



2

Lab

Triển khai Snort Inline

Thực hành

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

Lưu hành nội bộ

A. TỔNG QUAN

A.1 Mục tiêu

- Tìm hiểu và sử dụng phần mềm Snort (<https://www.snort.org>).
- Cài đặt và cấu hình Snort như một Network IPS để phát hiện và ngăn chặn tấn công trong hệ thống mạng.

A.2 Cài đặt môi trường

- Một máy Ubuntu Server làm router (**Router**).
- Một máy Kali Linux thực hiện tấn công (**Attacker**).
- Một máy Ubuntu Server cài đặt Snort (**Snort**).
- Một máy Metasploitable2 làm máy victim (**Victim**).
(<https://sourceforge.net/projects/metasploitable/>).

B. THỰC HÀNH

Sinh viên thực hiện bài thực hành với những yêu cầu bên dưới.

B.1 Tìm hiểu và sử dụng Snort

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

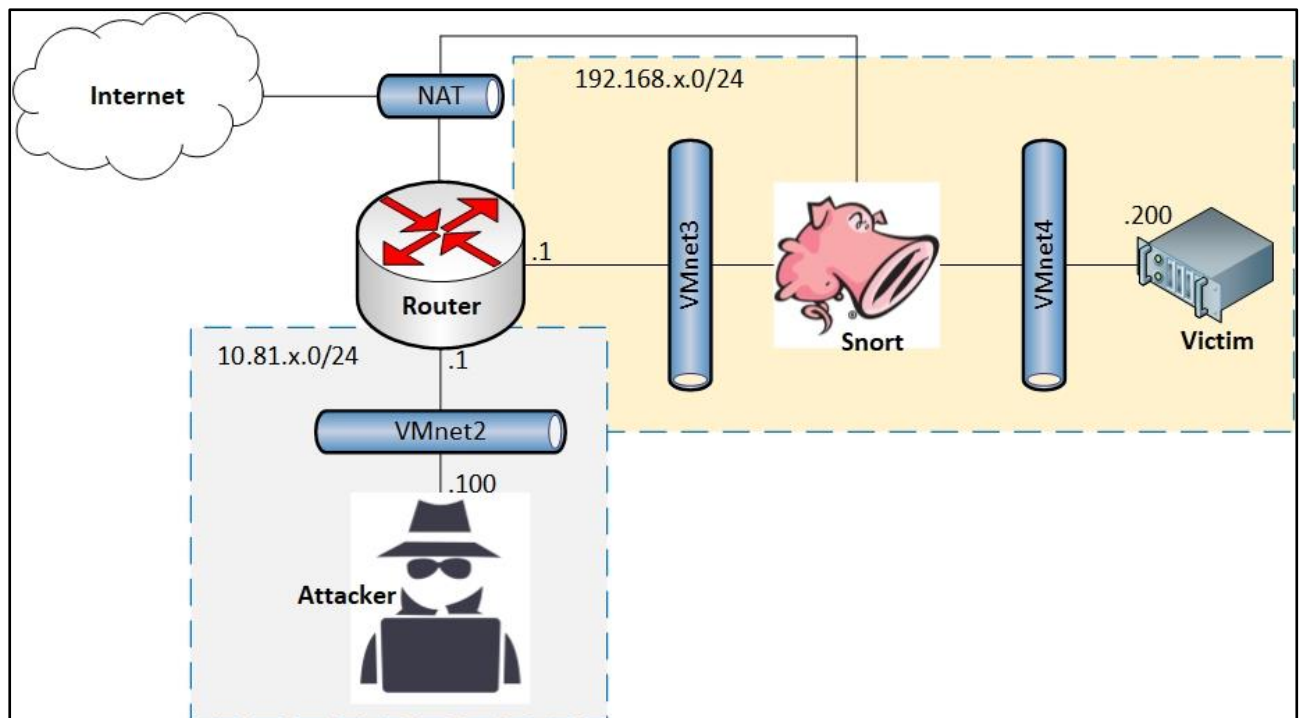
1.1a. Tìm hiểu về Snort? Snort cho phép chạy trên những chế độ (mode) nào?

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

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

Trong bài thực hành này, chúng ta sẽ thực hiện cài đặt và cấu hình Snort chạy như một hệ thống ngăn ngừa xâm nhập (Network Intrusion Prevention System), hay còn gọi là inline mode. Snort Inline tạo một cầu nối (bridge) giữa 2 network segment và có khả năng chuyển luồng dữ liệu giữa 2 segment. Snort kiểm tra lưu lượng đi qua nó và loại bỏ những lưu lượng nghi ngờ.

Mô hình mạng triển khai Snort:



Hình 1. Mô hình triển khai Snort Inline

Trong mô hình này có 4 máy: **Router**, **Attacker**, **Snort** và **Victim**. **Router** là một máy Linux sử dụng để các lớp mạng đi ra Internet. Máy **Attacker** là máy Kali Linux chứa các công cụ để tấn công máy Victim. Máy **Victim** là Metasploitable2 chứa các dịch vụ có chứa lỗ hổng để khai thác. Máy **Snort** là một máy cài đặt Snort, có ít nhất 2 card nối vào 2 VMnet.

