HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO

BÀI 6 - Cài đặt cấu hình HIDS/NIDS

Giảng viên hướng dẫn: Vũ Minh Mạnh

Sinh viên thực hiện: Nguyễn Quốc Vượng

Mã sinh viên: B21DCAT227

Lớp: D21CQAT03-B

Hà Nội, 2023

Môn học: INT13147 - Thực tập cơ sở Bài thực hành số 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

Hệ thống phát hiện tấn công và xâm nhập (IDS/IPS) là các công cụ quan trọng trong việc bảo vệ hệ thống và mạng khỏi các mối đe dọa bảo mật. Dưới đây là một khái quát về các hệ thống này và một số công cụ phổ biến:

1. Hệ thống phát hiện tấn công và xâm nhập (IDS/IPS):

- **Phát hiện tấn công (IDS)**: Theo dõi lưu lượng mạng và ghi lại các hoạt động không bình thường hoặc có thể là các cuộc tấn công. IDS thường phát hiện dựa trên quy tắc hoặc phân tích hành vi.
- **Phòng ngừa tấn công (IPS)**: Tương tự như IDS nhưng có khả năng ngăn chặn các cuộc tấn công bằng cách tự động cắt ngắn kết nối hoặc chặn các gói tin độc hại.

2. Phân loại các hệ thống phát hiện xâm nhập:

- **Dựa trên vị trí**: Có thể được triển khai ở mức đầu cuối (host-based) hoặc mạng (network-based).
- **Dựa trên phương pháp phát hiện**: Có thể phát hiện dựa trên chữ ký (signature-based) hoặc phát hiện dựa trên hành vi (anomaly-based).
- **Dựa trên mục tiêu**: Có thể tập trung vào phát hiện tấn công (intrusion detection) hoặc phòng ngừa tấn công (intrusion prevention).

3. Các kỹ thuật phát hiện xâm nhập:

- **Chữ ký (Signature)**: Sử dụng các quy tắc hoặc chữ ký để so sánh với lưu lượng mạng và phát hiện các cuộc tấn công đã biết.
- **Học máy (Machine Learning)**: Sử dụng các mô hình máy học để phân tích hành vi của lưu lượng mạng và phát hiện các hoạt động bất thường.
- **Phân tích giao thức (Protocol Analysis)**: Theo dõi và phân tích giao thức mạng để phát hiện các mẫu hoặc hành vi không bình thường.
- **Phân tích hành vi (Behavior Analysis)**: Theo dõi hành vi của hệ thống hoặc người dùng để phát hiện các hoạt động bất thường.

4. Kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập:

- **Snort**: Là một IDS/IPS mã nguồn mở, dựa trên chữ ký và hành vi. Nó cung cấp quy tắc mạnh mẽ để phát hiện các cuộc tấn công và hỗ trợ nhiều chế độ hoạt động.
- **Suricata**: Tương tự như Snort, Suricata là một IDS/IPS mã nguồn mở với khả năng đa luồng và hỗ trợ nhiều giao thức.
- **Zeek (trước đây là Bro)**: Zeek là một IDS mạng dựa trên phân tích giao thức. Nó tập trung vào việc phát hiện và phân tích hành vi mạng.

- **OSSEC**: Là một HIDS (Host-based IDS) mã nguồn mở, OSSEC giám sát các sự kiện trên hệ thống và phát hiện các hoạt động bất thường.
- **Wazuh**: Wazuh là một giải pháp bảo mật nhóm, kết hợp OSSEC với các tính năng giám sát và phản ứng mạng.

Các công cụ này cung cấp tính năng phong phú và có thể được tùy chỉnh để phù hợp với nhu cầu bảo mật cụ thể của mỗi tổ chức.

- Một số tài liệu tham khảo:
  + Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 2020.
  + Suricata: https://suricata.io/documentation/
  + Snort: https://www.snort.org/#documents
  + OSSEC: https://www.ossec.net/docs/
  + Wazuh: https://documentation.wazuh.com/current/index.html

