

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
MÔN THỰC TẬP CƠ SỞ



BÀI THỰC HÀNH 2.2
Tìm hiểu và cài đặt, cấu hình NIDS

Tên sinh viên: Nguyễn Văn Hùng

Mã sinh viên: B22DCAT136

Nhóm: 09

HÀ NỘI, THÁNG 03/2025

MỤC LỤC

MỤC LỤC	1
DANH MỤC CÁC HÌNH VẼ	2
I. GIỚI THIỆU CHUNG	3
1. Mục đích	3
2. Lý thuyết	3
2.1. Tổng quan về hệ thống phát hiện xâm nhập (IDS)	3
2.2. Các công cụ IDS	5
I. NỘI DUNG THỰC HÀNH	8
1. Chuẩn bị môi trường	8
2. Thực hành	8
2.1. Chuẩn bị các máy	8
2.2. Cài đặt và chạy thử Snort	9
2.3. Tạo luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống	10
2.4. Thực thi tấn công và phát hiện sử dụng Snort	12
TÀI LIỆU THAM KHẢO	16

DANH MỤC CÁC HÌNH VẼ

Hình 1 . Vị trí hệ thống IDS	3
Hình 2 . Các NIDS được bố trí giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng	4
Hình 3 . Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các host	4
Hình 4 . Kiến trúc Snort	6
Hình 5 . Máy Kali Linux	8
Hình 6 . Máy Ubuntu Linux Snort	8
Hình 7 . Thử kết nối hai máy	9
Hình 8 . Cấu hình địa chỉ mạng nội bộ	9
Hình 9 . Cấu hình địa chỉ mạng nội bộ trong file snort.conf	10
Hình 10 . Kiểm tra trạng thái Snort	10
Hình 11 . Kích hoạt cấu hình luật local.rules	11
Hình 12 . Thêm luật vào local.rules	12
Hình 13 . Ping từ máy Kali Linux	13
Hình 14 . Kiểm tra ping trên Ubuntu Linux Snort	13
Hình 15 . Rà quét Nmap trên Kali Linux	13
Hình 16 . Kiểm tra Nmap trên máy Ubuntu Linux Snort	14
Hình 17 . Tấn công TCP SYN Flood bằng hping3	14
Hình 18 . Kiểm tra kết quả tấn công TCP SYN Flood trên máy Ubuntu Linux Snort	14

I. GIỚI THIỆU CHUNG

1. Mục đích

- Tìm hiểu và luyện tập việc cài đặt và vận hành các hệ thống phát hiện xâm nhập cho host (HIDS) và cho mạng (NIDS).
- Luyện tập việc tạo và chỉnh sửa các luật phát hiện tấn công, xâm nhập cho các hệ thống phát hiện xâm nhập thông dụng.

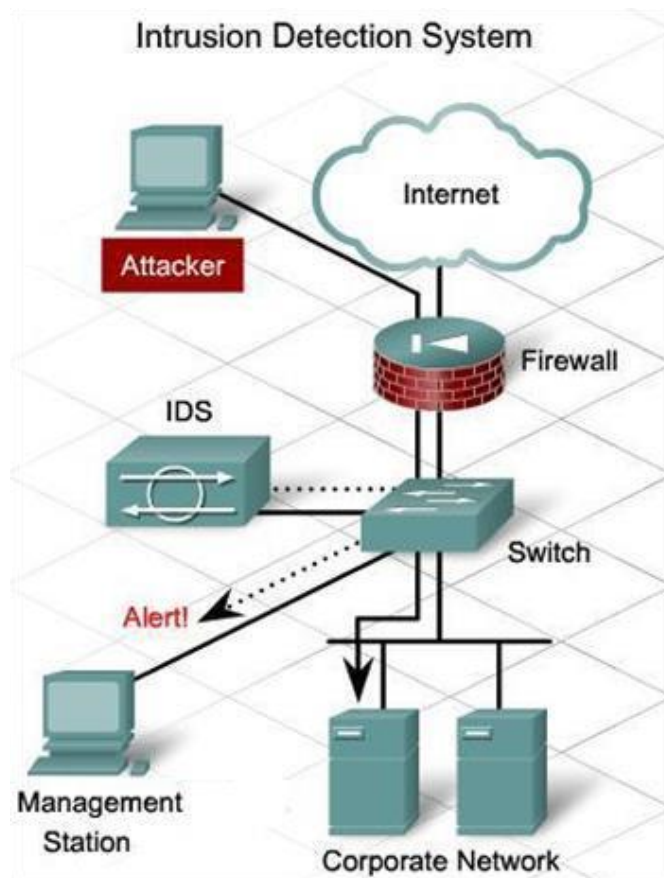
2. Lý thuyết

2.1. Tổng quan về hệ thống phát hiện xâm nhập (IDS)

a. Giới thiệu

IDS (Intrusion Detection System) là hệ thống phát hiện tấn công, xâm nhập trái phép. IDS không thể ngăn chặn mà chỉ có chức năng giám sát và cảnh báo khi có dấu hiệu đáng ngờ.

