

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH  
HỌC PHẦN: THỰC TẬP CƠ SỞ  
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 2.2  
TÌM HIỂU VÀ CÀI ĐẶT, CẤU HÌNH NIDS**

Sinh viên thực hiện:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
<b>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH</b> .....	<b>5</b>
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết .....	5
<b>1.2.1</b> Hệ thống phát hiện tấn công, xâm nhập .....	<b>5</b>
<b>1.2.2</b> Kiến trúc và tính năng một số hệ thống phát hiện tấn công, xâm nhập .....	<b>8</b>
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</b> .....	<b>11</b>
2.1 Chuẩn bị môi trường .....	11
2.2 Các bước thực hiện.....	11
<b>2.2.1</b> Cài đặt Snort.....	<b>11</b>
<b>2.2.2</b> Cấu hình và tạo luật Snort .....	<b>15</b>
<b>2.2.3</b> Thực hiện tấn công và phát hiện sử dụng Snort .....	<b>19</b>
TÀI LIỆU THAM KHẢO.....	25

## DANH MỤC CÁC HÌNH VẼ

Hình 1 Sơ đồ vị trí của IDS trong hệ thống mạng.....	5
Hình 2 Hoạt động của NIDS và HIDS .....	7
Hình 3 Kiến trúc của Snort.....	8
Hình 4 Địa chỉ IP của máy Ubuntu cài đặt Snort .....	11
Hình 5 Địa chỉ IP máy Kali tấn công .....	12
Hình 6 Cài đặt Snort.....	12
Hình 7 Chọn giao diện mạng để bắt gói tin.....	13
Hình 8 Cài đặt Snort thành công .....	14
Hình 9 Kiểm tra trạng thái hoạt động của Snort .....	15
Hình 10 Cấu hình cho Snort.....	16
Hình 11 Kiểm tra thông tin cấu hình.....	17
Hình 12 Kiểm tra thành công .....	18
Hình 13 Tạo luật cho Snort .....	19
Hình 14 Ping đến máy chạy Snort.....	20
Hình 15 Snort nhận được cảnh báo .....	21
Hình 16 Nmap đến máy chạy Snort .....	22
Hình 17 Snort nhận được cảnh báo .....	23
Hình 18 Hping đến máy chạy Snort.....	24
Hình 19 Snort nhận được cảnh báo .....	24

## DANH MỤC CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Thuật ngữ tiếng Anh/Giải thích</b>	<b>Thuật ngữ tiếng Việt/Giải thích</b>
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
HIDS	Host-based Intrusion Detection System	IDS dựa trên máy chủ
NIDS	Network-based Intrusion Detection System	IDS dựa trên mạng
SIEM	Security Information and Event Management	Quản lý thông tin và sự kiện bảo mật
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tải
ICMP	Internet Control Message Protocol	Giao thức kiểm soát tin nhắn Internet
SYN	Synchronize	Gói tin đồng bộ trong quá trình bắt tay ba bước của TCP

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## 1.1 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.

## 1.2 Tìm hiểu lý thuyết

### 1.2.1 Hệ thống phát hiện tấn công, xâm nhập

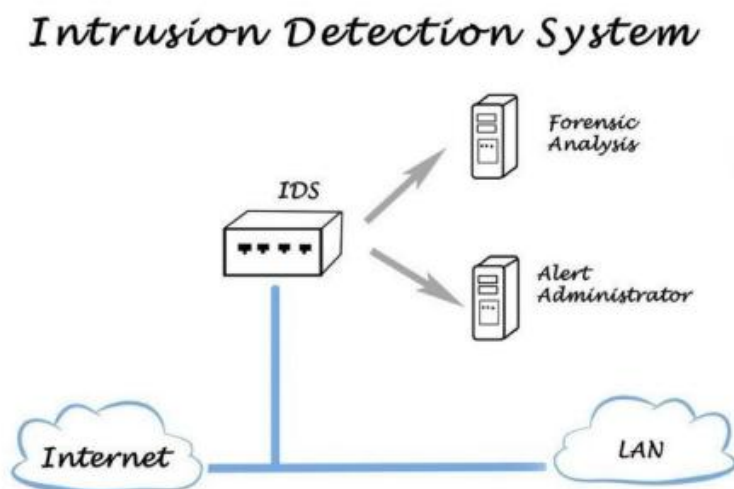
#### 1.2.1.1 Khái quát

Hệ thống phát hiện xâm nhập (IDS) là một công cụ bảo mật mạng dùng để giám sát lưu lượng mạng và các thiết bị để phát hiện hoạt động độc hại, hoạt động đáng ngờ hoặc vi phạm chính sách bảo mật.

IDS có thể giúp tăng tốc và tự động hóa việc phát hiện mối đe dọa mạng bằng cách cảnh báo người quản trị bảo mật về các mối đe dọa đã biết hoặc tiềm ẩn hoặc bằng cách gửi cảnh báo đến một công cụ bảo mật tập trung. Một công cụ bảo mật tập trung như hệ thống quản lý sự kiện và thông tin bảo mật (SIEM) có thể kết hợp dữ liệu từ các nguồn khác để giúp các nhóm bảo mật xác định và ứng phó với các mối đe dọa mạng có thể bị các biện pháp bảo mật khác bỏ qua.

IDS cũng có thể hỗ trợ các nỗ lực tuân thủ. Một số quy định, chẳng hạn như Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI-DSS), yêu cầu các tổ chức triển khai các biện pháp phát hiện xâm nhập.

IDS không thể tự mình ngăn chặn các mối đe dọa bảo mật. Ngày nay, các khả năng của IDS thường được tích hợp hoặc kết hợp vào các hệ thống phòng ngừa xâm nhập (IPS), có thể phát hiện các mối đe dọa bảo mật và tự động hành động để ngăn chặn chúng.



Hình 1 Sơ đồ vị trí của IDS trong hệ thống mạng

### 1.2.1.2 Phân loại

IDS được phân loại dựa trên vị trí chúng được đặt trong hệ thống và loại hoạt động chúng theo dõi.

Hệ thống phát hiện xâm nhập mạng (NIDS) giám sát lưu lượng truy cập vào và ra đến các thiết bị trên toàn mạng. NIDS được đặt tại các điểm chiến lược trong mạng, thường ngay sau tường lửa ở chu vi mạng để có thể đánh dấu bất kỳ lưu lượng truy cập độc hại nào đột nhập.

