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: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SIEM	Security Information and Event Management	Giải pháp giám sát, phát hiện và phản ứng nhanh với mối đe dọa.
DNS	Domain Name System	Giao thức tên miền
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ IP tự động
IIS	Internet Information Services	Dịch cụ Web Server chính của Microsoft
WAS	Windows Process Activation Service	Dịch vụ hỗ trợ cho IIS

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

I. 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.

II. Tìm hiểu lý thuyết

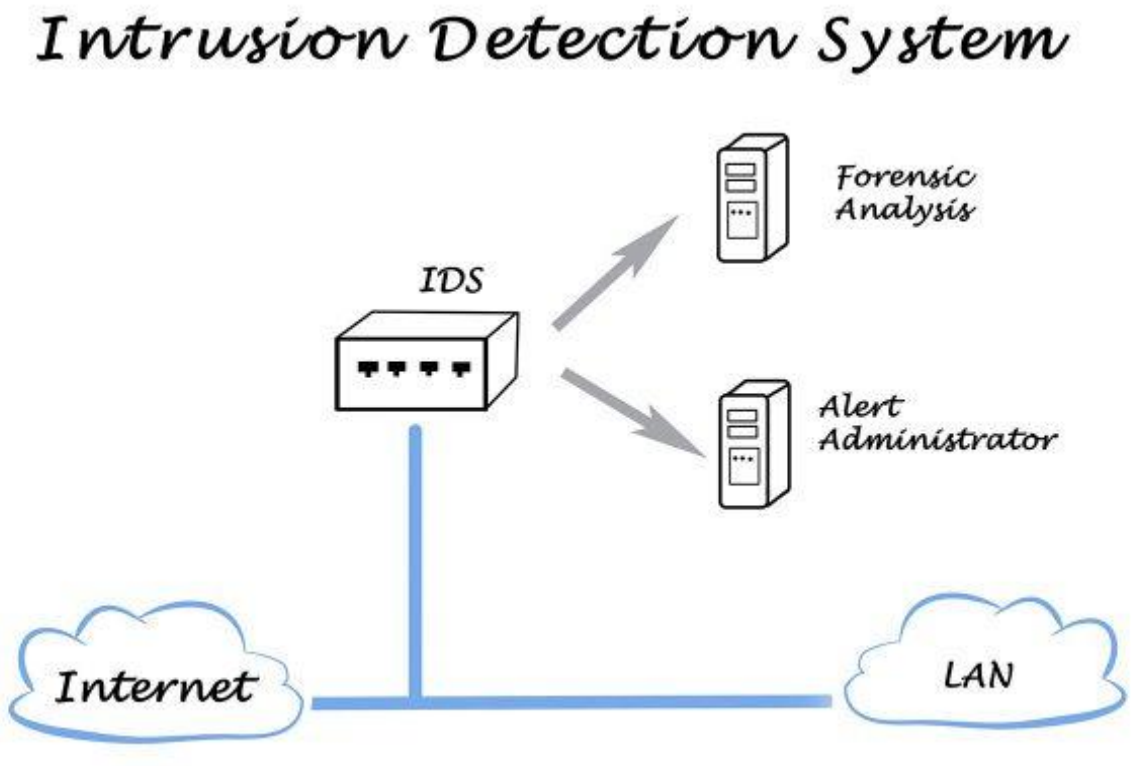
1. Hệ thống phát hiện tấn công, xâm nhập

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 ảnh 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.

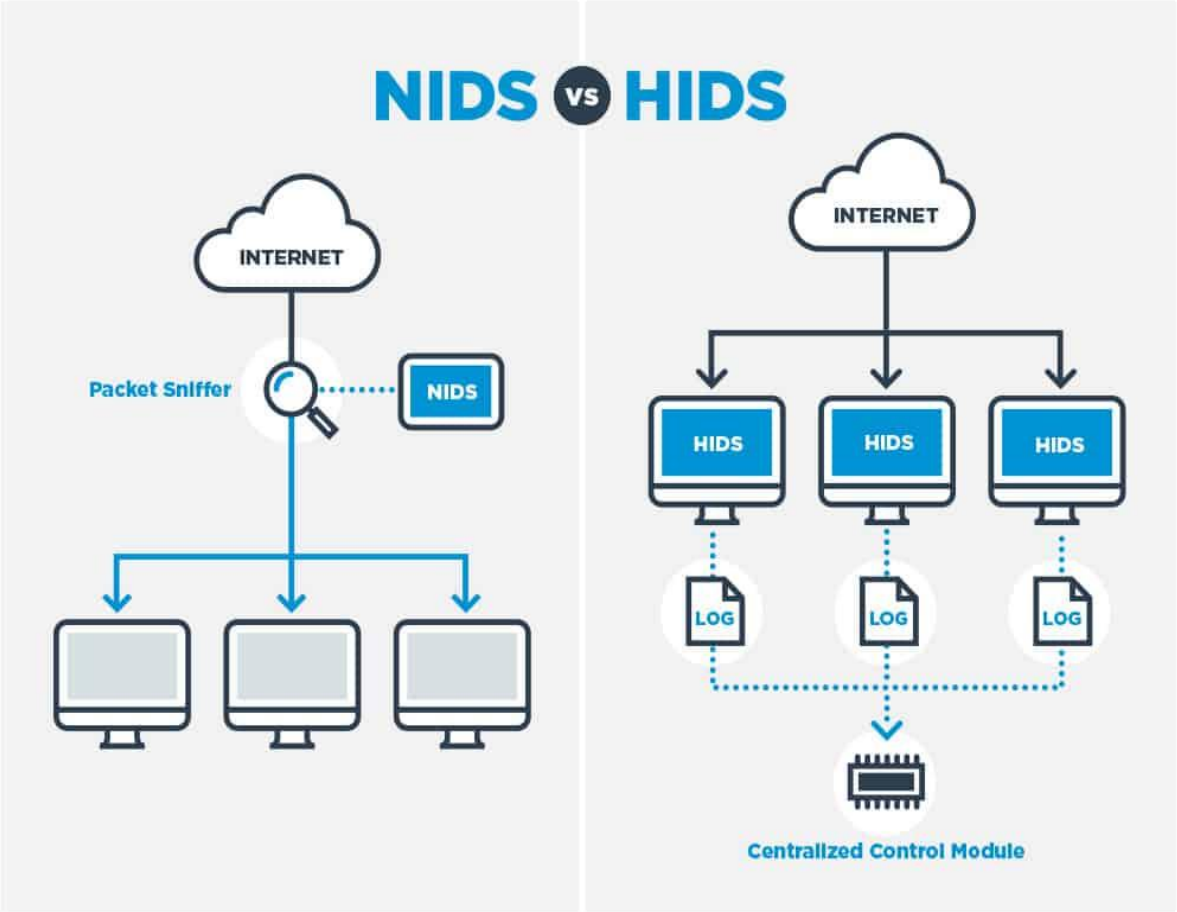
Để tránh cản trở luồng lưu lượng hợp lệ, NIDS thường được đặt "ngoài băng tần", nghĩa là lưu lượng không đi trực tiếp qua nó. NIDS phân tích các bản sao của các gói mạng thay vì chính các gói đó. Theo cách đó, lưu lượng hợp lệ không phải chờ phân tích, nhưng NIDS vẫn có thể bắt và đánh dấu lưu lượng 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 11 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.



Hình ảnh 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 hổng phần mềm trước khi nhà phát triển phần mềm biết về chúng hoặc có thời gian để vá chúng.