IDS thường được kết nối vào bộ định tuyến, switch, card mạng:



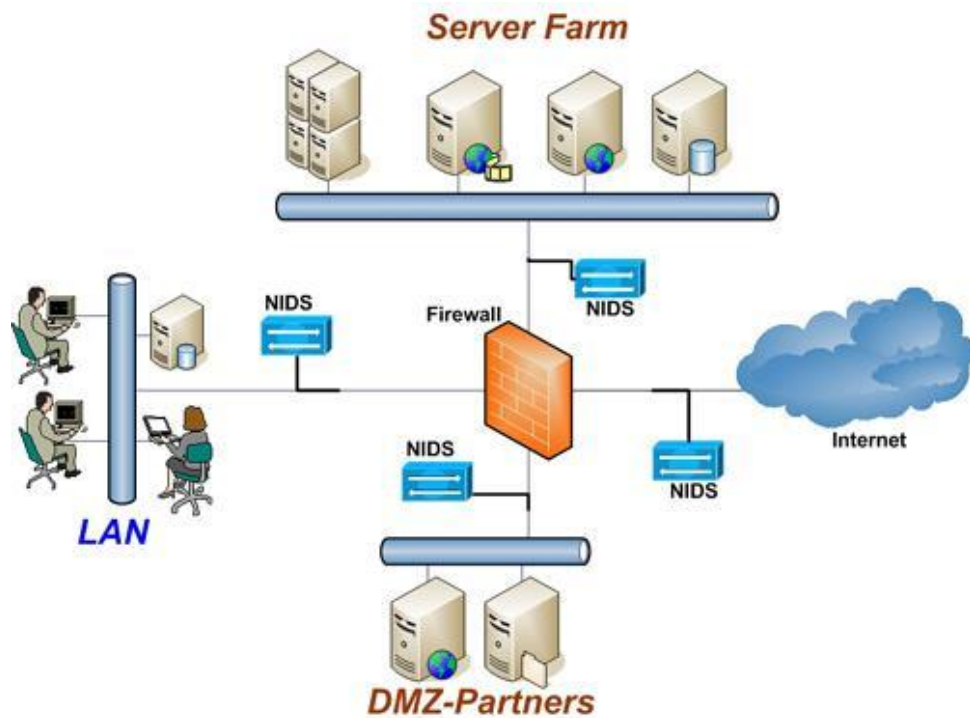
Hình 1. Vị trí hệ thống IDS

b. Phân loại

Có hai phương pháp phân loại chính gồm phân loại theo nguồn dữ liệu và phân loại theo phương pháp phân tích dữ liệu.

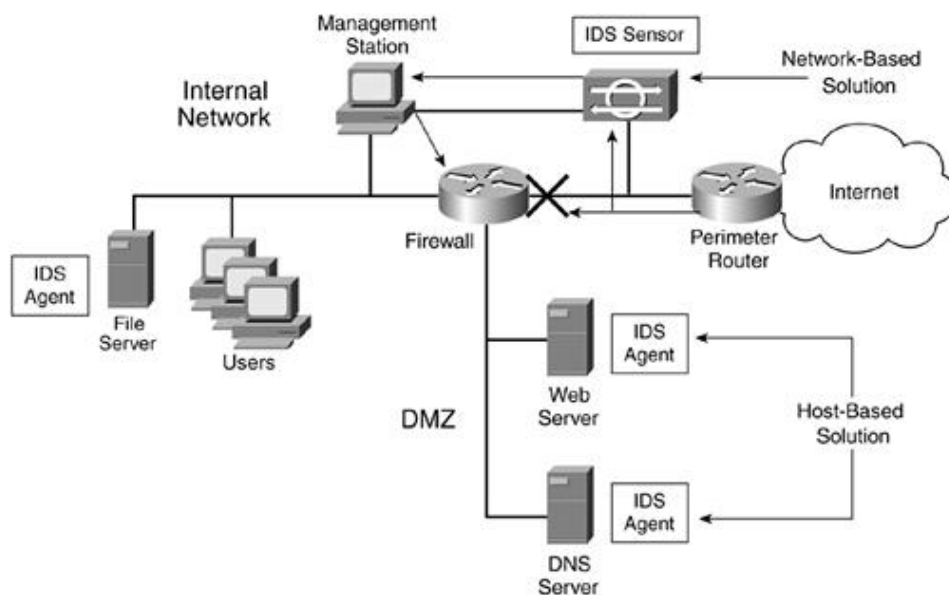
Theo nguồn dữ liệu, có 2 loại hệ thống phát hiện xâm nhập:

- Hệ thống phát hiện xâm nhập mạng (NIDS - Network-based IDS): NIDS phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng.



Hình 2. Các NIDS được bố trí giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng

- Hệ thống phát hiện xâm nhập cho host (HIDS – Host-based IDS): HIDS phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó.



Hình 3. Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các host

Theo kỹ thuật phân tích, có 2 kỹ thuật phân tích chính:

- Phát hiện xâm nhập dựa trên chữ ký, hoặc phát hiện sự lạm dụng (Signature-based / misuse intrusion detection): So sánh dữ liệu với cơ sở mẫu tấn công đã biết.
- Phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection): Phát hiện các hành vi bất thường so với hoạt động bình thường.

c. Các kỹ thuật phát hiện xâm nhập

- Phát hiện xâm nhập dựa trên chữ ký (Signature-based IDS): So sánh lưu lượng với cơ sở dữ liệu chứa các mẫu tấn công đã biết. Ví dụ: Snort, Suricata.

Ưu điểm:

- Phát hiện các tấn công, xâm nhập đã biết một cách hiệu quả.
- Tốc độ xử lý cao, yêu cầu tài nguyên tính toán tương đối thấp.

Nhược điểm:

- Không có khả năng phát hiện các tấn công, xâm nhập mới
- Đòi hỏi công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký, dấu hiệu của các tấn công xâm nhập
- Phát hiện dựa trên hành vi (Anomaly-based IDS): Phân tích hành vi bất thường so với dữ liệu chuẩn. Ví dụ: Zeek, OSSEC, Wazuh.