Lưu ý: Trong mô hình triển khai x là số thứ tự của nhóm.

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

Sinh viên thực hiện cấu hình 04 máy ảo theo mô hình được mô tả ở Hình 1.

Lưu ý: hướng dẫn này thực hiện trên VMware Workstation.

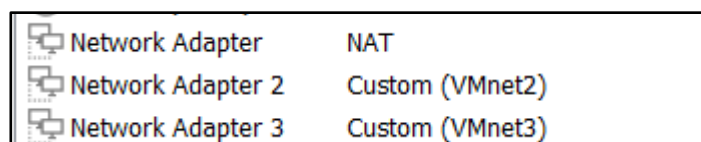
- Kiểm tra card VMnet8 (NAT) đã tồn tại và được bật DHCP.



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.229.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.30.0

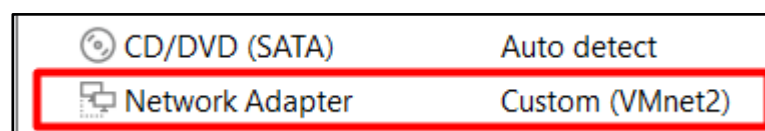
Hình 2. Kiểm tra card VMnet8

- Gán các card mạng cho máy **Router**.



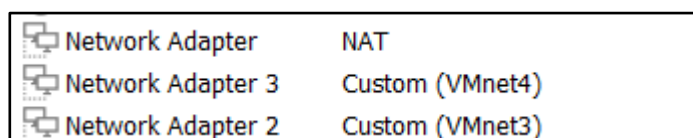
Network Adapter	NAT
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet3)

- Gán card mạng cho máy **Kali**



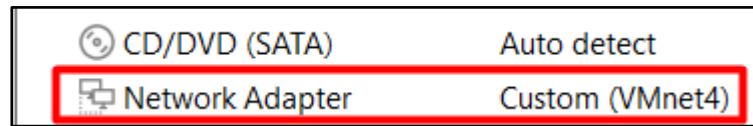
CD/DVD (SATA)	Auto detect
Network Adapter	Custom (VMnet2)

- Gán card mạng cho máy **Snort**



Network Adapter	NAT
Network Adapter 3	Custom (VMnet4)
Network Adapter 2	Custom (VMnet3)

- Gán card mạng cho máy **Victim**



2.1b. Cấu hình địa chỉ ip cho các máy

Dựa vào mô hình đã cho, thực hiện cấu hình địa chỉ IP tương ứng cho các interface của các máy ảo.

2.1c. Cấu hình NAT outbound cho máy router

NAT outbound cho phép các máy trong mạng có thể đi ra Internet. Sau khi cấu hình NAT thành công. Máy Kali có thể kết nối Internet.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping google.com
PING google.com (142.250.199.78) 56(84) bytes of data.
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=1 ttl=112 time=47.9 ms
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=2 ttl=113 time=45.2 ms
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=3 ttl=115 time=35.2 ms
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=4 ttl=113 time=44.9 ms

```

Tham khảo bài viết tại <https://www.howtoforge.com/nat iptables> (Step #8) để cấu hình NAT trên máy Router. **Lưu ý:** tham khảo để chọn ra các bước làm phù hợp.

2.1d. Cài đặt và cấu hình Snort

Lưu ý: hướng dẫn này thực hiện cài đặt Snort trên Ubuntu Server.

- Cài đặt Snort từ công cụ APT.

```

ubuntu@snort:~$
ubuntu@snort:~$ sudo apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libauthen-sasl-perl libdaq2 libencode-locale-perl libfile-listing-perl libfont-afm-perl
  libhtml-form-perl libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl
  libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libio-html-perl libio-socket-ssl-perl liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl
  libnet-ssleay-perl libtimedate-perl liburi-perl libwww-perl libwww-robotrules-perl oinkmaster
  snort-common snort-common-libraries snort-rules-default
Suggested packages:
  libdigest-hmac-perl libgssapi-perl libdata-dump-perl libcrypt-ssleay-perl libauthen-ntlm-perl
  snort-doc

```

- Sau khi cài đặt thành công, kiểm tra phiên bản Snort.

```
ubuntu@snort:~$  
ubuntu@snort:~$ snort --version  
  
--> 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 1.7.4  
Using PCRE version: 8.38 2015-11-23  
Using ZLIB version: 1.2.8
```

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

```
ubuntu@snort:~$ sudo snort --daq-list  
Available DAQ modules:  
pcap(v3): readback live multi unpriv  
ipfw(v3): live inline multi unpriv  
dump(v2): readback live inline multi unpriv  
afpacket(v5): live inline multi unpriv  
ubuntu@snort:~$
```

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

```
ubuntu@snort:~$  
ubuntu@snort:~$ sudo rm -rf /etc/snort/rules/*  
ubuntu@snort:~$
```

- Tạo file rule của nhóm định nghĩa. Ví dụ ở đây là nhóm 0.

