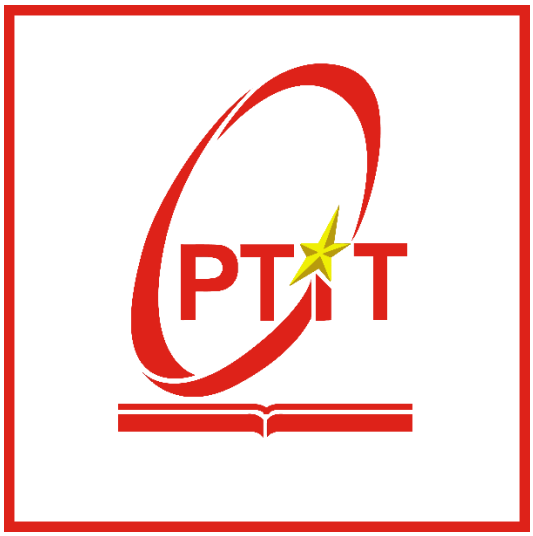
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



Môn học: **THỰC TẬP CƠ SỞ**

BÁO CÁO BÀI THỰC HÀNH SỐ 6

CÀI ĐẶT CẤU HÌNH HIDS/NIDS

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 3/2024 ~

Mục Lục

BÀI 6: Cài đặt, cấu hình HIDS/NIDS

1 Mục đích

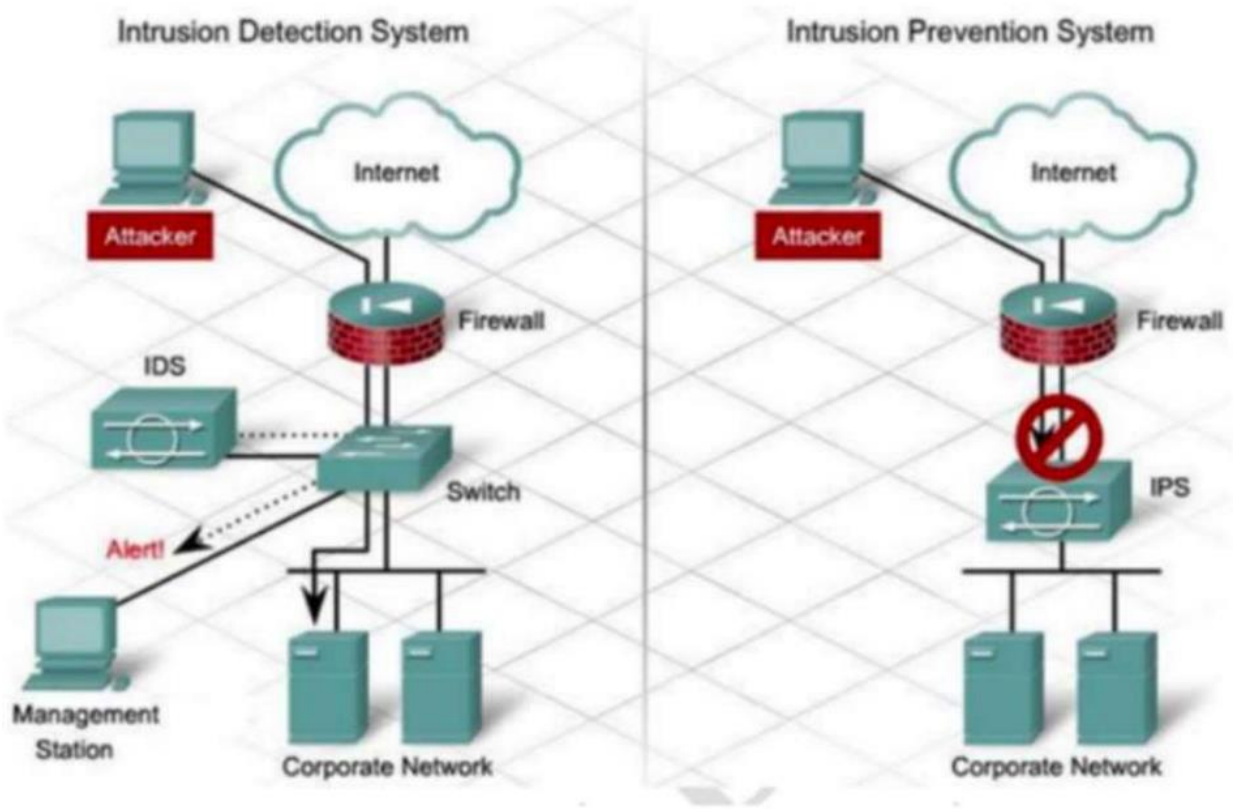
Luyện tập việc cài đặt và vận hành các hệ thống phát hiện xâm nhập cho host (HIDS) và cho mạng (NIDS).

Luyện tập việc tạo và chỉnh sửa các luật phát hiện tấn công, xâm nhập cho các hệ thống phát hiện xâm nhập thông dụng.

2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết

a) 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



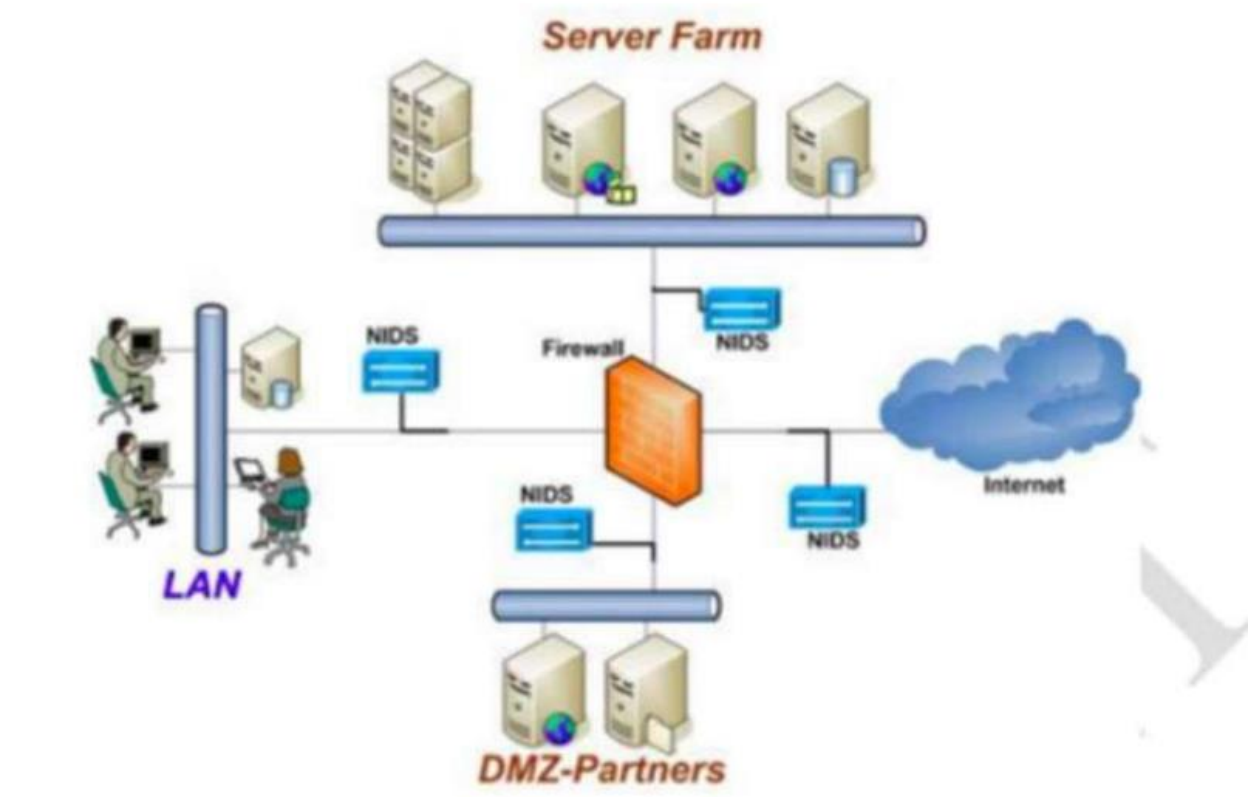
Hình 1: Vị trí các hệ thống IDS và IPS trong sơ đồ mạng