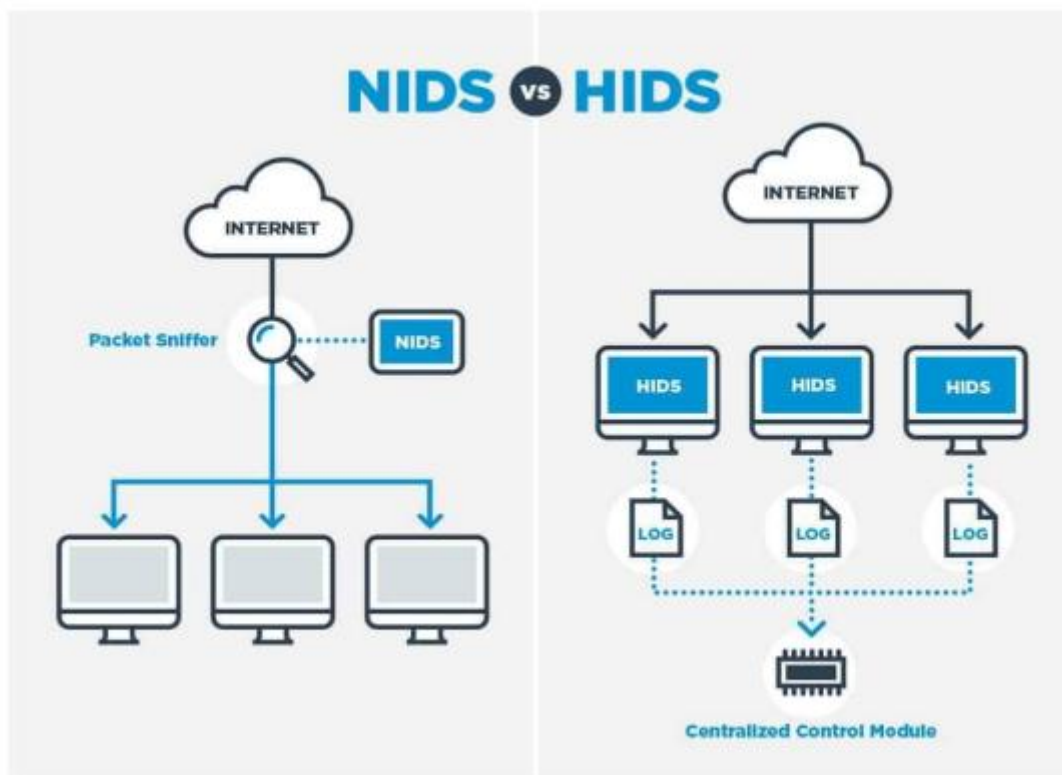
NIDS cũng có thể được đặt bên trong mạng để bắt các mối đe dọa nội bộ hoặc tin tặc đã chiếm đoạt tài khoản người dùng. Ví dụ, NIDS có thể được đặt sau mỗi tường lửa nội bộ trong một mạng phân đoạn để giám sát lưu lượng truyền giữa các mạng con.

Để tránh cản trở luồng lưu lượng hợp lệ, NIDS thường được đặt "ngoài băng tần", nghĩa là lưu lượng không đi trực tiếp qua nó. NIDS phân tích các bản sao của các gói mạng thay vì chính các gói đó. Theo cách đó, lưu lượng hợp lệ không phải chờ phân tích, nhưng NIDS vẫn có thể bắt và đánh dấu lưu lượng độc hại.

Hệ thống phát hiện xâm nhập máy chủ (HIDS) được cài đặt trên một điểm cuối cụ thể, như máy tính xách tay, bộ định tuyến hoặc máy chủ. HIDS chỉ giám sát hoạt động trên thiết bị đó, bao gồm lưu lượng truy cập đến và đi từ thiết bị đó. HIDS thường hoạt động bằng cách chụp ảnh nhanh định kỳ các tệp hệ điều hành quan trọng và so sánh các ảnh chụp nhanh này theo thời gian. Nếu HIDS nhận thấy có thay đổi, chẳng hạn như tệp nhật ký bị chỉnh sửa hoặc cấu hình bị thay đổi, nó sẽ cảnh báo nhóm bảo mật.

Các nhóm bảo mật thường kết hợp các hệ thống phát hiện xâm nhập dựa trên mạng và các hệ thống phát hiện xâm nhập dựa trên máy chủ. NIDS xem xét lưu lượng truy cập nói chung, trong khi HIDS có thể tăng cường bảo vệ xung quanh các tài sản có giá trị cao. HIDS cũng có thể giúp phát hiện hoạt động độc hại từ một nút mạng bị xâm phạm, như ransomware lây lan từ một thiết bị bị nhiễm.

Trong khi NIDS và HIDS là phổ biến nhất, các nhóm bảo mật có thể sử dụng các IDS khác cho các mục đích chuyên biệt. IDS dựa trên giao thức (PIDS) giám sát các giao thức kết nối giữa máy chủ và thiết bị. PIDS thường được đặt trên máy chủ web để giám sát các kết nối HTTP hoặc HTTPS.



Hình 2 Hoạt động của NIDS và HIDS

#### 1.2.1.3 Các kỹ thuật phát hiện xâm nhập

##### - Phát hiện dựa trên chữ ký

Phát hiện dựa trên chữ ký phân tích các gói tin mạng để tìm chữ ký tấn công - các đặc điểm hoặc hành vi riêng biệt liên quan đến một mối đe dọa cụ thể. Một chuỗi mã xuất hiện trong một biến thể phần mềm độc hại cụ thể là một ví dụ về chữ ký tấn công.

IDS dựa trên chữ ký duy trì cơ sở dữ liệu về các chữ ký tấn công mà nó so sánh với các gói tin mạng. Nếu một gói tin kích hoạt một sự trùng khớp với một trong các chữ ký, IDS sẽ đánh dấu nó. Để có hiệu quả, cơ sở dữ liệu chữ ký phải được cập nhật thường xuyên với thông tin tình báo về mối đe dọa mới khi các cuộc tấn công mạng mới xuất hiện và các cuộc tấn công hiện tại phát triển. Các cuộc tấn công hoàn toàn mới chưa được phân tích để tìm chữ ký có thể tránh được IDS dựa trên chữ ký.

##### - Phát hiện dựa trên sự bất thường

Các phương pháp phát hiện dựa trên bất thường sử dụng máy học để tạo ra và liên tục tinh chỉnh một mô hình cơ sở của hoạt động mạng bình thường. Sau đó, nó so sánh hoạt động mạng với mô hình và đánh dấu các độ lệch, chẳng hạn như một quy trình sử dụng nhiều băng thông hơn bình thường hoặc một thiết bị mở một cổng

Vì báo cáo bất kỳ hành vi bất thường nào, IDS dựa trên bất thường thường có thể phát hiện các cuộc tấn công mạng mới có thể tránh được phát hiện dựa trên chữ ký. Ví dụ, IDS dựa trên bất thường có thể phát hiện các khai thác zero-day các cuộc tấn công lợi dụng lỗ

hồng phần mềm trước khi nhà phát triển phần mềm biết về chúng hoặc có thời gian để vá chúng

