạng, sử dụng các quy tắc để tìm gói tin khớp với chúng, sau đó tạo cảnh báo cho người dùng. Snort cung cấp khả năng phát hiện tấn công, ghi log gói tin, từ đó giúp người dùng có thể phát hiện sớm và tìm cách ngăn chặn các hoạt động gây nguy hiểm đến hệ thống.

Snort cho phép chạy trên những mode:

- + Sniffer mode: đây là chế độ cơ bản nhất của mọi hệ thống NIDS. Khi ở trong chế độ này, Snort sẽ phát hiện và hiển thị header của các gói tin: TCP, ICMP, UDP, IP, ... ra màn hình.
- + Packet logger mode (chế độ ghi log gói tin): đây là chế độ làm việc mà Snort sẽ thực hiện ghi log lại các gói tin đã phát hiện được rồi sau đó lưu trữ lại trong kho lưu trữ log của Snort hoặc một ví trí lưu trữ khác mà người dùng cấu hình chỉ định. Việc ghi log lại sẽ giúp cho chúng ta thực hiện theo dõi và truy vết sau này.
- + NIDS mode (Network Intrusion Detection System Mode): ở chế độ này, Snort không ghi lại từng gói tin đã bắt được như Sniffer mode. Thay vào đó Snort áp dụng các quy tắc trên tất cả các gói được bắt. Nếu một gói không khớp với bất kỳ quy tắc nào, gói tin đó sẽ bị loại bỏ (drop) và sẽ không thực hiện ghi lại log của gói này.

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

- IDS/IPS: Phát hiện & ngăn chặn xâm nhập mạng
- Sniffing & Logging: Ghi log, phân tích gói tin
- Phân tích real-time: Giám sát & phát hiện tấn công
- Quy tắc linh hoạt: Tùy chỉnh quy tắc phát hiện
- Tích hợp SIEM: Hỗ trợ Splunk, ELK, BASE, Snorby
- Dễ triển khai: Hỗ trợ nhiều hệ điều hành & giao diện

B.2 Cài đặt và cấu hình Snort để giám sát 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.

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


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


Name	Host only	Shared with guests	Connected	DHCP	IP Address
VMnet8	NAT	NAT	Connected	Enabled	192.168.85.0


- Gán các card mạng cho máy Router.


Floppy	Using file autoinst.tlp
Network Adapter	NAT
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet3)
USB Controller	Present

- Gán card mạng cho máy Kali


 **kali-linux-2024.3-vmware-amd64**

 Power on this virtual machine


 Edit virtual machine settings

 Upgrade this virtual machine


▼ **Devices**

 Memory


2 GB

 Processors


4

 Hard Disk (SCSI)


80.1 GB

 Network Adapter 2


Custom (VMnet2)

 USB Controller

Present

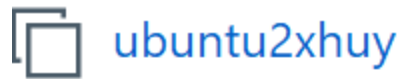
 Sound Card

Auto detect

 Display

Auto detect

- Gán card mạng cho máy Snort



 Power on this virtual machine

 Edit virtual machine settings


▼ Devices

 Memory	4 GB
 Processors	2
 Hard Disk (SCSI)	20 GB
 CD/DVD 2 (SATA)	Using file C:\Use...
 CD/DVD (SATA)	Using file autoin...
 Floppy	Using file autoin...
 Network Adapter	NAT
 Network Adapter 2	Custom (VMnet3)
 Network Adapter 3	Custom (VMnet4)
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

▼ Description

- Gán card mạng cho máy Victim






Metasploitable2-Linux

 Power on this virtual machine

 Edit virtual machine settings

 Upgrade this virtual machine

▼ Devices

 Memory	512 MB
 Processors	1
 Hard Disk (SCSI)	8 GB
 CD/DVD (IDE)	Auto detect
 Network Adapter	Custom (VMnet4)
 USB Controller	Present
 Display	Auto detect

2.1b. Cấu hình địa chỉ ip cho các máy

- cấu hình subnet cho các vmnet

VMnet2	Host-only	-	Connected	-	10.81.85.0
VMnet3	Host-only	-	Connected	-	192.168.8.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.85.0
VMnet4	Host-only	-	Connected	-	192.168.100.0

- Cấu hình địa chỉ ip cho máy kali (attacker)

```

(kali@kali)-[~]
$ 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 02:42:20:1f:96:c4 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 10.81.85.100 netmask 255.255.255.0 broadcast 10.81.85.255
    ether 00:0c:29:3f:1f:45 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 63 bytes 11545 (11.2 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 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

- Cấu hình địa chỉ ip cho máy router