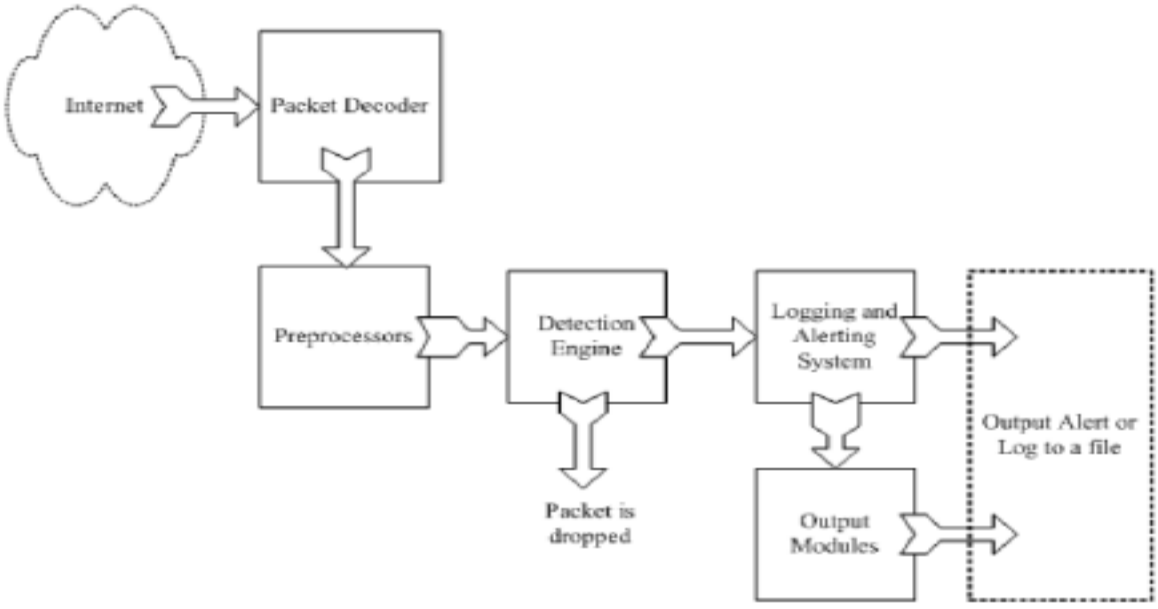
1.2.2 *Kiến trúc và tính năng một số hệ thống phát hiện tấn công, xâm nhập*

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 ảnh 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 tiểu chuẩn để áp dụng luật với gói tin đó.

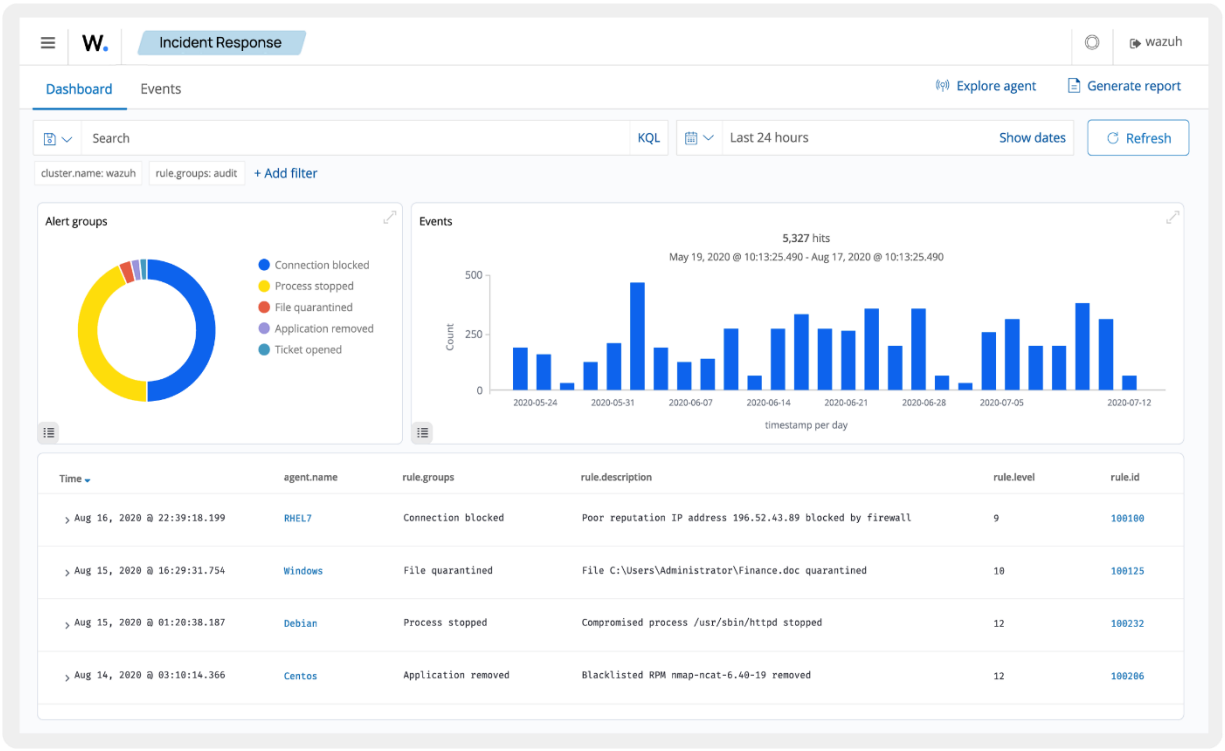
alert tcp 192.168.0.0/22 23 -> any any

-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.



Hình ảnh 4: Cách hoạt động của Wazuh.

*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

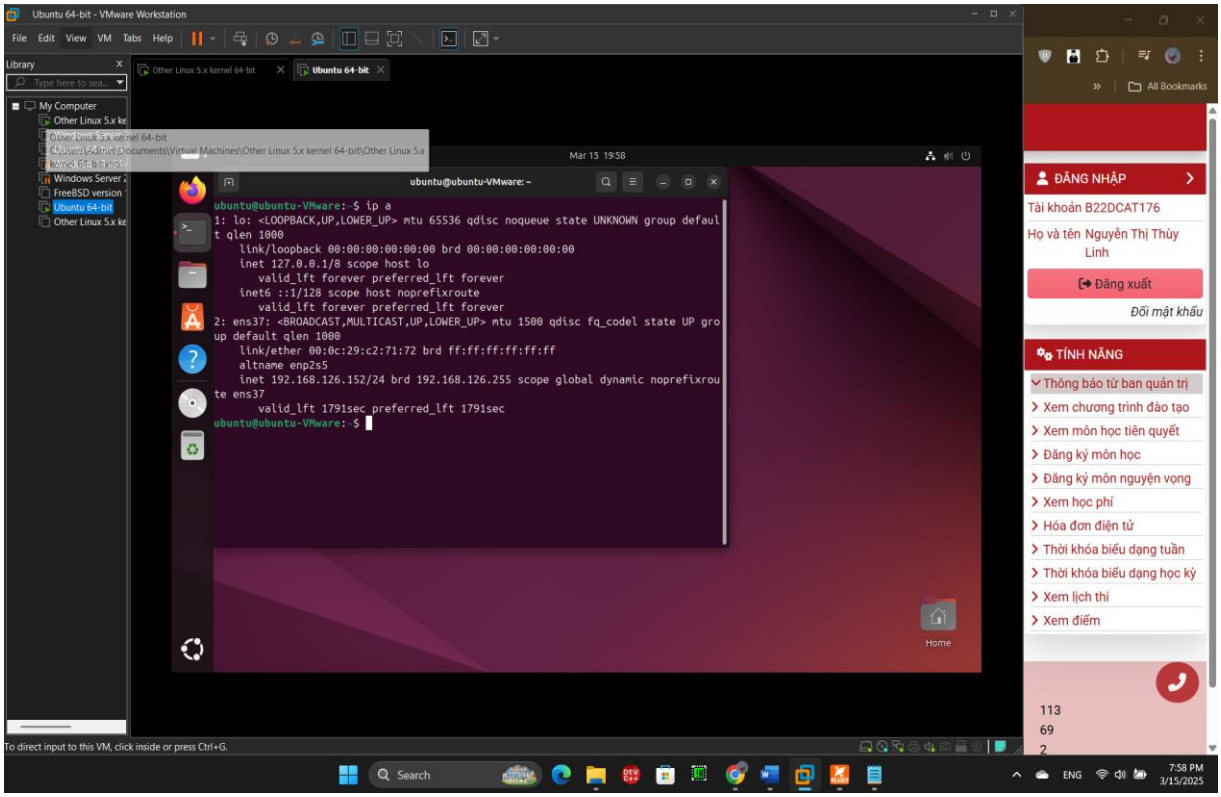
I. Chuẩn bị môi trường

- 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.