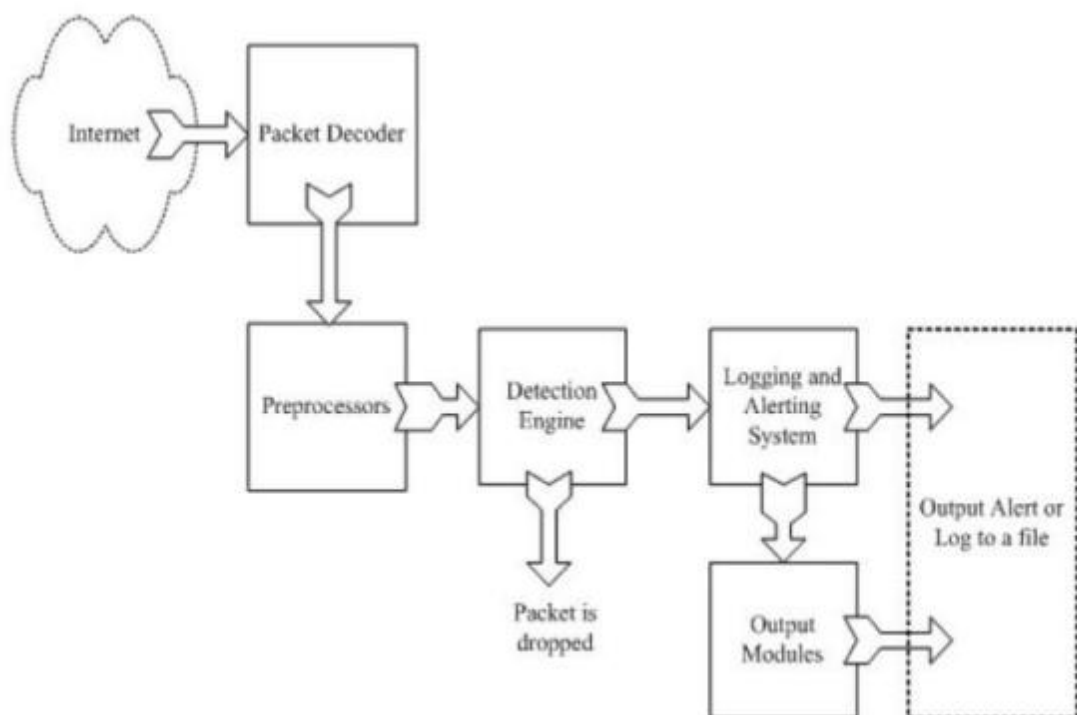
## **1.2.2 Kiến trúc và tính năng một số hệ thống phát hiện tấn công, xâm nhập**

### **1.2.2.1 Snort**

Snort là một NIDS được Martin Roesh phát triển dưới mô hình mã nguồn mở. Tuy Snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời mà không phải sản phẩm thương mại nào cũng có thể có được. Với kiến trúc thiết kế theo kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình bằng việc cài đặt hay viết thêm mới các module. Cơ sở dữ liệu luật của Snort đã lên tới 2930 luật và được cập nhật thường xuyên bởi một cộng đồng người sử dụng. Snort có thể chạy trên nhiều hệ thống nền như Windows, Linux, OpenBSD, FreeBSD, NetBSD, Solaris, HP-UX, AIX, IRIX, MacOS.+

Snort được chia thành nhiều thành phần. Những thành phần này làm việc với nhau để phát hiện các cách tấn công cụ thể và tạo ra output theo một định dạng được yêu cầu. Snort gồm các thành phần chính sau:

- Module giải mã gói tin
- Module tiền xử lý
- Module phát hiện
- Module log và cảnh báo
- Module kết xuất thông tin



*Hình 3 Kiến trúc của Snort*



Khi Snort hoạt động, nó lắng nghe và bắt các gói tin. Gói tin sau khi qua module giải mã và tiền xử lý sẽ vào module phát hiện. Nếu phát hiện xâm nhập, gói tin sẽ được đưa vào module Log và cảnh báo. Module kết xuất sẽ tạo cảnh báo theo định dạng yêu cầu.

Cấu trúc luật của Snort:

Ví dụ: *alert tcp 192.168.0.0/22 23 -> any any (content:"confidential"; msg: "Detected confidential")*

Ta thấy cấu trúc có dạng sau: |Rule Header| Rule Option| |

Phần Header: chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa tiêu chuẩn để áp dụng luật với gói tin đó.

*alert tcp 192.168.0.0/22 23 -> any any*

Phần Option: chứa thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Phần Option chứa các tiêu chuẩn phụ thêm để đối sánh với gói tin.

*any (content:"confidential"; msg: "Detected confidential")*

#### 1.2.2.2 Wazuh

Wazuh là một nền tảng mã nguồn mở với các chức năng security detection (phát hiện lỗ hổng bảo mật), visibility (tăng cường khả năng quan sát), và compliance monitoring (giám sát tuân thủ các quy định và tiêu chuẩn an ninh thông tin). Wazuh ban đầu được phát triển dựa trên OSSEC HIDS và sau đó được tích hợp thêm Elastic Stack cùng với OpenSCAP để trở thành một giải pháp an ninh toàn diện với nhiều khả năng.

Chức năng chính:

- Giám sát an ninh: Wazuh giám sát các sự kiện và hành động trên hệ thống để phát hiện các hoạt động bất thường.
- Phân tích nhật ký: Hệ thống có khả năng thu thập và phân tích nhật ký từ nhiều nguồn khác nhau, giúp phát hiện các mối đe dọa tiềm ẩn.
- Quản lý tuân thủ: Hỗ trợ các tiêu chuẩn tuân thủ như PCI-DSS, GDPR và HIPAA.

Kiến trúc:

- Wazuh Agent: Cài đặt trên các máy chủ hoặc thiết bị đầu cuối để thu thập dữ liệu và gửi về máy chủ Wazuh
- Wazuh Manager: Xử lý dữ liệu thu thập từ các agent và thực hiện phân tích.
- Wazuh API: Cho phép tích hợp với các ứng dụng khác và cung cấp giao diện lập trình cho người dùng

Tính năng nổi bật:

- Phát hiện xâm nhập: Sử dụng quy tắc và mô hình để phát hiện các xâm nhập vào hệ thống.

- Quản lý sự kiện: Tích hợp với Elasticsearch và Kibana để phân tích và hiển thị dữ liệu theo thời gian thực.
- Cảnh báo: Gửi thông báo khi phát hiện các hành vi bất thường hoặc sự cố bảo mật.

Công cụ hỗ trợ:

- Tích hợp dễ dàng với các công cụ như Elastic Stack, Grafana, và nhiều giải pháp bảo mật khác.

Tính khả dụng:

- Wazuh là mã nguồn mở, cho phép người dùng tự do tùy chỉnh và phát triển dựa trên nhu cầu của tổ chức.

Wazuh được sử dụng rộng rãi trong nhiều lĩnh vực khác nhau, từ doanh nghiệp đến chính phủ, nhờ vào tính linh hoạt và khả năng mở rộng của nó.

