**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



**MÔN HỌC THỰC TẬP CƠ SỞ**

**BÀI THỰC HÀNH SỐ 6**

**Tìm hiểu và cài đặt, cấu hình NIDS**

**Giảng viên hướng dẫn :** Đỗ Xuân Chợ

**Sinh viên thực hiện      :** Hoàng Trung Kiên

**Lớp                                :**  D20CQAT02-B

**Mã sinh viên                    :** B20DCAT098

Hà nội – 3/2023

**I.KIẾN THỨC LÝ THUYẾT**

**1.Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập**

Khái quát:

- Xâm nhập là tập các hành động nhằm thỏa hiệp với mục tiêu an toàn( tính bảo mật, toàn vẹn và sẵn dùng) của tài nguyên hoặc máy tính.

- Các hệ thống tấn công xâm nhập (IDS) 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.

- Hệ thống tấn công, xâm nhập IDS có nhiệm vụ chính là:

+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.

+Thông thường hệ thống IDS thường kết nối vào các bộ định tuyến, 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.

**2.Kiến trúc của một hệ thống IDS**

-Hệ thống cảm biến: thu thập những sự kiện liên quan đến an ninh hệ thống.

-Hệ thống phân tích: phát hiện tấn công và các hành vi đáng nghi dựa trên hệ thống cảm biến.

-Không gian lưu trữ: lưu trữ các sự kiện và kết quả phân tích.

-Giao diện điều khiển: để cài đặt hệ thống IDS, cập nhật các trạng thái bảo mật và kiểm tra các sự kiện/bản ghi từ hệ thống phân tích.

**3.Phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.**

-Các hệ thống phát hiện xâm nhập (IDS) thường được sử dụng như một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng; IDS – Intrusion Detection System: hệ thống phát hiện tấn công, xâm nhập.

Phân loại theo nguồn dữ liệu:

+Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS): phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng. Trong một sơ  đồ mạng, 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): phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó.

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

Được chia làm hai kỹ thuật chính: Phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên các bất thường.

- Phát hiện xâm nhập dựa trên chữ ký: trước hết cần xây dựng csdl các chữ ký, hoặc các dấu hiệu của các loại tấn công xâm nhập đã biết. Hầu hết các chữ kí, dấu hiệu được nhận dạng và mã hóa thủ công và dạng thường gặp là các luật phát hiện. bước tiếp theo là sử dụng csdl các chữ ký để giám sát các hành vi của hệ thống hoặc mạng, cảnh báo nếu phát hiện chữ ký của tấn công.

- 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 ƣ 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, nó 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 (Anomaly intrusion detection) 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 gồm 2 giai đoạn: là huấn luyện và ƣ là phát hiện.

-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 này, 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.

-Giai đoạn 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.

-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 có tỷ lệ cảnh báo sai tương đối cao so với phương pháp ƣ 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, nó cũng tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại

**5.Tìm hiểu về kiến trúc và chức năng của một số hệ thống phát hiện tấn công, xâm nhập 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. Nó được tạo ra bởi Cisco. Hệ thống có thể được chạy ở ba chế độ khác nhau và có thể thực hiện các chiến lược phòng thủ, vì vậy nó là một hệ thống ngăn chặn xâm nhập cũng như một hệ thống phát hiện xâm nhập.

Kiến trúc:

Snort bao gồm nhiều thành phần, với mỗi phần có một chức năng riêng. Các phần chính đó là:

+Môđun giải mã gói tin (Packet Decoder)

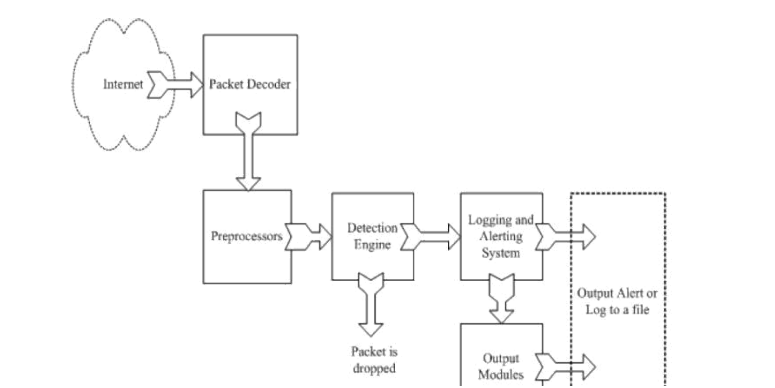
+Môđun tiền xử lý (Preprocessors)