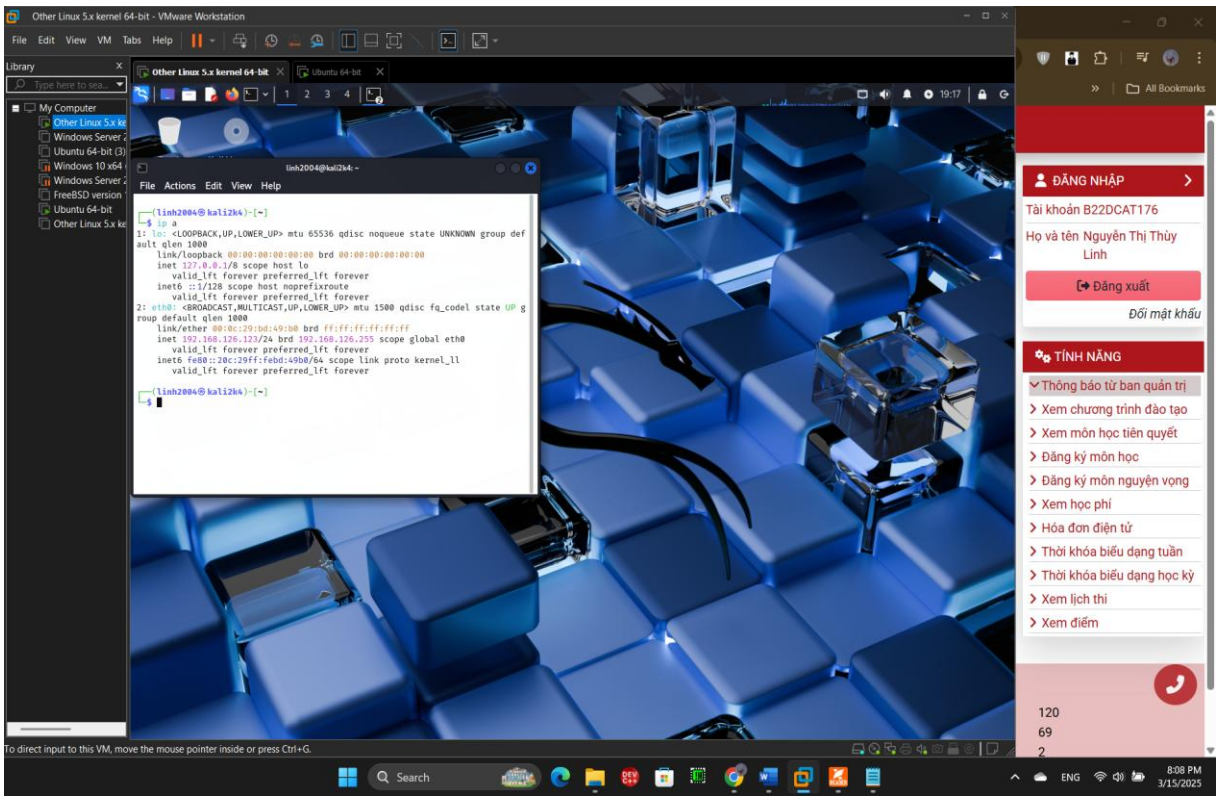
II. Các bước thực hiện

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.

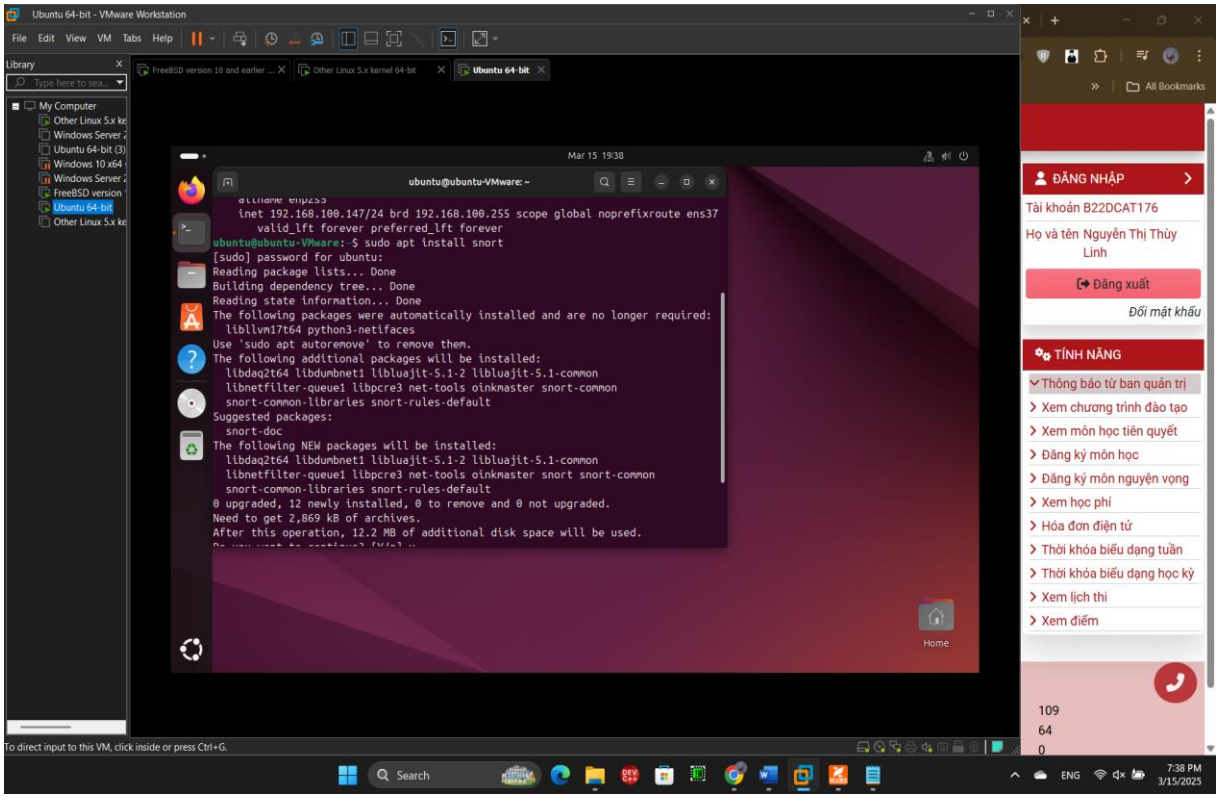


Hình ảnh 5: Địa chỉ IP của máy Ubuntu cài đặt Snort.



