

**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:

B22DCAT063 Lê Tiến Dương

Giảng viên hướng dẫn: PGS. TS. Hoàng Xuân Dậu

**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> Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập, phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.....	5
<b>1.2.2</b> Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập: Snort, OSSEC.....	8
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</b> .....	<b>13</b>
2.1 Chuẩn bị môi trường .....	13
2.2 Các bước thực hiện.....	13
<b>2.2.1</b> Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.1.....	13
<b>2.2.2</b> Bước 2: Tải, cài đặt và chạy thử Snort.....	14
<b>2.2.3</b> Bước 3: Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống.....	17
<b>2.2.4</b> Bước 4: Thực thi tấn công và phát hiện sử dụng Snort.....	18
TÀI LIỆU THAM KHẢO .....	22

## DANH MỤC CÁC HÌNH VẼ

Hình 1 – Hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System).....	5
Hình 2 – Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký.....	6
Hình 3 – Phát hiện xâm nhập dựa trên bất thường.....	7
Hình 4 – Kiến trúc của Snort.....	8
Hình 5 – Kiến trúc của Ossec.....	11
Hình 6 – Đổi tên và kiểm tra IP máy Kali Linux .....	13
Hình 7 – Đổi tên và kiểm tra IP máy cài Snort .....	14
Hình 8 – Tải Snort.....	14
Hình 9 – Kiểm tra phiên bản của Snort.....	15
Hình 10 – Kiểm tra trạng thái hoạt động của Snort .....	15
Hình 11 – Chạy thử Snort .....	16
Hình 12 – Kiểm tra log của Snort .....	16
Hình 13 – Tạo thêm luật trong file cấu hình .....	17
Hình 14 – Kiểm tra cấu hình Snort .....	18
Hình 15 – Kiểm tra lại địa chỉ IP máy cài Snort .....	18
Hình 16 – Ping từ máy Kali sang máy cài Snort.....	19
Hình 17 – Kiểm tra kết quả trên máy Snort .....	19
Hình 18 – Từ máy Kali sử dụng công cụ nmap .....	20
Hình 19 – Trên máy Snort kiểm tra kết quả.....	20
Hình 20 – Từ máy Kali sử dụng công cụ hping3 .....	21
Hình 21 – Kiểm tra kết quả trên máy Snort .....	21

## 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	Hệ thống phát hiện xâm nhập dựa trên máy chủ
NIDS	Network-based Intrusion Detection System	Hệ thống phát hiện xâm nhập dựa trên mạng
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
OSSEC	Open Source Security	Phần mềm mã nguồn mở phát hiện xâm nhập dựa trên máy chủ
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tải

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## 1.1 Mục đích

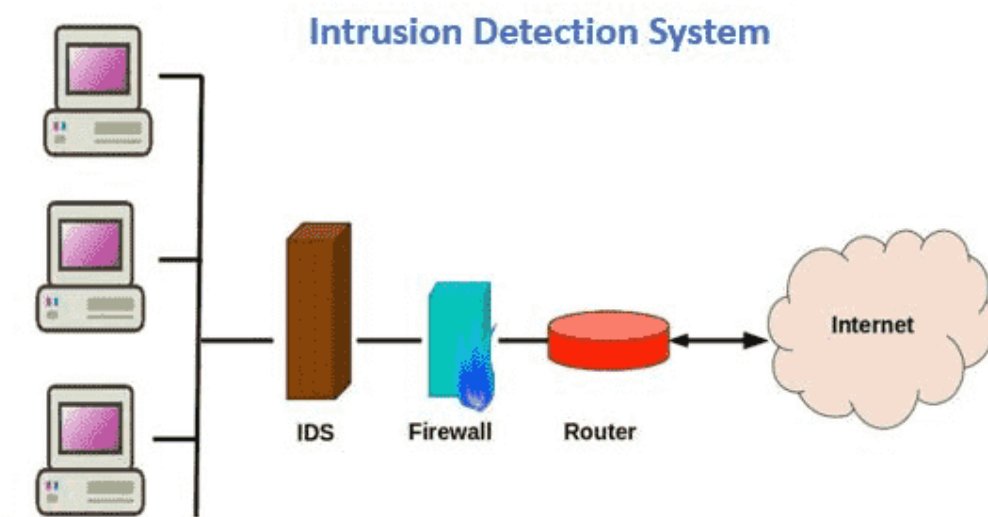
Mục đích của bài thực hành “2.2: Tìm hiểu và cài đặt NIDS” là rèn luyện kỹ năng cài đặt và vận hành hệ thống phát hiện xâm nhập cho host (HIDS) và cho mạng (NIDS). Luyện tập việc tạo và chỉnh sửa các luật phát hiện tấn công, xâm nhập cho các hệ thống phát hiện xâm nhập thông dụng.

## 1.2 Tìm hiểu lý thuyết

**1.2.1 Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập, phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.**

### 1.2.1.1 Tổng quan về hệ thống phát hiện tấn công, xâm nhập

Hệ thống phát hiện xâm nhập (IDS - Intrusion Detection System) là một giải pháp bảo mật giúp phát hiện các cuộc tấn công hoặc hành vi đáng ngờ trong hệ thống mạng hoặc thiết bị. IDS không chặn mà chỉ cảnh báo cho quản trị viên khi có mối đe dọa.



Hình 1 – Hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System)

Nhiệm vụ chính của các hệ thống IDS bao gồm:

- Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập.
- Khi phát hiện các hành vi tấn công, xâm nhập, thì ghi logs các hành vi này cho phân tích bổ sung sau này.
- Gửi thông báo cho người quản trị về các hành vi tấn công, xâm nhập đã phát hiện được.

Nói tóm lại, IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh báo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

### 1.2.1.2 Phân loại các hệ thống phát hiện xâm nhập

IDS được chia thành hai loại chính:

- *HIDS (Host-based Intrusion Detection System)*: Giám sát các tệp log, thay đổi file, tiến trình, và các hoạt động khác trên một hệ thống máy chủ cụ thể.
- *NIDS (Network-based Intrusion Detection System)*: Giám sát lưu lượng mạng để phát hiện các cuộc tấn công bằng cách phân tích gói tin.

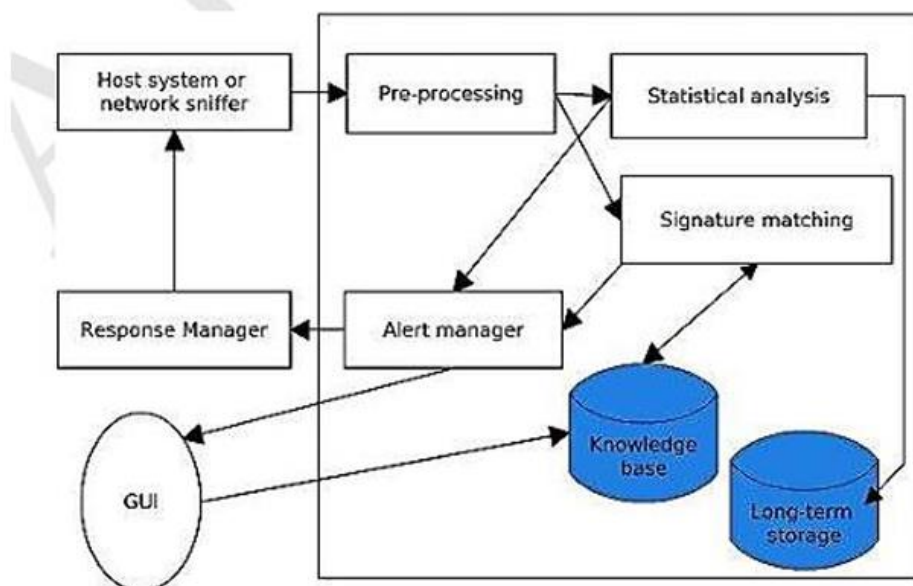
Theo phương pháp phân tích dữ liệu, có 2 kỹ thuật phân tích chính, gồm:

- *Phát hiện xâm nhập dựa trên chữ ký, hoặc phát hiện sự lạm dụng* (Signature-based / misuse intrusion detection).
- *Phát hiện xâm nhập dựa trên các bất thường* (Anomaly intrusion detection).

### 1.2.1.3 Các kỹ thuật phát hiện xâm nhập

- **Phát hiện xâm nhập dựa trên chữ ký**

Phát hiện xâm nhập dựa trên chữ ký trước hết cần xây dựng cơ sở dữ liệu các chữ ký, hoặc các dấu hiệu của các loại tấn công, xâm nhập đã biết. Hầu hết các chữ ký, dấu hiệu được nhận dạng và mã hóa thủ công và dạng biểu diễn thường gặp là các luật phát hiện (Detection rule). Bước tiếp theo là sử dụng cơ sở dữ liệu các chữ ký để giám sát các hành vi của hệ thống, hoặc mạng, và cảnh báo nếu phát hiện chữ ký của tấn công, xâm nhập. Hình dưới đây biểu diễn lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký điển hình, trong đó Knowledge base là cơ sở dữ liệu lưu các chữ ký tấn công, xâm nhập.