```

2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:aa:6f:86 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.85.128/24 brd 192.168.85.255 scope global dynamic noprefixroute
    ens33
        valid_lft 1683sec preferred_lft 1683sec
    inet6 fe80::c808:7aea:6d4d:91f3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:aa:6f:90 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.81.85.1/24 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feaa:6f90/64 scope link
        valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:aa:6f:9a brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet 192.168.85.1/24 scope global ens38
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feaa:6f9a/64 scope link
        valid_lft forever preferred_lft forever
xhuy@xhuy-virtual-machine:~$

```

- Cấu hình ip cho máy snort

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f5:e7:15 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.85.129/24 brd 192.168.85.255 scope global dynamic noprefixroute
    ens33
        valid_lft 1743sec preferred_lft 1743sec
        inet6 fe80::b8b8:40f1:369d:ded1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f5:e7:1f brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet6 fe80::bde2:a97e:a457:c81f/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f5:e7:29 brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet6 fe80::304b:e04b:7d7d:d000/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
xhuy2@xhuy2-virtual-machine:~$
```

- Cấu hình ip cho máy victim

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:fa:dd:2a brd ff:ff:ff:ff:ff:ff
    inet 192.168.85.200/24 scope global eth0
msfadmin@metasploitable:~$
```

2.1c. Cấu hình NAT outbound cho máy router

```

xhuy@xhuy-virtual-machine:~$ sudo iptables --table nat --flush
xhuy@xhuy-virtual-machine:~$ sudo iptables --delete-chain
xhuy@xhuy-virtual-machine:~$ sudo iptables --table nat --delete-chain
xhuy@xhuy-virtual-machine:~$ sudo iptables --table nat --append POSTROUTING --out-interface ens33 -j MASQUERADE
xhuy@xhuy-virtual-machine:~$ sudo iptables --append FORWARD --in-interface ens37/ens38 -j ACCEPT
Warning: weird character in interface `ens37/ens38' ('/' and ' ' are not allowed by the kernel).
xhuy@xhuy-virtual-machine:~$ sudo iptables --append FORWARD --in-interface ens37 -j ACCEPT
xhuy@xhuy-virtual-machine:~$ sudo iptables --append FORWARD --in-interface ens38 -j ACCEPT
xhuy@xhuy-virtual-machine:~$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
bash: /proc/sys/net/ipv4/ip_forward: Permission denied
xhuy@xhuy-virtual-machine:~$ cat /proc/sys/net/ipv4/ip_forward
0
xhuy@xhuy-virtual-machine:~$ sudo nano /proc/sys/net/ipv4/ip_forward
xhuy@xhuy-virtual-machine:~$ cat /proc/sys/net/ipv4/ip_forward
1
xhuy@xhuy-virtual-machine:~$ service iptables restart

```

- Máy kali có thể ping được ra ngoài sau cấu hình NAT.

```

(kali@kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=32.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=32.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=32.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=29.7 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4006ms
rtt min/avg/max/mdev = 29.683/31.788/32.846/1.247 ms

(kali@kali)-[~]
$ ping google.com
PING google.com (172.253.118.101) 56(84) bytes of data.
64 bytes from sl-in-f101.1e100.net (172.253.118.101): icmp_seq=1 ttl=127 time=40.7 ms
64 bytes from sl-in-f101.1e100.net (172.253.118.101): icmp_seq=2 ttl=127 time=47.7 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 40.678/44.195/47.712/3.517 ms

```

2.1d. Cài đặt và cấu hình Snort

- Cài đặt snort từ công cụ APT


```
xhuy2@xhuy2-virtual-machine:~$ sudo apt-get install snort
[sudo] password for xhuy2:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1
  net-tools oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1
```

- Kiểm tra phiên bản snort

```
xhuy2@xhuy2-virtual-machine:~$ snort --version

o''~
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 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
```

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

```
xhuy2@xhuy2-virtual-machine:~$ sudo snort --daq-list
Available DAQ modules:
pcap(v3): readback live multi unpriv
nfq(v7): live inline multi
ipfw(v3): live inline multi unpriv
dump(v3): readback live inline multi unpriv
afpacket(v5): live inline multi unpriv
```

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

```
xhuy2@xhuy2-virtual-machine:~$ sudo rm -rf /etc/snort/rules/*
```

- Tạo file rule của nhóm định nghĩa

```
xhuy2@xhuy2-virtual-machine:~$ sudo touch /etc/snort/rules/nhom10.rules
xhuy2@xhuy2-virtual-machine:~$
```

- Tạo file cấu hình snort của nhóm tại /etc/snort/nhomX-snort.conf (với X là số thứ tự của nhóm) với nội dung như bên dưới để bật mode inline.