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

### 2.1 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>

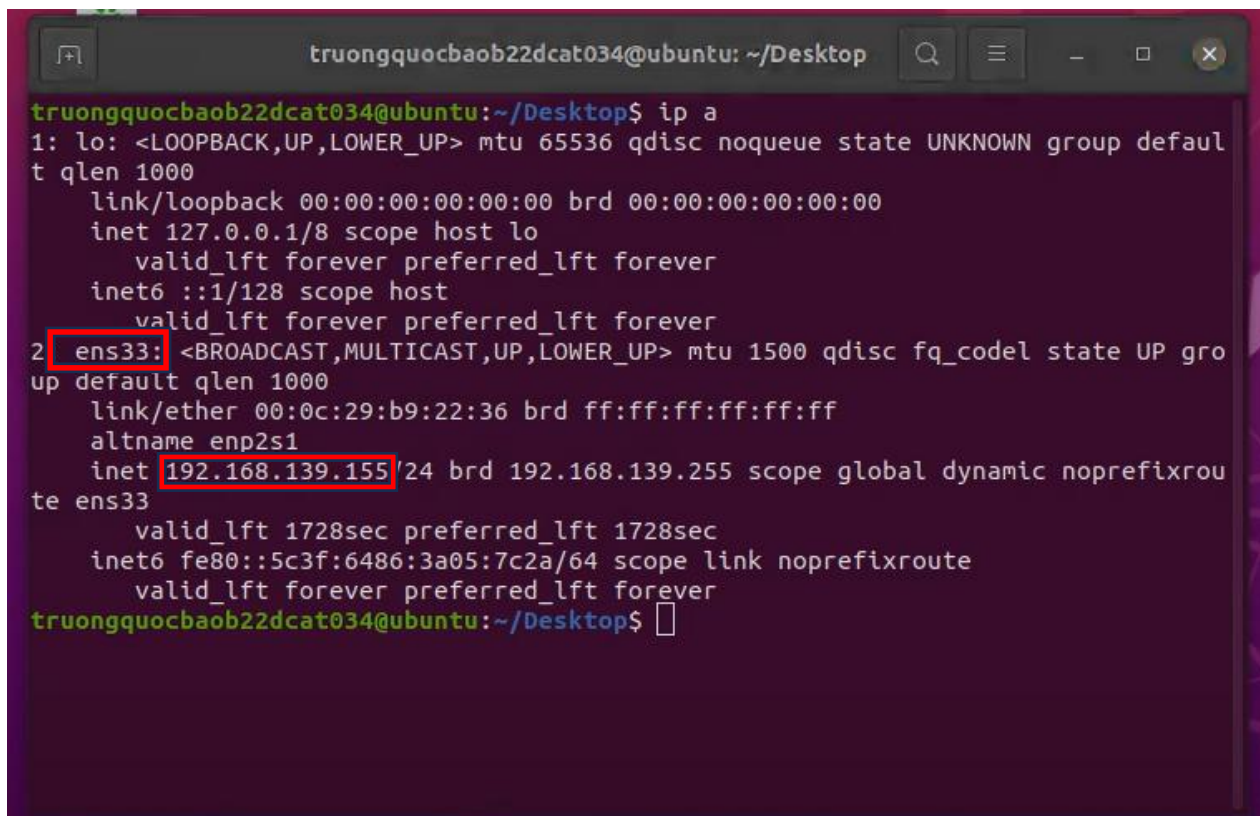
### 2.2 Các bước thực hiện

#### 2.2.1 Cài đặt Snort

Tiến hành cài đặt các máy ảo Kali Linux, Ubuntu Linux như trong các bài thực hành trước.

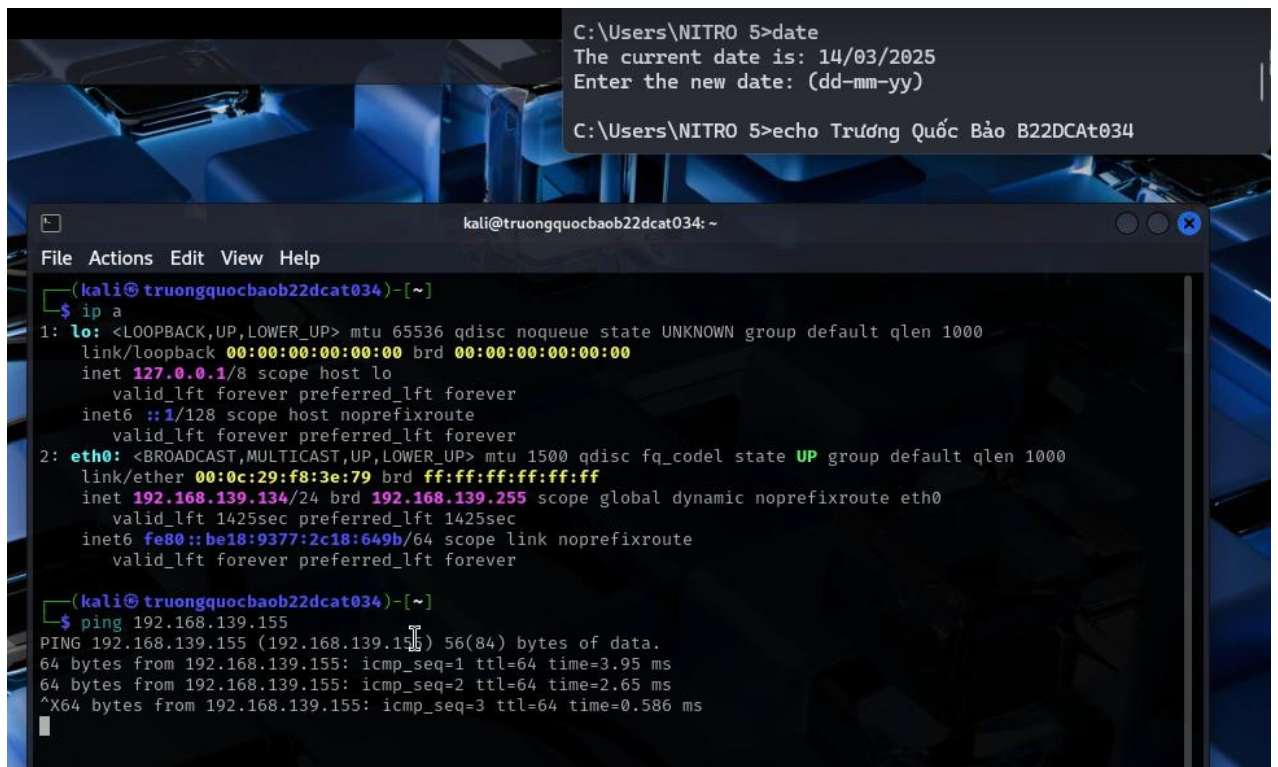
Đảm bảo có địa chỉ IP hợp lệ và có kết nối mạng LAN.

Kiểm tra ping thử giữa các máy để đảm bảo kết nối và cài đặt thành công.