Hình ảnh 6 : Địa chỉ IP của máy Kali tấn công

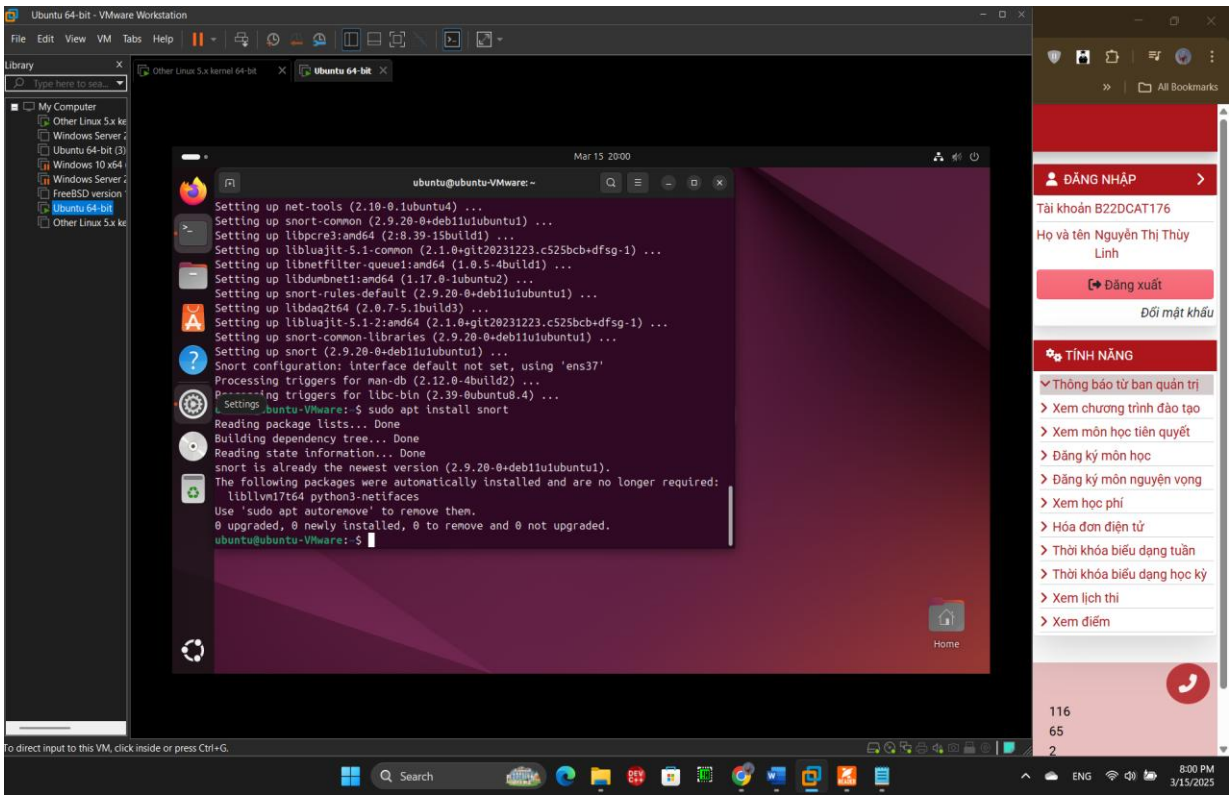
- Tiến hành cài đặt Snort bằng lệnh "*sudo apt install snort*".



Hình ảnh 7: Cài đặt Snort.

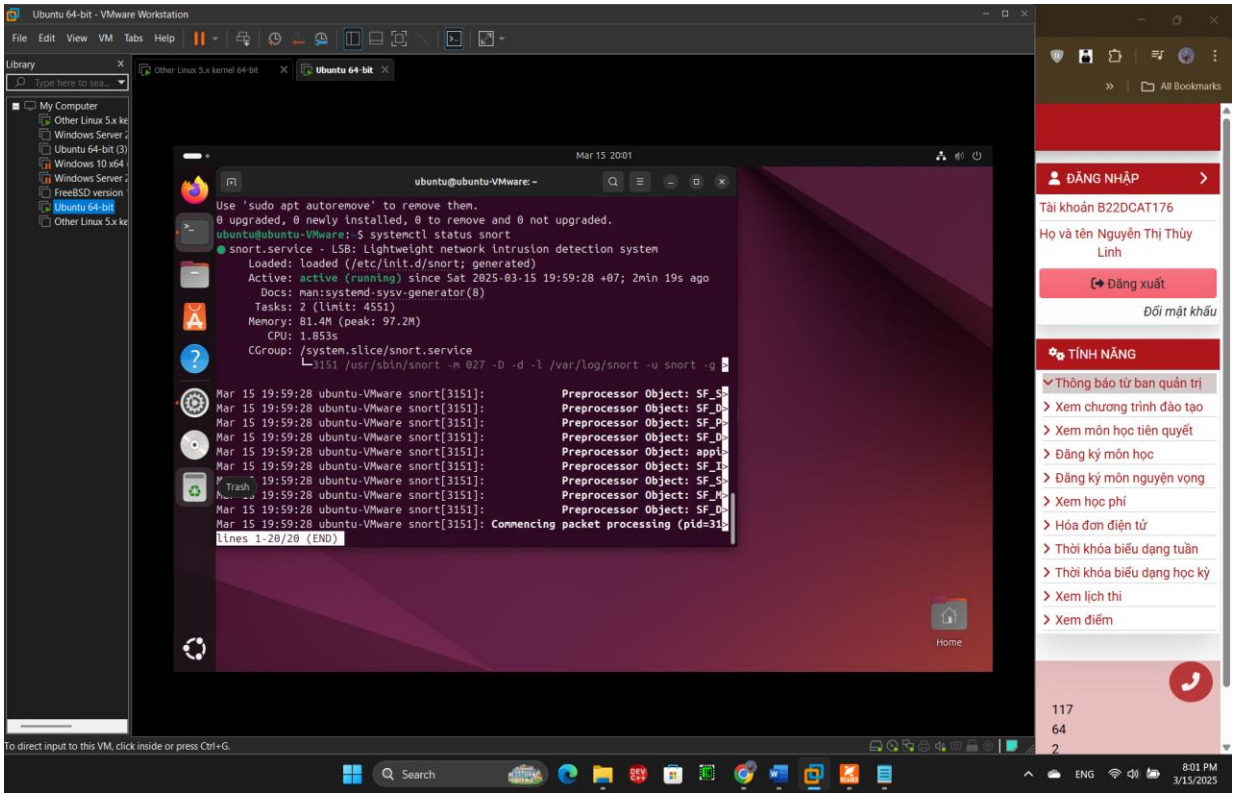
- Lựa chọn cấu hình giao diện mạng để Snort bắt các gói tin trong quá trình cài đặt Snort.

Kiểm tra bằng lệnh "ip a" hoặc "ifconfig" trên máy Ubuntu Linux xem giao diện mạng nào đang được sử dụng. Ở đây là "ens37". Sau đó, cài đặt Snort thành công.



Hình ảnh 8 : Cài đặt Snort thành công.

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



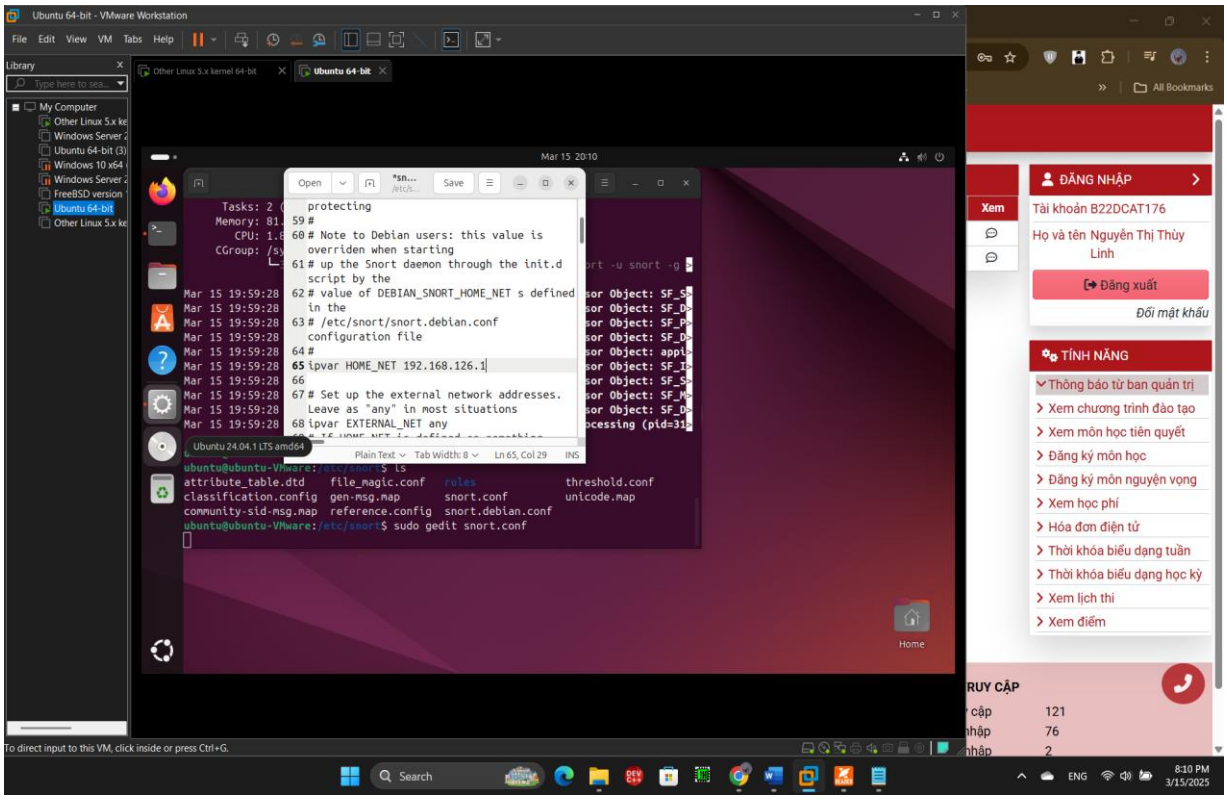
Hình ảnh 9: Kiểm tra trạng thái hoạt động của Snort.