+Môđun phát hiện (Detection Engine)

+Môđun log và cảnh báo (Logging and Alerting System)

+Môđun kết xuất thông tin (Output Module)

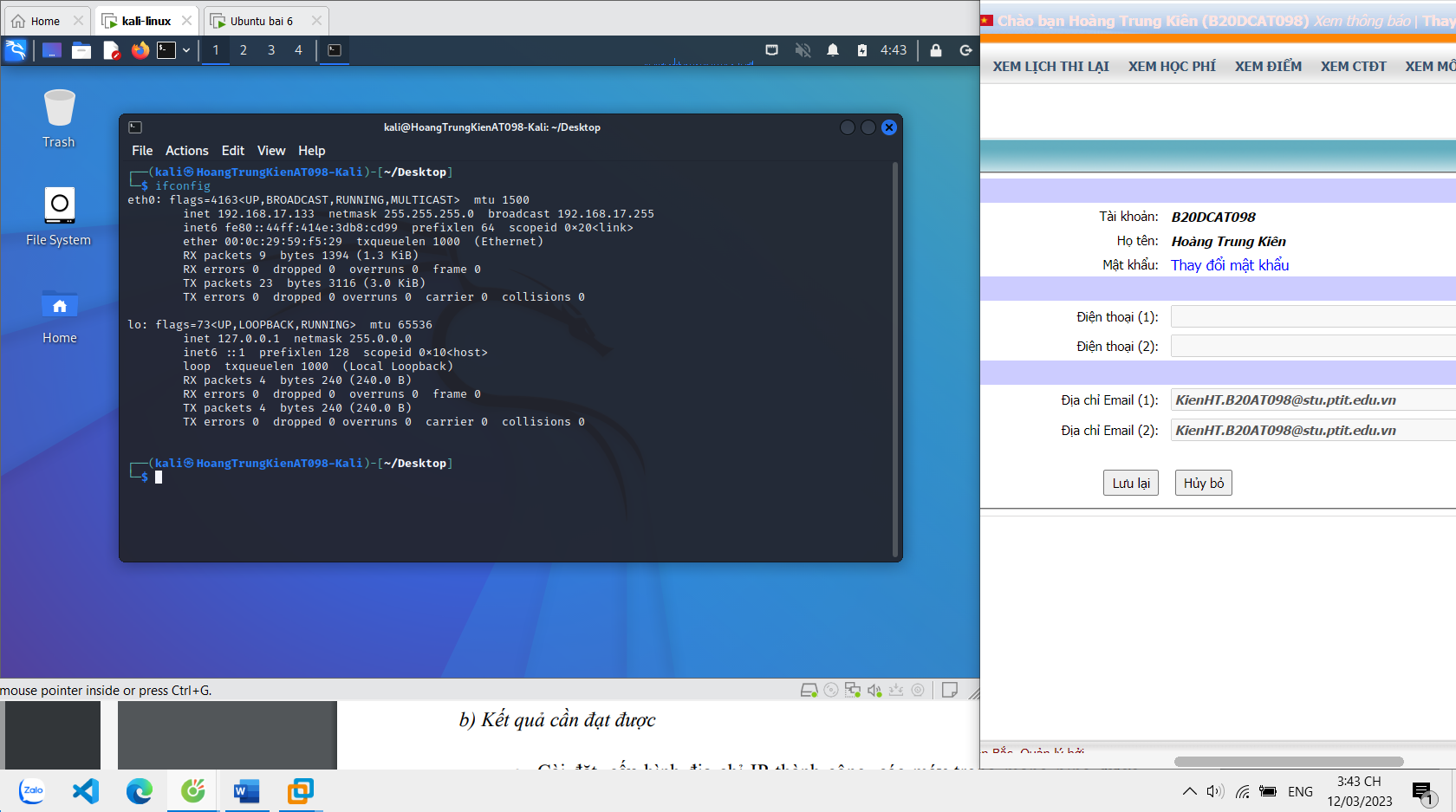
-Kiến trúc của Snort được mô tả trong hình sau:

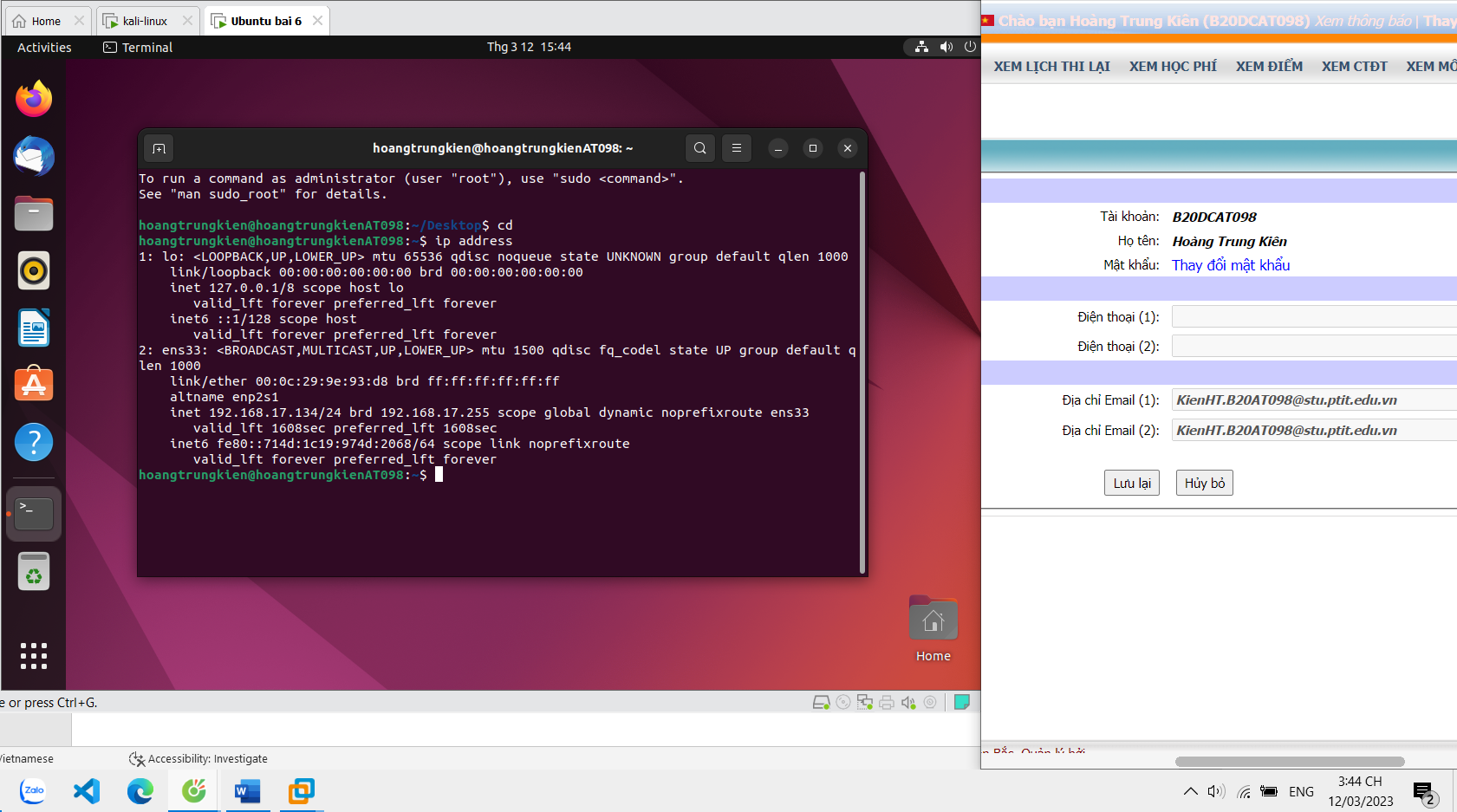


Khi Snort hoạt động nó sẽ thực hiện việc lắng nghe và thu bắt tất cả các gói tin nào di chuyển qua nó. Các gói tin sau khi bị bắt được đưa vào Module Giải mã gói tin. Tiếp theo gói tin sẽ được đưa vào mô đun Tiền xử lý, rồi môđun Phát hiện. Tại đây tùy theo việc có phát hiện được xâm nhập hay không mà gói tin có thể được bỏ qua để lưu thông tiếp hoặc được đưa vào môđun Log