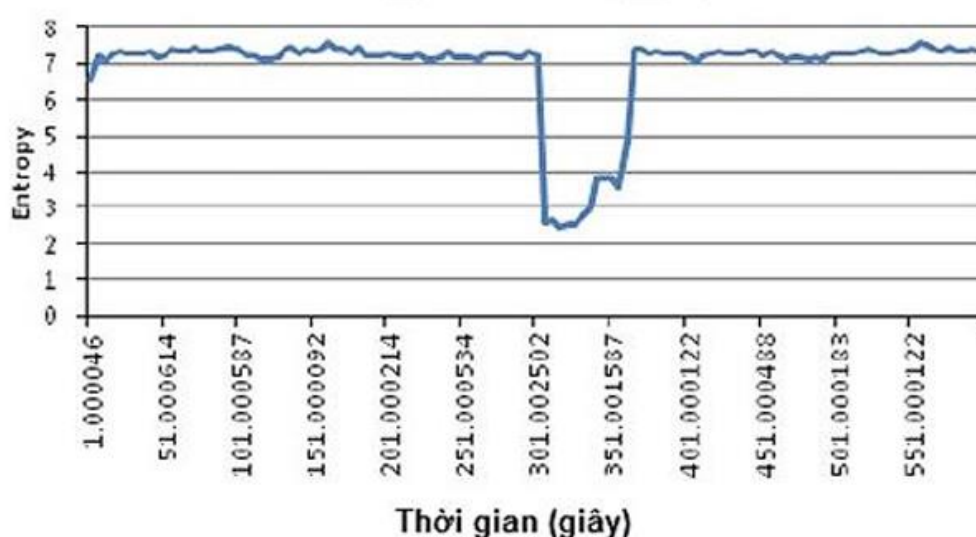
Hình 2 – Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký

Ưu điểm lớn nhất của phát hiện xâm nhập dựa trên chữ ký là có khả năng phát hiện các tấn công, xâm nhập đã biết một cách hiệu quả. Ngoài ra, phương pháp này cho tốc độ xử lý cao, đồng thời yêu cầu tài nguyên tính toán tương đối thấp. Nhờ vậy, các hệ thống phát hiện

xâm nhập dựa trên chữ ký được ứng dụng rộng rãi trong thực tế. Tuy nhiên, nhược điểm chính của phương pháp này là không có khả năng phát hiện các tấn công, xâm nhập mới, do chữ ký của chúng chưa tồn tại trong cơ sở dữ liệu các chữ ký. Hơn nữa, phương pháp này cũng đòi hỏi nhiều công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký, dấu hiệu của các tấn công, xâm nhập.

- **Phát hiện xâm nhập dựa trên bất thường**

Phát hiện xâm nhập dựa trên bất thường dựa trên giả thiết: các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường. Quá trình xây dựng và triển khai một hệ thống phát hiện xâm nhập dựa trên bất thường thường gồm 2 giai đoạn: (1) huấn luyện và (2) phát hiện. Trong giai đoạn huấn luyện, hồ sơ (profile) của đối tượng trong chế độ làm việc bình thường được xây dựng. Để thực hiện giai đoạn huấn luyện, cần giám sát đối tượng trong một khoảng thời gian đủ dài để thu thập được đầy đủ dữ liệu mô tả các hành vi của đối tượng trong điều kiện bình thường làm dữ liệu huấn luyện. Tiếp theo, thực hiện huấn luyện dữ liệu để xây dựng mô hình phát hiện, hay hồ sơ của đối tượng. Trong giai đoạn phát hiện, thực hiện giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và các hành vi lưu trong hồ sơ của đối tượng.



*Hình 3 – Phát hiện xâm nhập dựa trên bất thường*

Hình trên biểu diễn giá trị entropy của IP nguồn của các gói tin theo cửa sổ trượt từ lưu lượng bình thường và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS. Có thể thấy sự khác biệt rõ nét giữa giá trị entropy của lưu lượng bình thường và lưu lượng tấn công và như vậy nếu một ngưỡng entropy được chọn phù hợp ta hoàn toàn có thể phát hiện sự xuất hiện của cuộc tấn công DDoS dựa trên sự thay đổi đột biến của giá trị entropy. Ưu điểm của phát hiện xâm nhập dựa trên bất thường là có tiềm năng phát hiện các loại tấn công, xâm nhập mới mà không yêu cầu biết trước thông tin về chúng. Tuy nhiên, phương pháp này thường có tỷ lệ cảnh báo sai tương đối cao so với phương pháp phát hiện dựa trên chữ ký. Điều này làm giảm khả năng ứng dụng thực tế của phát hiện xâm nhập dựa trên bất thường. Ngoài ra, phương pháp này cũng tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại.

## 1.2.2 Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập: Snort, OSSEC

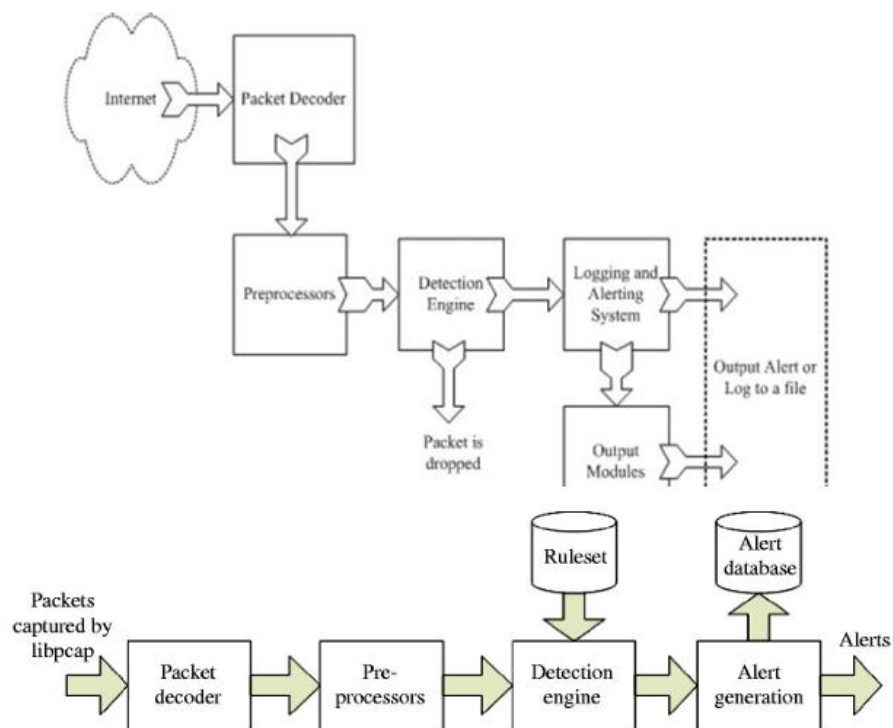
### 1.2.2.1 Snort

- **Giới thiệu**

Snort là một công cụ IDS/IPS, thực hiện giám sát các gói tin ra vào hệ thống.

- Snort là một mã nguồn mở miễn phí với nhiều tính năng trong việc bảo vệ hệ thống bên trong, phát hiện sự tấn công từ bên ngoài vào hệ thống.
- Snort được viết bởi Martin Roesch vào năm 1998. Hiện tại, Snort được phát triển bởi Sourcefire, nơi mà Roesch đang là người sáng lập và CTO, và được sở hữu bởi Cisco từ năm 2013.

- **Kiến trúc của Snort**



Hình 4 – Kiến trúc của Snort

Trong mô hình kiến trúc trên, hệ thống Snort được chia thành 4 phần:

- *Module Decoder*: Xử lý giải mã các gói tin.
- *Module Preprocessors*: Tiền xử lý.
- *Module Detection Engine*: Phát hiện.
- *Module Logging and Alerting System*: Lưu log và cảnh báo.

- **Các luật của Snort**

Cấu trúc của một rule được chia thành 02 phần: **[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.
- *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 này chứa các tiêu chuẩn phụ thêm để đối sánh với gói tin.

Cấu trúc phần Header: **|Action|Protocol|Address|port|Direction|Address|Port|**

- *Action*: Thể hiện hành động sẽ được thực hiện khi một gói tin kích hoạt quy tắc. Trong đó:
  - *alert*: Tạo một cảnh báo và ghi lại gói tin.
  - *log*: Chỉ ghi lại gói tin mà không tạo cảnh báo.
  - *pass*: Bỏ qua gói tin, không thực hiện hành động nào.
  - *activate*: Tạo ra cảnh báo và kích hoạt thêm các luật khác để kiểm tra thêm điều kiện của gói tin.
  - *dynamic*: Đây là luật được gọi bởi các luật khác có Action khai báo là Activate.
- *Protocol*: Xác định loại giao thức của gói tin, ví dụ: TCP, UDP, ICMP, hoặc any (tất cả).
- *Source IP Address*: Địa chỉ IP nguồn của gói tin.
- *Source Port*: Cổng nguồn của gói tin. Có thể là một số cụ thể hoặc từ khoảng cụ thể.
- *Direction Operator*: Thể hiện hướng của gói tin. Có thể là -> (nguồn tới đích) hoặc <- (đích tới nguồn).
- *Destination IP Address*: Địa chỉ IP đích của gói tin.
- *Destination Port*: Cổng đích của gói tin. Cũng có thể là một số cụ thể hoặc từ khoảng cụ thể.

Cấu trúc phần Option:

Phần Option nằm ngay sau phần Header và được bao bọc trong dấu ngoặc đơn. Nếu có nhiều Option thì sẽ phân biệt bởi dấu chấm phẩy ";". Một Option gồm có 2 phần: một là từ khóa và một là tham số. 02 phần này sẽ phân cách nhau bằng dấu hai chấm ":".

Các option có thể là: msg (tin nhắn cảnh báo), content (nội dung gói tin), sid (số nhận dạng duy nhất), rev (số phiên bản quy tắc), content: Chứa một chuỗi hoặc byte pattern để so khớp với dữ liệu gói tin ...

Ví dụ về cấu trúc một quy tắc Snort:

alert tcp any any -> any 80 (msg:"Potential Web Attack"; content: "/bin/bash"; sid:100001;).

### 1.2.2.2 Ossec

OSSEC là phần mềm mã nguồn mở giúp phát hiện xâm nhập dựa trên host (HIDS) Nó đa nền tảng, có thể mở rộng và có nhiều cơ chế bảo mật khác nhau.