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 "192.168.126.1"

-Lưu lại để hoàn tất.



Hình ảnh 10: Cấu hình cho Snort.

-Ta kiểm tra cấu hình đúng hay chưa bằng lệnh

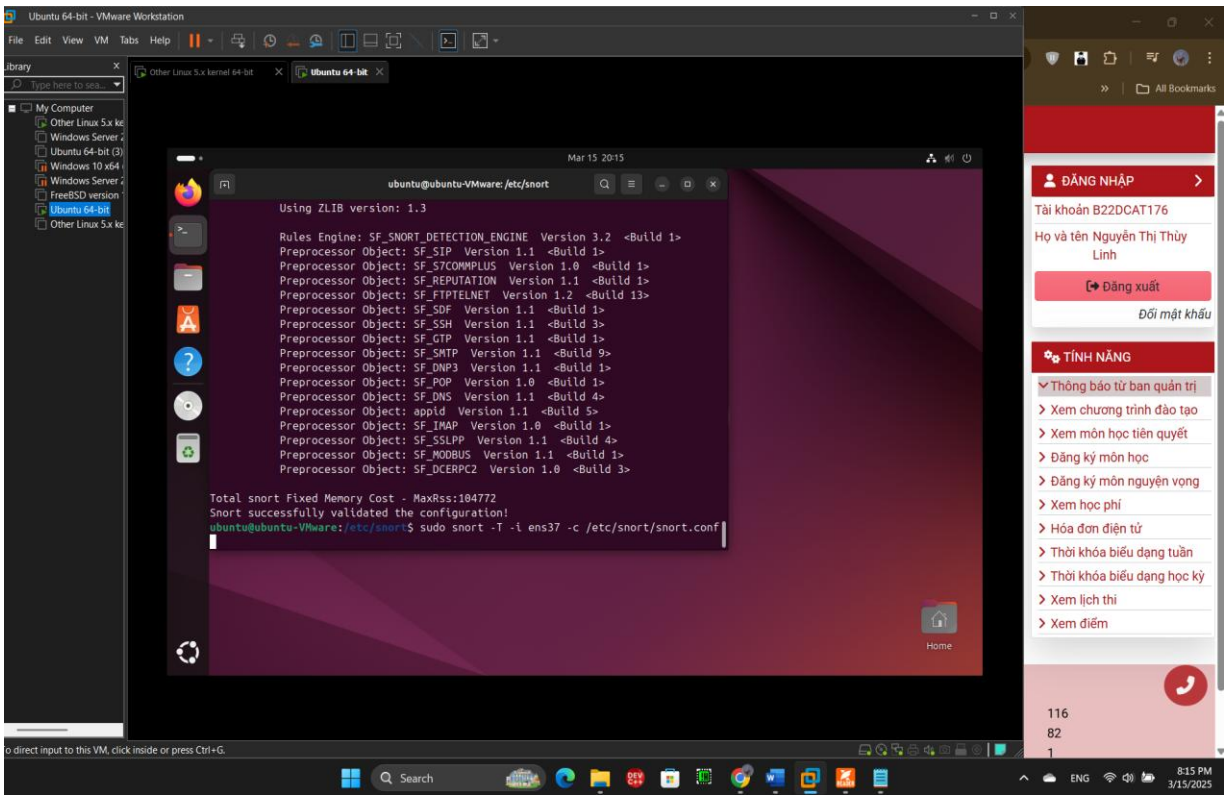
"sudo snort -T -t ens33 -c /etc/snort/snort.conf"

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

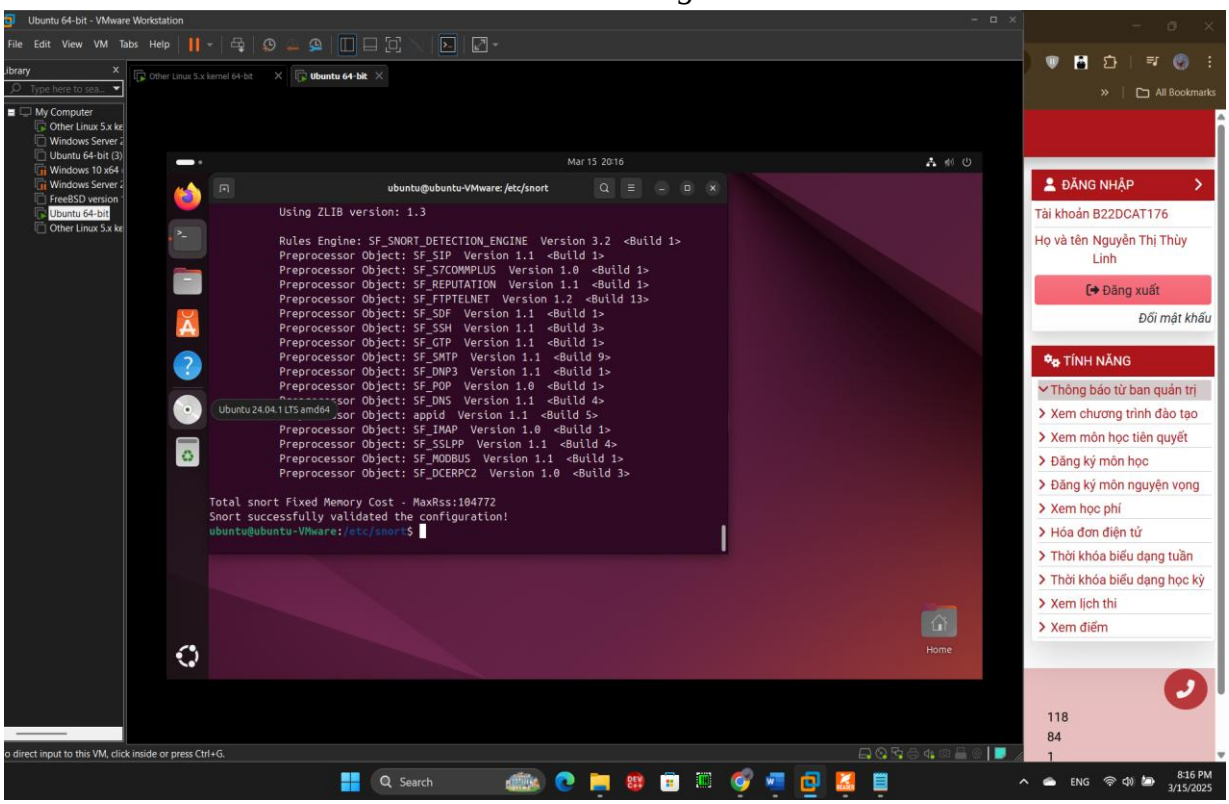
-t ens33 → Chỉ định giao diện mạng (ens33) để Snort kiểm tra.