và cảnh báo để xử lý. Khi các cảnh báo được xác định mô đun Kết xuất thông tin sẽ thực hiện việc đưa cảnh báo ra theo đúng định dạng mong muốn.

**II.BÁO CÁO THỰC HÀNH**

 Các máy có địa chỉ IP và kết nối mạng LAN.

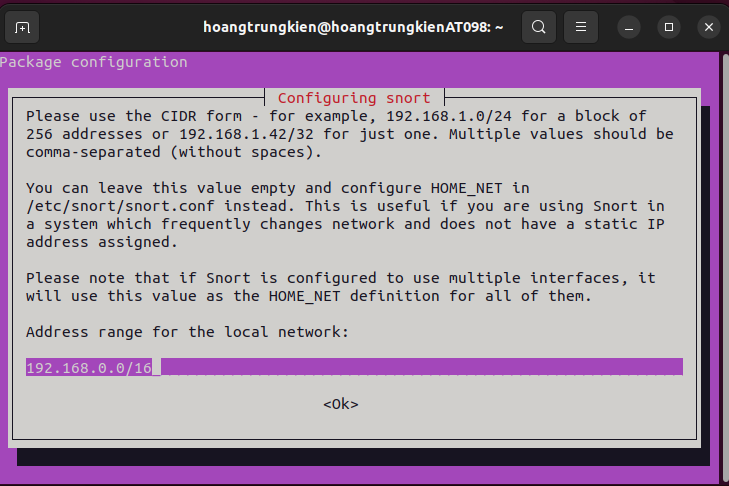




Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.

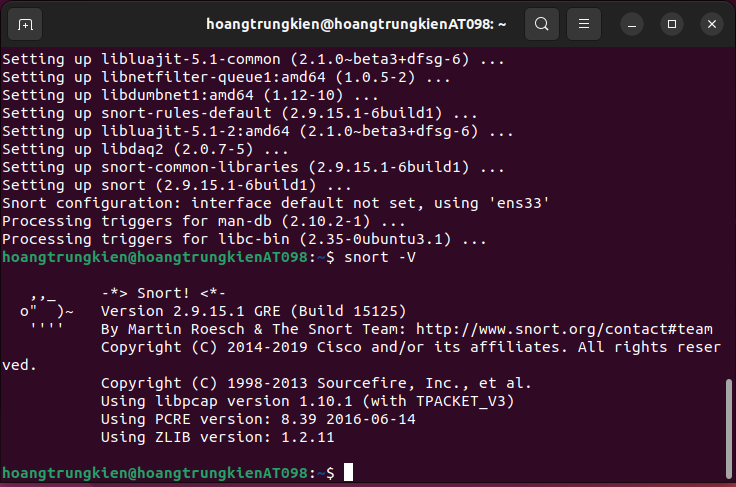
Gõ lệnh sudo apt-get install snort\* để cài đặt và ấn ok