```
ubuntu@snort:~$  
ubuntu@snort:~$ sudo touch /etc/snort/rules/nhom0.rules  
ubuntu@snort:~$
```

- 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.

```
ubuntu@snort:~$  
ubuntu@snort:~$ cat /etc/snort/nhom0-snort.conf  
config daq: afpacket  
config daq_mode: inline  
  
include /etc/snort/rules/nhom0.rules  
ubuntu@snort:~$
```

- Kiểm tra file cấu hình snort bằng lệnh sau:

```
ubuntu@snort:~$  
ubuntu@snort:~$  
ubuntu@snort:~$ sudo snort -T -c /etc/snort/nhom0-snort.conf -Q -i enp0s8:enp0s9
```

Lưu ý: **enp0s8** và **enp0s9** là cặp interface sử dụng cho mode inline.

- Chạy snort trong mode inline với dòng lệnh sau:

```
ubuntu@snort:~$  
ubuntu@snort:~$ sudo snort -c /etc/snort/nhom0-snort.conf -Q -i enp0s8:enp0s9  
Enabling inline operation  
Running in IDS mode  
  
--== Initializing Snort ==--  
Initializing Output Plugins!  
Initializing Preprocessors!  
Initializing Plug-ins!  
Parsing Rules file "/etc/snort/nhom0-snort.conf"  
Tagged Packet Limit: 256  
Log directory = /var/log/snort
```

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

- Máy **Kali** ping google.com

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#  
root@kali:~# ping google.com  
PING google.com (142.250.204.142) 56(84) bytes of data.  
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=1 ttl=51 time=36.4 ms  
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=2 ttl=115 time=35.9 ms  
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=3 ttl=51 time=36.3 ms
```

- Máy **Kali** ping máy **Victim**

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#  
root@kali:~# ping 192.168.0.200  
PING 192.168.0.200 (192.168.0.200) 56(84) bytes of data.  
64 bytes from 192.168.0.200: icmp_seq=1 ttl=63 time=1.92 ms  
64 bytes from 192.168.0.200: icmp_seq=2 ttl=63 time=1.93 ms  
64 bytes from 192.168.0.200: icmp_seq=3 ttl=63 time=1.84 ms
```

- Máy **Victim** ping google.com


```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ping google.com
PING google.com (172.217.31.238) 56(84) bytes of data.
64 bytes from hkg07s28-in-f14.1e100.net (172.217.31.238): icmp_seq=1 ttl=113 time=29.2 ms
64 bytes from hkg07s28-in-f14.1e100.net (172.217.31.238): icmp_seq=2 ttl=115 time=48.0 ms
```

Tham khảo thêm hướng dẫn tại đường dẫn: <https://www.snort.org/documents> để cài đặt, cấu hình hình cho Snort.

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/nhomX.rules` như sau:

```
ubuntu@snort:~$
ubuntu@snort:~$ cat /etc/snort/rules/nhom0.rules
alert icmp any any -> 192.168.0.0/24 any (msg: ICMP test detected"; GID:1; sid:10000001; rev:001;)
ubuntu@snort:~$
```

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

```
WARNING: No preprocessors configured for policy 0.
04/07-18:32:31.924358  [**] [1:10000001:1] ICMP test detected" [**] [Priority: 0] {ICMP} 10.81.0.100
-> 192.168.0.200
04/07-18:32:31.924358 10.81.0.100 -> 192.168.0.200
ICMP TTL:63 TOS:0x0 ID:29103 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:1331 Seq:40 ECHO
=====
```

```
[**] [1:10000001:1] ICMP test detected" [**]
[Priority: 0]
04/07-18:31:53.692339 10.81.0.100 -> 192.168.0.200
ICMP TTL:63 TOS:0x0 ID:24060 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:1331 Seq:2 ECHO
```

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.

C. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm**.
- Ghi lại chi tiết những việc (**Report**) mà nhóm đã tìm hiểu, thực hiện, quan sát thấy và kèm ảnh chụp màn hình các kết quả; giải thích kết quả quan sát được.
- Nộp bài theo 2 hình thức:
 - Nộp trực tiếp trên lớp: báo cáo và demo kết quả với GVTH.
 - Nộp báo cáo tại website môn học theo thời gian quy định.

Yêu cầu của báo cáo

- File **.PDF**, tập trung vào nội dung của bài thực hành, không mô tả những lý thuyết không cần thiết.
- Đặt tên file theo định dạng: **[Mã lớp]-LabX_NhomY.PDF**.
Ví dụ: [NT204.K11.ATTT]-Lab1_Nhom0.PDF
- Nếu báo cáo có nhiều file, nén tất cả các file vào một file .ZIP với tên theo định dạng **[Mã lớp]-LabX_NhomY.ZIP**.

~HẾT~