**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: Ngô Quang Thắng-B22DCAT287

Giảng viên hướng dẫn: Quản Trọng Thế

**HỌC KỲ 2 NĂM HỌC 2024-2025**

**MỤC LỤC**

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 3](#_Toc194160583)

[1.1 Mục đích 3](#_Toc194160584)

[1.2 Tìm hiểu lý thuyết 3](#_Toc194160585)

[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. 3](#_Toc194160586)

[1.2.2. Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập: Snort, OSSEC 8](#_Toc194160587)

[CHƯƠNG 2. NỘI DUNG THỰC HÀNH 14](#_Toc194160588)

[2.1 Chuẩn bị môi trường 14](#_Toc194160589)

[2.2 Các bước thực hiện 14](#_Toc194160590)

[-Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.1. 14](#_Toc194160591)

[- Bước 2: Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường. 17](#_Toc194160592)

[- Bước 3: Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống: 19](#_Toc194160593)

[- Bước 4: Thực thi tấn công và phát hiện sử dụng Snort 20](#_Toc194160594)

[TÀI LIỆU THAM KHẢO 23](#_Toc194160595)

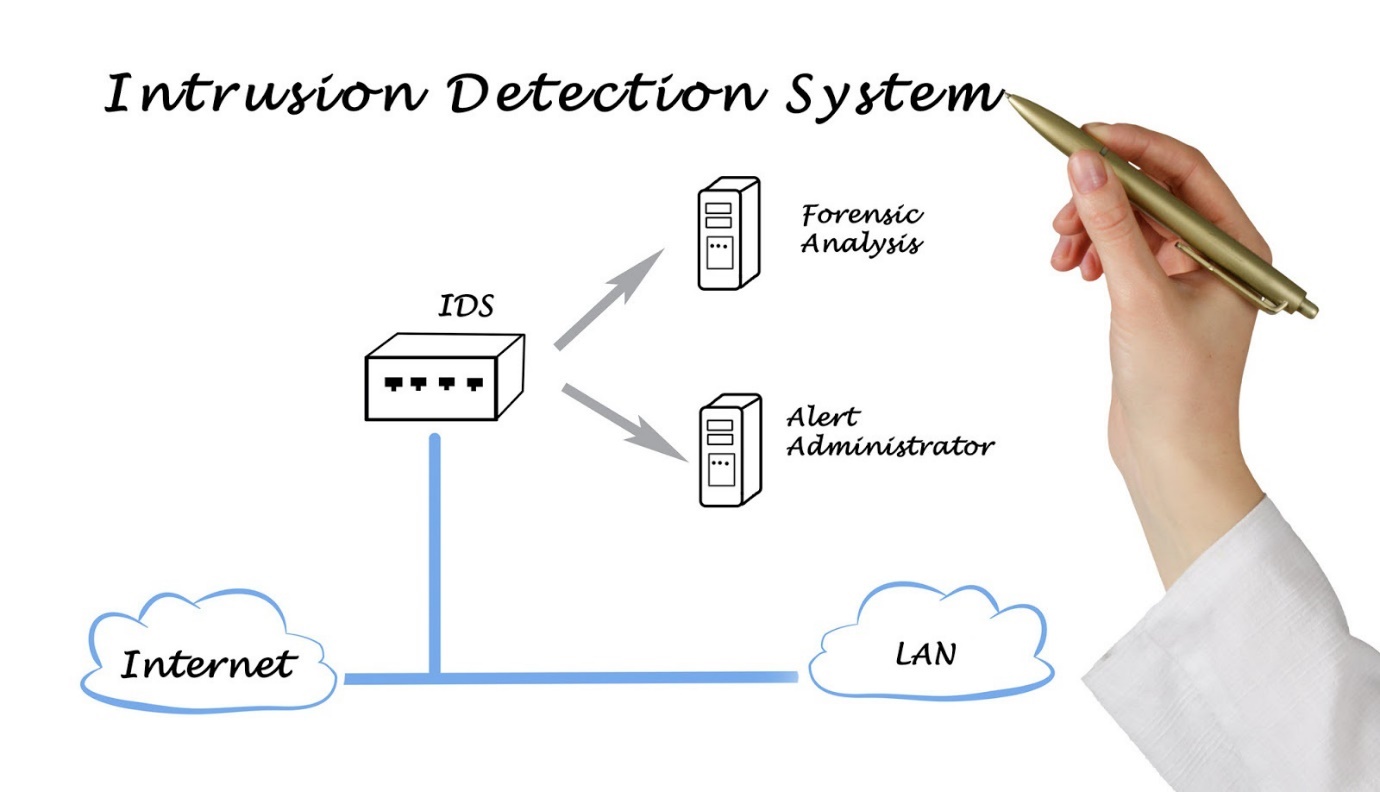
1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH
   1. Mục đích

* Luyện tập việc 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. 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**. Giới thiệu về hệ thống phát hiện tấn công, xâm nhập

Các hệ thống phát hiện tấn công, xâm nhập (IDS – Instrusion Detection System) là một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng theo mô hình phòng thủ có chiều sâu (defence in depth). Các hệ thống IDS có thể được đặt trước hoặc sau tường lửa trong mô hình mạng tùy theo mục đích sử dụng. IDS thường được kết nối vào bộ chuyển mạch (switch) phía sau tường lửa



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 các hành vi tấn công, xâm nhập đã phát hiện được.