Ưu điểm:

- Có tiềm năng phát hiện các loại tấn công, xâm nhập mới mà không yêu cầu biết trước thông tin.

Nhược điểm:

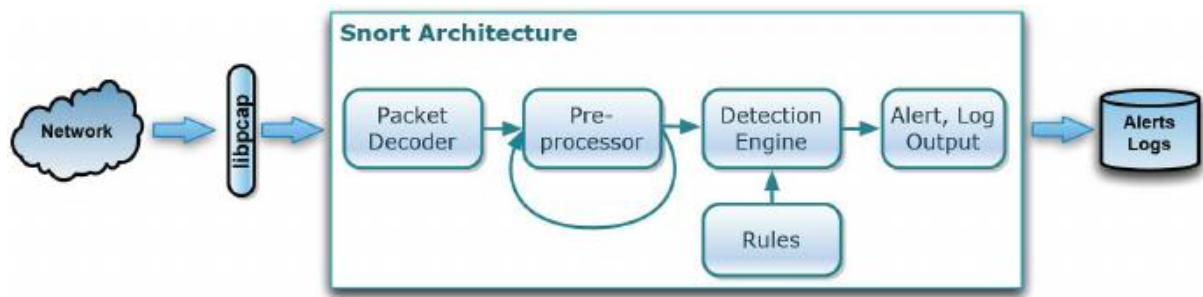
- Tỷ lệ cảnh báo sai tương đối cao.
- Tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại.

2.2. Các công cụ IDS

2.2.1. Snort

Snort là một hệ thống phát hiện và ngăn chặn xâm nhập mạng (IDS/IPS), hoạt động bằng cách phân tích lưu lượng mạng theo các luật (rules) để phát hiện tấn công hoặc hoạt động đáng ngờ.

Kiến trúc Snort có nhiều thành phần:



Hình 4. Kiến trúc Snort

- Packet Capture : Nhận dữ liệu từ giao diện mạng (dùng libpcap)
- Pre-processor: Xử lý, chuẩn hóa và phân loại gói tin trước khi phân tích
- Detection Engine: So sánh gói tin với các luật (Rules) để phát hiện tấn công
- Alert, Log Output: Cảnh báo hoặc ghi log khi phát hiện tấn công

Luật trong Snort (Rules):

- Cấu trúc của một luật Snort:
- `action protocol source_ip source_port -> dest_ip dest_port (options)`
- Giải thích:
 - action: Hành động khi gói tin khớp với luật (alert, log, drop,...)
 - protocol: Giao thức cần giám sát (tcp, udp, icmp,...)
 - source_ip: Địa chỉ ip nguồn
 - source_port: Cổng nguồn
 - dest_ip: Địa chỉ ip đích
 - dest_port: Cổng đích
 - options: Các điều kiện kiểm tra bổ sung
- Ví dụ:


```

alert icmp any any -> $HOME_NET any (msg:"Phát hiện gói ping"; sid:10001;)
      
```

Giải thích:

- alert → Hành động cảnh báo
- icmp → Giao thức ICMP (dùng cho ping)
- any any -> \$HOME_NET any → Gói ICMP từ bất kỳ nguồn nào đến mạng nội bộ
- msg:"Phát hiện gói ping" → Nội dung cảnh báo
- sid:10001; → Mã số quy tắc

2.2.2. Suricata

Suricata là một công cụ giám sát bảo mật mạng, IPS và IDS hiệu suất cao. Đây là mã nguồn mở với hiệu suất cao, có khả năng phát hiện dựa trên chữ ký, thống kê và hành vi.

Tính năng chính:

- Hỗ trợ phân tích gói tin tốc độ cao, tận dụng đa luồng và GPU.
- Hỗ trợ phân tích lưu lượng TLS, HTTP, DNS, SMB để phát hiện các mối đe dọa.
- Hỗ trợ các quy tắc Snort, giúp dễ dàng chuyển đổi từ Snort sang Suricata.
- Tích hợp tốt với các công cụ SIEM như Wazuh, Splunk.

2.2.3. OSSEC

OSSEC là một hệ thống phát hiện xâm nhập dựa trên máy chủ (HIDS) mã nguồn mở, có khả năng giám sát log, phát hiện rootkit, kiểm tra tính toàn vẹn tập tin và phát hiện hành vi đáng ngờ trên máy chủ.

Tính năng chính:

- Kiểm tra log, phân tích và gửi cảnh báo bảo mật.
- Hỗ trợ giám sát tính toàn vẹn của tập tin.
- Có thể phát hiện rootkit, brute-force attack, hoặc thay đổi quyền trên hệ thống.
- Có thể tích hợp với các công cụ SIEM.

2.2.4. Wazuh

Wazuh là một nền tảng bảo mật mã nguồn mở, được xây dựng dựa trên OSSEC nhưng mở rộng thêm khả năng giám sát hệ thống, phát hiện xâm nhập và tích hợp với SIEM.

Tính năng chính:

- Giám sát log và cảnh báo bảo mật theo thời gian thực.
- Kiểm tra tuân thủ bảo mật theo các tiêu chuẩn như PCI-DSS, GDPR...
- Phát hiện rootkit và phân tích malware.
- Tích hợp mạnh với ELK Stack để hiển thị dữ liệu và quản lý log.