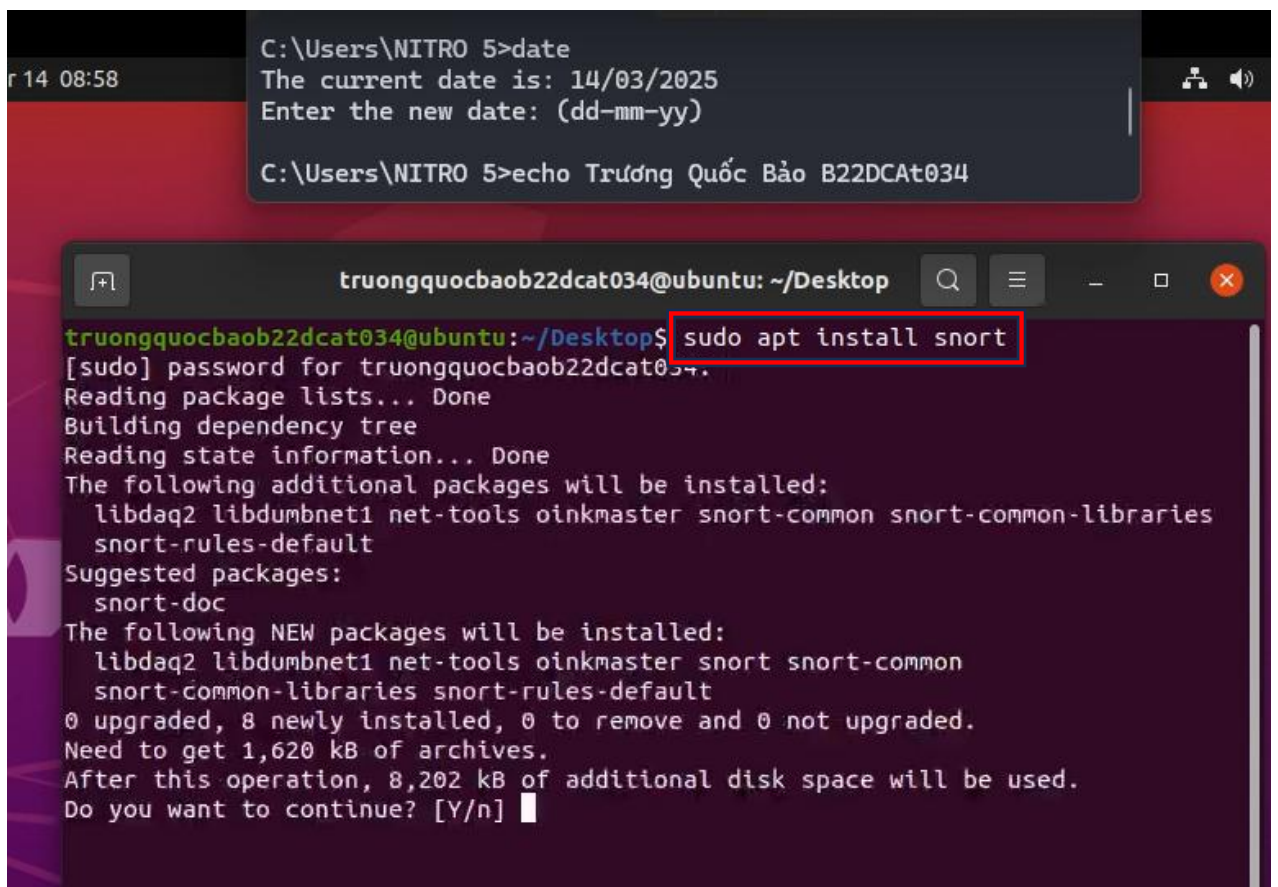
```
truongquocbaob22dcat034@ubuntu: ~/Desktop
truongquocbaob22dcat034@ubuntu:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        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:b9:22:36 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.139.155/24 brd 192.168.139.255 scope global dynamic noprefixroute ens33
        valid_lft 1728sec preferred_lft 1728sec
    inet6 fe80::5c3f:6486:3a05:7c2a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
truongquocbaob22dcat034@ubuntu:~/Desktop$
```

Hình 4 Địa chỉ IP của máy Ubuntu cài đặt Snort



Hình 5 Địa chỉ IP máy Kali tấn công

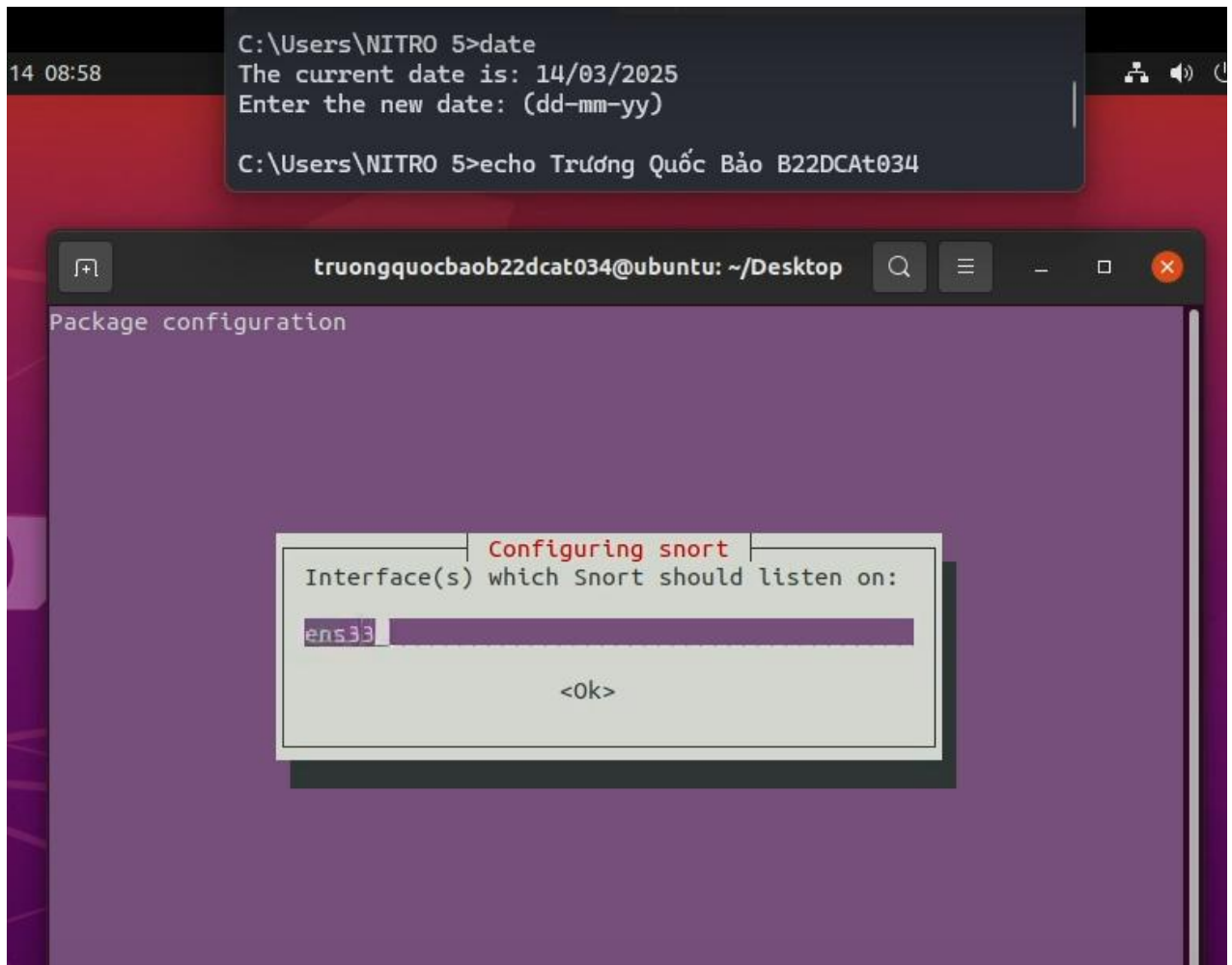
Tiến hành cài đặt Snort bằng lệnh “sudo apt install snort”



Hình 6 Cài đặt Snort

Lựa chọn cấu hình giao diện mạng để Snort bắt các gói tin trong quá trình cài đặt Snort.