-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.



Hình ảnh 11: Kiểm tra thông tin cấu hình



Hình ảnh 12: Kiểm tra thành công.

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

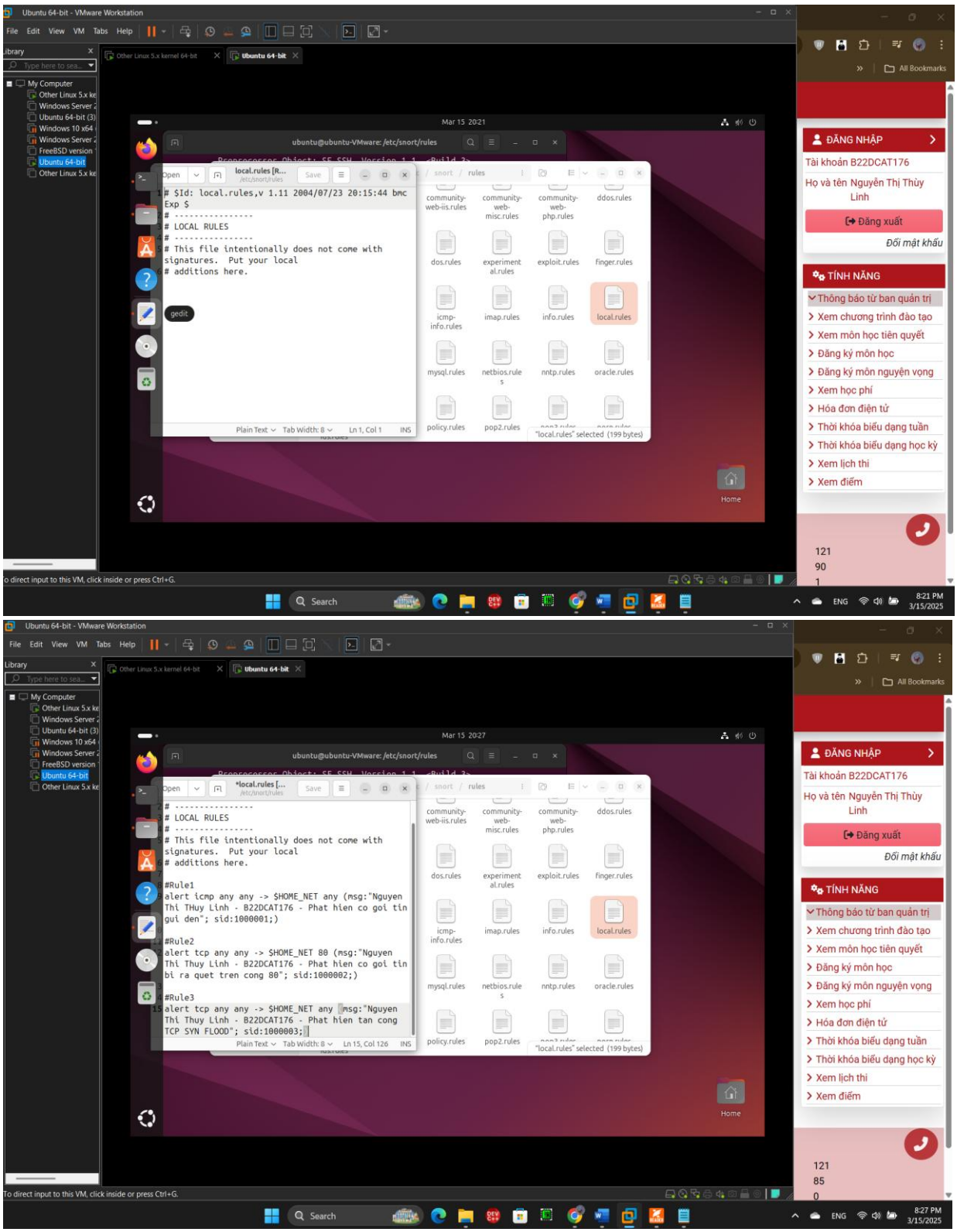
-Di chuyển đến đường dẫn "/etc/snort/rules/local.rules"

-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 en33”. Lệnh này cho phép ta xem các cảnh báo khi bị tấn công sau khi cấu hình.



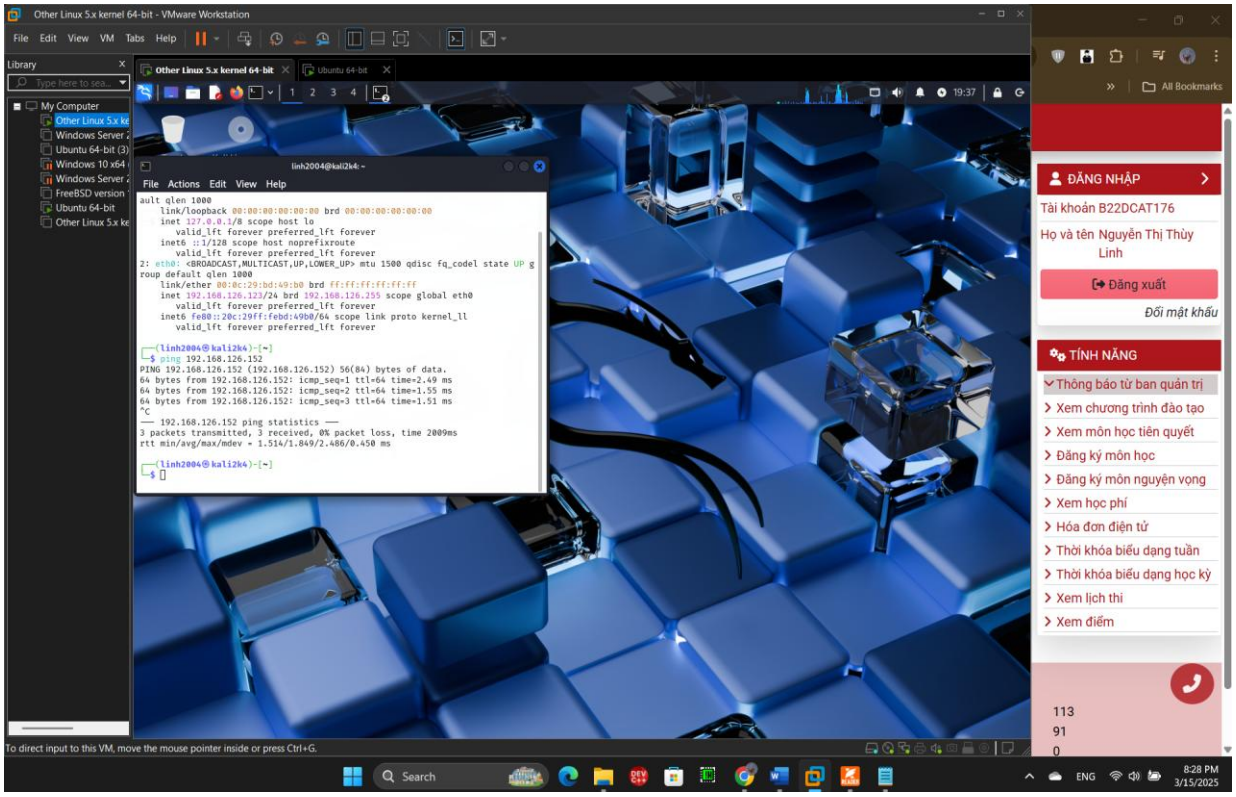
Hình ảnh 13: Tạo luật cho Snort.

2.2.3 Thực hiện tấn công và phát hiện sử dụng Snort

-Sử dụng file snort.alert.fast để xem log những địa chỉ nào đã từng ping tới máy Snort.