#### **Các tính năng của Ossec:**

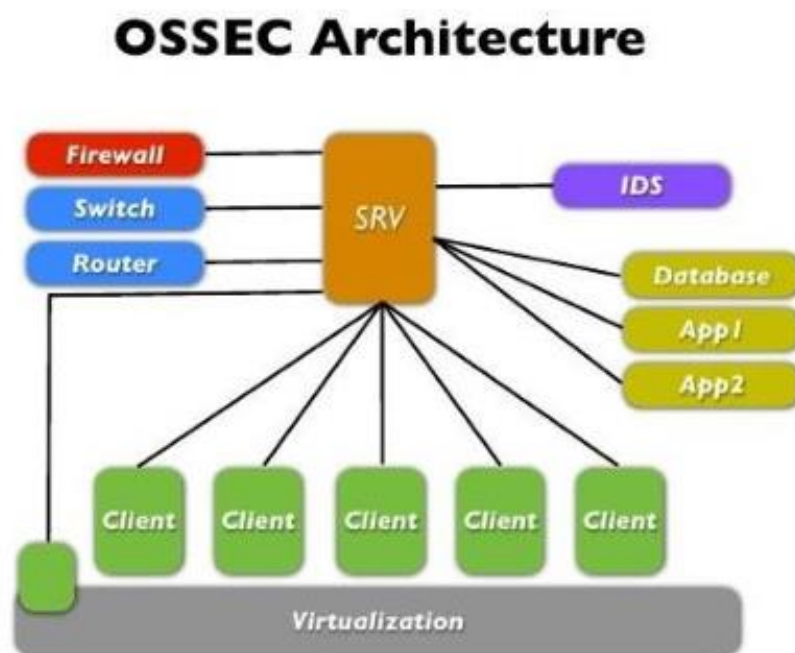
- Log based Intrusion Detection (LIDs) and Log Monitoring:
  - Chủ động theo dõi và phân tích dữ liệu real-time từ nhiều nguồn sinh log.
  - Ngoài ra, Ossec sẽ thu thập, phân tích và kiểm tra mối tương quan các log và cho ta biết những điều đáng ngờ đang xảy ra trong hệ thống (bị tấn công, lỗi, sử dụng sai,...), các phần mềm được cài đặt thêm, các rule firewall bị đổi.
- Compliance Auditing: Kiểm soát các ứng dụng và hệ thống nhằm tuân thủ các yêu cầu, tiêu chuẩn về bảo mật như PCI-DSS và CIS.
- Rootkit and Malware Detection:
  - Tin tặc thường muốn che dấu hành động và quay lại hệ thống đã xâm nhập được.
  - Ossec phân tích ở cấp độ file và tiến trình nhằm phát hiện các ứng dụng độc hại, các rootkit hay các file hệ thống bị sửa đổi theo cách phổ biến với rootkit.
- File Integrity Monitoring (FIM): Phát hiện các thay đổi đối với hệ thống.
- Active Response:
  - Các hành vi ứng phó lại các cuộc tấn công vào hệ thống trong thời gian thực.
  - Giúp ngăn sự cố lan rộng trước khi admin có thể hành động.
- System Inventory: Thu thập các thông tin hệ thống như phần mềm được cài đặt, hardware,...

#### **Điểm nổi trội của Ossec:**

- Đa nền tảng (Linux, Mac OS, Window, Solaris).
- Real-time Alert (Cảnh báo thời gian thực):
  - Kết hợp với smtp, sms, syslog sẽ cho phép người dùng nhận cảnh báo trên các thiết bị có hỗ trợ email.
  - Ngoài ra tính năng Active-response có thể giúp block 1 cuộc tấn công ngay lập tức.
- Có thể tích hợp với các hệ thống hiện đại (SIM/SEM).
- Mô hình Server-Agent/Agentless, cho phép Server dễ dàng quản lý tập trung các chính sách trên nhiều OS.
- Giám sát trên agent, agentless (Client không cài đặt được gói agent) như router, firewall.

#### **Kiến trúc và mô hình hoạt động của Ossec:**

Ossec hoạt động theo mô hình Server-Agent/Agentless.



Hình 5 – Kiến trúc của Ossec

#### Manager (Server):

Lưu trữ cơ sở dữ liệu của việc kiểm tra tính toàn vẹn file Kiểm tra các log, event. Quản lý, lưu tất cả các rule, decoder (bộ giải mã), cấu hình chính. Điều này giúp dễ dàng quản lý, dù cho có lượng lớn Agent Server không chạy trên Windows OS.

#### Agent

Bản chất thì là 1 phần mềm được cài đặt trên máy client giúp thu thập các thông tin và gửi cho Server để phân tích, thống kê.

- Chiếm lượng memory và CPU nhỏ, không đáng kể.
- 1 số thông tin được thu thập theo thời gian thực.
- 1 số thông tin thì lại được thu thập định kỳ.

Nhưng khi nói Agent thì là để chỉ máy Client được cài gói Ossec-agent. Chú ý: Windows OS chỉ có thể làm Agent chứ không làm Server được.

#### Agentless

Là các hệ thống không cài được gói agent Trên các Agentless này có thể thực hiện việc kiểm tra tính toàn vẹn. Giúp monitor firewall, router hay thậm chí cả hệ thống Unix

#### Ảo hóa/ VMware

Cho phép cài đặt agent trên các guest OS (Máy ảo) Ngoài ra cũng được cài đặt trong VMware ESX nhưng có thể dẫn đến sự cố không hỗ trợ. Khi cài đặt trong VMware ESX giúp nhận được thời điểm các VM guest được khởi tạo, xóa đi, khởi động... Ossec cũng

giám sát việc login, logouts và các lỗi bên trong ESX server Ngoài ra nó cũng cảnh báo nếu bất kỳ tùy chọn cấu hình không an toàn nào được bật.

### **Firewalls, switches and routers**

Chính là các Agentless Ossec có thể nhận và phân tích nhật ký hệ thống từ nhiều firewall, switch, router. Nó support tất cả Cisco routers, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, Netscreen firewall, Checkpoint và nhiều thiết bị khác.

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

### 2.1 Chuẩn bị môi trường

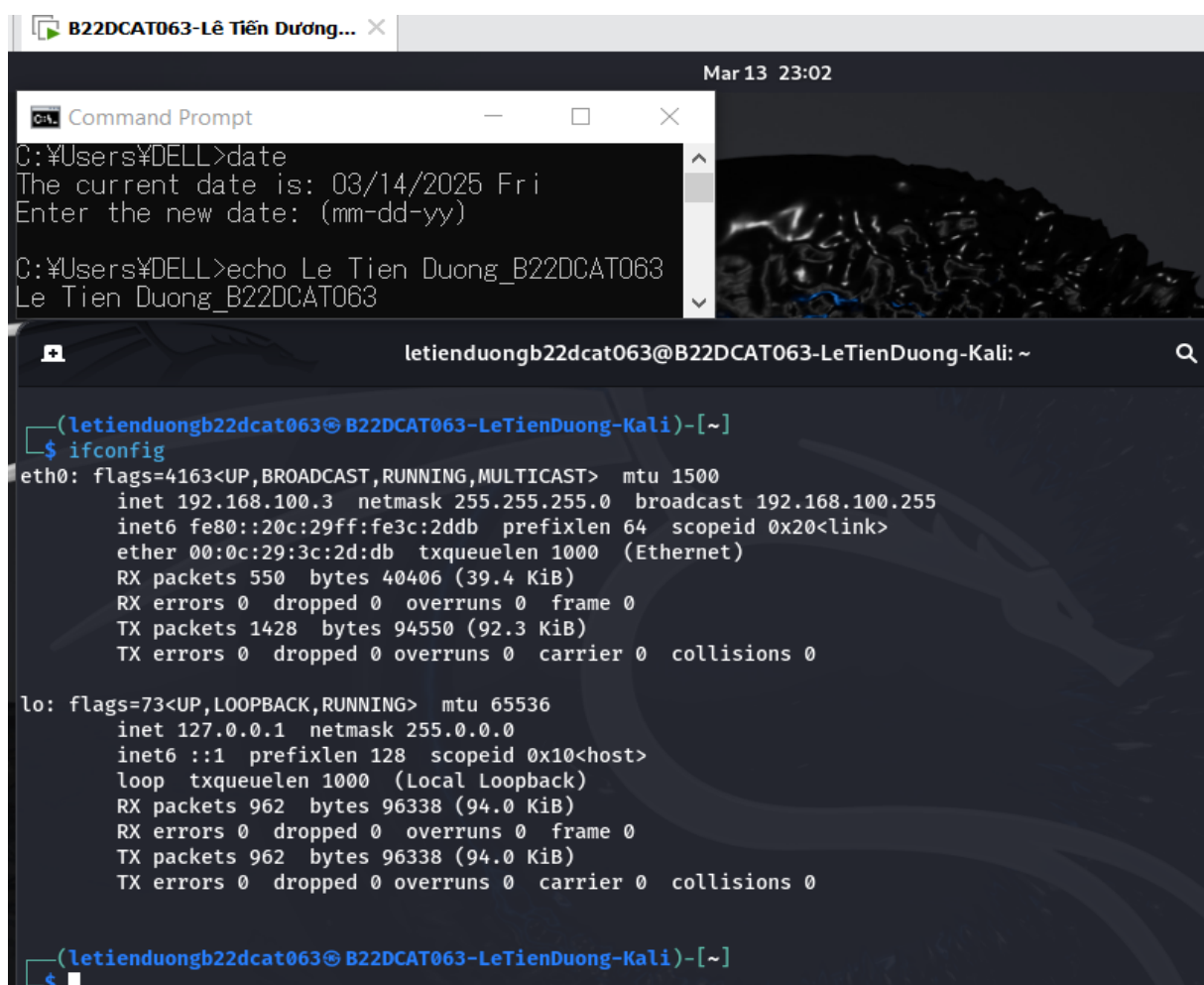
- 01 máy tính (máy thật hoặc máy ảo) chạy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng (LAN hoặc Internet).
- 01 máy tính (máy thật hoặc máy ảo) chạy Kali Linux (bản 2021 trở lên).
- Bộ phần mềm Snort.