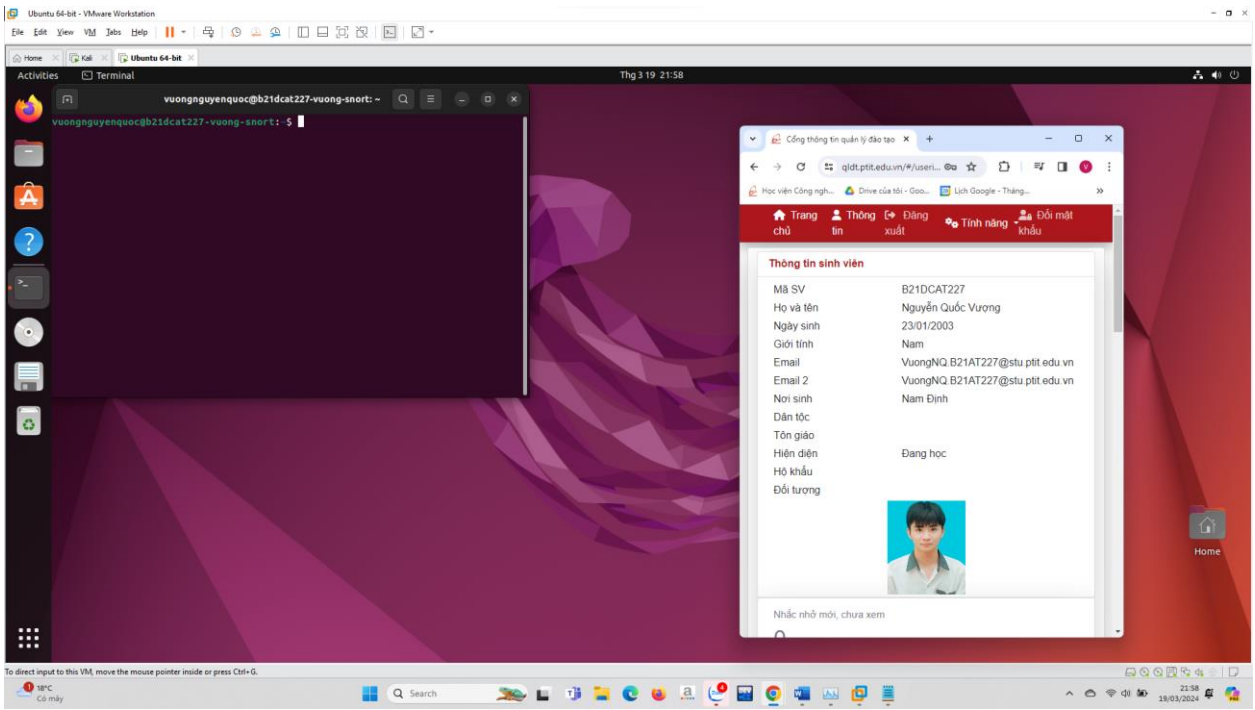
2.2 Chuẩn bị môi trường, công cụ

- 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

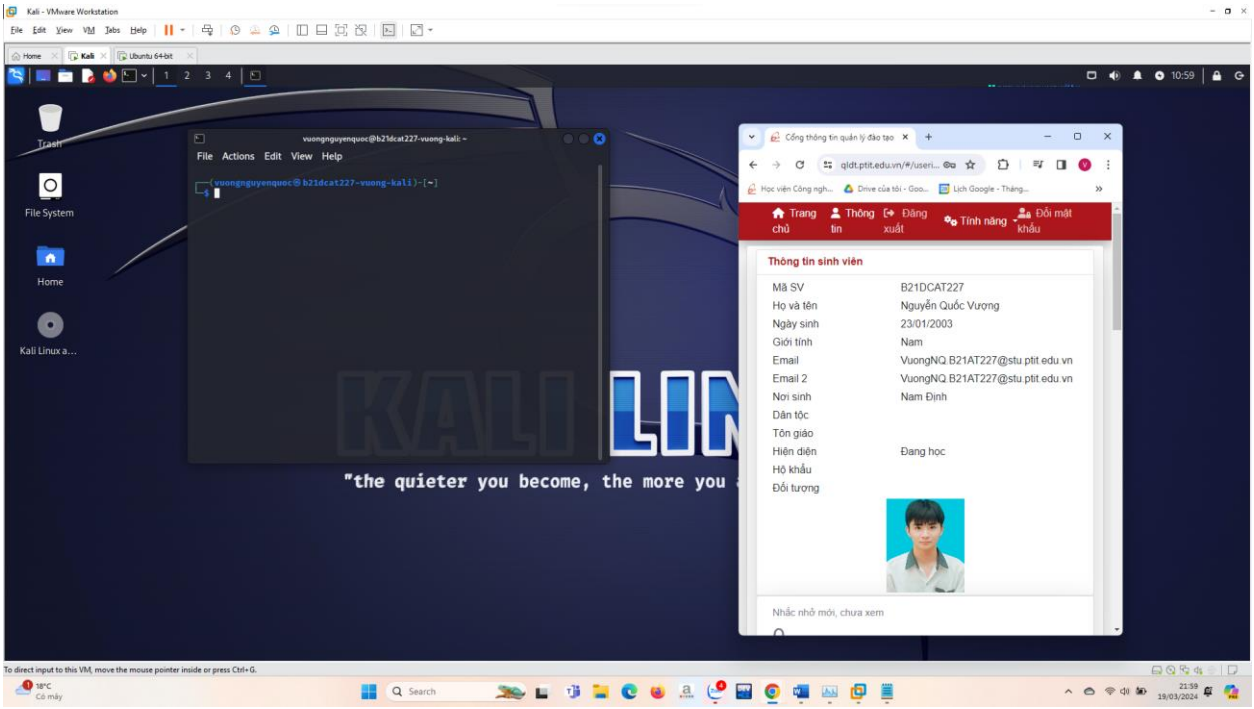
2.3 Các bước thực hiện

- Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.2. Máy Kali Linux được đổi tên thành <Mã SV-Tên SV>-Kali và máy cài Snort thành <Mã SV-Tên SV>-Snort.