Kiểm tra bằng lệnh “ip a” hoặc “ifconfig” trên máy Ubuntu Linux xem giao diện mạng nào đang được sử dụng. Ở đây là “ens33”



*Hình 7 Chọn giao diện mạng để bắt gói tin*

Sau khi cài đặt hoàn tất, kiểm tra phiên bản của Snort bằng lệnh “snort --version”. Nếu thấy logo con lợn và thông tin phiên bản tức là đã cài đặt thành công.



```
C:\Users\NITRO 5>date
The current date is: 14/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo B22DCat034

truongquocbaob22dcat034@ubuntu: ~/Desktop
Unpacking oinkmaster (2.0-4) ...
Setting up oinkmaster (2.0-4) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up snort-common (2.9.7.0-5build1) ...
Setting up libdaq2 (2.0.4-3build2) ...
Setting up libdumbnet1:amd64 (1.12-9build1) ...
Setting up snort-rules-default (2.9.7.0-5build1) ...
Setting up snort-common-libraries (2.9.7.0-5build1) ...
Setting up snort (2.9.7.0-5build1) ...
Processing triggers for systemd (245.4-4ubuntu3.24) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.17) ...
truongquocbaob22dcat034@ubuntu:~/Desktop$ snort --version

o''_
o''_~
''''

-*> Snort! <*-
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 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

truongquocbaob22dcat034@ubuntu:~/Desktop$
```

Hình 8 Cài đặt Snort thành công

Kiểm tra trạng thái hoạt động của Snort bằng lệnh “systemctl status snort”, nếu thấy chữ màu xanh “active (running)” là thành công. Hoặc có thể active bằng lệnh “systemctl start snort”.

```
C:\Users\NITRO 5>date
The current date is: 14/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo B22DCat034

truongquocbaob22dcat034@ubuntu: ~/Desktop
truongquocbaob22dcat034@ubuntu:~/Desktop$ systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
   Loaded: loaded (/etc/systemd/system/snort.service; generated)
   Active: active (running) since Fri 2025-03-14 08:59:38 PDT; 29s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 2 (limit: 4538)
   Memory: 144.2M
    CGroup: /system.slice/snort.service
            └─2266 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g >

Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_REPUTATI>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_GTP Ver>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_POP Ver>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_SSH Ver>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_DNP3 Ve>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_IMAP Ve>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_SIP Ver>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_FTPTELNE>
Mar 14 08:59:38 ubuntu snort[2266]: Preprocessor Object: SF_SSLPP V>
Mar 14 08:59:38 ubuntu snort[2266]: Commencing packet processing (pid=2266)

[1]+  Stopped                  systemctl status snort
truongquocbaob22dcat034@ubuntu:~/Desktop$
```

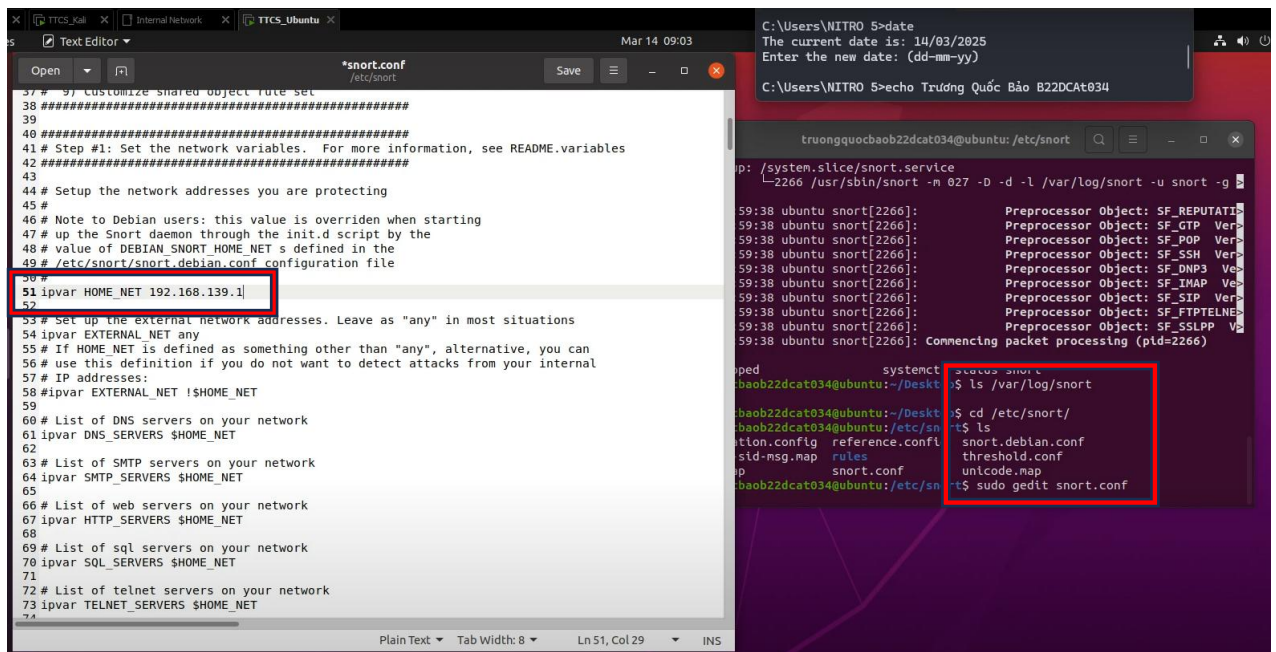
Hình 9 Kiểm tra trạng thái hoạt động của Snort

### 2.2.2 Cấu hình và tạo luật Snort

Cấu hình cho Snort ở đường dẫn tệp “/etc/snort/snort.conf”

Chỉnh sửa địa chỉ IP của HOME\_NET thành dải địa chỉ IP của máy Ubuntu và Linux đang sử dụng chung mạng LAN. Ở đây là “192.168.139.1/24”

Lưu lại để hoàn tất.



Hình 10 Cấu hình cho Snort

Ta kiểm tra cấu hình đúng hay chưa bằng lệnh “sudo snort -T -t ens33 -c /etc/snort/snort.conf”

-T → Chế độ kiểm tra cấu hình (Test Mode), không thực thi.

-t ens33 → Chỉ định giao diện mạng (ens33) để Snort kiểm tra.

-c /etc/snort/snort.conf → Sử dụng file cấu hình /etc/snort/snort.conf.

Snort sẽ chạy thử ở “test mode” để áp dụng cấu hình vừa cài đặt.