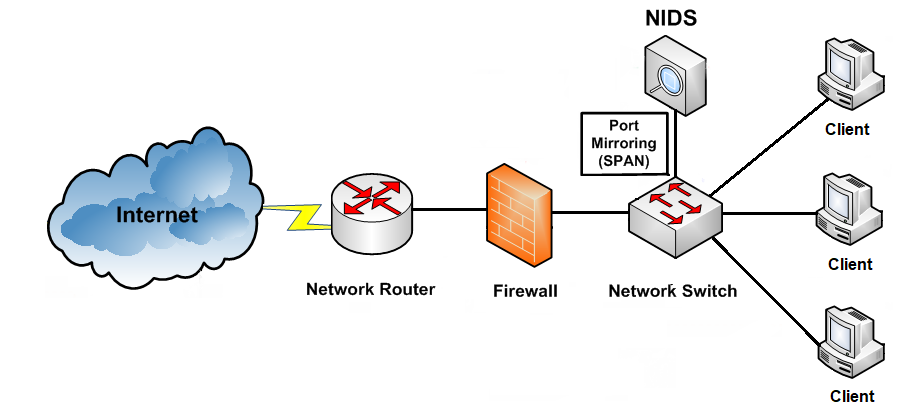
Nói tóm lại, IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh bảo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

**1.2.1.2**. Phân loại hệ thống phát hiện tấn công, xâm nhập

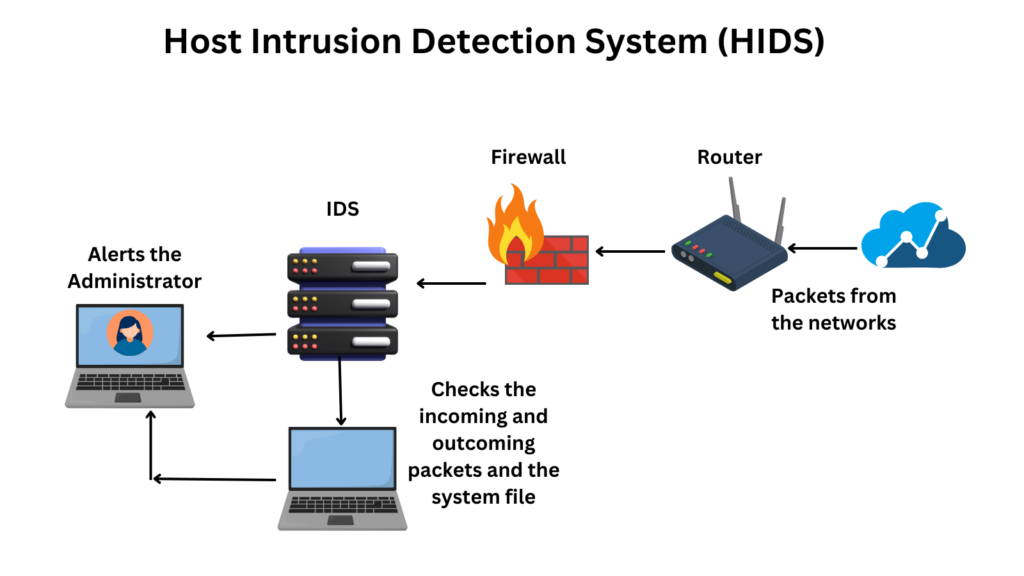
Có 2 phương pháp phân loại chính các hệ thống IDS gồm (1) phân loại theo nguồn dữ liệu và (2) phân loại theo phương pháp phân tích dữ liệu.

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 dưới đây biểu diễn một sơ đồ mạng, trong đó các NIDS được bố trí để 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 dưới đây minh họa một sơ đồ mạng, trong đó sử dụng NIDS để giám sát lưu lượng tại cổng mạng và HIDS để giám sát các host thông qua các IDS agent. Một trạm quản lý (Management station) được thiết lập để thu nhập các thông tin từ các NIDS và HIDS để xử lý và đưa ra quyết định cuối cùng



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)