I. NỘI DUNG THỰC HÀNH

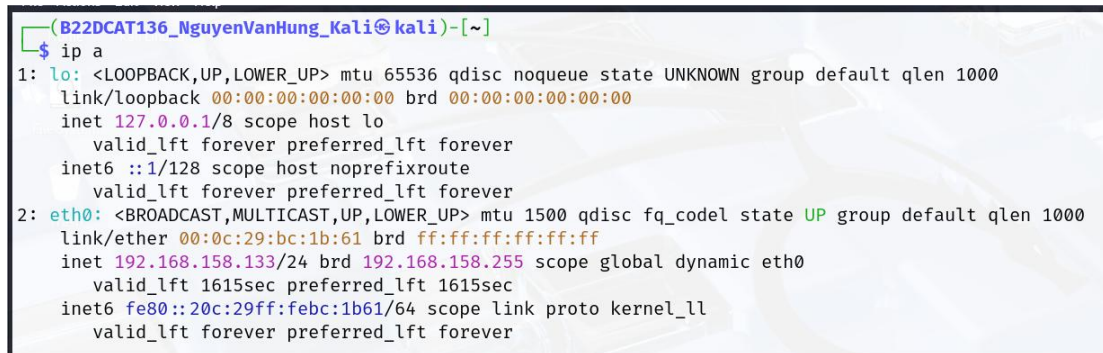
1. Chuẩn bị môi trường

- 01 máy tính (máy thật hoặc máy ảo) chạy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng (LAN hoặc Internet).
- 01 máy tính (máy thật hoặc máy ảo) chạy Kali Linux (bản 2021 trở lên)
- Bộ phần mềm Snort tải tại <https://www.snort.org/downloads>

2. Thực hành

2.1. Chuẩn bị các máy

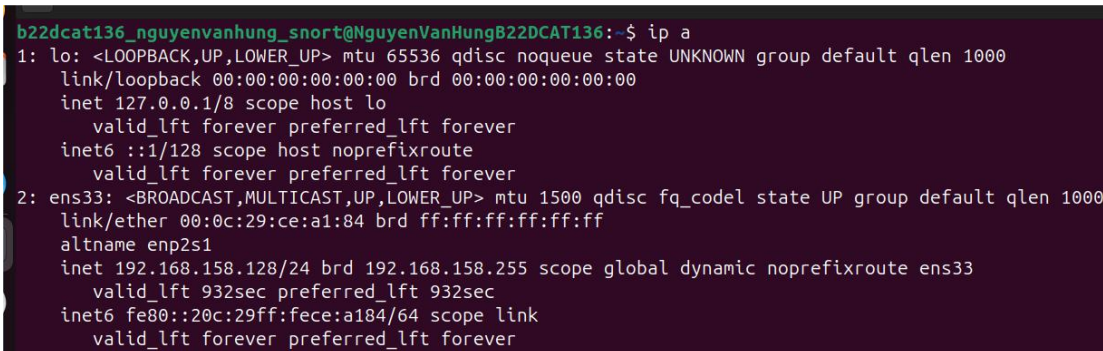
Máy Kali Linux:



```
(B22DCAT136_NguyenVanHung_Kali)kali-[]  
$ ip a  
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 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:bc:1b:61 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.158.133/24 brd 192.168.158.255 scope global dynamic eth0  
        valid_lft 1615sec preferred_lft 1615sec  
    inet6 fe80::20c:29ff:febc:1b61/64 scope link proto kernel_ll  
        valid_lft forever preferred_lft forever
```

Hình 5. Máy Kali Linux

Máy Ubuntu Linux:



```
b22dcat136_nguyenvanhung_snort@NguyenVanHungB22DCAT136:~$ ip a  
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 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:ce:a1:84 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.158.128/24 brd 192.168.158.255 scope global dynamic noprefixroute ens33  
        valid_lft 932sec preferred_lft 932sec  
    inet6 fe80::20c:29ff:fece:a184/64 scope link  
        valid_lft forever preferred_lft forever
```

Hình 6. Máy Ubuntu Linux Snort

Ping thử từ máy Kali Linux tới Ubuntu Linux:

```
(B22DCAT136_NguyenVanHung_Kali@kali)-[~]
$ ip a
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 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:bc:1b:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.158.133/24 brd 192.168.158.255 scope global dynamic eth0
        valid_lft 1328sec preferred_lft 1328sec
    inet6 fe80::20c:29ff:febc:1b61/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(B22DCAT136_NguyenVanHung_Kali@kali)-[~]
$ ping 192.168.158.128
PING 192.168.158.128 (192.168.158.128) 56(84) bytes of data.
64 bytes from 192.168.158.128: icmp_seq=1 ttl=64 time=12.6 ms
64 bytes from 192.168.158.128: icmp_seq=2 ttl=64 time=0.818 ms
^C
— 192.168.158.128 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.818/6.692/12.567/5.874 ms

(B22DCAT136_NguyenVanHung_Kali@kali)-[~]
$
```

Hình 7. Thử kết nối hai máy

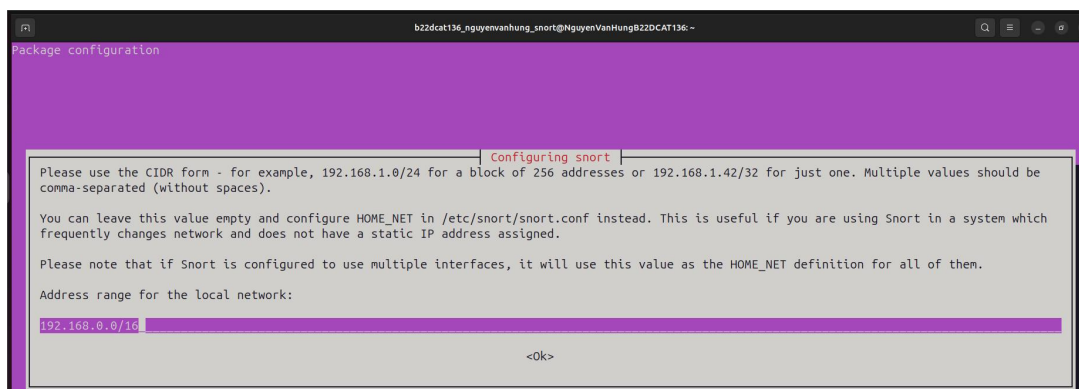
2.2. Cài đặt và chạy thử Snort

Cài đặt Snort:

```
sudo apt update
```

```
sudo apt install -y snort
```

Trong quá trình cài đặt, bạn sẽ được yêu cầu cấu hình dải địa chỉ mạng nội bộ (HOME_NET) mà Snort sẽ giám sát:



Hình 8. Cấu hình địa chỉ mạng nội bộ

Mặc định được đặt là 192.168.0.0/16, nghĩa là toàn bộ dải 192.168.x.x:

- Có thể giữ nguyên nếu muốn giám sát toàn bộ dải 192.168.x.x
- Chỉnh sửa nếu bạn muốn giám sát một phần nhỏ hơn: Ví dụ: 192.168.158.0/24
- Bỏ trống nếu muốn tự cấu hình trong file /etc/snort/snort.conf

Cấu hình HOME_NET trong file /etc/snort/snort/snort.conf:

- Tìm dòng: **ipvar HOME_NET any**

- Đổi thành: **ipvar HOME_NET 192.168.158.128** → Chỉ giám sát máy Ubuntu Linux

```

GNU nano 7.2 /etc/snort/snort.conf *
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file

#ipvar HOME_NET any
ipvar HOME_NET 192.168.158.128

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
  
```

Hình 9. Cấu hình địa chỉ mạng nội bộ trong file snort.conf

Khởi động lại Snort để áp dụng thay đổi: *sudo systemctl restart snort*

Kiểm tra Snort đã cài đặt thành công chưa:

snort -V: Kiểm tra phiên bản

systemctl status snort: Kiểm tra trạng thái

```

b22dcat136_nguyenvanhung_snort@NguyenVanHungB22DCAT136:/var/log/snort$ snort -V
...
Version 2.9.20 GRE (Build 02)
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) 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: 1.3

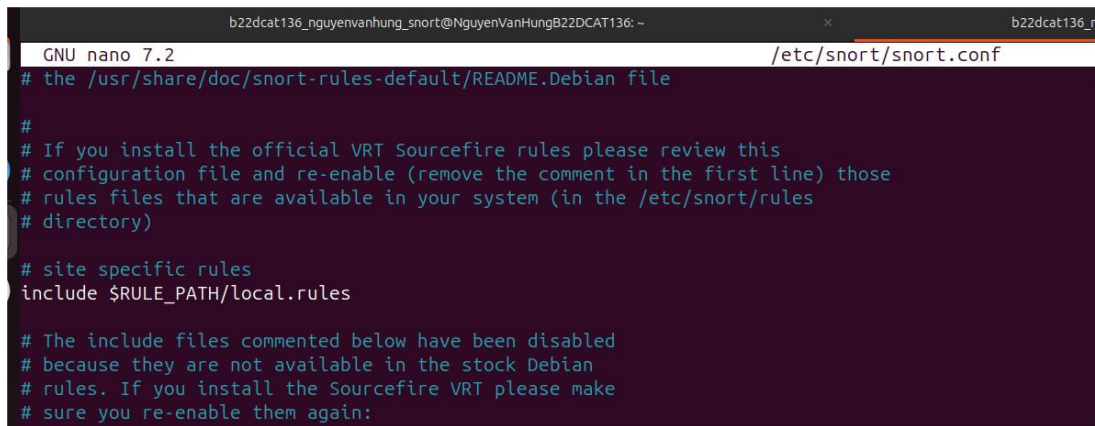
b22dcat136_nguyenvanhung_snort@NguyenVanHungB22DCAT136:/var/log/snort$ sudo systemctl status snort
● snort.service - LSB: lightweight network intrusion detection system
   Loaded: loaded (/etc/init.d/snort; generated)
   Active: active (running) since Fri 2025-03-28 14:00:45 +07; 4min 27s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 5882 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 4551)
   Memory: 79.9M (peak: 95.6M)
      CPU: 2.015s
   CGroup: /system.slice/snort.service
           └─5903 /usr/sbin/snort -m 027 -D -l /var/log/snort -u snort -g snort --pid-path /run/snort/ -C /etc/snort/snort.conf -S "[HOME_NET=[192.168.0.0/16]]" -i ens33

Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_NDDBUS Version 1.1 <Build 1>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Mar 28 14:00:45 NguyenVanHungB22DCAT136 snort[5903]: Commencing packet processing (pid=5903)
  
```

Hình 10. Kiểm tra trạng thái Snort

2.3. Tạo luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống

Mở file cấu hình snort.conf, tìm dòng **include \$RULE_PATH/local.rules**, đảm bảo được kích hoạt.



```
GNU nano 7.2 /etc/snort/snort.conf
# the /usr/share/doc/snort-rules-default/README.Debian file
#
# If you install the official VRT Sourcefire rules please review this
# configuration file and re-enable (remove the comment in the first line) those
# rules files that are available in your system (in the /etc/snort/rules
# directory)
#
# site specific rules
include $RULE_PATH/local.rules
#
# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:
```

Hình 11. Kích hoạt cấu hình luật *local.rules*

Mở file luật Snort: *sudo nano /etc/snort/rules/local.rules*

- Thêm luật phát hiện gói ping gửi đến:

```
alert icmp any any -> $HOME_NET any
(msg:"b22dcat136_nguyenvanhung_snort phát hiện có các gói ping gửi đến.";
itype:8; sid:1000001;)
```

Giải thích:

- *alert* → Sinh cảnh báo khi phát hiện gói tin phù hợp.
- *icmp any any -> \$HOME_NET any* → Bắt tất cả gói ICMP từ bất kỳ địa chỉ IP và cổng nào gửi đến mạng nội bộ (*\$HOME_NET*).
- *(msg ...)* → Hiển thị thông báo khi phát hiện gói tin.
- *itype:8;* → Chỉ bắt các gói ICMP có loại Echo Request (tức là các gói ping).
- *sid:1000001;* → Số ID của luật, giúp Snort phân biệt với các luật khác.