### 2.2 Các bước thực hiện

#### 2.2.1 Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.1

Máy Kali Linux được đổi tên thành B22DCAT063-LeTienDuong-Kali và máy cài Snort được đổi tên thành B22DCAT063-LeTienDuong-Snort. Các máy có địa chỉ IP và kết nối mạng LAN.

Đổi tên và kiểm tra IP máy Kali Linux.



Hình 6 – Đổi tên và kiểm tra IP máy Kali Linux

Đổi tên và kiểm tra địa chỉ IP máy cài Snort.

The screenshot shows a terminal window titled "B22DCAT063-Lê Tiến Dương...". Inside, a "Command Prompt" window is open, showing the execution of the following commands:  
1. `date`: The current date is 03/14/2025 Fri. The user is prompted to enter a new date in mm-dd-yy format.  
2. `echo Le Tien Duong_B22DCAT063`: The output is "Le Tien Duong\_B22DCAT063".  
Below the Command Prompt, the terminal window shows the output of the `ifconfig` command:  
- `ens33`: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
 inet 192.168.100.147 netmask 255.255.255.0 broadcast 192.168.100.255  
 inet6 fe80::20c:29ff:fed7:a829 prefixlen 64 scopeid 0x20<link>  
 ether 00:0c:29:d7:a8:29 txqueuelen 1000 (Ethernet)  
 RX packets 26171 bytes 34086634 (34.0 MB)  
 RX errors 0 dropped 0 overruns 0 frame 0  
 TX packets 12062 bytes 1006061 (1.0 MB)  
 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 0x10<host>  
 loop txqueuelen 1000 (Local Loopback)  
 RX packets 4915 bytes 389852 (389.8 KB)  
 RX errors 0 dropped 0 overruns 0 frame 0  
 TX packets 4915 bytes 389852 (389.8 KB)  
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
The terminal prompt is `letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$`.

Hình 7 – Đổi tên và kiểm tra IP máy cài Snort

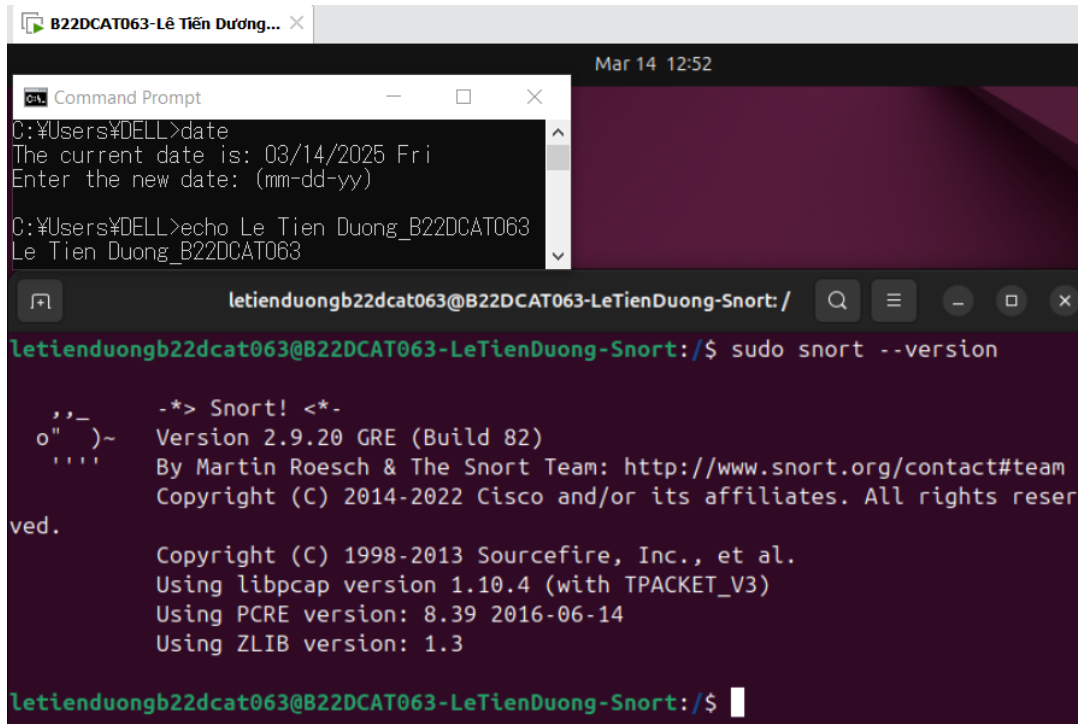
### 2.2.2 Bước 2: Tải, cài đặt và chạy thử Snort

Tải Snort: `sudo apt update`      `sudo apt install snort`

The screenshot shows a terminal window titled "B22DCAT063-Lê Tiến Dương...". Inside, a "Command Prompt" window is open, showing the execution of the following commands:  
1. `date`: The current date is 03/14/2025 Fri. The user is prompted to enter a new date in mm-dd-yy format.  
2. `echo Le Tien Duong_B22DCAT063`: The output is "Le Tien Duong\_B22DCAT063".  
Below the Command Prompt, the terminal window shows the output of the `sudo apt install snort` command:  
- Reading package lists... Done  
- Building dependency tree... Done  
- Reading state information... Done  
- The following packages were automatically installed and are no longer required:  
 libllvm17t64 python3-netifaces  
 Use 'sudo apt autoremove' to remove them.  
- The following additional packages will be installed:  
 libdaq2t64 libdumbnet1 liblua5.1-2 liblua5.1-common  
 libnetfilter-queue1 libpcrc3 oinkmaster snort-common snort-common-libraries  
 snort-rules-default  
- Suggested packages:  
 snort-doc  
- The following NEW packages will be installed:  
 libdaq2t64 libdumbnet1 liblua5.1-2 liblua5.1-common  
 libnetfilter-queue1 libpcrc3 oinkmaster snort-common  
 snort-common-libraries snort-rules-default  
- 0 upgraded, 11 newly installed, 0 to remove and 65 not upgraded.  
- Need to get 2,666 kB of archives.  
- After this operation, 11.4 MB of additional disk space will be used.  
- Do you want to continue? [Y/n] y

Hình 8 – Tải Snort

Kiểm tra phiên bản Snort.



```
B22DCAT063-Lê Tiến Dương... x
Mar 14 12:52
Command Prompt
C:\Users\DELL>date
The current date is: 03/14/2025 Fri
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /
letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$ sudo snort --version

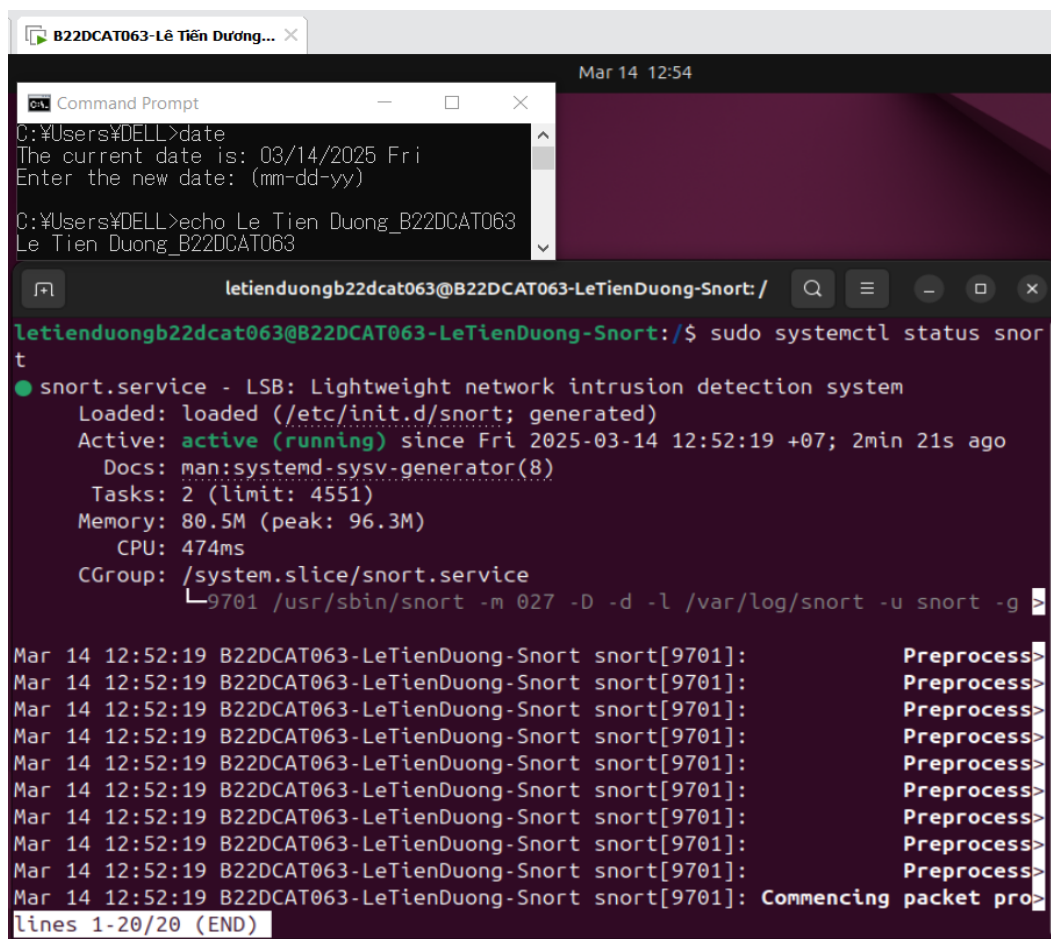
,,_      -*> Snort! <*-
o" )~    Version 2.9.20 GRE (Build 82)
' '      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
        Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.

        Copyright (C) 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

letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$
```