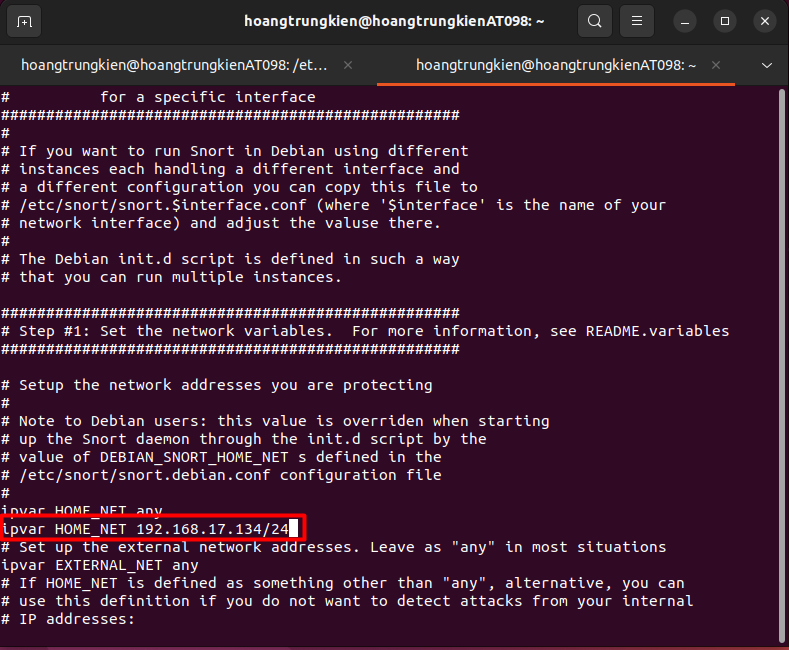
Để kiểm tra phiên bản

Gõ lệnh: snort -V



Cấu hình Snort



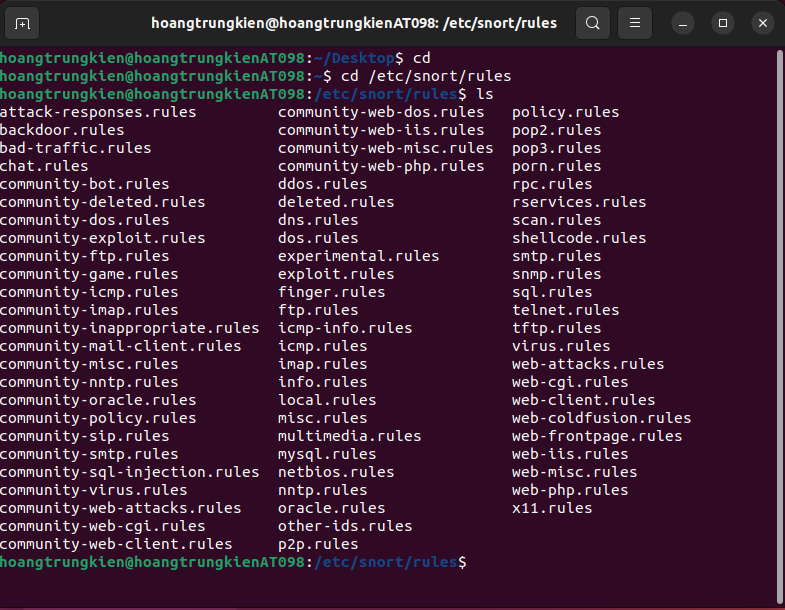


Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống:

+ Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi 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.

+ 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 đang bị tấn công TCP SYN Flood.