- Thêm luật phát hiện có các gói tin rà quét trên cổng 80:

```
alert tcp any any -> $HOME_NET 80 (msg:"b22dcat136_nguyenvanhung_snort
phát hiện có các gói tin rà quét trên cổng 80."; flags:S; threshold:type threshold,
track by_src, count 5, seconds 10; sid:1000002;)
```

Giải thích:

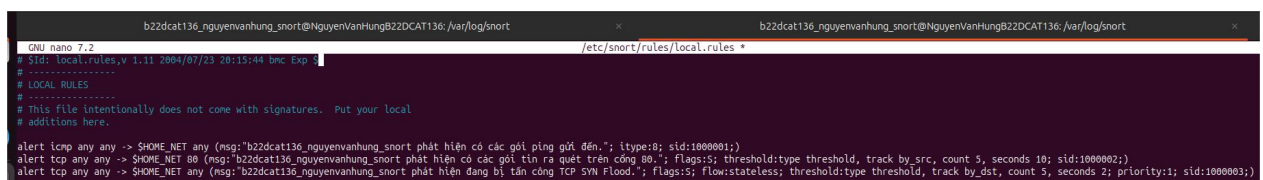
- *tcp any any -> \$HOME_NET 80* → Bắt các gói TCP từ bất kỳ nguồn nào gửi đến cổng 80 của mạng nội bộ (*\$HOME_NET*).
- *flags:S;* → Chỉ bắt các gói tin có cờ SYN, thường xuất hiện trong quá trình thiết lập kết nối.
- *threshold:type threshold, track by_src, count 5, seconds 10;*
 - *type threshold* → Áp dụng ngưỡng cảnh báo.

- track by_src → Theo dõi địa chỉ nguồn (by_src), tức là kiểm tra nếu một địa chỉ IP gửi nhiều gói SYN.
- count 5, seconds 10 → Chỉ cảnh báo nếu một địa chỉ IP gửi ít nhất 5 gói SYN trong vòng 10 giây.
- sid:1000002; → ID của luật.
- Thêm luật phát hiện đang bị tấn công TCP SYN Flood:

alert tcp any any -> \$HOME_NET any (msg:"b22dcat136_nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood."; flags:S; flow:stateless; threshold:type threshold, track by_dst, count 5, seconds 2; priority:1; sid:1000003;)

Giải thích:

- flags:S; → Chỉ bắt các gói SYN.
- flow:stateless; → Bắt cả các gói không thuộc một luồng kết nối hợp lệ (dấu hiệu của tấn công).
- threshold:type threshold, track by_dst, count 5, seconds 2;
 - track by_dst → Theo dõi địa chỉ đích (by_dst), tức là kiểm tra nếu một máy chủ nhận quá nhiều gói SYN.
 - count 5, seconds 2 → Cảnh báo nếu một địa chỉ IP nhận ít nhất 5 gói SYN trong vòng 2 giây.
- priority:1; → Đặt mức độ ưu tiên cao nhất cho cảnh báo này.
- sid:1000003; → ID của luật.



Hình 12. Thêm luật vào local.rules

2.4. Thực thi tấn công và phát hiện sử dụng Snort

a. Phát hiện gói tin ping từ bất kỳ máy nào gửi đến Snort

Ping từ máy Kali Linux đến máy snort: *ping 192.168.158.128*

```

(B22DCAT136_NguyenVanHung_Kali@kali)-[~]
$ ping 192.168.158.128
PING 192.168.158.128 (192.168.158.128) 56(84) bytes of data.
64 bytes from 192.168.158.128: icmp_seq=1 ttl=64 time=0.722 ms
64 bytes from 192.168.158.128: icmp_seq=2 ttl=64 time=1.84 ms
^C
— 192.168.158.128 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1017ms
rtt min/avg/max/mdev = 0.722/1.278/1.835/0.556 ms

```

Hình 13. Ping từ máy Kali Linux

Kiểm tra kết quả trên file ghi log của snort: **var/log/snort/snort.alert.fast**
sudo cat snort.alert.fast

```

b22dc136_nguyenvanhung_snort@NguyenVanHungB22DCAT136: /var/log/snort
b22dc136_nguyenvanhung_snort@NguyenVanHungB22DCAT136: /var/log/snort$ ll
total 8
drwxr-sr-x 2 snort adm 4096 Mar 28 20:09 ./
drwxrwxr-x 18 root  syslog 4096 Mar 28 19:40 ../
-rw-r----- 1 snort adm 0 Mar 28 20:49 snort.alert
-rw-r----- 1 snort adm 0 Mar 28 20:49 snort.alert.fast
-rw-r----- 1 snort adm 0 Mar 28 20:49 snort.log
b22dc136_nguyenvanhung_snort@NguyenVanHungB22DCAT136: /var/log/snort$ ll
total 20
drwxr-sr-x 2 snort adm 4096 Mar 28 20:09 ./
drwxrwxr-x 18 root  syslog 4096 Mar 28 19:40 ../
-rw-r----- 1 snort adm 120 Mar 28 20:50 snort.alert
-rw-r----- 1 snort adm 360 Mar 28 20:50 snort.alert.fast
-rw-r----- 1 snort adm 532 Mar 28 20:50 snort.log
b22dc136_nguyenvanhung_snort@NguyenVanHungB22DCAT136: /var/log/snort$ sudo cat snort.alert.fast
03/28/20:50:14.179677  [**] [1:1000001:0] b22dc136_nguyenvanhung_snort phát hiện có các gói ping gửi đến. [**] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
03/28/20:50:15.197452  [**] [1:1000001:0] b22dc136_nguyenvanhung_snort phát hiện có các gói ping gửi đến. [**] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
b22dc136_nguyenvanhung_snort@NguyenVanHungB22DCAT136: /var/log/snort$