- Khái quát: Các hệ thống phát hiện, ngăn chặn tấn công, xâm nhập (IDS/IPS) là một lớp phòng về 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). IDS (Intrusion Detection System) là hệ thống phát hiện tấn công, xâm nhập và IPS (Intrusion Prevention System) là hệ thống ngăn chặn tấn công, xâm nhập. Các hệ thống IDS/IPS có thể được đặt trước hoặc

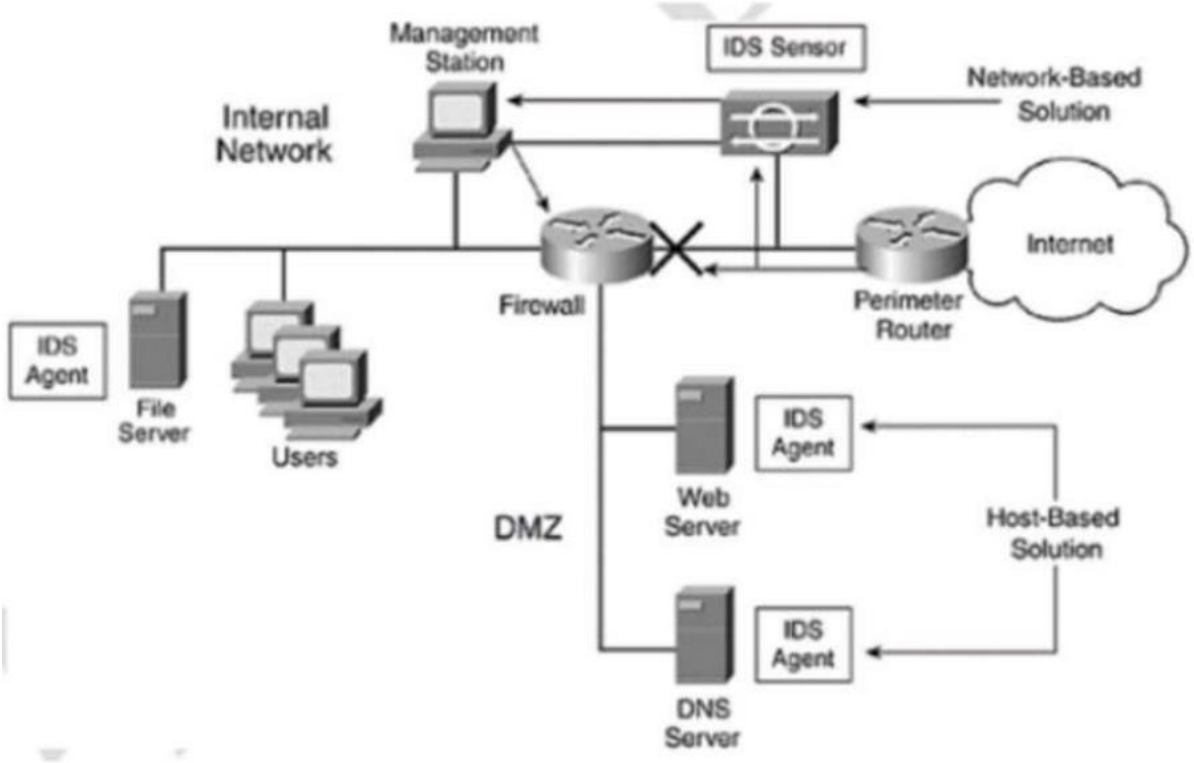
sau tường lửa trong mô hình mạng, tùy theo mục đích sử dụng. Hình 1 cung cấp vị trí các hệ thống IDS và IPS trong sơ đồ mạng, trong đó IDS thường được kết nối vào bộ switch phía sau tường lửa, còn IPS được ghép vào giữa đường truyền từ cổng mạng, phía sau tường lửa.

- Nhiệm vụ chính của hệ thống IDS/IPS 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
  - Ngăn chặn hoặc dừng các hành vi tấn công, xâm nhập;
  - Gửi thông báo cho người quản trị về các các hành vi tấn công, xâm nhập đã phát hiện được.
- Về cơ bản IDS và IPS giống nhau về chức năng giám sát lưu lượng trong mạng hoặc các sự kiện trong hệ thống. Tuy nhiên, IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công, xâm nhập bị phát hiện. Trong khi đó, 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.

- Phân loại:



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



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

Có 2 phương pháp phân loại chính các hệ thống IDS và IPS, 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.
- 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 5.20 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 (1) phát hiện xâm nhập dựa trên chữ ký, hoặc phát hiện sự lạm dụng (Signature-based / misuse intrusion detection) và (2) phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection).

b) Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập, như Snort, Suricata, Zeek, OSSEC, Wazuh...

- Snort: Snort là phần mềm IDS được phát triển bởi Martin Roesh dưới dạng mã nguồn mở. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá rất cao về khả năng phát hiện xâm nhập. Tuy snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời. Với kiến trúc kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình. Snort có thể chạy trên nhiều hệ thống như Windows, Linux, OpenBSD, FreeBSD, Solaris … Bên cạnh việc có thể hoạt động như một ứng dụng bắt gói tin thông thường, Snort còn được cấu hình để chạy như một NIDS.

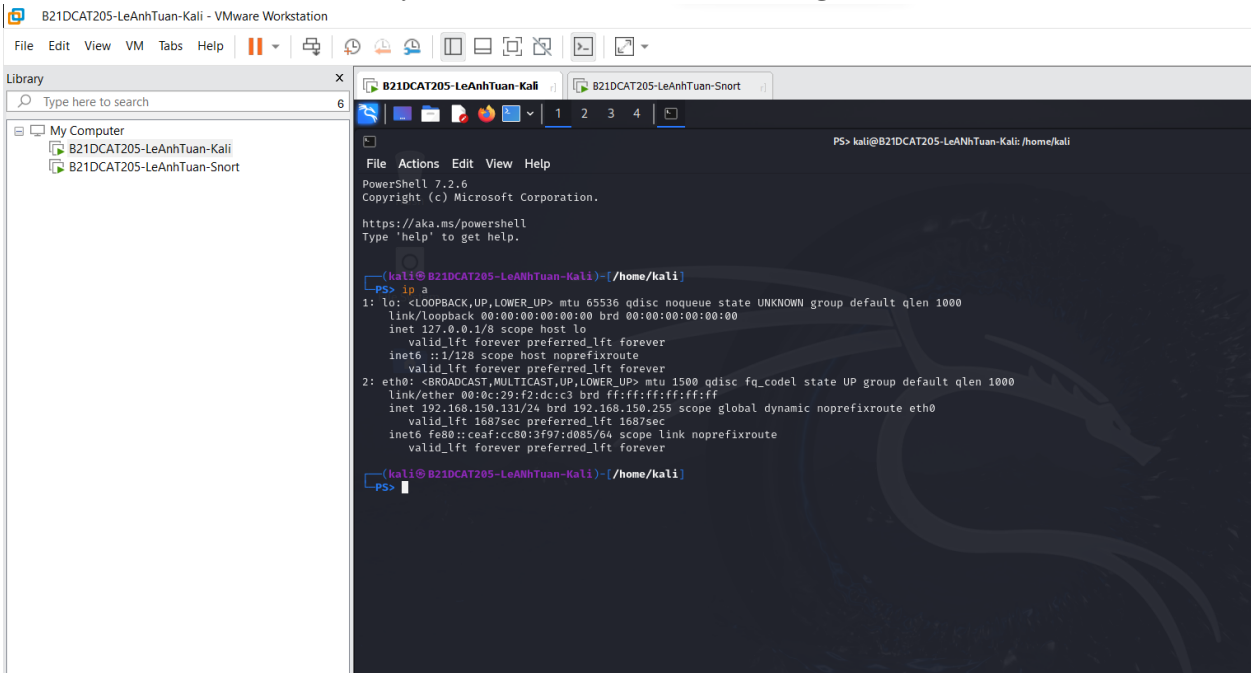
- Suricata: Suricata là giải pháp IDS/IPS mã nguồn mở hiệu quả cho các hệ thống mạng chưa được đầu tư các giải pháp IDS/IPS thương mại. Nó được xây dựng từ các thành phần khác nhau và khả năng hoạt động của nó tùy thuộc vào cách thức cấu hình, cài đặt cho hệ thống. Ở chế độ mặc định được xem là cơ chế hoạt động tương đối tối ưu cho việc phát hiện các dạng tấn công mạng.