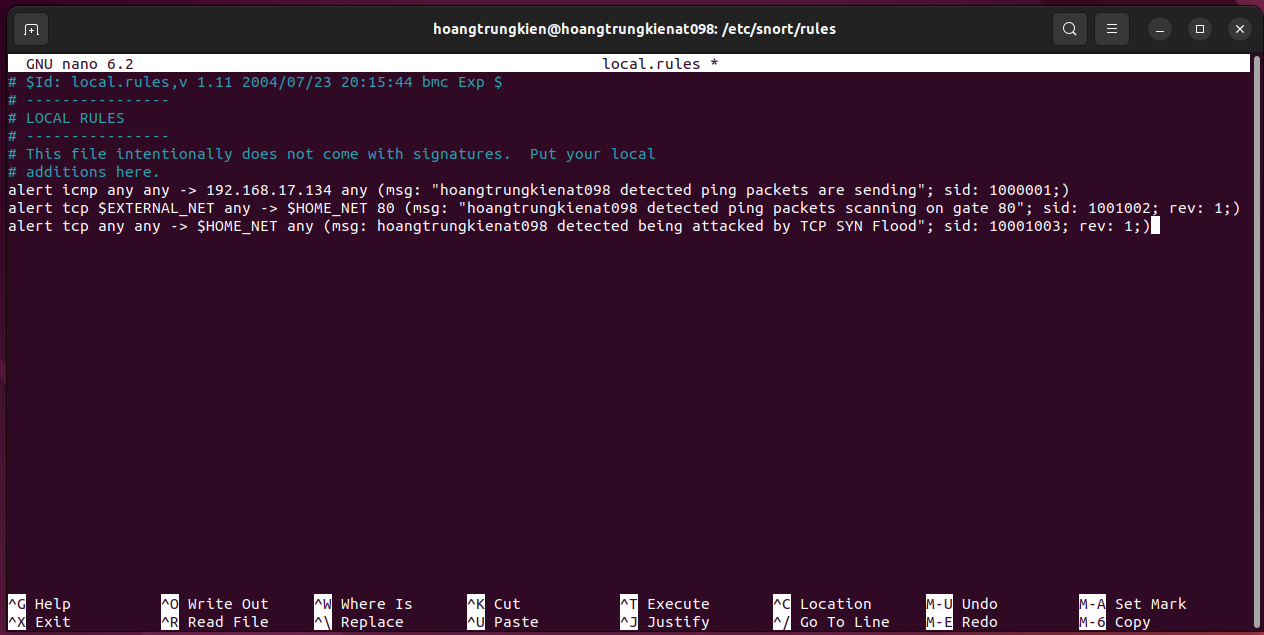




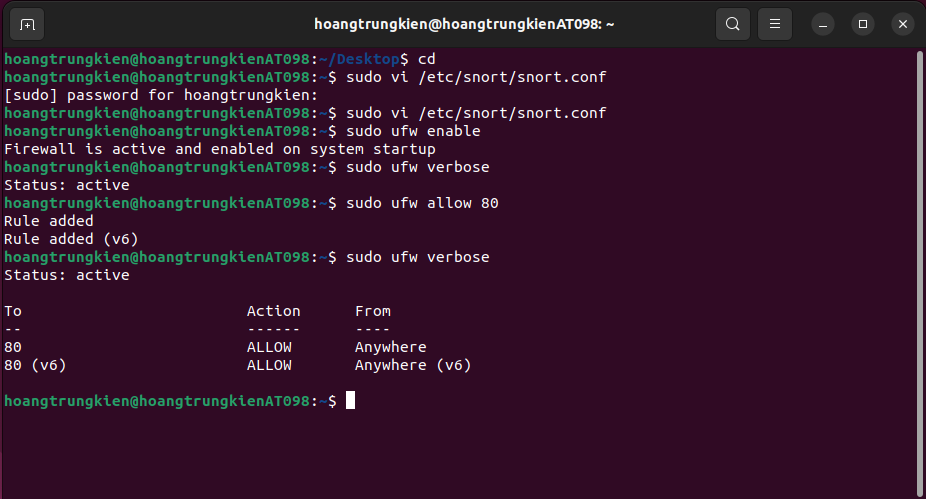
alert icmp any any -> 192.168.17.134 any (msg: "hoangtrungkienat098 detected ping packets are sending"; sid: 1000001;)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 80 (msg: "hoangtrungkienat098 detected ping packets scanning on gate 80"; sid: 1001002; rev: 1;)

alert tcp any any -> $HOME\_NET any (msg: hoangtrungkienat098 detected being attacked by TCP SYN Flood"; sid: 10001003; rev: 1;)