Hình 9 – Kiểm tra phiên bản của Snort

Kiểm tra trạng thái hoạt động của Snort.



```
B22DCAT063-Lê Tiến Dương... x
Mar 14 12:54
Command Prompt
C:\Users\DELL>date
The current date is: 03/14/2025 Fri
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /
letienduongb22dcat063@B22DCAT063-LeTienDuong-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 2025-03-14 12:52:19 +07; 2min 21s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 2 (limit: 4551)
   Memory: 80.5M (peak: 96.3M)
      CPU: 474ms
   CGroup: /system.slice/snort.service
           └─9701 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g >

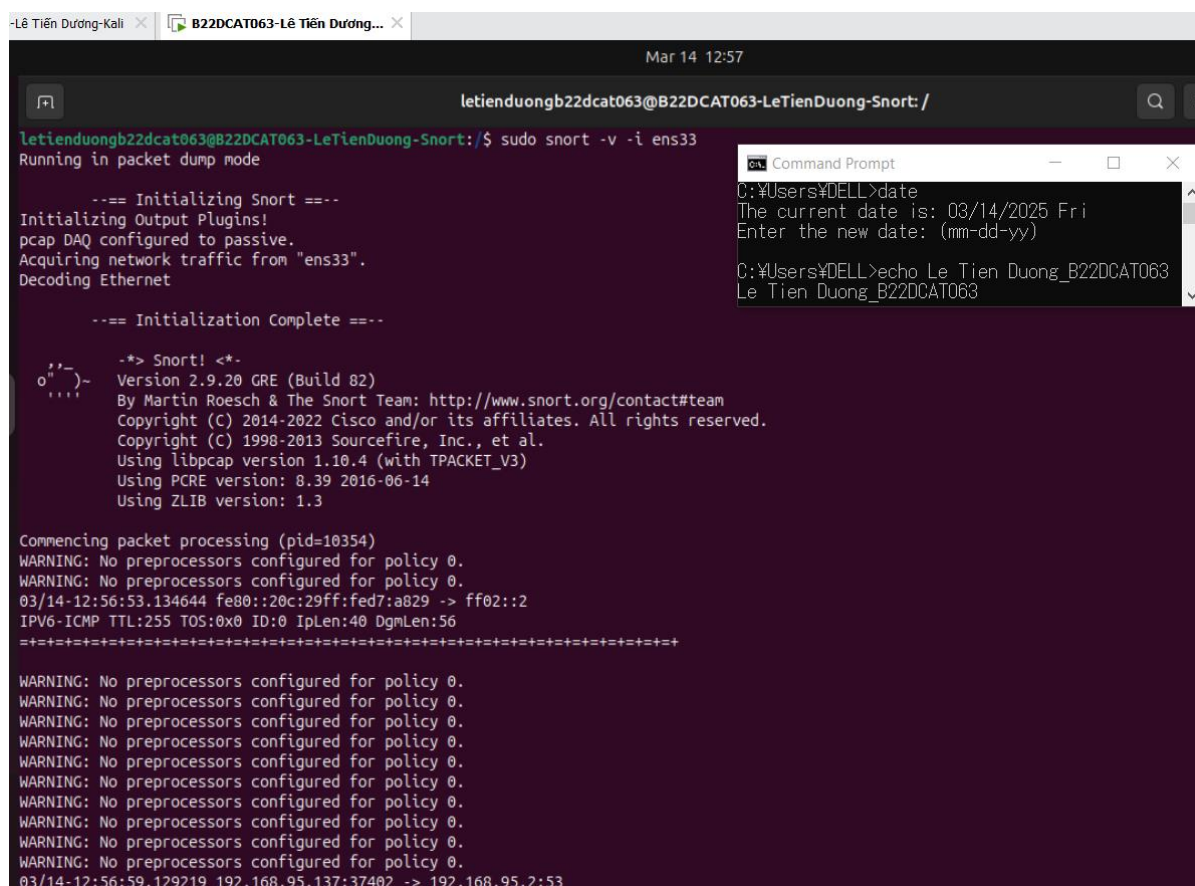
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Preprocess>
Mar 14 12:52:19 B22DCAT063-LeTienDuong-Snort snort[9701]: Commencing packet pro>
lines 1-20/20 (END)
```

Hình 10 – Kiểm tra trạng thái hoạt động của Snort



Chạy thử Snort.

*sudo snort -v -i ens33*



```
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$ sudo snort -v -i ens33
Running in packet dump mode

==== Initializing Snort ====
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

==== Initialization Complete ====

-> Snort! <-
o""-
'""-
...-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 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

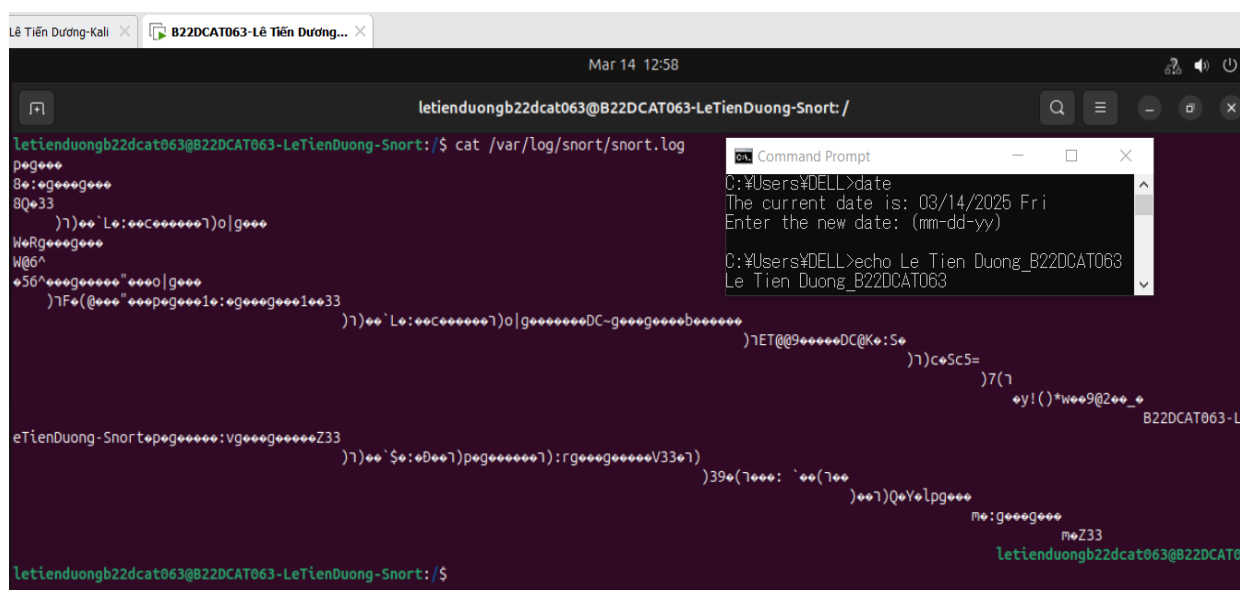
Commencing packet processing (pid=10354)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/14-12:56:53.134644 fe80::20c:29ff:fed7:a829 -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:56
=====

WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
03/14-12:56:59.129219 192.168.95.137:37402 -> 192.168.95.2:53
```

Hình 11 – Chạy thử Snort

Kiểm tra log của Snort.

*cat /var/log/snort/snort.log*



```
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$ cat /var/log/snort/snort.log
p0g000
80:0g000g000
80033
)1)00`Lo:00c000000)0|g000
WeRg000g000
W06^
050^000g000000"0000|g000
)1F0(@000"000p0g00010:0g000g000I0033
)1)00`Lo:00c000000)0|g000000DC-g000g000b000000
)1ET@090000DC@K0:S0
)1)c0Sc5=
)7(1
0y!()*w009@200_0
B22DCAT063-L
eTienDuong-Snort0p0g000000:vg000g000000Z33
)1)00`$0:0D000)0p0g000000)1:rg000g000000V3301
)390(10000: `00(100
)000)Q0Y0lp000
m0:g000g000
m0Z33
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$
```