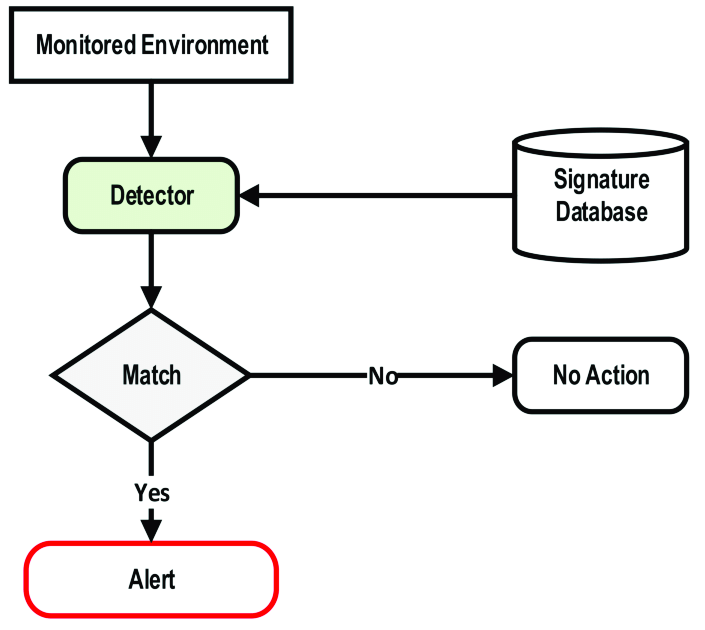
− Phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection).

**1.2.1.3**. Các kỹ thuật phát hiện xâm nhập

**1**. Phát hiện xâm nhập dựa trên chữ ký (Signature-based Intrusion Detection)

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.



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.

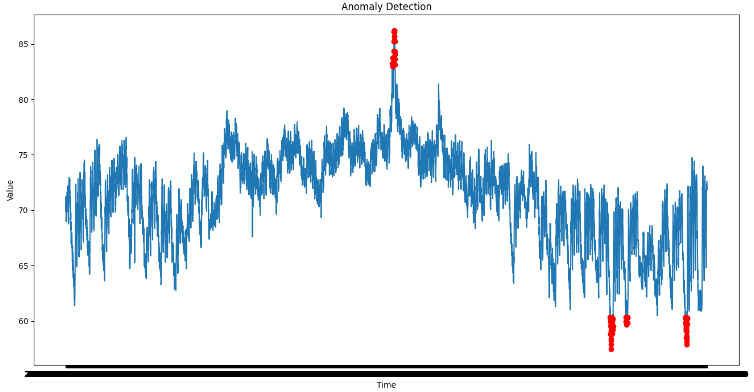
**2**. Phát hiện xâm nhập dựa trên bất thường(Anomaly-based Detection)

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 trên biểu diễn giá trị value của IP nguồn của các gói tin theo cửa sổ trượt từ lưu lượng bình thường và value 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 value 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 value.

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

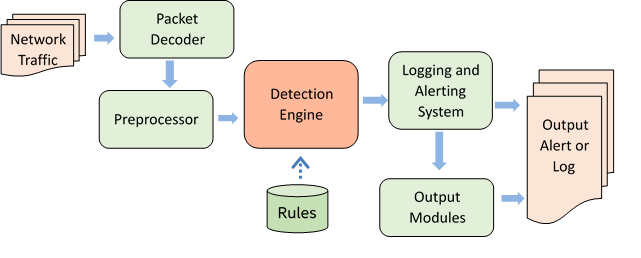
**a**. Giới thiệu

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.

**b**. 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

**c**. 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 chưa 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

**a**. Ossec là gì?

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.

**b**. 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, harware,…

**c**. 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-respone 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

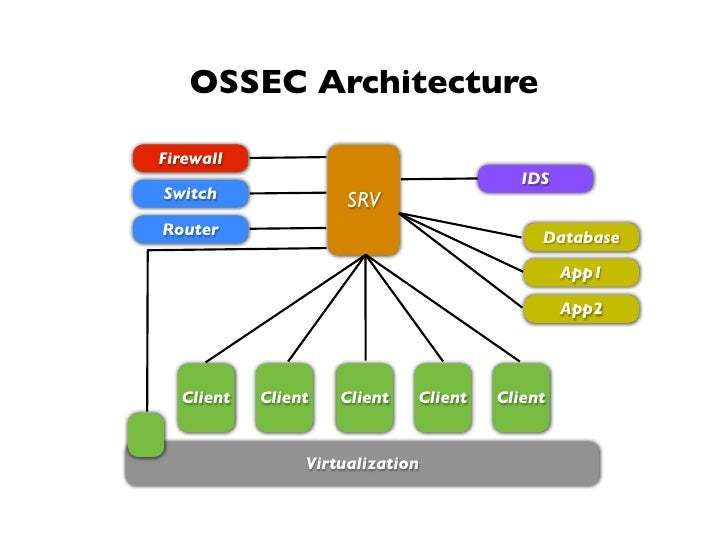
trung các chính sách trên nhiều OS.

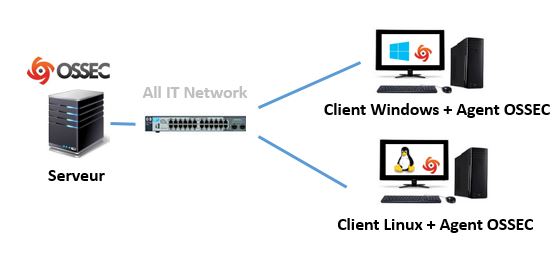
− Giám sát trên agent, agentless (Client không cài đặt được gói agent) như

router, firewall

**d**. Kiến trúc và mô hình hoạt động của Ossec

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





🟊 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.