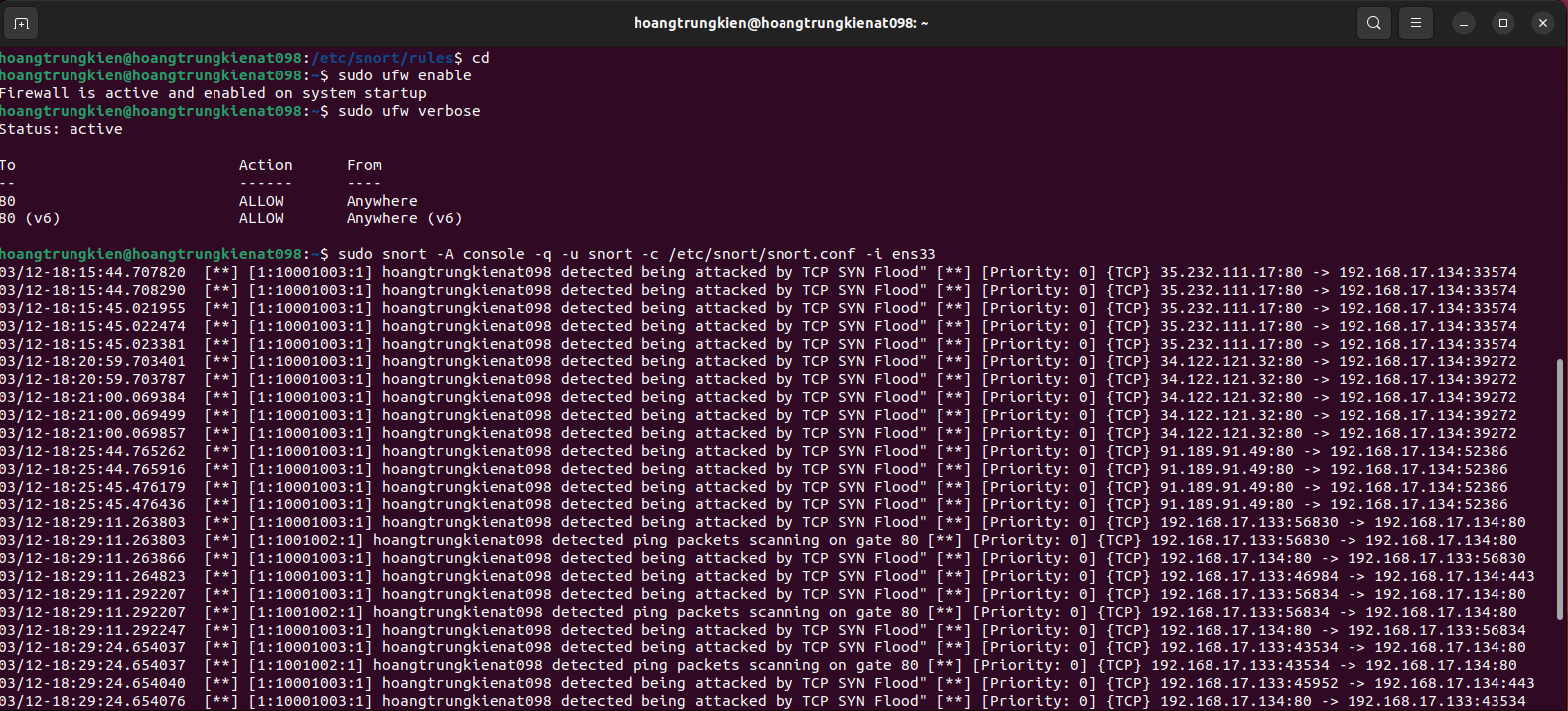


Trước tiên phải kích hoạt firewall và cổng 80 trên máy Snort

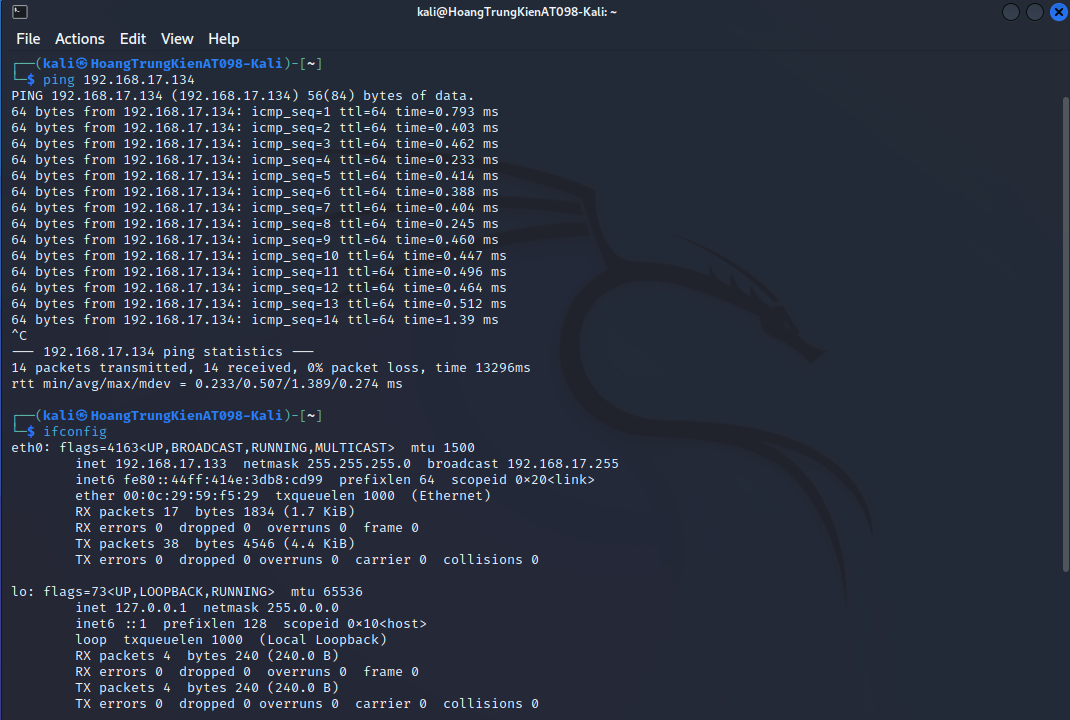


Thực thi tấn công và phát hiện sử dụng Snort:

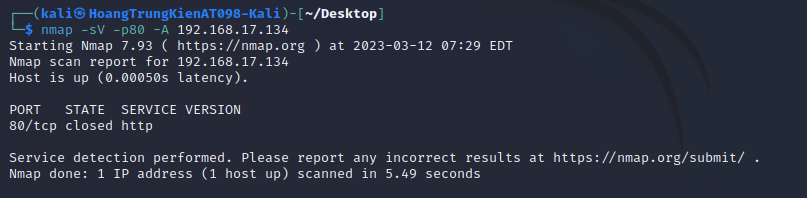