- Zeek: Zeek được trình bày như một công cụ để hỗ trợ quản lý ứng phó sự cố an ninh . Nó hoạt động bằng cách bổ sung dựa trên chữ ký các công cụ để tìm và theo dõi các sự kiện mạng phức tạp. Nó được đặc trưng bằng cách cung cấp phản hồi nhanh, ngoài việc sử dụng nhiều luồng và giao thức. Nó không chỉ giúp xác định các sự kiện bảo mật, mà còn nhằm mục đích tạo điều kiện khắc phục sự cố

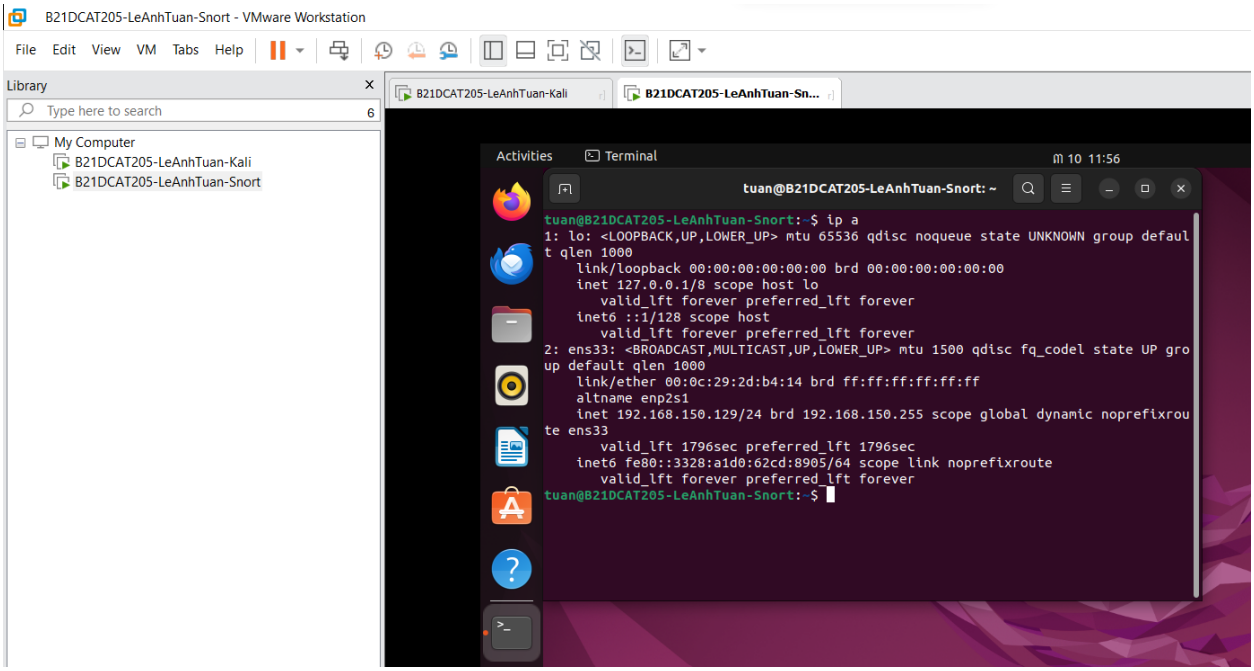
- OSSEC: OSSEC là hệ thống phát hiện xâm nhập dựa trên host (HIDS) dựatrên log mã nguồn mở, miễn phí, đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau. OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường. Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC. OSSEC có một công cụ phân tích và tương quan mạnh mẽ, tích hợp giám sát và phân tích log, kiểm tra tính toàn vẹn của file, kiểm tra registry của Windows, thực thi chính sách tập trung, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra. Các hành động này cũng có thể được định nghĩa trước bằng luật trong OSSEC để OSSEC hoạt động theo ý muốn của người quản trị. Ngoài việc được triển khai như một HIDS, nó thường được sử dụng như một công cụ phân tích log, theo dõi và phân tích các bản ghi lại, IDS, các máy chủ Web và các bản ghi xác thực. OSSEC chạy trên hầu hết các hệ điều hành, bao gồm Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris và Microsoft Windows. OSSEC còn có thể được tích hợp trong trong các hệ thống bảo mật lớn hơn là SIEM (Security information and event management). OSSEC chỉ có thể cài đặt trên Windows với tư cách là một agent.

2.2 Cài đặt

Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.2. Máy Kali Linux được đổi tên thành **B21DCAT205-LeAnhTuan-Kali** và máy cài Snort thành **B21DCAT205-LeAnhTuan-Snort**. Các máy có địa chỉ IP và kết nối mạng LAN.