```
xhuy2@xhuy2-virtual-machine:~$ cat /etc/snort/nhom10-snort.conf
config daq: afpacket
config daq-mode: inline

include /etc/snort/rules/nhom10.rules
```

- Kiểm tra file cấu hình snort

```
xhuy2@xhuy2-virtual-machine:~$ sudo snort -T -c /etc/snort/nhom10-snort.conf -Q
-i ens37:ens38
```

```
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 1.10.1 (with TPACKET_V3)
    Using PCRE version: 8.39 2016-06-14
    Using ZLIB version: 1.2.11

Snort successfully validated the configuration!
Snort exiting
xhuy2@xhuy2-virtual-machine:~$
```

- Chạy snort trong mode inline

```

xhuy2@xhuy2-virtual-machine:~$ sudo snort -c /etc/snort/nhom10-snort.conf -Q -i
ens37:ens38
Enabling inline operation
Running in IDS mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/nhom10-snort.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort

+++++
Initializing rule chains...
0 Snort rules read
    0 detection rules
    0 decoder rules
    0 preprocessor rules
0 Option Chains linked into 0 Chain Headers
+++++

+-----[Rule Port Counts]-----+
|               tcp               udp               icmp               ip

```

- kiểm tra kết nối của các máy

+ kali ping google.com

```

(kali㉿kali)-[~]
$ ping google.com
PING google.com (172.253.118.100) 56(84) bytes of data.
64 bytes from sl-in-f100.1e100.net (172.253.118.100): icmp_seq=1 ttl=127 time=62.3 ms
64 bytes from sl-in-f100.1e100.net (172.253.118.100): icmp_seq=2 ttl=127 time=31.7 ms
64 bytes from sl-in-f100.1e100.net (172.253.118.100): icmp_seq=3 ttl=127 time=67.1 ms
^C
— google.com ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 31.716/53.705/67.130/15.674 ms

```

+ kali ping máy victim

```

(kali㉿kali)-[~]
$ ping 192.168.85.200
PING 192.168.85.200 (192.168.85.200) 56(84) bytes of data.
64 bytes from 192.168.85.200: icmp_seq=1 ttl=63 time=7.73 ms
64 bytes from 192.168.85.200: icmp_seq=2 ttl=63 time=4.46 ms
64 bytes from 192.168.85.200: icmp_seq=3 ttl=63 time=3.86 ms
^C
— 192.168.85.200 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.855/5.349/7.731/1.702 ms

```

+ máy victim ping google.com

```
msfadmin@metasploitable:~$ ping google.com
PING google.com (142.250.76.238) 56(84) bytes of data.
64 bytes from nchkg-a-d-in-f14.1e100.net (142.250.76.238): icmp_seq=1 ttl=127 time=44.9 ms
64 bytes from nchkg-a-d-in-f14.1e100.net (142.250.76.238): icmp_seq=2 ttl=127 time=37.2 ms
64 bytes from nchkg-a-d-in-f14.1e100.net (142.250.76.238): icmp_seq=3 ttl=127 time=68.0 ms
```

2.1e. Viết rule cho Snort

- Viết rule phát hiện gói ICMP gửi đến lớp mạng 192.168.x.0/24 trong file
/etc/snort/rules/nhom10.rules

```
xhuy2@xhuy2-virtual-machine:~$ cat /etc/snort/rules/nhom10.rules
alert icmp any any -> 192.168.85.0/24 any (msg: "ICMP test detected"; SID:1; rev:001;)
```

- kiểm tra log của snort trên console.

```
xhuy2@xhuy2-virtual-machine: /etc/snort
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Commencing packet processing (pid=30969)
Decoding Ethernet
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/29-17:26:57.344705  [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] {ICMP} 10.81.85.100 -> 192.168.85.200
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/29-17:26:58.343860  [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] {ICMP} 10.81.85.100 -> 192.168.85.200
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/29-17:26:59.345220  [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] {ICMP} 10.81.85.100 -> 192.168.85.200
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/29-17:27:00.346614  [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] {ICMP} 10.81.85.100 -> 192.168.85.200
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/29-17:27:01.348102  [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] {ICMP} 10.81.85.100 -> 192.168.85.200
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/29-17:27:02.350013  [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] {ICMP} 10.81.85.100 -> 192.168.85.200
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/29-17:27:03.350752  [**] [1:10000001:1] ICMP test detected [**] [Priority: 0] {ICMP} 10.81.85.100 -> 192.168.85.200
```

- kiểm tra log của snort trên var/log/snort/alert.