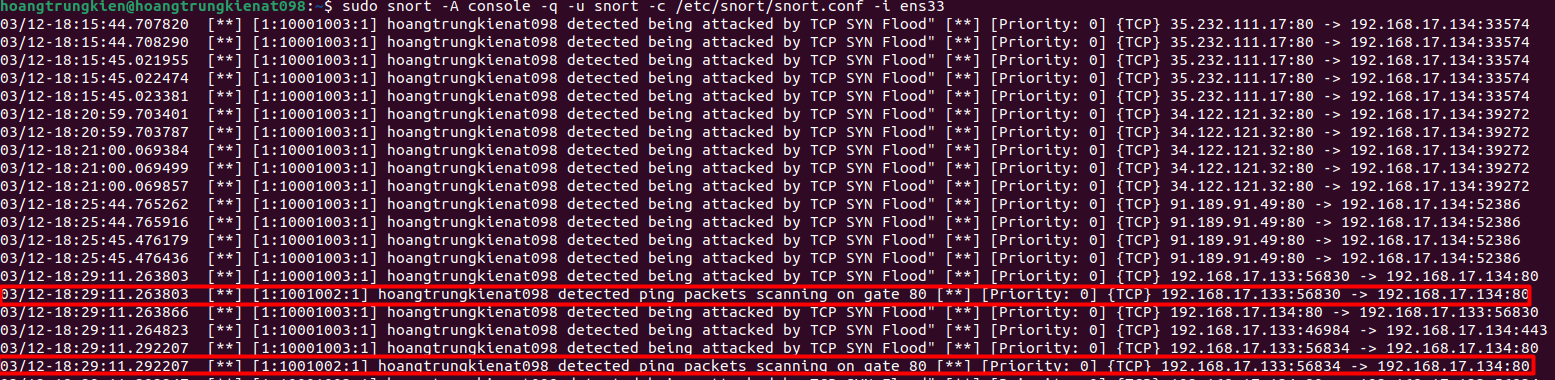


+ Từ máy Kali, sử dụng lệnh ping để ping máy Snort. Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.



+ 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





+ 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.