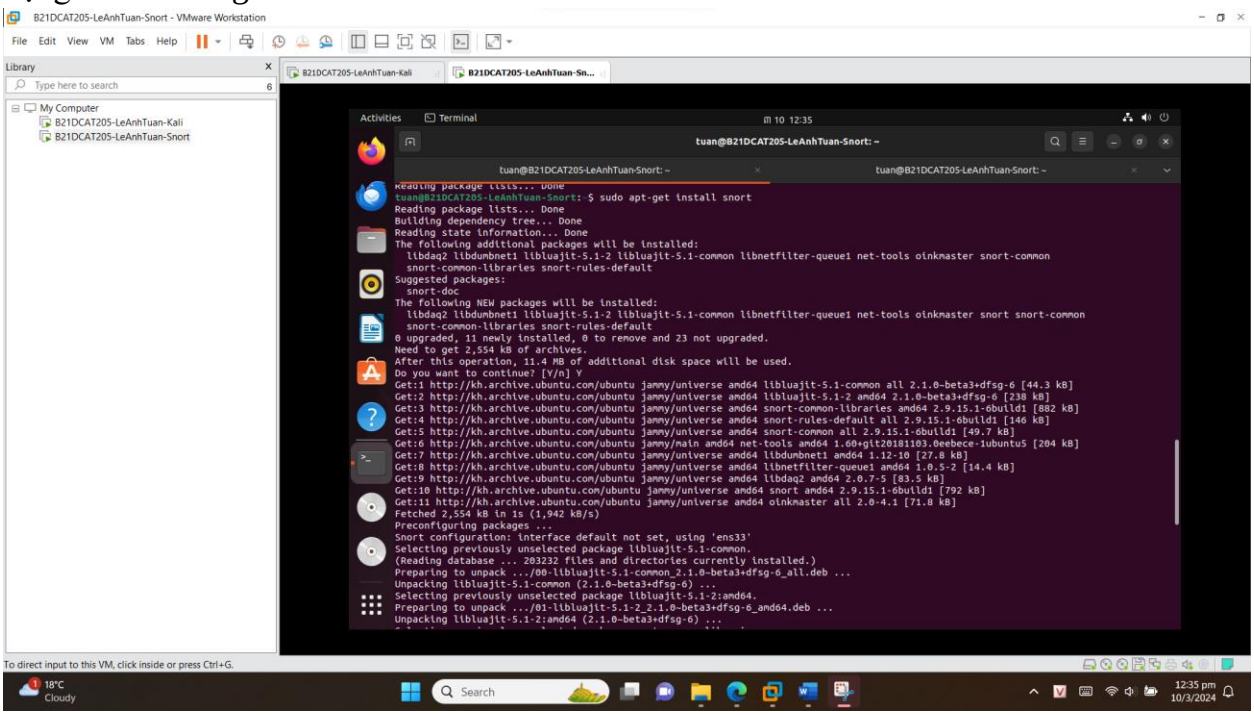


Hình 4: Máy B21DCAT205-LeAnhTuan-Kali



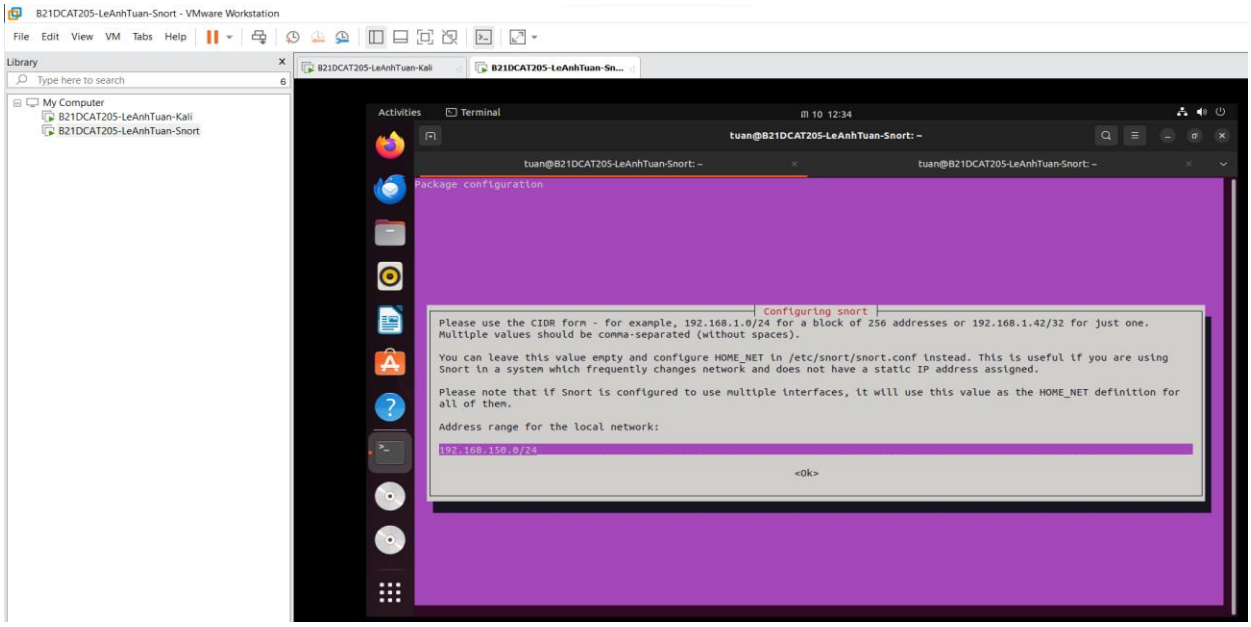
Hình 5: Máy B21DCAT205-LeAnhTuan-Snort

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

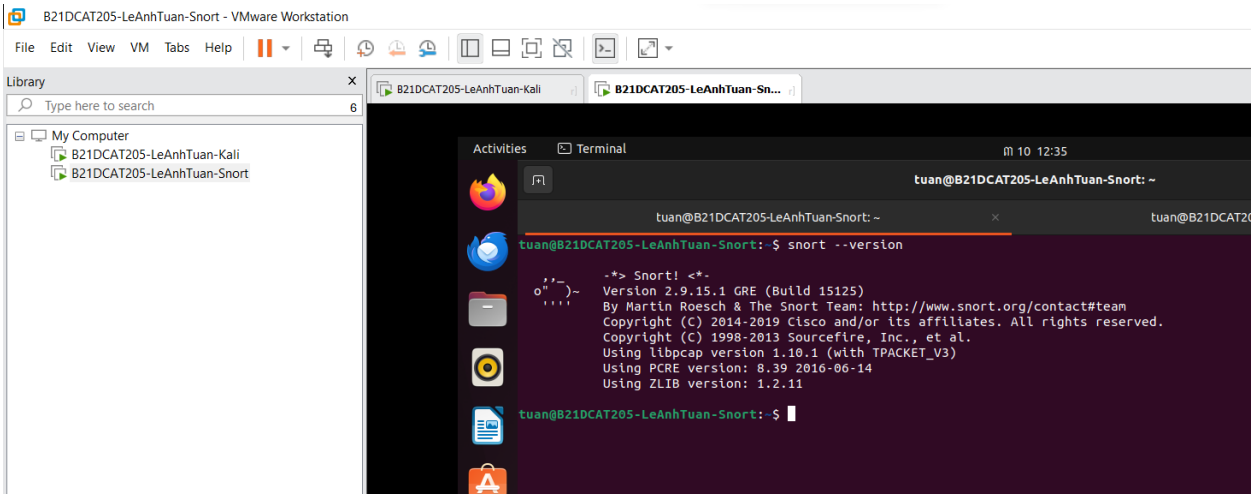


Hình 6:Cài đặt Snort bằng câu lệnh sudo apt get install snort

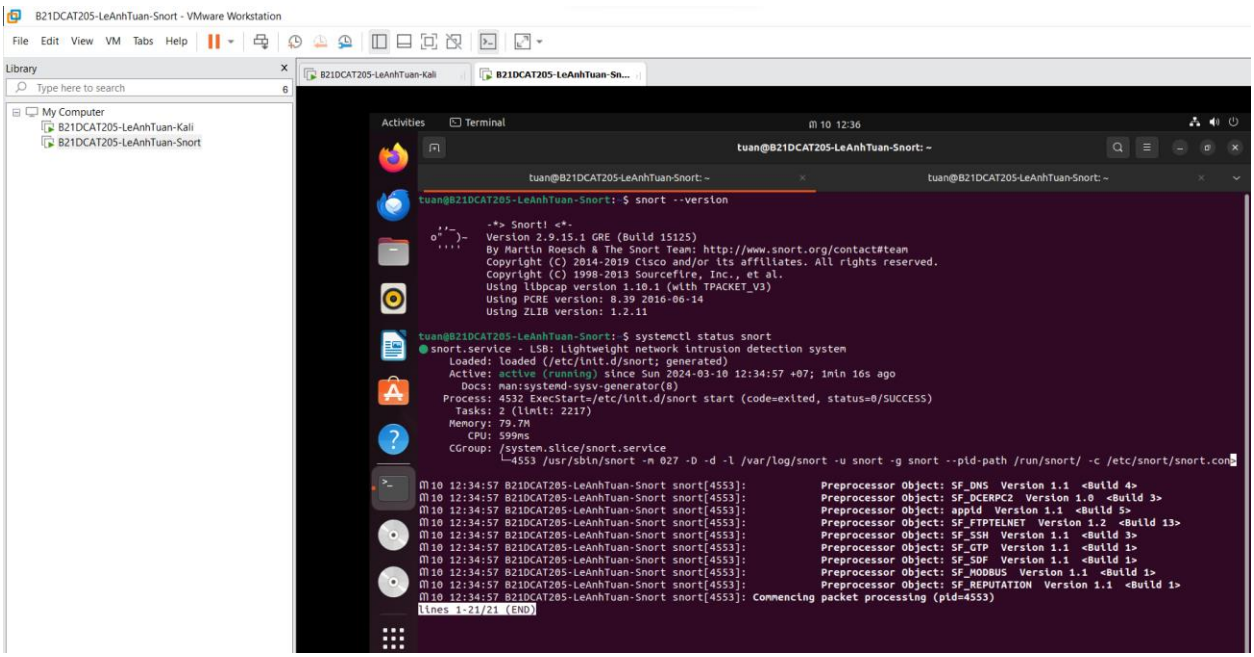
Do máy Ubuntu có địa chỉ IP nằm trong dải 192.168.150.0/24 nên ta cấu hình dải địa chỉ Ip như hình dưới



Hình 7: Cấu hình Snort với IP Address range



Hình 8: Kiểm tra phiên bản Snort sau khi cài đặt xong