Hình 12 – Kiểm tra log của Snort



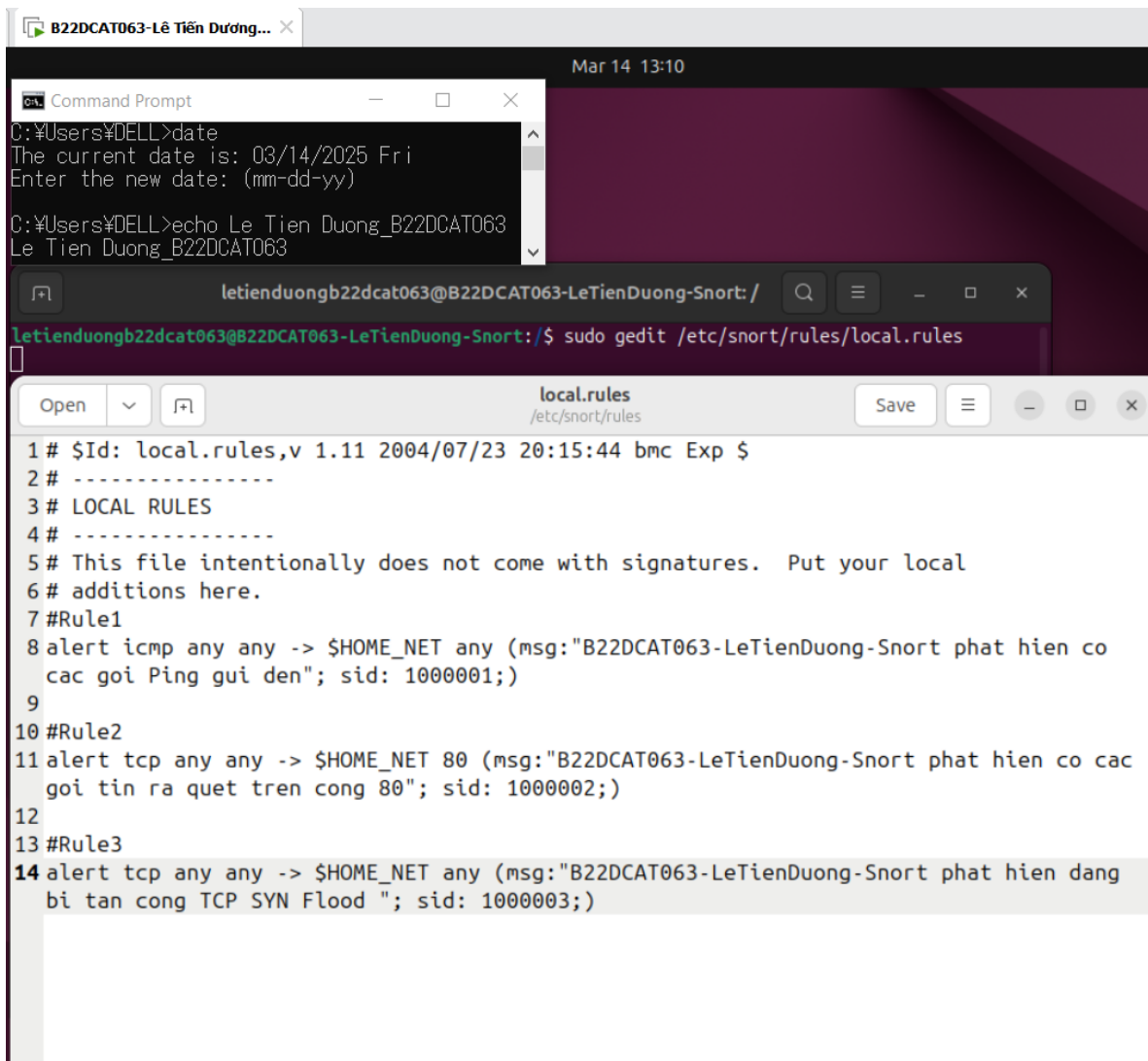
### 2.2.3 Bước 3: Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống

Tạo các luật Snort:

- Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiện thị thông điệp khi phát hiện: “B22CAT303-NguyenKhacTri -Snort phát hiện có các gói Ping gửi đến.”.
- Phát hiện các gói tin rà quét từ bất kỳ một máy nào gửi đến máy chạy Snort trên cổng 80. Hiện thị thông điệp khi phát hiện: “B22CAT303-NguyenKhacTri-Snort phát hiện có các gói tin rà quét trên cổng 80.”.
- Phát hiện tấn công TCP SYN Flood từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiện thị thông điệp khi phát hiện: “B22CAT303-NguyenKhacTri -Snort phát hiện đang bị tấn công TCP SYN Flood.”.

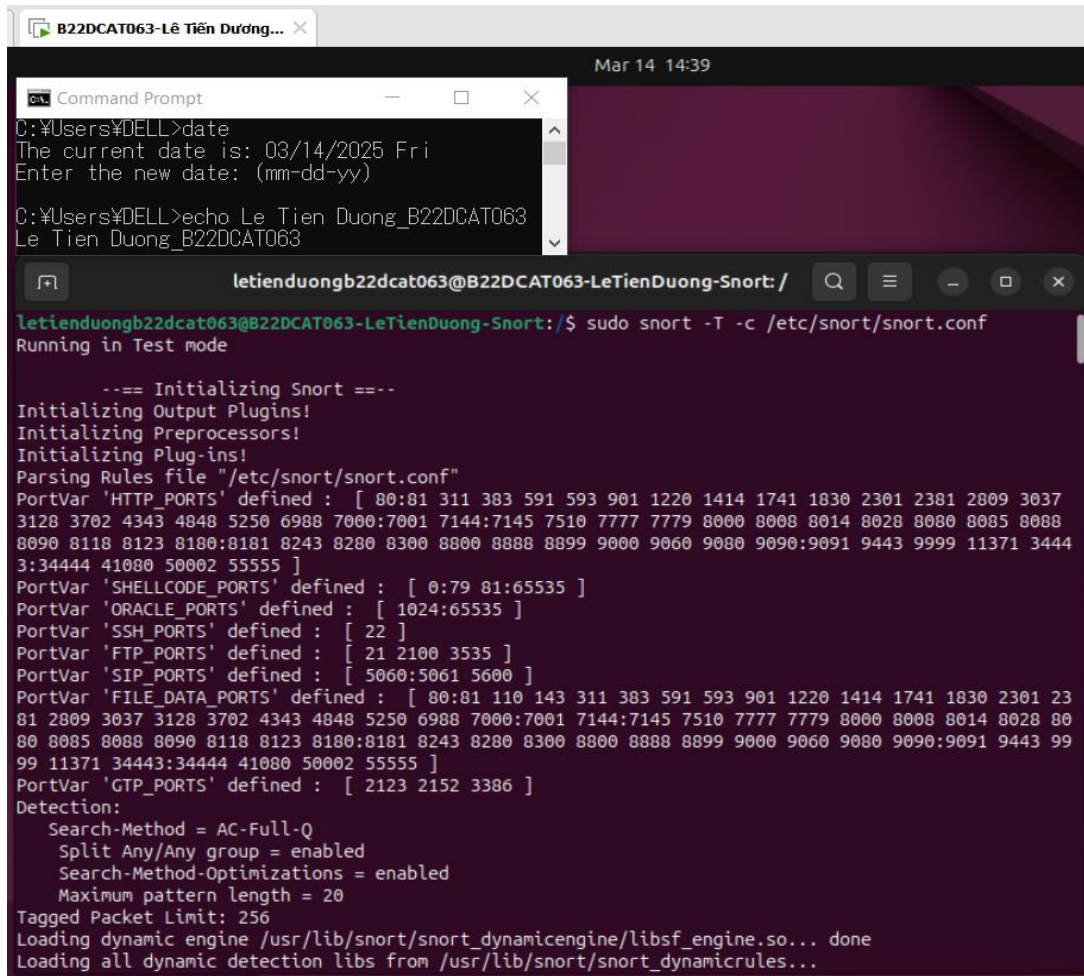
Mở file cấu hình để tạo thêm luật:

```
sudo gedit /etc/snort/rules/local.rules
```



Hình 13 – Tạo thêm luật trong file cấu hình

Kiểm tra file cấu hình Snort: *sudo snort -T -c /etc/snort/snort.conf*



```
Command Prompt
C:\Users\DELL>date
The current date is: 03/14/2025 Fri
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

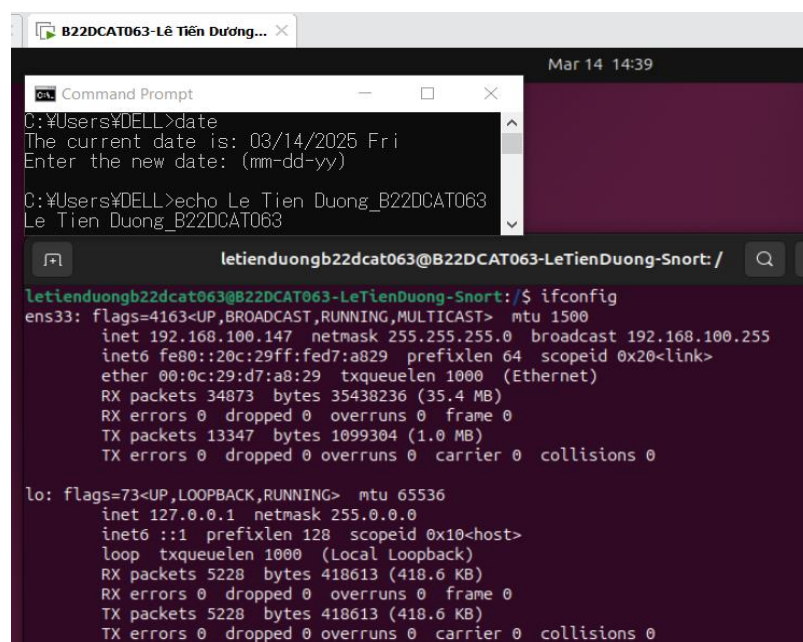
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

--== 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 3037
3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088
8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 3444
3:34444 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 23
81 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 80
80 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 99
99 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/snort_dynamicengine/libsfe_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
```

Hình 14 – Kiểm tra cấu hình Snort

#### 2.2.4 Bước 4: Thực thi tấn công và phát hiện sử dụng Snort

Kiểm tra lại IP máy cài Snort.



```
lettienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.147 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fed7:a829 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:d7:a8:29 txqueuelen 1000 (Ethernet)
    RX packets 34873 bytes 35438236 (35.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13347 bytes 1099304 (1.0 MB)
    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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5228 bytes 418613 (418.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5228 bytes 418613 (418.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 15 – Kiểm tra lại địa chỉ IP máy cài Snort

Từ máy Kali, sử dụng lệnh ping để ping đến máy Snort.