Nếu không có lỗi xảy ra, ta nhận được thông báo thành công.



```
Mar 14 09:05 C:\Users\NITRO 5>date
The current date is: 14/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo B22DCat034

truongquocbaob22dcat034@ubuntu: /etc/snort
ataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this plat
form. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
truongquocbaob22dcat034@ubuntu: /etc/snort$ sudo -T -i ens33 -c /etc/snort/snort.conf
sudo: -i: invalid timeout value
sudo: unable to initialize policy plugin
truongquocbaob22dcat034@ubuntu: /etc/snort$ sudo snort -T -i ens33 -c /etc/snort/snort.conf
Running in Test mode

---== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 303
7 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000:8008 8014 8028 8080 8085 8
088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 1137
1 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301
2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 802
8 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9
443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libs_f_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
```

Hình 11 Kiểm tra thông tin cấu hình

```
Mar 14 09:05 C:\Users\NITRO 5>date
The current date is: 14/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo B22DCAt034

truongquocbaob22dcatt034@ubuntu: /etc/snort
Patterns      : 0.51
Match Lists   : 1.02
DFA
  1 byte states : 1.02
  2 byte states : 14.05
  4 byte states : 0.00
-----
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".

--== Initialization Complete ==--

o"~)~
'~~~
-*> Snort! <*-
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 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

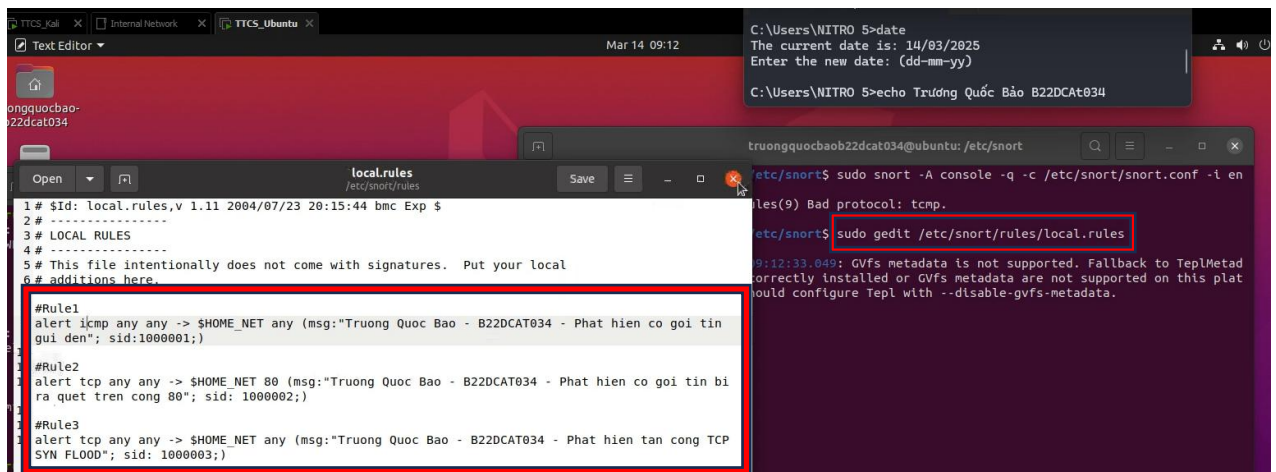
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>

Snort successfully validated the configuration!
Snort exiting
```

Hình 12 Kiểm tra thành công

Ta sẽ cấu hình các luật để nhận cảnh báo khi bị tấn công như sau:

- Di chuyển đến đường dẫn “/etc/snort/rules/local.rules”
- Sử dụng text editor như gedit để cấu hình luật
- Ta tạo 3 luật để Snort phát hiện tấn công như bên dưới:
- Lưu lại để hoàn thành.
- Khởi chạy giám sát trên terminal bằng lệnh “sudo snort -A console -q -c /etc/snort/snort.conf -i ens33”. Lệnh này cho phép ta xem các cảnh báo khi bị tấn công sau khi cấu hình.



Hình 13 Tạo luật cho Snort

Giải thích các lệnh:

- Rule1:

Đưa ra cảnh báo (“alert”) với thông điệp (“msg”) về các gói tin ICMP từ bất kỳ địa chỉ IP nào (“any”) từ bất kỳ cổng nào (“any”) đến (“->”) địa chỉ IP của “HOME\_NET” từ bất kỳ cổng nào (“any”).

- Rule2:

Đưa ra cảnh báo (“alert”) với thông điệp (“msg”) về các gói tin TCP từ bất kỳ địa chỉ IP nào (“any”) từ bất kỳ cổng nào (“any”) đến (“->”) địa chỉ IP của “HOME\_NET” trên cổng 80.

- Rule3:

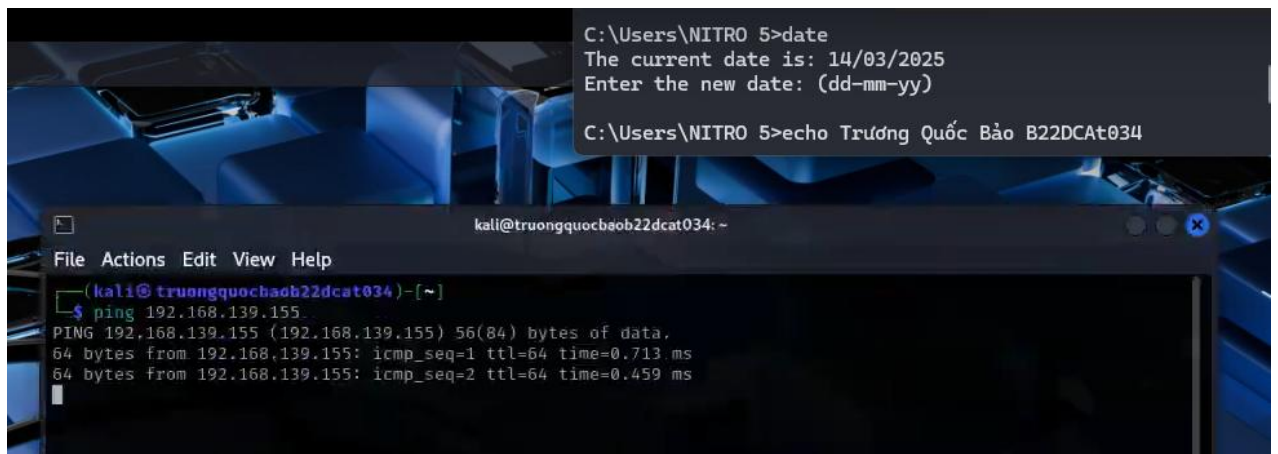
Đưa ra cảnh báo (“alert”) với thông điệp (“msg”) về các gói tin TCP từ bất kỳ địa chỉ IP nào (“any”) từ bất kỳ cổng nào (“any”) đến (“->”) địa chỉ IP của “HOME\_NET” từ bất kỳ cổng nào (“any”).

### 2.2.3 Thực hiện tấn công và phát hiện sử dụng Snort

Sử dụng lệnh “sudo snort -A console -q -c /etc/snort/snort.conf -i ens33” để mở terminal giám sát.

Thực hiện tấn công thứ nhất:

- Từ máy Kali, sử dụng lệnh ping để ping máy Snort. Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.