1. 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
  1. Các bước thực hiện

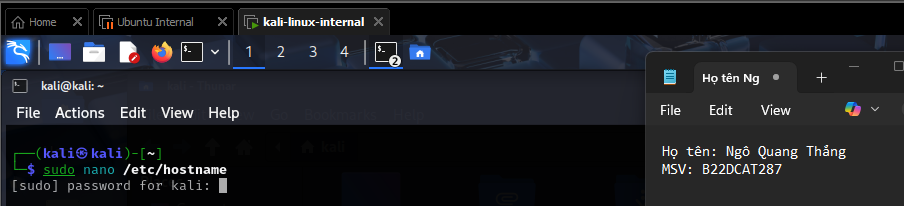
-**Bước 1**: Chuẩn bị các máy tính như mô tả trong mục 2.1.

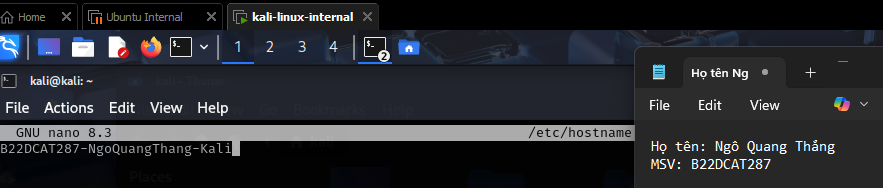
**Với máy Kali Linux:**

o Thay đổi tên trong tệp hostname:

*sudo nano /etc/hostname*

o Sửa thành: *B22DCAT287-NgoQuangThang-Kali*

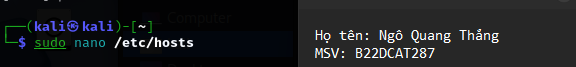


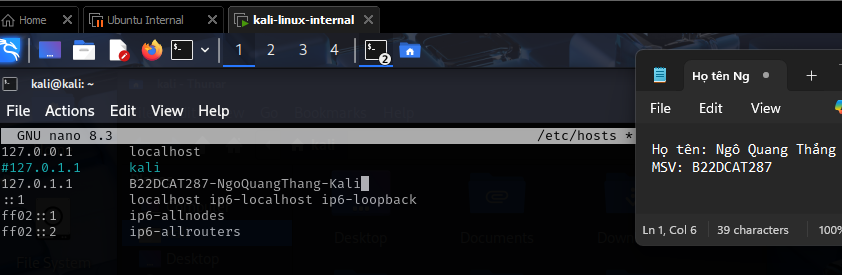


o Tiếp tục thực hiện thay đổi trong tệp hosts:

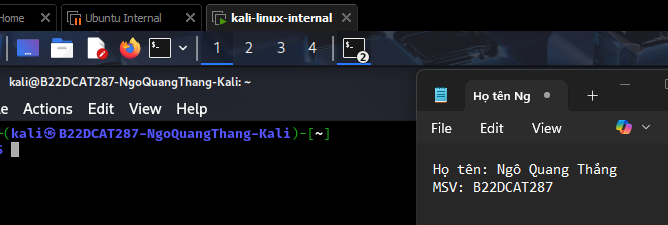
*sudo nano /etc/hosts*

o Thay đổi thành: *127.0.1.1 B22DCAT287-NgoQuangThang-Kali*





o Thực hiện lệnh : *sudo reboot* -> ta thay đổi thành công

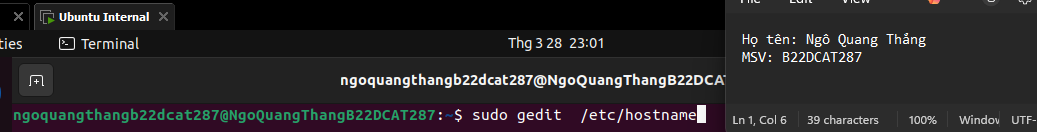


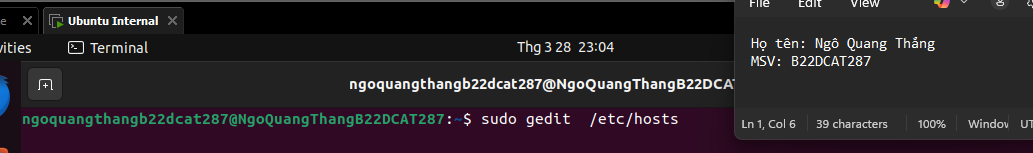
**Với máy Ubuntu:**

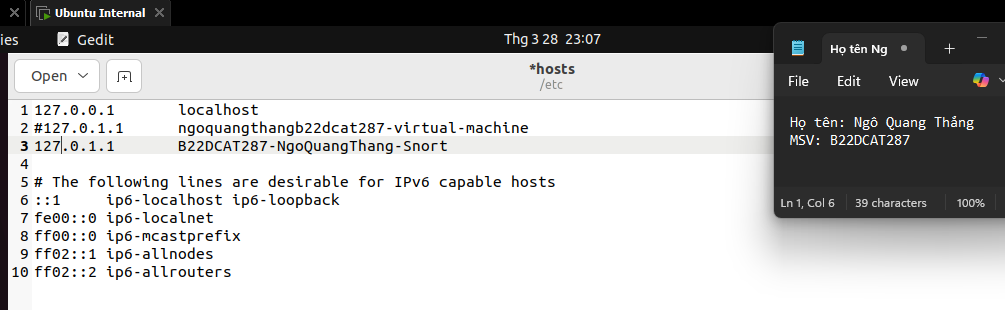
o Thực hiện các lệnh tương tự như bên kali với tên:

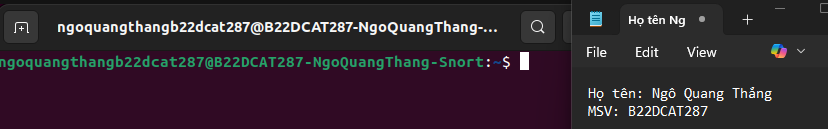
*B22DCAT287-NgoQuangThang-snort*

-> sau đó: *sudo reboot* ta thay đổi thành công





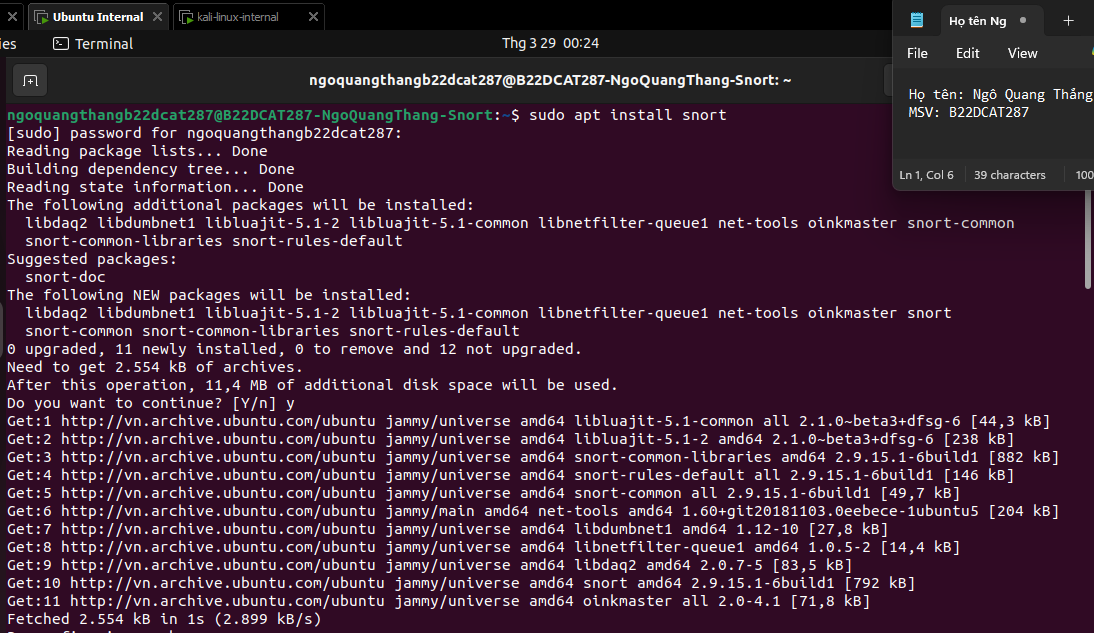




- **Bước 2**: Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.

o Thực hiện cài đặt snort:

*sudo apt install snort*



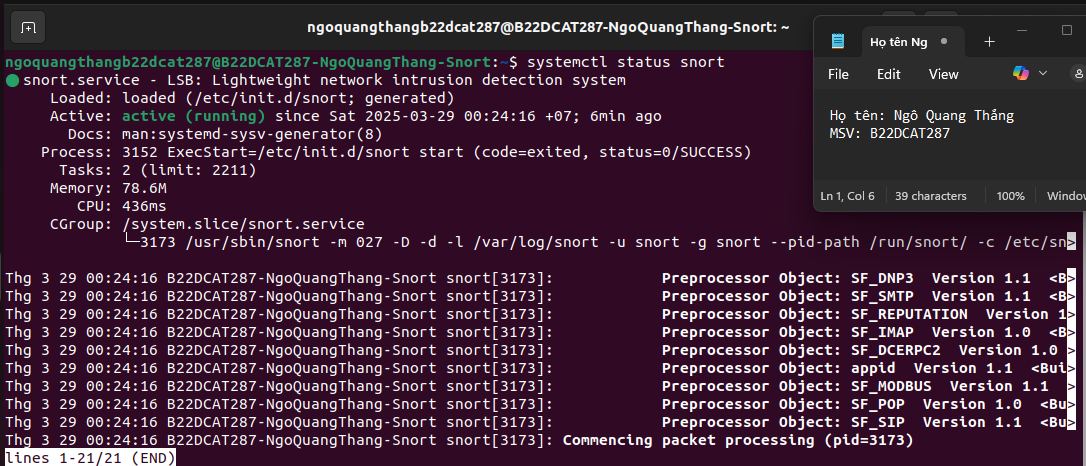
o Kiểm tra phiên bản xem đã cài đặt thành công chưa:

*snort –version*



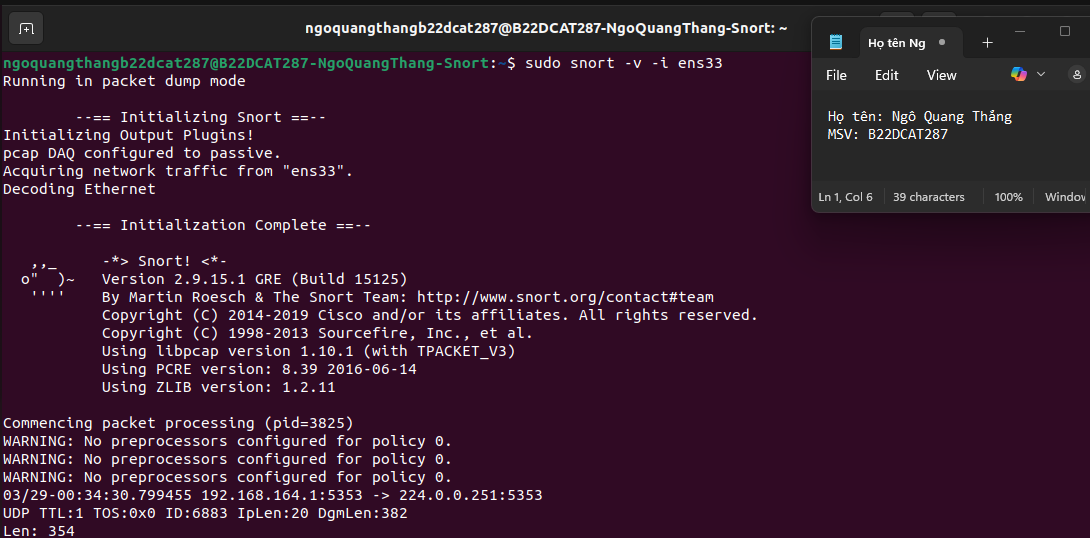
o Kiểm tra xem snort đã hoạt động chưa:

*systemctl status snort*



o Thực hiện khởi động snort:

*sudo snort -v -i ens33*



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

o Thay đổi trong tệp local.rules:

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



+ Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện: “-Snort phát hiện có các gói Ping gửi đến.”

*#Rule 1: ping*

*alert icmp any any -> $HOME\_NET any (msg:"B22DCAT287-NgoQuangThang kiem tra co cac goi ping gui đen"; sid:1000001; rev:1;)*

+ Phát hiện các gói tin rà quét từ bất kỳ một máy nào gửi đến máy chạy Snort trên cổng 80. Hiển thị thông điệp khi phát hiện: “-Snort phát hiện có các gói tin rà quét trên cổng 80.”

*#Rule2: TCP scan port 80*

*alert tcp any any -> $HOME\_NET 80 (msg:"B22DCAT287-NgoQuangThang kiem tra co cac goi tin ra quet tren cong 80"; sid:1000002; rev:1;)*

+ Phát hiện tấn công TCP SYN Flood từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện: “-Snort phát hiện đang bị tấn công TCP SYN Flood.”

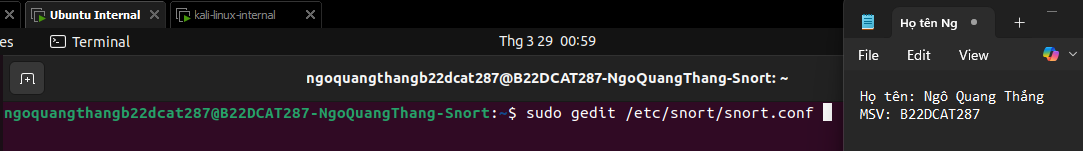
*#Rule3: TCP SYN Flood*

*alert tcp any any -> $HOME\_NET any (msg:"B22DCAT287-NgoQuangThang kiem tra bi tan cong TCP SYN Flood"; sid:1000003; rev:1;)*



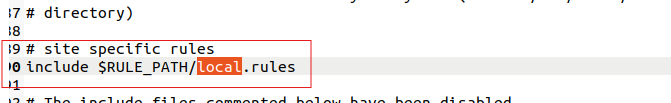
o Kiểm tra các luật được thêm chưa(thường mặc định là tự động them)

*sudo gedit /etc/snort/snort.conf*



o Kiểm tra thấy:

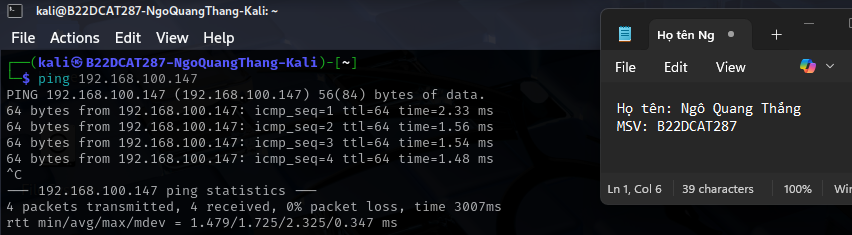
*include $RULE\_PATH/local.rules* -> được thêm thành công