```
B22DCAT063-Lê Tiến Dương-Sn... x
Mar 14 00:40
Command Prompt
C:\Users\DELL>date
The current date is: 03/14/2025 Fri
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

lettienduongb22dcat063@B22DCAT063-LeTienDuong-Kali: ~
(lettienduongb22dcat063@B22DCAT063-LeTienDuong-Kali)-[~]
$ ping 192.168.100.147
PING 192.168.100.147 (192.168.100.147) 56(84) bytes of data:
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=0.540 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=0.979 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=0.992 ms
64 bytes from 192.168.100.147: icmp_seq=4 ttl=64 time=0.445 ms
64 bytes from 192.168.100.147: icmp_seq=5 ttl=64 time=0.868 ms
64 bytes from 192.168.100.147: icmp_seq=6 ttl=64 time=1.07 ms
64 bytes from 192.168.100.147: icmp_seq=7 ttl=64 time=0.926 ms
64 bytes from 192.168.100.147: icmp_seq=8 ttl=64 time=1.07 ms
64 bytes from 192.168.100.147: icmp_seq=9 ttl=64 time=0.436 ms
64 bytes from 192.168.100.147: icmp_seq=10 ttl=64 time=0.532 ms
^C
--- 192.168.100.147 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 0.436/0.786/1.073/0.251 ms
```

Hình 16 – Ping từ máy Kali sang máy cài Snort

Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

```
B22DCAT063-Lê Tien Duong... x Mar 14 14:42
```

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

C:\Users\YDELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063
```

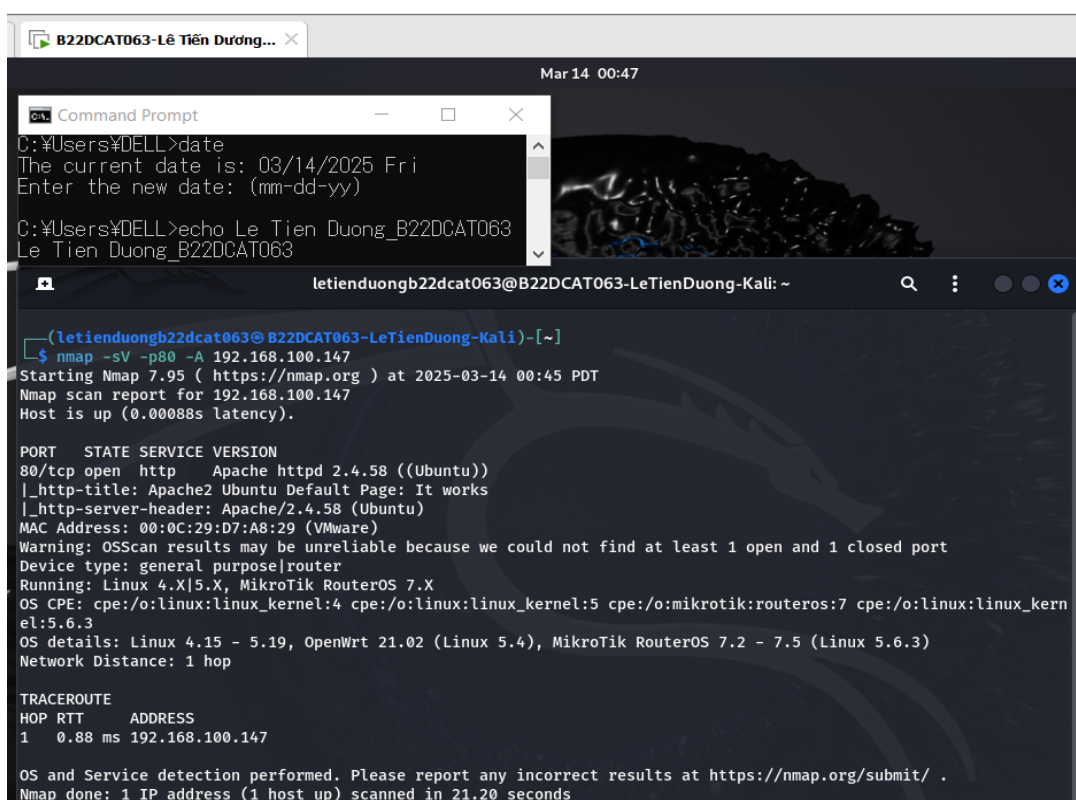
```
lettienduongb22dcato63@B22DCAT063-LeTienDuong-Snort: / [Q] [=] [-] [x]
```

```
lettienduongb22dcato63@B22DCAT063-LeTienDuong-Snort:/$ cat /var/log/snort/snort.alert.fast
03/14-12:55:54.669777 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {IPv6-ICMP} :: -> ff02::16
03/14-12:55:54.677696 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {ICMP} 0.0.0.0 -> 224.0.0.22
03/14-12:55:54.893749 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {ICMP} 0.0.0.0 -> 224.0.0.22
03/14-12:55:55.405945 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {IPv6-ICMP} :: -> ff02::16
03/14-12:55:55.950297 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
03/14-12:55:55.956036 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {IPv6-ICMP} :: -> ff02::16
03/14-12:55:56.110828 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {IPv6-ICMP} :: -> ff02::1:ffdf:a829
03/14-12:55:56.814484 [[**]] [1:527:8] BAD-TRAFFIC same SRC/DST [[**]] [Classification: Potentially Bad Traffic]
[Priority: 2] {IPv6-ICMP} :: -> ff02::16
03/14-14:40:33.277471 [[**]] [1:1000001:0] B22DCAT063-LeTienDuong-Snort phat hien co cac goi Ping gui den [[**]]
[Priority: 0] {ICMP} 192.168.100.3 -> 192.168.100.147
03/14-14:40:34.279405 [[**]] [1:1000001:0] B22DCAT063-LeTienDuong-Snort phat hien co cac goi Ping gui den [[**]]
[Priority: 0] {ICMP} 192.168.100.3 -> 192.168.100.147
03/14-14:40:35.282104 [[**]] [1:1000001:0] B22DCAT063-LeTienDuong-Snort phat hien co cac goi Ping gui den [[**]]
[Priority: 0] {ICMP} 192.168.100.3 -> 192.168.100.147
03/14-14:40:36.284946 [[**]] [1:1000001:0] B22DCAT063-LeTienDuong-Snort phat hien co cac goi Ping gui den [[**]]
[Priority: 0] {ICMP} 192.168.100.3 -> 192.168.100.147
03/14-14:40:37.286967 [[**]] [1:1000001:0] B22DCAT063-LeTienDuong-Snort phat hien co cac goi Ping gui den [[**]]
[Priority: 0] {ICMP} 192.168.100.3 -> 192.168.100.147
03/14-14:40:38.289020 [[**]] [1:1000001:0] B22DCAT063-LeTienDuong-Snort phat hien co cac goi Ping gui den [[**]]
[Priority: 0] {ICMP} 192.168.100.3 -> 192.168.100.147
03/14-14:40:39.290341 [[**]] [1:1000001:0] B22DCAT063-LeTienDuong-Snort phat hien co cac goi Ping gui den [[**]]
[Priority: 0] {ICMP} 192.168.100.3 -> 192.168.100.147
```

Hình 17 – Kiểm tra kết quả trên máy Snort



Từ máy Kali, sử dụng công cụ nmap để quét máy Snort (dùng lệnh: `nmap -sV -p80 -A <địa chỉ IP máy Snort>`).

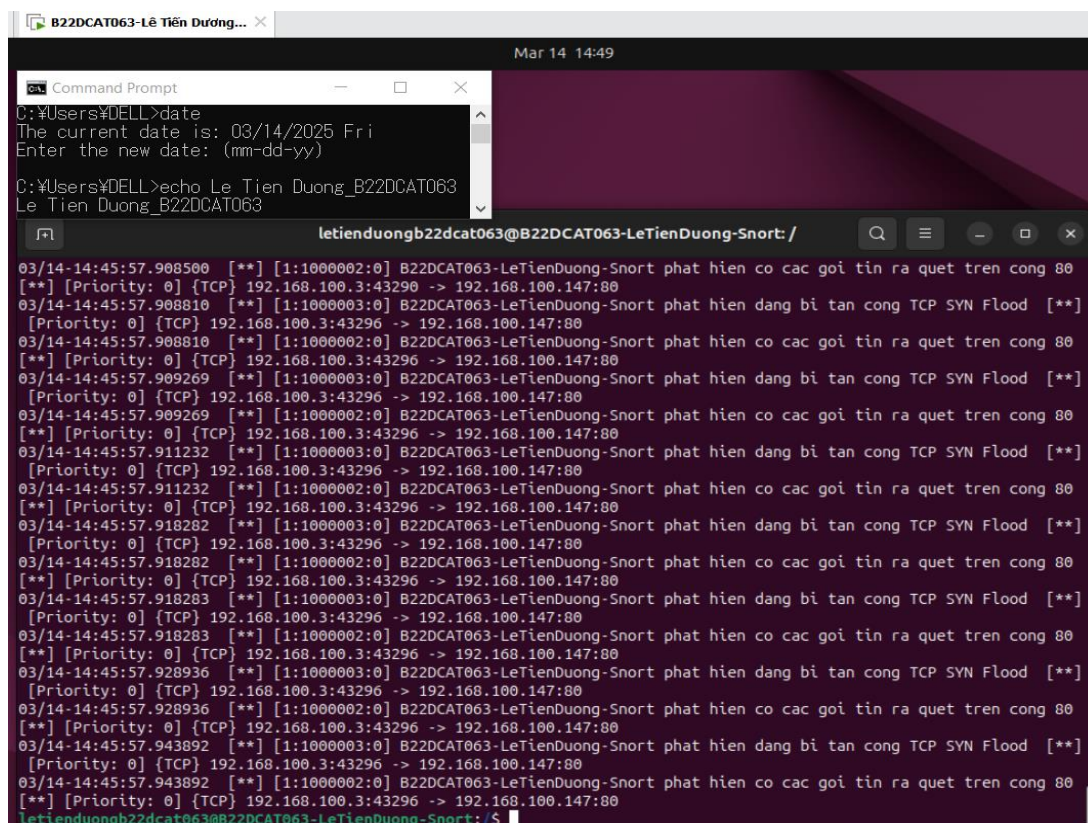


The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window titled 'letienduongb22dcat063@B22DCAT063-LeTienDuong-Kali: ~' displays the output of an nmap scan. In the background, a Windows Command Prompt window is visible, showing the date and a command to echo a string.

```
letienduongb22dcat063@B22DCAT063-LeTienDuong-Kali: ~  
$ nmap -sV -p80 -A 192.168.100.147  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 00:45 PDT  
Nmap scan report for 192.168.100.147  
Host is up (0.00088s 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:D7:A8:29 (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  
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X  
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kern  
el:5.6.3  
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)  
Network Distance: 1 hop  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1 0.88 ms 192.168.100.147  
  
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 21.20 seconds
```