```
xhuy2@xhuy2-virtual-machine: /etc/snort
ICMP TTL:63 TOS:0x0 ID:26626 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49150 Seq:43 ECHO

[**] [1:10000001:1] ICMP test detected [**]
[Priority: 0]
03/29-17:17:36.345077 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:26864 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49150 Seq:44 ECHO

[**] [1:10000001:1] ICMP test detected [**]
[Priority: 0]
03/29-17:17:37.347796 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:27115 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49150 Seq:45 ECHO

[**] [1:10000001:1] ICMP test detected [**]
[Priority: 0]
03/29-17:17:38.347944 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:27145 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49150 Seq:46 ECHO

[**] [1:10000001:1] ICMP test detected [**]
[Priority: 0]
03/29-17:17:39.350489 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:27273 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49150 Seq:47 ECHO

[**] [1:10000001:1] ICMP test detected [**]
[Priority: 0]
03/29-17:17:40.351249 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:27504 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49150 Seq:48 ECHO

[**] [1:10000001:1] ICMP test detected [**]
[Priority: 0]
03/29-17:17:41.353944 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:27637 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49150 Seq:49 ECHO

xhuy2@xhuy2-virtual-machine: /etc/snort$
```

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

```

0 packets dropped by kernel
msfadmin@metasploitable:~$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
06:35:27.810489 IP 10.81.85.100 > 192.168.85.200: ICMP echo request, id 57222, seq 75, length 64
06:35:27.810523 IP 192.168.85.200 > 10.81.85.100: ICMP echo reply, id 57222, seq 75, length 64

```

- viết rule#1

```

xhuy2@xhuy2-virtual-machine:/var/log/snort$ cat /etc/snort/rules/nhom10.rules
alert icmp any any -> 192.168.85.0/24 any (msg: "ICMP test detected"; GID:1; sid:10000001; rev:001;)
drop icmp any any -> 192.168.85.200 any (msg: "drop ICMP"; GID:2; sid:10000003; rev:002;)

```

- sau khi viết áp dụng rule #1

```

0 packets dropped by kernel
msfadmin@metasploitable:~$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
06:46:41.479839 arp who-has 192.168.85.200 tell 192.168.85.1
06:46:41.479875 arp reply 192.168.85.200 is-at 00:0c:29:fa:dd:2a (oui Unknown)
06:46:41.480173 IP 192.168.85.200.48682 > dns.google.domain: 46244+ PTR? 200.85.168.192.in-addr.arpa. (45)
06:46:41.523178 IP dns.google.domain > 192.168.85.200.48682: 46244 NXDomain 0/0/0 (45)
06:46:41.523291 IP 192.168.85.200.45855 > dns.google.domain: 9305+ PTR? 1.85.168.192.in-addr.arpa. (43)
06:46:41.560907 IP dns.google.domain > 192.168.85.200.45855: 9305 NXDomain 0/0/0 (43)
06:46:41.562962 IP 192.168.85.200.58852 > dns.google.domain: 4756+ PTR? 8.8.8.8.in-addr.arpa. (38)
06:46:41.603670 IP dns.google.domain > 192.168.85.200.58852: 4756 1/0/0 PTR[Idomain]
06:46:46.479096 arp who-has 192.168.85.1 tell 192.168.85.200
06:46:46.479851 arp reply 192.168.85.1 is-at 00:0c:29:aa:6f:9a (oui Unknown)

```

- kiểm tra file alert log của snort

```
xhuy2@xhuy2-virtual-machine: /var/log/snort

ICMP TTL:63 TOS:0x0 ID:799 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:4161 Seq:3 ECHO

[**] [2:10000003:2] drop ICMP [**]
[Priority: 0]
03/29-17:59:11.293901 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:852 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:4161 Seq:4 ECHO

[**] [2:10000003:2] drop ICMP [**]
[Priority: 0]
03/29-17:59:12.318377 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:917 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:4161 Seq:5 ECHO

[**] [2:10000003:2] drop ICMP [**]
[Priority: 0]
03/29-17:59:13.341566 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:1148 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:4161 Seq:6 ECHO

[**] [2:10000003:2] drop ICMP [**]
[Priority: 0]
03/29-17:59:14.366475 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:1373 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:4161 Seq:7 ECHO

[**] [2:10000003:2] drop ICMP [**]
[Priority: 0]
03/29-17:59:15.390773 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:1402 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:4161 Seq:8 ECHO

[**] [2:10000003:2] drop ICMP [**]
[Priority: 0]
03/29-17:59:16.415045 10.81.85.100 -> 192.168.85.200
ICMP TTL:63 TOS:0x0 ID:1415 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:4161 Seq:9 ECHO
```

--HẾT--