Hình 9: Kiểm tra trạng thái hoạt động của Snort

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

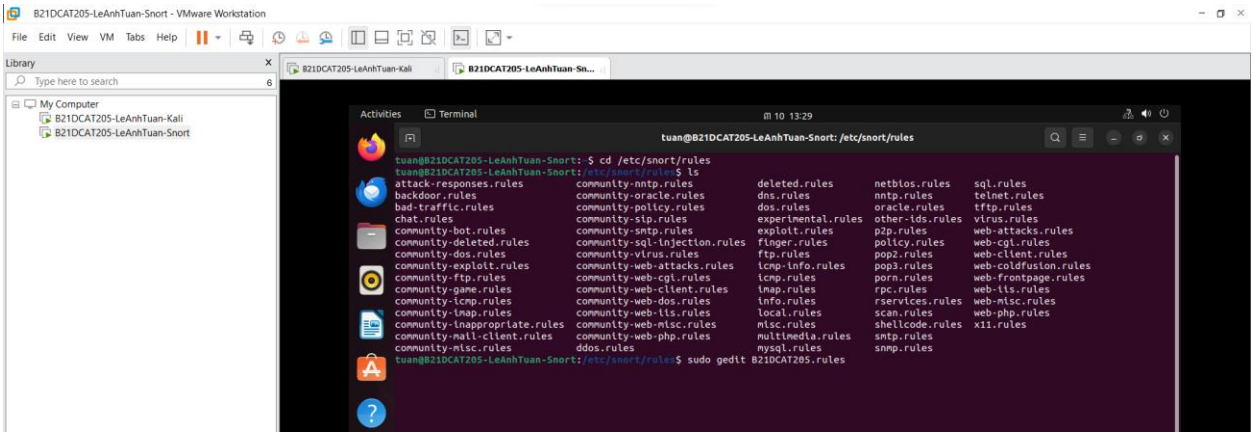
Trước tiên ta vào thư mục **/etc/snort/rules**

Sau đó tạo một file mới có tên **B21DCAT205.rules** là nơi chứa các luật gồm:

- 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."

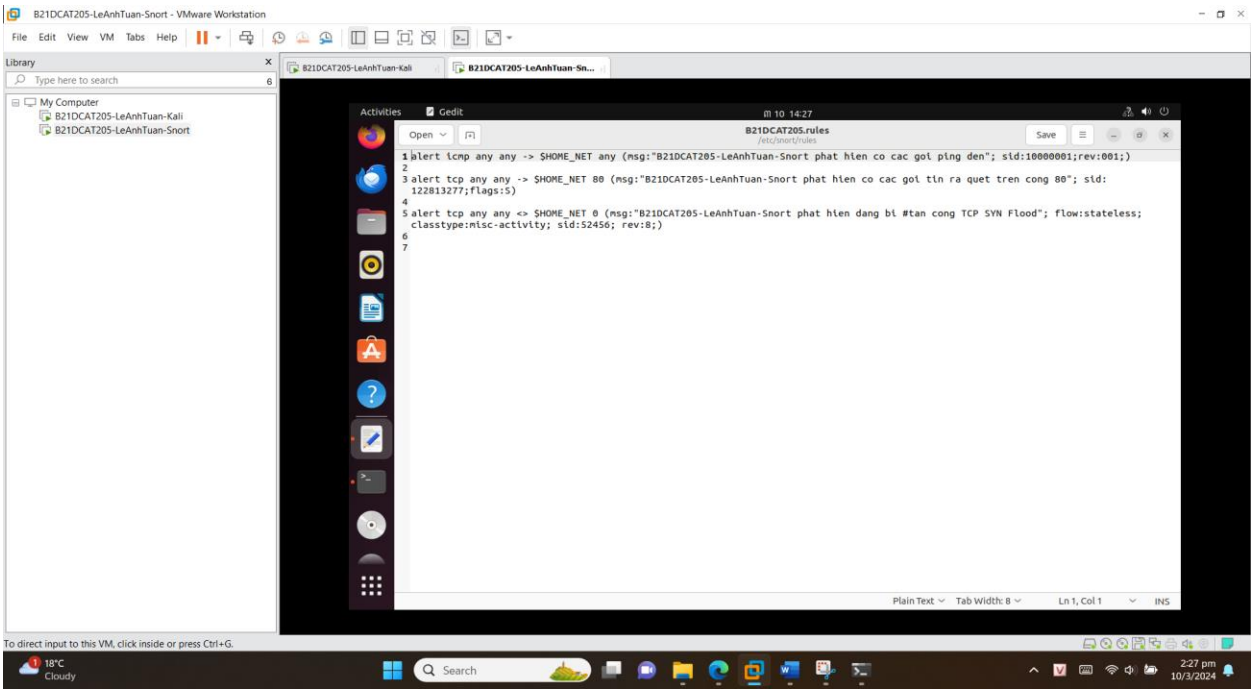
- Phát hiện các gói tin rà quét từ bất kỳ một máy nào gửi đến máy chạy Snort trên cổng 80. Hiển thị thông điệp khi phát hiện: "- Snort phát hiện có các gói tin rà quét trên cổng 80."

- 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."