```

Hình 14. Kiểm tra ping trên Ubuntu Linux Snort

b. Phát hiện các gói tin rà quét từ bất kỳ máy nào gửi đến máy chạy Snort

Thực hiện rà quét trên cổng 80: **nmap -sV -p80 -A 192.168.158.128**

```

(B22DCAT136_NguyenVanHung_Kali@kali)-[~]
$ nmap -sV -p80 -A 192.168.158.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 09:51 EDT
Nmap scan report for 192.168.158.128
Host is up (0.0026s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 00:0C:29:CE:A1:84 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|6.X|2.6.X|3.X (97%), MikroTik RouterOS 7.X (95%), Synology DiskStation Manager 5.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6.0 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/o:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 5.0 - 5.14 (97%), OpenWrt 21.02 (Linux 5.4) (97%), Linux 4.19 (95%), Linux 6.0 (95%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (95%), Linux 5.4 - 5.10 (91%), Linux 2.6.32 (91%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 2.62 ms 192.168.158.128

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.46 seconds

```

Hình 15. Rà quét Nmap trên Kali Linux

Kiểm tra trên máy snort: *sudo cat snort.alert.fast*


```
03/28-20:50:13.197426 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói ping gửi đến. [[*]] [Priority: 0] [ICMP] 192.168.158.128 -> 192.168.158.128
b22cat136.nguyenvanhung_snort@NguyenVanHungB22CAT136: /var/log/snort$ sudo cat snort.alert.fast
03/28-20:50:14.179677 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói ping gửi đến. [[*]] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
03/28-20:50:15.197452 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói ping gửi đến. [[*]] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
03/28-20:51:21.965697 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:3742 -> 192.168.158.128:80
03/28-20:51:22.156633 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:3744 -> 192.168.158.128:80
03/28-20:51:22.276635 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói ping gửi đến. [[*]] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
03/28-20:51:22.302269 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói ping gửi đến. [[*]] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
03/28-20:51:22.506373 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:3759 -> 192.168.158.128:42561
03/28-20:51:22.658400 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:3759 -> 192.168.158.128:42561
03/28-20:51:22.818579 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:3759 -> 192.168.158.128:42561
03/28-20:51:22.912419 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:3757 -> 192.168.158.128:42561
03/28-20:51:22.963491 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:3759 -> 192.168.158.128:42561
03/28-20:51:24.184551 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:3759 -> 192.168.158.128:80
03/28-20:51:24.485704 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:3760 -> 192.168.158.128:80
03/28-20:51:24.619934 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói ping gửi đến. [[*]] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
03/28-20:51:24.636573 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói ping gửi đến. [[*]] [Priority: 0] [ICMP] 192.168.158.133 -> 192.168.158.128
03/28-20:51:24.839392 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:37615 -> 192.168.158.128:44156
03/28-20:51:24.991836 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:37615 -> 192.168.158.128:44156
03/28-20:51:25.144662 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:37615 -> 192.168.158.128:44156
03/28-20:51:25.246185 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:37613 -> 192.168.158.128:44156
03/28-20:51:25.297194 [[*]] [1:1228:7] SCAN nmap XMAS [[*]] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.158.133:37615 -> 192.168.158.128:44156
03/28-20:51:25.446433 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:46040 -> 192.168.158.128:80
03/28-20:51:25.447732 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:46072 -> 192.168.158.128:80
03/28-20:51:25.448132 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:46078 -> 192.168.158.128:80
03/28-20:51:25.460832 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:46122 -> 192.168.158.128:80
03/28-20:51:25.461232 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:46136 -> 192.168.158.128:80
03/28-20:51:25.467283 [[*]] [1:1852:3] WEB-MISC robots.txt access [[*]] [Classification: access to a potentially vulnerable web application] [Priority: 2] [TCP] 192.168.158.133:46040 -> 192.168.158.128:80
03/28-20:51:25.531187 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:46164 -> 192.168.158.128:80
03/28-20:51:25.531475 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:46172 -> 192.168.158.128:80
03/28-20:51:25.692968 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:46206 -> 192.168.158.128:80
03/28-20:51:25.851357 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:46208 -> 192.168.158.128:80
03/28-20:51:26.474940 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 192.168.158.133:46250 -> 192.168.158.128:80
03/28-20:51:26.631182 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện có các gói tin rà quét trên cổng 80. [[*]] [Priority: 0] [TCP] 192.168.158.133:46260 -> 192.168.158.128:80
b22cat136.nguyenvanhung_snort@NguyenVanHungB22CAT136: /var/log/snort$
```