- **Bước 4**: Thực thi tấn công và phát hiện sử dụng Snort

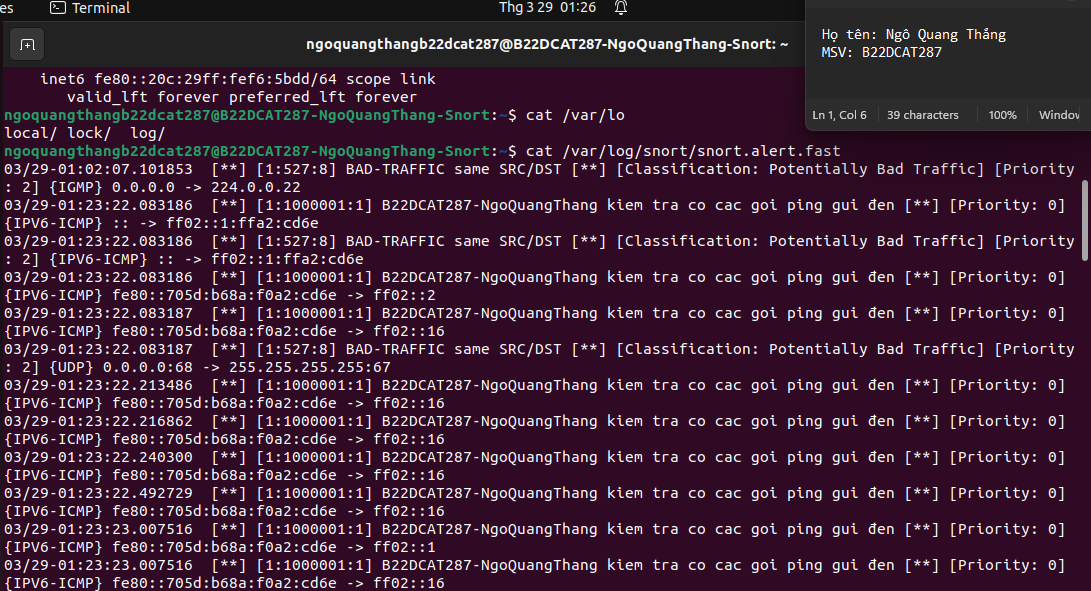
+ Từ máy Kali, sử dụng lệnh ping để ping máy Snort.

*ping 192.168.100.147*



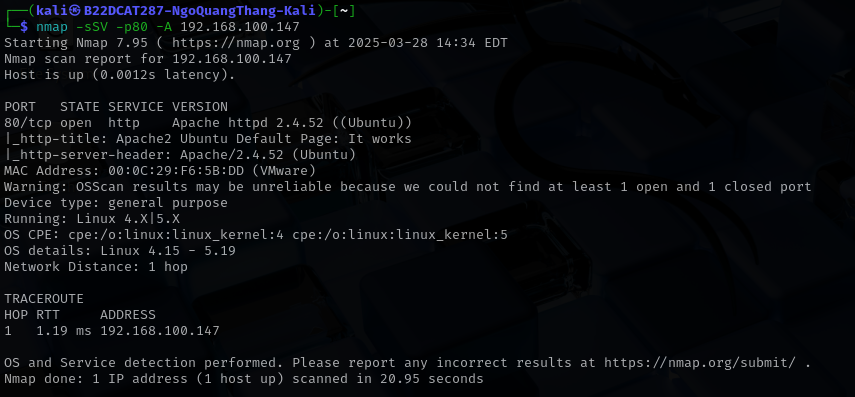
o Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