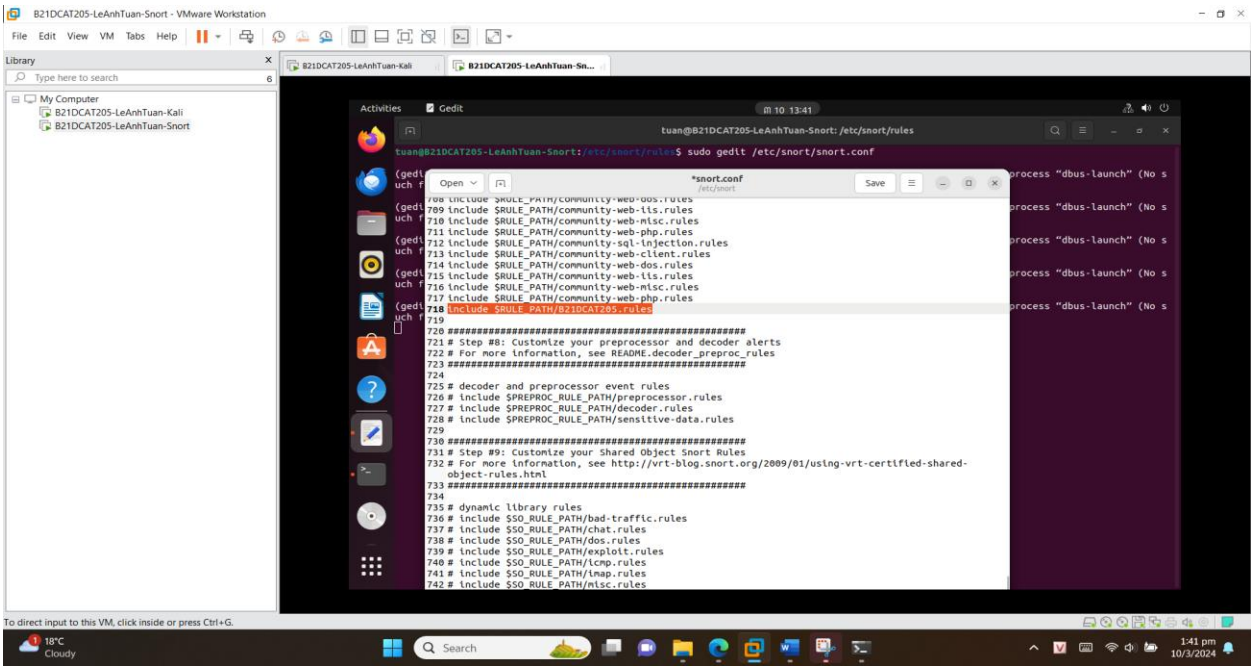
Hình 10: Tạo mới luật trong file B21DCAT205.rules

Sau khi cấu hình xong ta chọn **Save** để lưu.



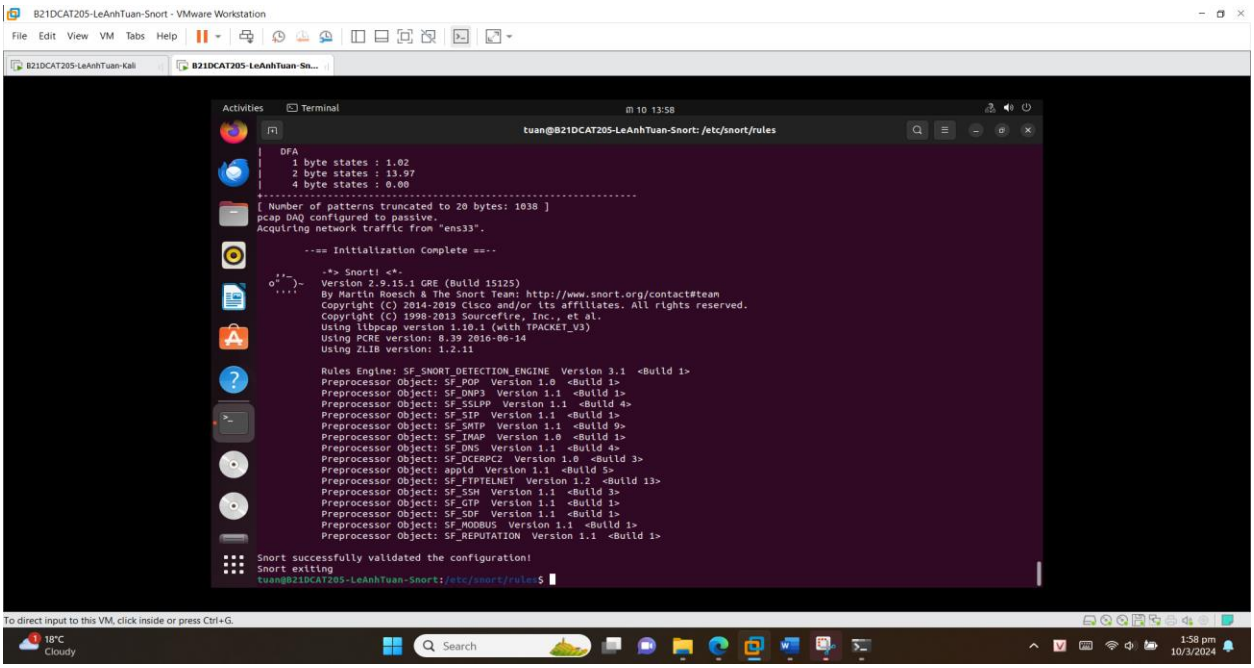
Hình 11: Các luật được cấu hình

Để kích hoạt các rules Sử dụng câu lệnh **cd gedit /etc/snort/snort.conf** , sau đó điền khai báo đường dẫn luật vừa mới tạo như hình dưới.



Hình 12: Khai báo đường dẫn luật mới tạo

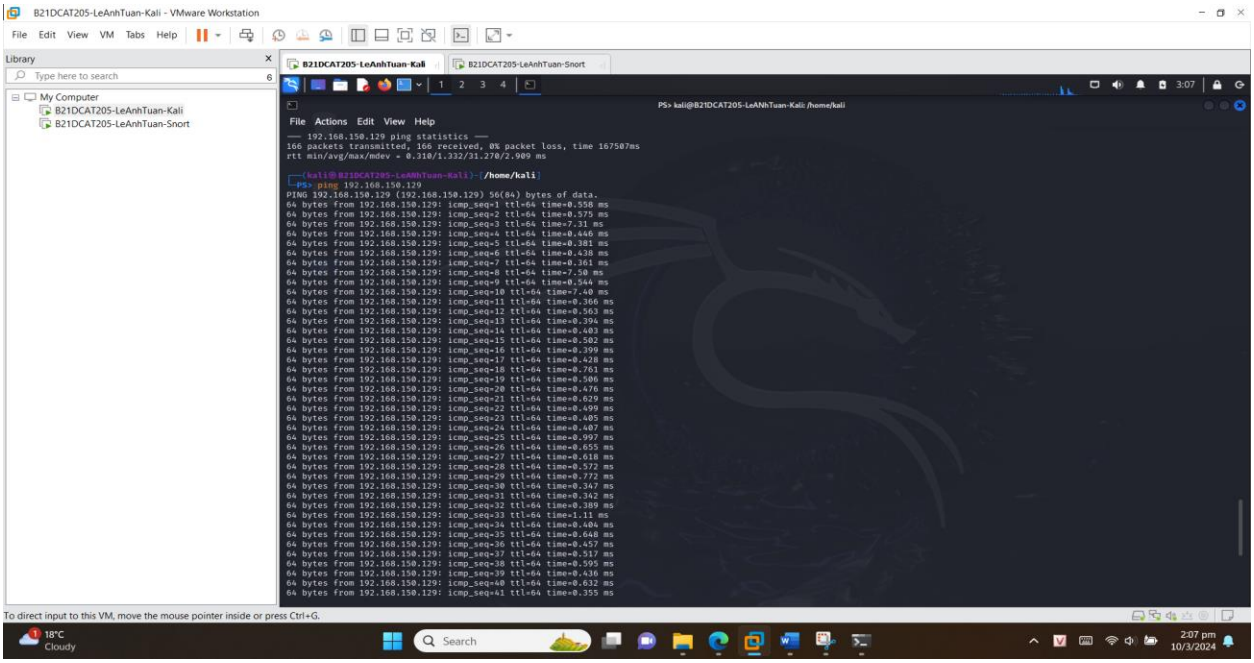
Cập nhật các thay đổi: **sudo snort –T –c /etc/snort/snort.conf – i <interface>** với **interface** là **ens33**