*Hình 14 Ping đến máy chạy Snort*

Máy Snort đã nhận được thông báo về gói tin ICMP do lệnh Ping từ máy Kali như đã cấu hình ở luật Rule1.



```
Mar 14 09:13 C:\Users\NITRO 5>date
The current date is: 14/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo B22DCAT034

truongquocbaob22dcat034@ubuntu: /etc/snort
s33
ERROR: /etc/snort/rules/local.rules(9) Bad protocol: tcmp.
Fatal Error, Quitting..
truongquocbaob22dcat034@ubuntu:/etc/snort$ sudo gedit /etc/snort/rules/local.rules

(gedit:3635): Tepl-WARNING **: 09:12:33.049: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata

truongquocbaob22dcat034@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -i ens33

03/14-09:13:06.980975 [**] [1:1000001:0] Trương Quốc Bảo - B22DCAT034 - Phát hiện có gói tin gửi đến [**] [Priority: 0] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:06.980975 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:06.981000 [**] [1:1000001:0] Trương Quốc Bảo - B22DCAT034 - Phát hiện có gói tin gửi đến [**] [Priority: 0] {ICMP} 192.168.139.155 -> 192.168.139.134
03/14-09:13:06.981000 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.155 -> 192.168.139.134
03/14-09:13:07.988945 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:07.988945 [**] [1:1000001:0] Trương Quốc Bảo - B22DCAT034 - Phát hiện có gói tin gửi đến [**] [Priority: 0] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:07.988945 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:07.988973 [**] [1:1000001:0] Trương Quốc Bảo - B22DCAT034 - Phát hiện có gói tin gửi đến [**] [Priority: 0] {ICMP} 192.168.139.155 -> 192.168.139.134
03/14-09:13:07.988973 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.155 -> 192.168.139.134
03/14-09:13:09.012996 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:09.012996 [**] [1:1000001:0] Trương Quốc Bảo - B22DCAT034 - Phát hiện có gói tin gửi đến [**] [Priority: 0] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:09.012996 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.134 -> 192.168.139.155
03/14-09:13:09.013023 [**] [1:1000001:0] Trương Quốc Bảo - B22DCAT034 - Phát hiện có gói tin gửi đến [**] [Priority: 0] {ICMP} 192.168.139.155 -> 192.168.139.134
03/14-09:13:09.013023 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.139.155 -> 192.168.139.134
```

Hình 15 Snort nhận được cảnh báo

Thực hiện tấn công số 2:

- Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort (dùng lệnh: `nmap -sV -p80 -A <địa chỉ IP máy Snort>`). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

```
C:\Users\NITRO 5>date
The current date is: 14/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo B22DCat034

kali@truongquocbaob22dc034: ~
File Actions Edit View Help
kali@truongquocbaob22dc034: ~
$ nmap -sV -p80 -A 192.168.135.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 12:18 EDT
Nmap scan report for 192.168.135.155.non-exists.ptr.local (192.168.135.155)
Host is up (0.00026s latency).

PORT      STATE      SERVICE VERSION
80/tcp    filtered  http

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%), IBM i 7.4 (89%), R
eactOS 0.3.7 (89%), Sanyo PLC-XU88 digital video projector (89%), Sonus GSX9000 VoIP proxy (88%), Asus WL-500
gP wireless broadband router (88%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 Enterprise Ed
ition SP2 (88%), Microsoft Windows Server 2003 SP2 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.09 ms  192.168.139.2.non-exists.ptr.local (192.168.139.2)
2   0.70 ms  192.168.135.155.non-exists.ptr.local (192.168.135.155)

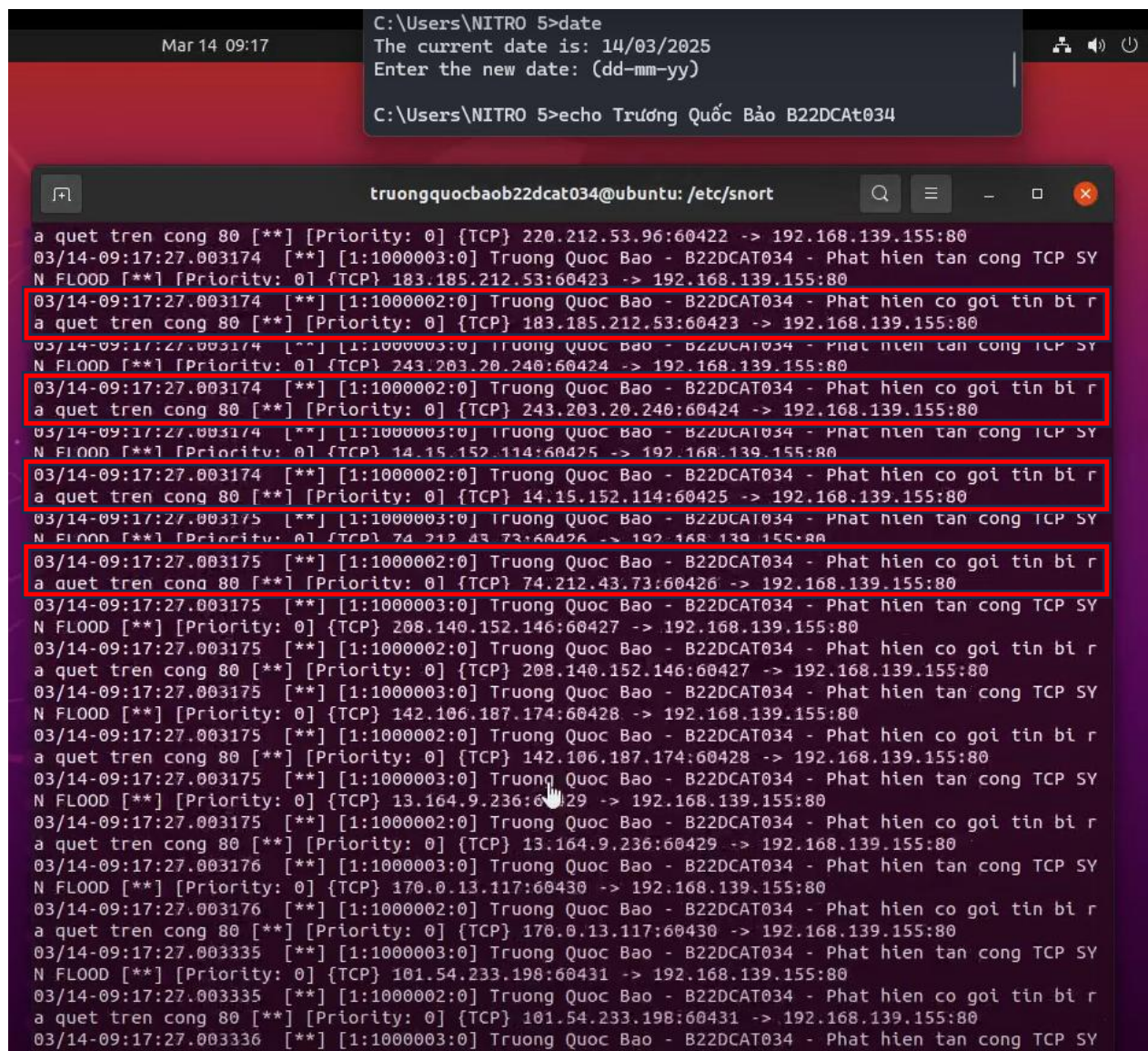
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds

kali@truongquocbaob22dc034: ~
$
```

*Hình 16 Nmap đến máy chạy Snort*

Máy Snort đã nhận được cảnh báo về gói tin bị rà quét trên cổng 80.





Hình 17 Snort nhận được cảnh báo

Thực hiện tấn công số 3:

- Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort (dùng lệnh: `hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source <địa chỉ IP máy Snort>`). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.







## **TÀI LIỆU THAM KHẢO**

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 2020.
- [4] Snort: <https://www.snort.org/#documents>
- [5] Wazuh: <https://documentation.wazuh.com/current/index.html>