Hình 18 – Từ máy Kali sử dụng công cụ nmap

Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

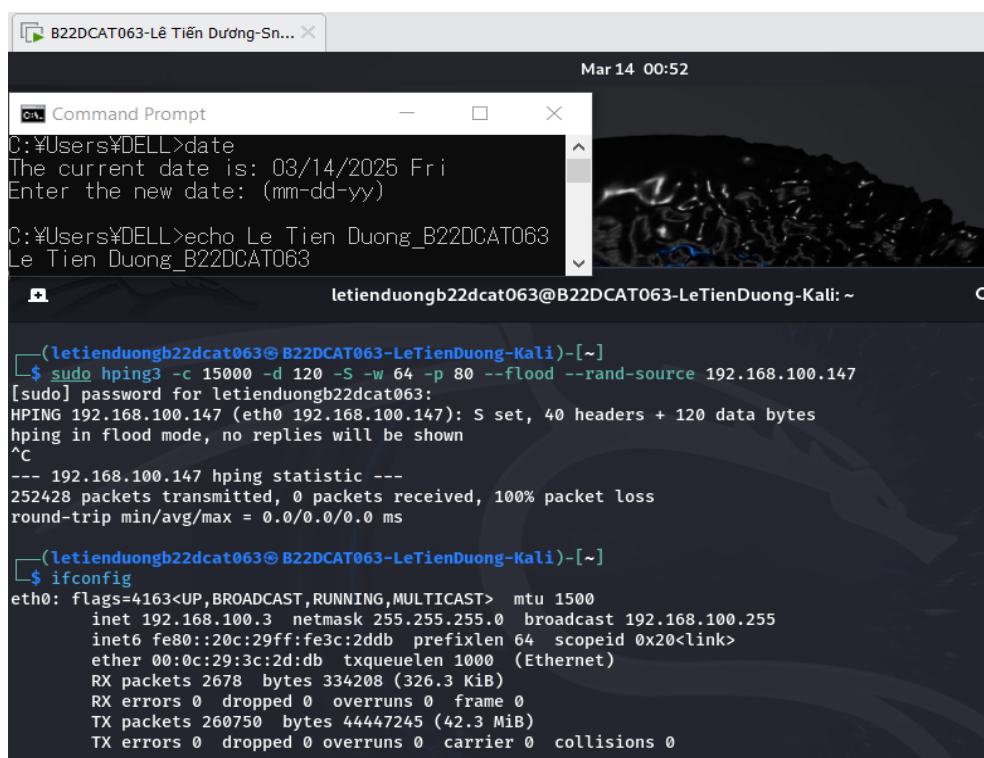


The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window titled 'letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /' displays the output of a Snort scan. In the background, a Windows Command Prompt window is visible, showing the date and a command to echo a string.

```
letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /  
03/14-14:45:57.908500  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.908810  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]  
[Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.908810  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.909269  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]  
[Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.909269  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.911232  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]  
[Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.911232  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.918282  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]  
[Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.918282  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.918283  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]  
[Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.918283  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.928936  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]  
[Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.928936  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.943892  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]  
[Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
03/14-14:45:57.943892  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80  
[**] [Priority: 0] [TCP] 192.168.100.3:43296 -> 192.168.100.147:80  
letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /$
```

Hình 19 – Trên máy Snort kiểm tra kết quả

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 192.168.100.147).



```
B22DCAT063-Lê Tiến Dương-Sn...
Mar 14 00:52

Command Prompt
C:\Users\DELL>date
The current date is: 03/14/2025 Fri
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

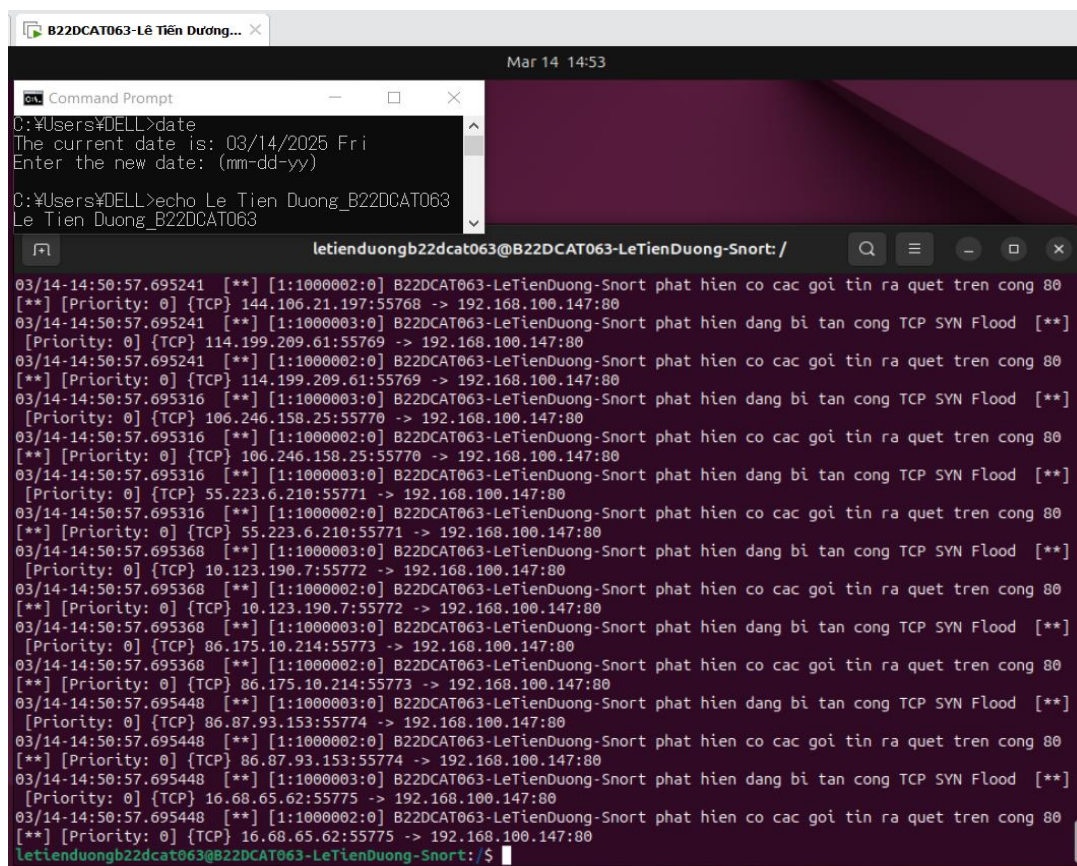
letienduongb22dcat063@B22DCAT063-LeTienDuong-Kali: ~

(letienduongb22dcat063@B22DCAT063-LeTienDuong-Kali)-[~]
$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.100.147
[sudo] password for letienduongb22dcat063:
HPING 192.168.100.147 (eth0 192.168.100.147): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.100.147 hping statistic ---
252428 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(letienduongb22dcat063@B22DCAT063-LeTienDuong-Kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe3c:2ddb prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3c:2d:db txqueuelen 1000 (Ethernet)
    RX packets 2678 bytes 334208 (326.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 260750 bytes 44447245 (42.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 20 – Từ máy Kali sử dụng công cụ hping3

Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.



```
B22DCAT063-Lê Tiến Dương-Sn...
Mar 14 14:53

Command Prompt
C:\Users\DELL>date
The current date is: 03/14/2025 Fri
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort: /

03/14-14:50:57.695241  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 144.106.21.197:55768 -> 192.168.100.147:80
03/14-14:50:57.695241  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]
[Priority: 0] [TCP] 114.199.209.61:55769 -> 192.168.100.147:80
03/14-14:50:57.695241  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 114.199.209.61:55769 -> 192.168.100.147:80
03/14-14:50:57.695316  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]
[Priority: 0] [TCP] 106.246.158.25:55770 -> 192.168.100.147:80
03/14-14:50:57.695316  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 106.246.158.25:55770 -> 192.168.100.147:80
03/14-14:50:57.695316  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]
[Priority: 0] [TCP] 55.223.6.210:55771 -> 192.168.100.147:80
03/14-14:50:57.695316  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 55.223.6.210:55771 -> 192.168.100.147:80
03/14-14:50:57.695368  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]
[Priority: 0] [TCP] 10.123.190.7:55772 -> 192.168.100.147:80
03/14-14:50:57.695368  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 10.123.190.7:55772 -> 192.168.100.147:80
03/14-14:50:57.695368  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]
[Priority: 0] [TCP] 86.175.10.214:55773 -> 192.168.100.147:80
03/14-14:50:57.695368  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 86.175.10.214:55773 -> 192.168.100.147:80
03/14-14:50:57.695448  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]
[Priority: 0] [TCP] 86.87.93.153:55774 -> 192.168.100.147:80
03/14-14:50:57.695448  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 86.87.93.153:55774 -> 192.168.100.147:80
03/14-14:50:57.695448  [**] [1:1000003:0] B22DCAT063-LeTienDuong-Snort phát hiện đang bị tấn công TCP SYN Flood [**]
[Priority: 0] [TCP] 16.68.65.62:55775 -> 192.168.100.147:80
03/14-14:50:57.695448  [**] [1:1000002:0] B22DCAT063-LeTienDuong-Snort phát hiện có các gói tin ra quét trên cổng 80
[**] [Priority: 0] [TCP] 16.68.65.62:55775 -> 192.168.100.147:80
letienduongb22dcat063@B22DCAT063-LeTienDuong-Snort:/$
```

Hình 21 – Kiểm tra kết quả trên máy Snort

## **TÀI LIỆU THAM KHẢO**

- [1] Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BCVT, 2020.
- [2] Suricata: <https://suricata.io/documentation/>
- [3] Snort: <https://www.snort.org/#documents>
- [4] OSSEC: <https://www.ossec.net/docs/>
- [5] Wazuh: <https://documentation.wazuh.com/current/index.html>