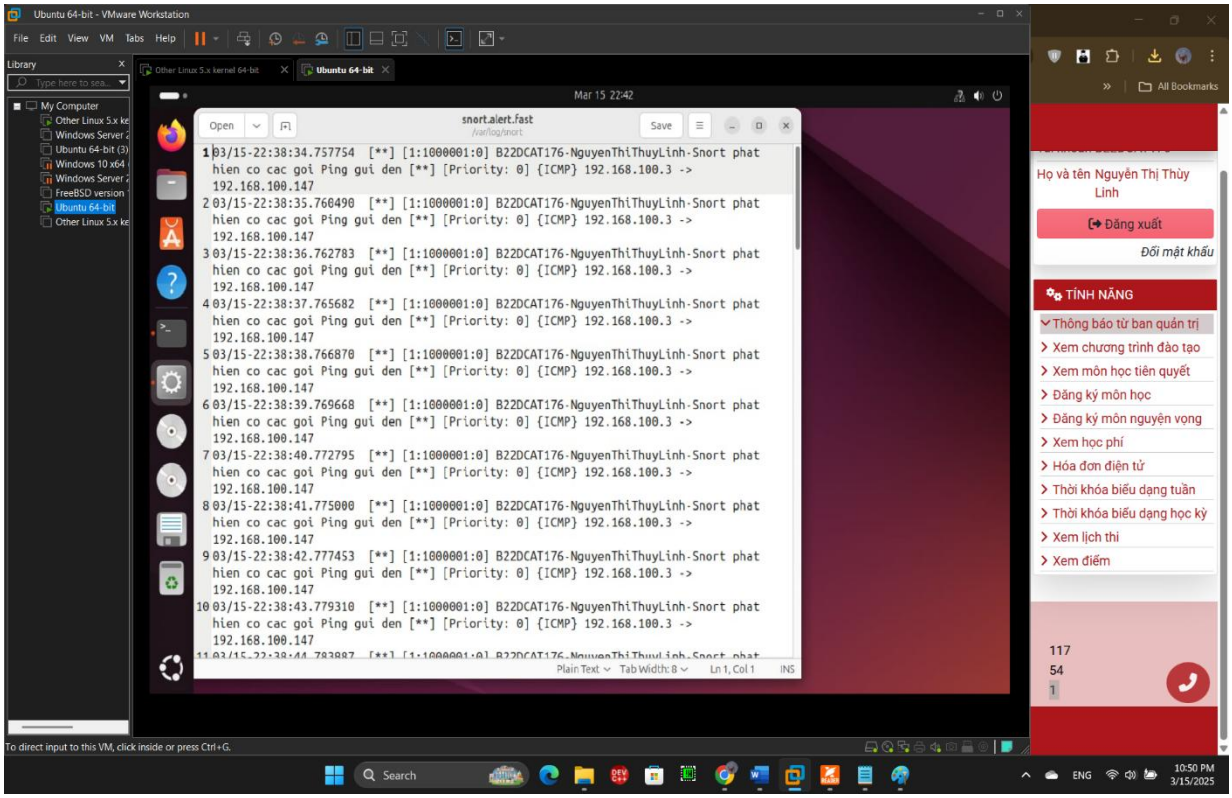
Thực hiện tấn công thứ nhất:

-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 ảnh 14: Thực hiện ping từ máy Kali.

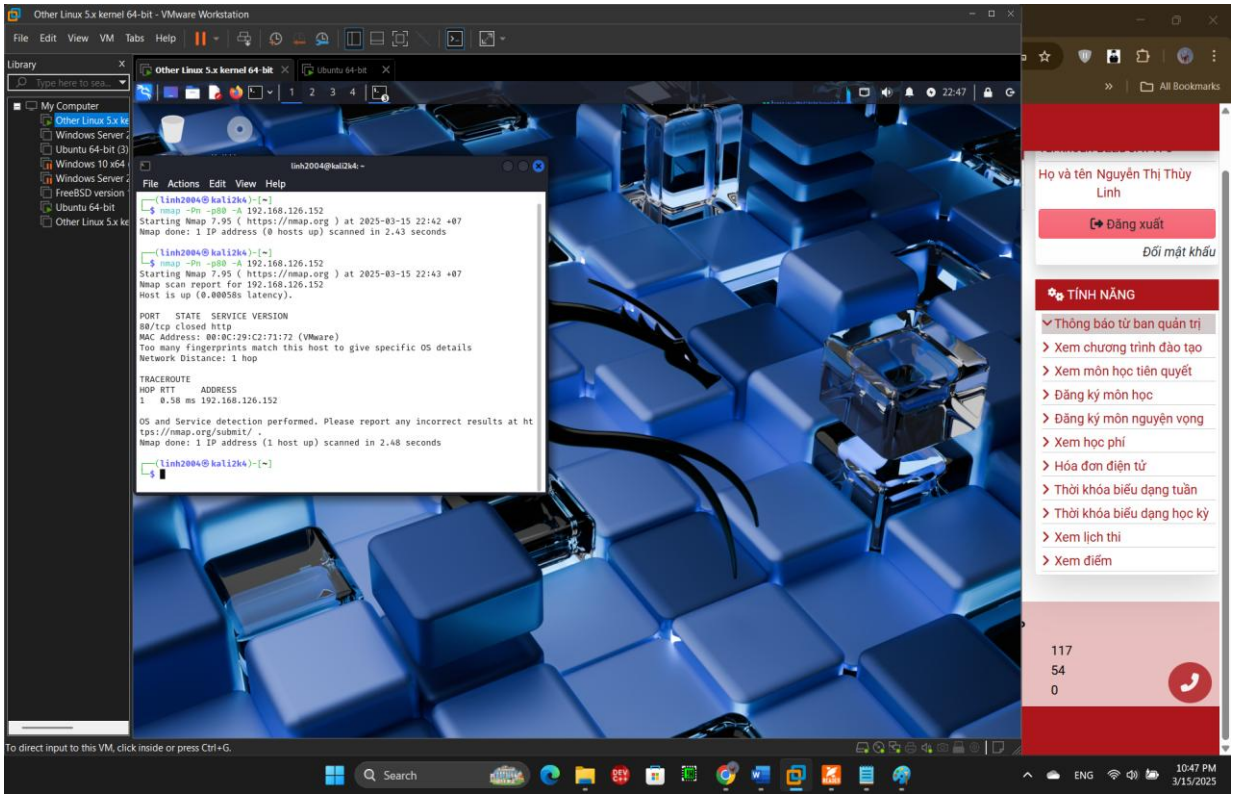
- Máy Snort đã nhận được thông báo về gói tin ICMP do lệnh Ping từ máy Kali như đã cấu hình ở luật Rule1.



Hình ảnh 15: Snort nhận được cảnh báo.

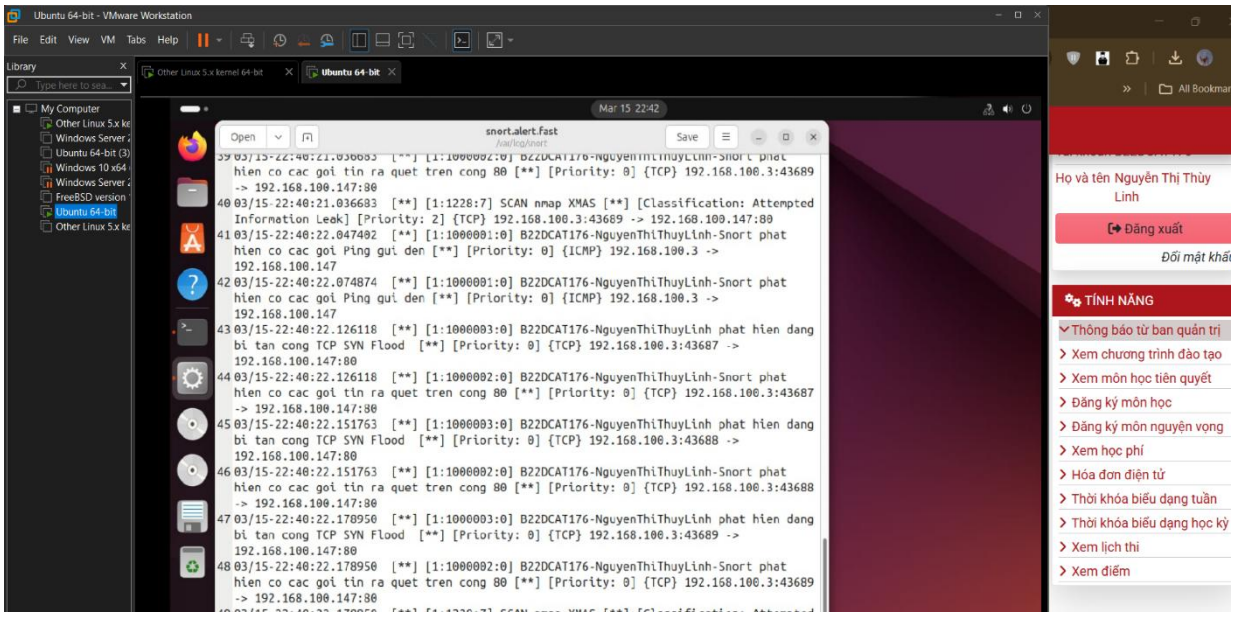
Thực hiện tấn công số 2:

- 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.