*cat /var/log/snort/snort.alert.fast*



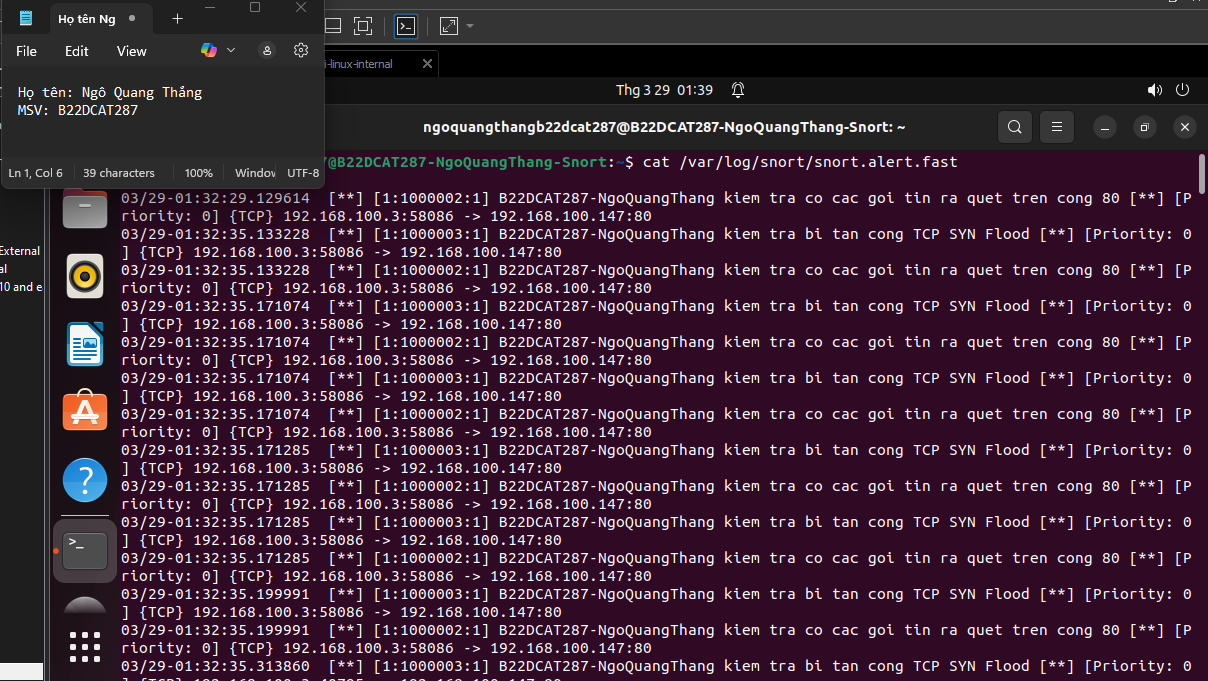
+ Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort :

*nmap -sV -p80 - A 192.168.100.147.*



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

*cat /var/log/snort/snort.alert.fast*

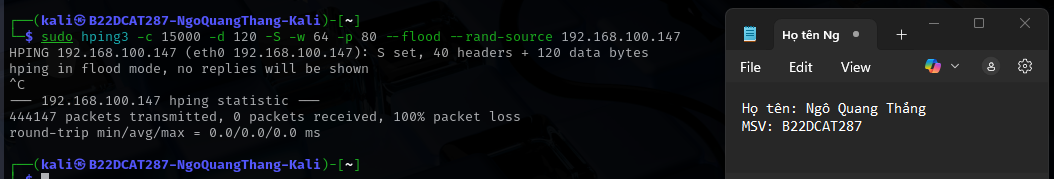


+ Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort

*sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.100.147*

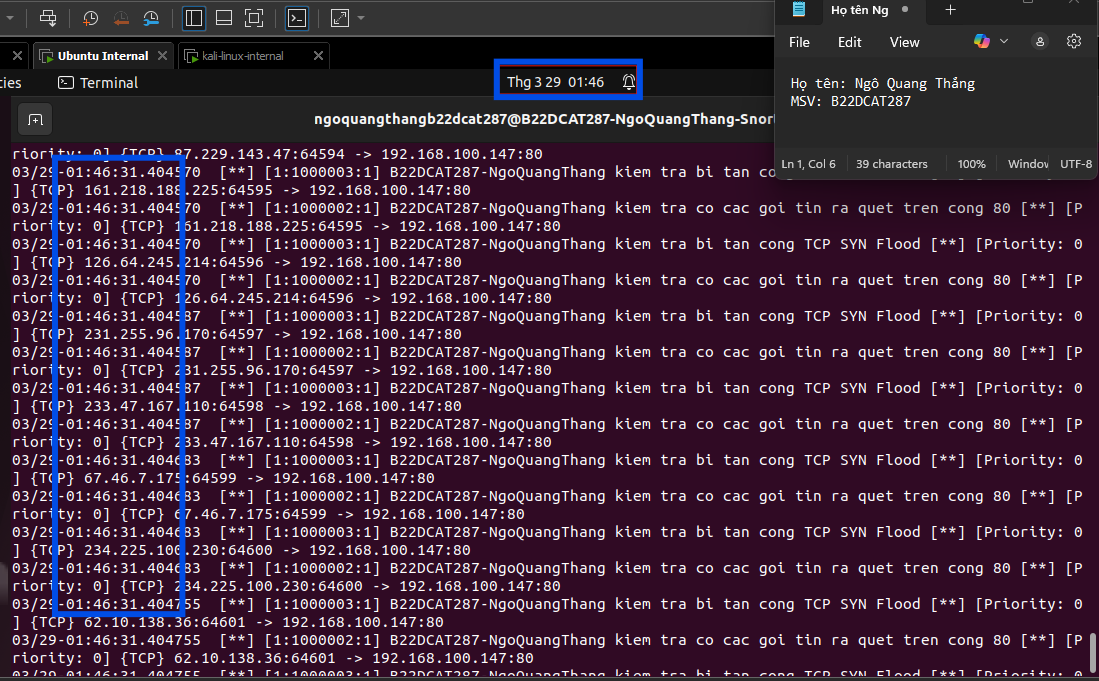
o Nếu máy không cài sẵn có thể cài đặt:

*sudo apt update && sudo apt install hping3 -y*



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

*cat /var/log/snort/snort.alert.fast*



TÀI LIỆU THAM KHẢO

[1]. Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 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