Hình 16. Kiểm tra Nmap trên máy Ubuntu Linux Snort

Ta thấy có thông báo bị có gói ping gửi đến, tấn công TCP SYN Flood và rà quét trên cổng 80 vì khi Nmap nó có thể sử dụng ICMP Echo Request (ping) để kiểm tra xem mục tiêu có đang hoạt động không, đồng thời với tùy chọn -sV -A, Nmap sẽ gửi nhiều gói SYN để quét cổng.

c. Phát hiện tấn công TCP SYN Flood

Tấn công TCP SYN Flood máy Snort bằng hping3:

hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.158.128

```
(B22DCAT136_NguyenVanHung_Kali@kali)-[~]
$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.158.128
[sudo] password for B22DCAT136_NguyenVanHung_Kali:
HPING 192.168.158.128 (eth0 192.168.158.128): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.158.128 hping statistic —
177653 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Hình 17. Tấn công TCP SYN Flood bằng hping3

Kiểm tra kết quả:

```
b22cat136.nguyenvanhung_snort@NguyenVanHungB22CAT136: /var/log/snort$
03/28-20:53:44.867685 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 157.151.95.214:48750 -> 192.168.158.128:80
03/28-20:53:44.867927 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 107.151.53.213:48755 -> 192.168.158.128:80
03/28-20:53:44.868113 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 27.3.214.237:48760 -> 192.168.158.128:80
03/28-20:53:44.868311 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 63.45.5.8:48765 -> 192.168.158.128:80
03/28-20:53:44.868557 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 45.21.198.29:48770 -> 192.168.158.128:80
03/28-20:53:44.868725 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 139.184.87.4:48775 -> 192.168.158.128:80
03/28-20:53:44.869337 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 50.73.12.96:48780 -> 192.168.158.128:80
03/28-20:53:44.869237 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 74.213.91.28:48785 -> 192.168.158.128:80
03/28-20:53:44.869493 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 236.60.12.21:48790 -> 192.168.158.128:80
03/28-20:53:44.869691 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 198.59.131.33:48795 -> 192.168.158.128:80
03/28-20:53:44.869911 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 145.135.49.14:48800 -> 192.168.158.128:80
03/28-20:53:44.870110 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 207.154.201.135:48805 -> 192.168.158.128:80
03/28-20:53:44.870398 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 184.105.137.40:48810 -> 192.168.158.128:80
03/28-20:53:44.870611 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 103.156.5.107:48815 -> 192.168.158.128:80
03/28-20:53:44.870943 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 155.87.54.95:48820 -> 192.168.158.128:80
03/28-20:53:44.871100 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 50.27.276.110:48825 -> 192.168.158.128:80
03/28-20:53:44.871453 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 46.218.251.40:48830 -> 192.168.158.128:80
03/28-20:53:44.871749 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 251.77.96.111:48835 -> 192.168.158.128:80
03/28-20:53:44.872000 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 118.95.14.126:48840 -> 192.168.158.128:80
03/28-20:53:44.872158 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 218.101.181.59:48845 -> 192.168.158.128:80
03/28-20:53:44.872406 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 218.215.176.216:48850 -> 192.168.158.128:80
03/28-20:53:44.872481 [[*]] [1:528:51] BAD TRAFFIC loopback traffic [[*]] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 127.0.0.1:228.54:48852 -> 192.168.158.128:80
03/28-20:53:44.872694 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 46.227.43.247:48855 -> 192.168.158.128:80
03/28-20:53:44.872856 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 242.131.147.201:48860 -> 192.168.158.128:80
03/28-20:53:44.873055 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 114.110.4.32:48865 -> 192.168.158.128:80
03/28-20:53:44.873360 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 83.177.154.13:48870 -> 192.168.158.128:80
03/28-20:53:44.873482 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 116.50.103.69:48875 -> 192.168.158.128:80
03/28-20:53:44.873739 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 237.44.237.89:48880 -> 192.168.158.128:80
03/28-20:53:44.873960 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 238.115.101.12:48885 -> 192.168.158.128:80
03/28-20:53:44.874257 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 129.190.250.88:48890 -> 192.168.158.128:80
03/28-20:53:44.874465 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 99.73.153.31:48895 -> 192.168.158.128:80
03/28-20:53:44.874675 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 12.701.238.43:48900 -> 192.168.158.128:80
03/28-20:53:44.874915 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 113.27.24.126:48905 -> 192.168.158.128:80
03/28-20:53:44.875199 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 58.122.168.57:48910 -> 192.168.158.128:80
03/28-20:53:44.875290 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 182.39.21.195:48915 -> 192.168.158.128:80
03/28-20:53:44.875549 [[*]] [1:1000000:0] b22cat136.nguyenvanhung_snort phát hiện đang bị tấn công TCP SYN Flood. [[*]] [Priority: 1] [TCP] 162.206.214.211:48920 -> 192.168.158.128:80
b22cat136.nguyenvanhung_snort@NguyenVanHungB22CAT136: /var/log/snort$
```

Hình 18. Kiểm tra kết quả tấn công TCP SYN Flood trên máy Ubuntu Linux Snort

TÀI LIỆU THAM KHẢO

- [1] Hoàng Xuân Dậu, Nguyễn Thị Thanh Thủy, *Bài giảng Cơ sở an toàn thông tin*, Học viện Công nghệ Bưu chính Viễn thông, Hà Nội 2016
- [2] <https://docs.suricata.io/en/latest/>
- [3] <https://www.ossec.net/docs/>
- [4] <https://documentation.wazuh.com/current/index.html>
- [5] https://www.researchgate.net/figure/Schematic-data-flow-in-the-Snort-IDS_fig1_264149701
- [6] <https://www.snort.org/#documents>