Hình ảnh 16: Nmap đến máy chạy Snort.

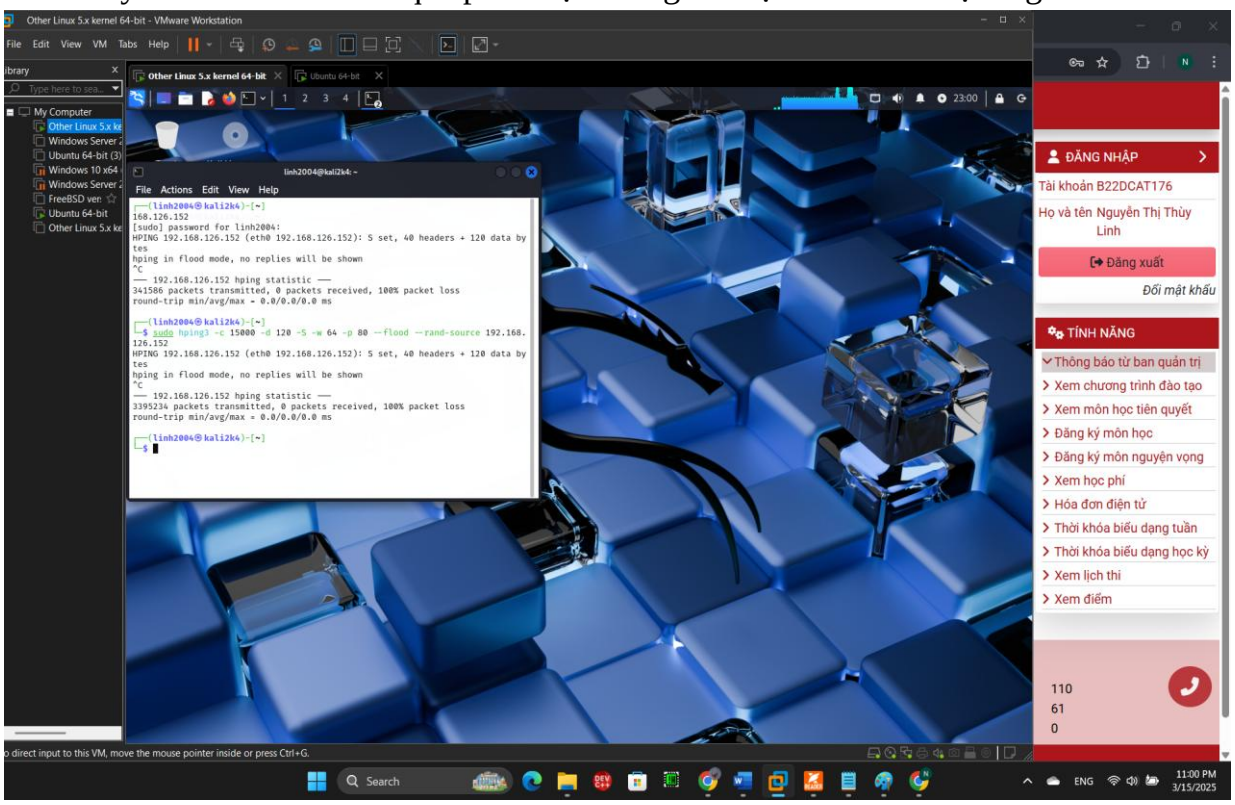
- Máy Snort đã nhận được cảnh báo về gói tin bị rà quét trên cổng 80.



Hình 17: Snort nhận được cảnh báo

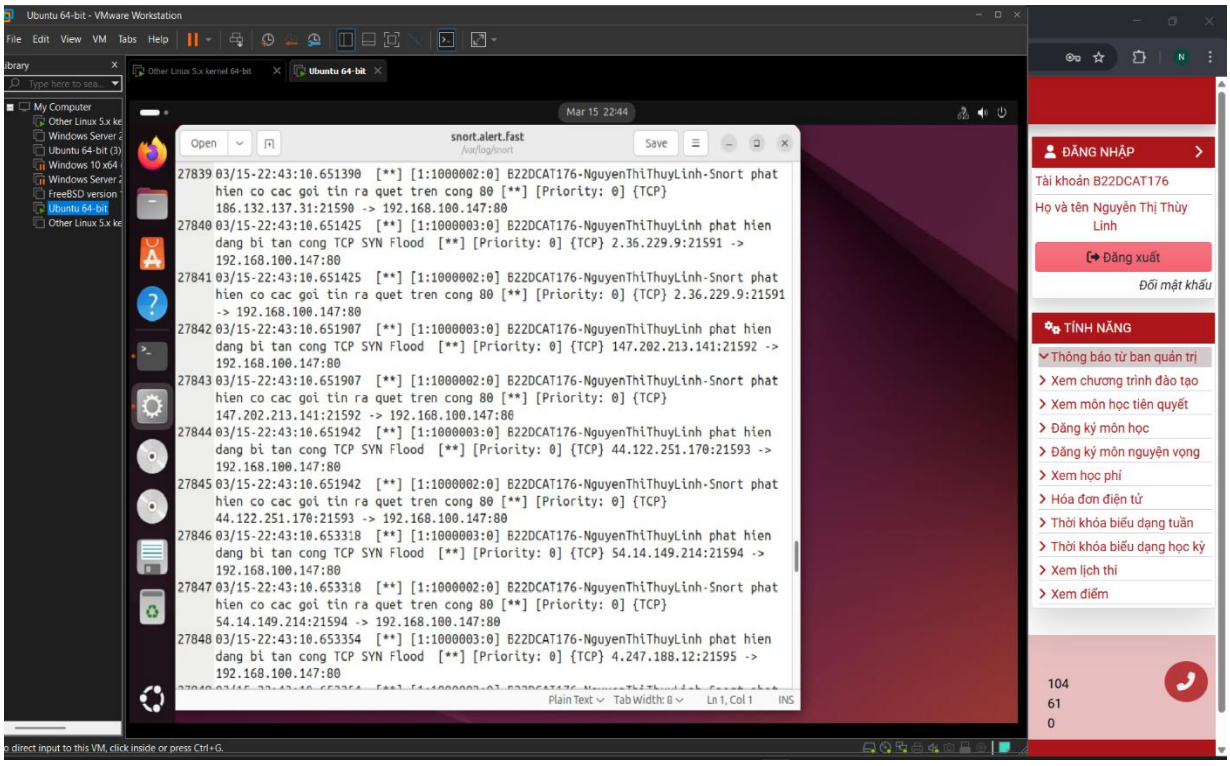
Thực hiện tấn công số 3:

-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.



Hình ảnh 18: Hping đến máy chạy Snort.

-Máy Snort đã nhận được cảnh báo về tấn công TCP SYN FLOOD.



Hình ảnh 19: Nmap đến máy chạy Snort.

TÀI LIỆU THAM KHẢO

[1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.

[2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.

[3] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.