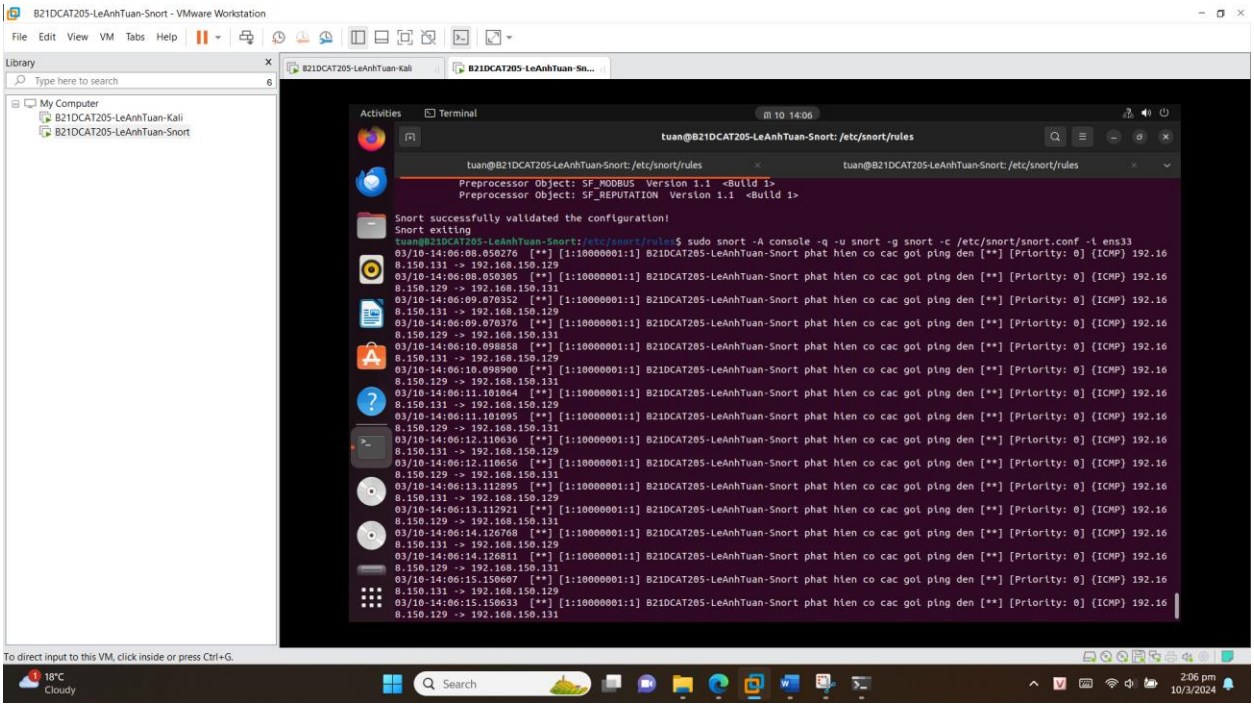
Hình 13: Cập nhật thay đổi luật thành công

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

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

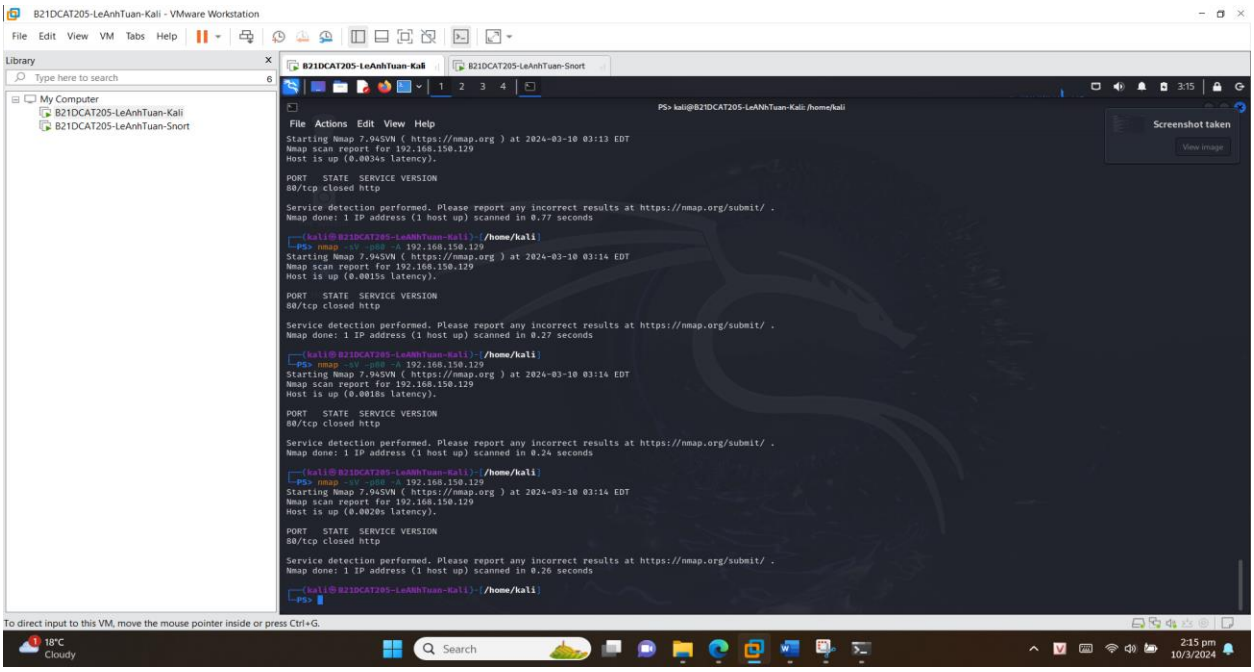


Hình 14: Ping tới máy Snort



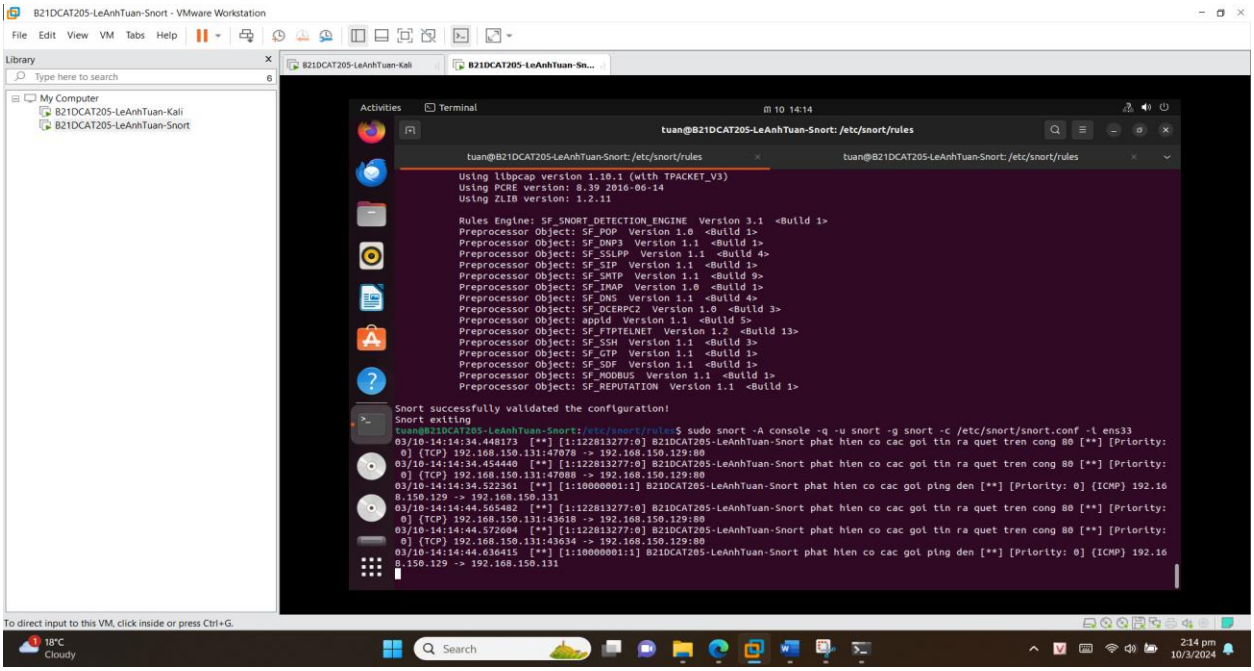
Hình 15: Phát hiện có máy ping tới.

Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort ,dùng lệnh: nmap -sV -p80 -A <ip máy đích>



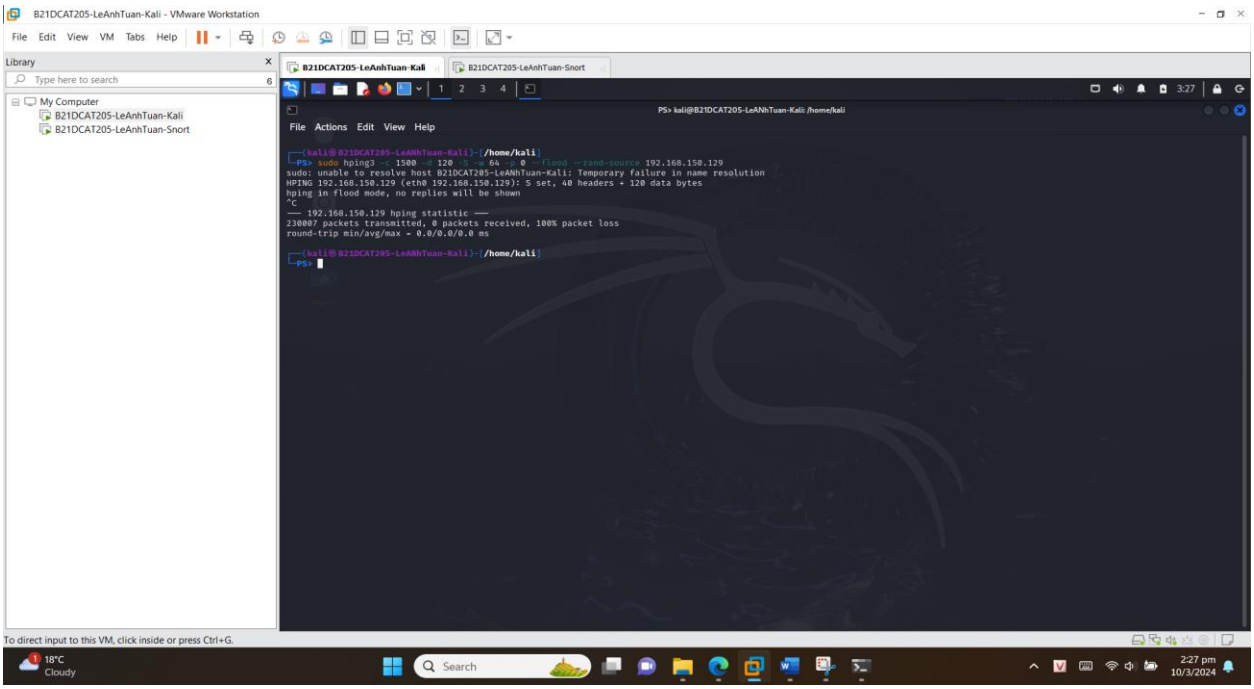
Hình 16: Sử dụng công cụ nmap để rà quét máy Snort

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



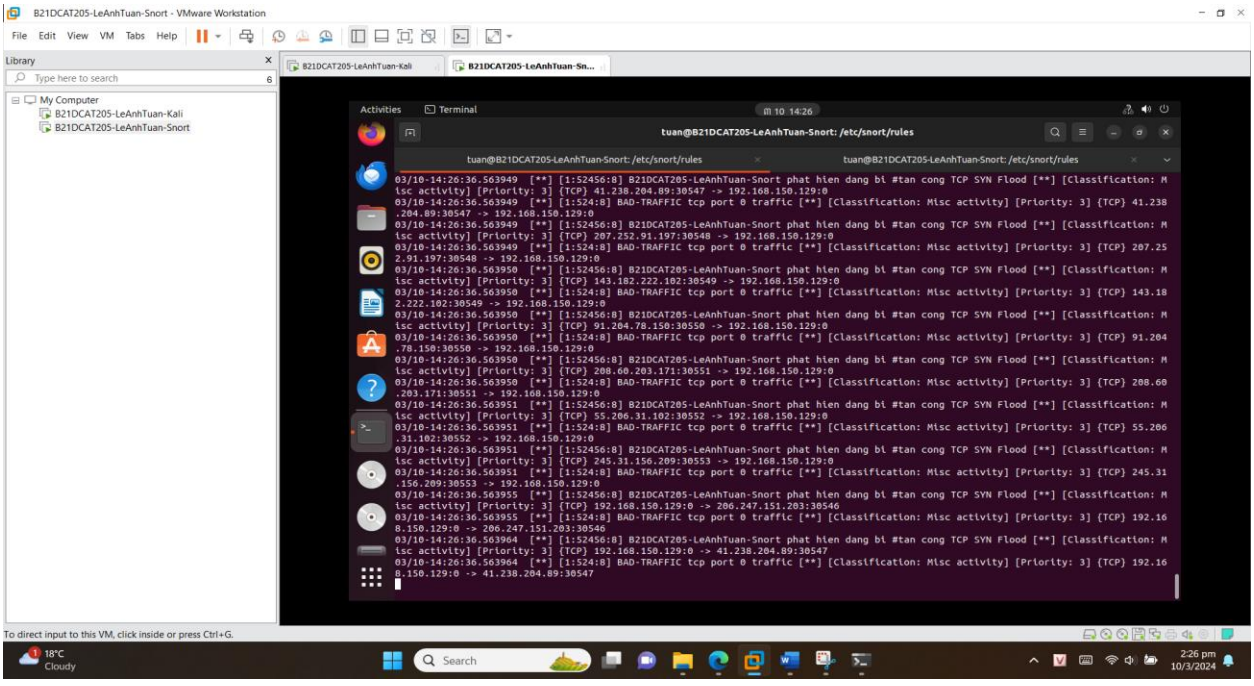
Hình 17:Phát hiện có các gói tin quét trên cổng 80

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



Hình 18: sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort

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



Hình 19: Phát hiện bị tấn công TCP SYN Flood

3 Kết luận

- Hệ thống phát hiện xâm nhập Snort hoạt động ổn định.
- Các luật mới được tạo và lưu vào trong file luật của Snort.
- Snort phát hiện thành công các rà quét tấn công kể trên (hiển thị trên giao diện terminal hoặc log của Snort).

4 Tài liệu tham khảo

- Documentation - Suricata
- Snort - Network Intrusion Detection & Prevention System
- OSSEC Documentation — OSSEC
- Wazuh documentation
- Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 2020.