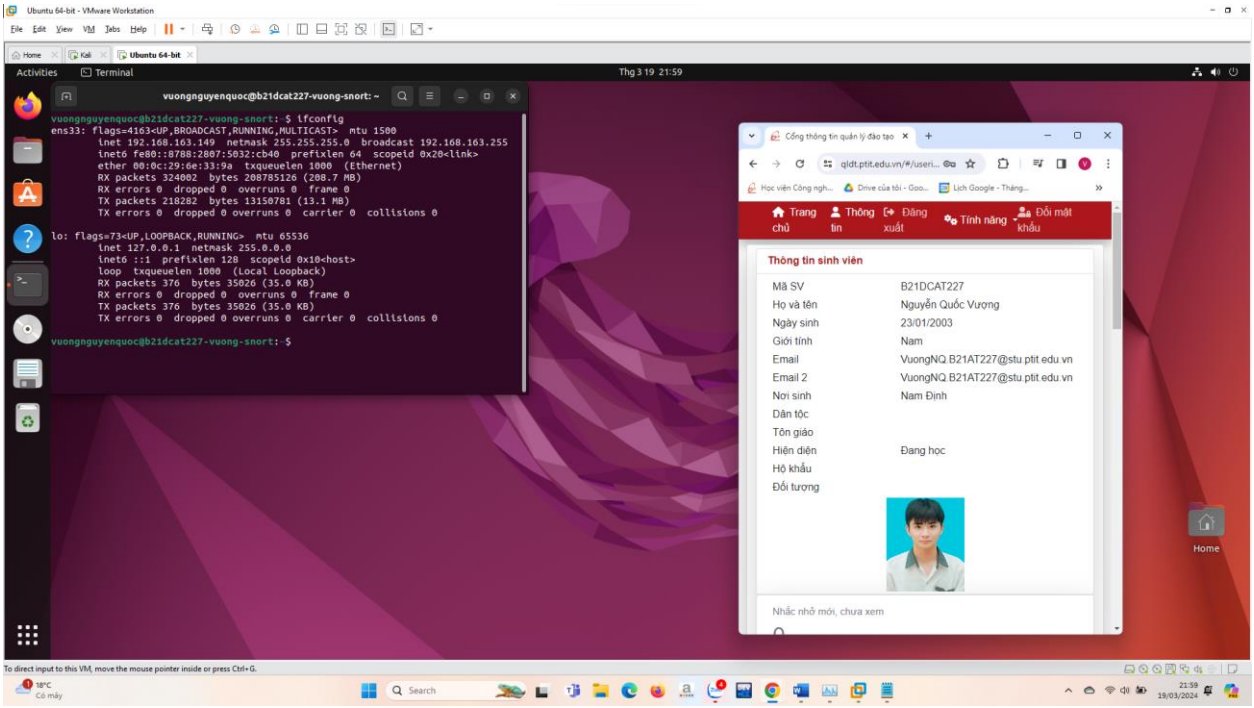
Máy Snort:

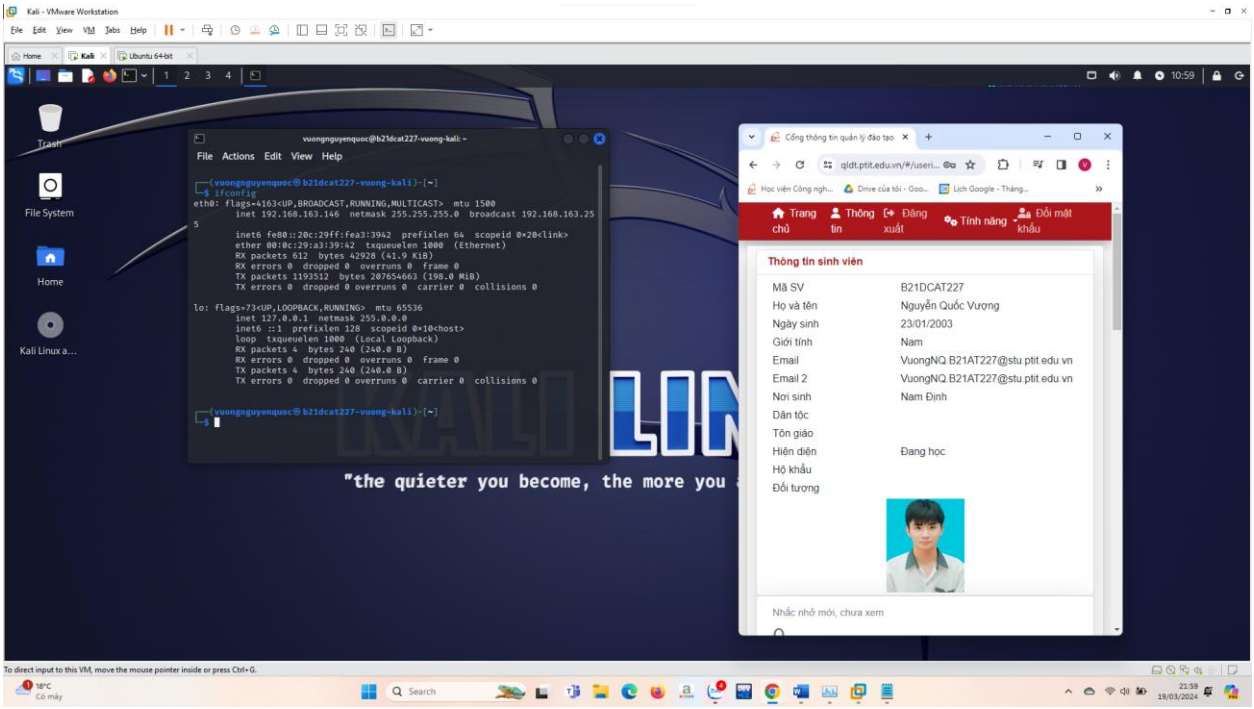


Máy Kali:

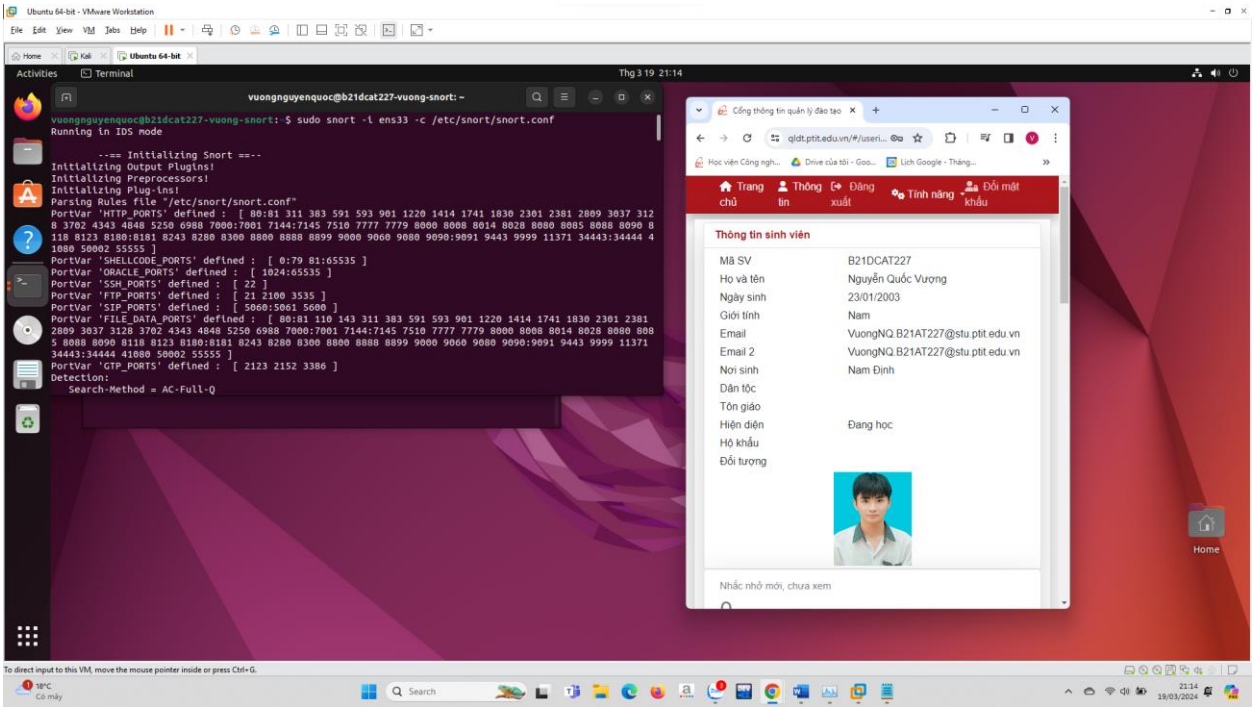


Các máy có địa chỉ IP và kết nối mạng LAN.



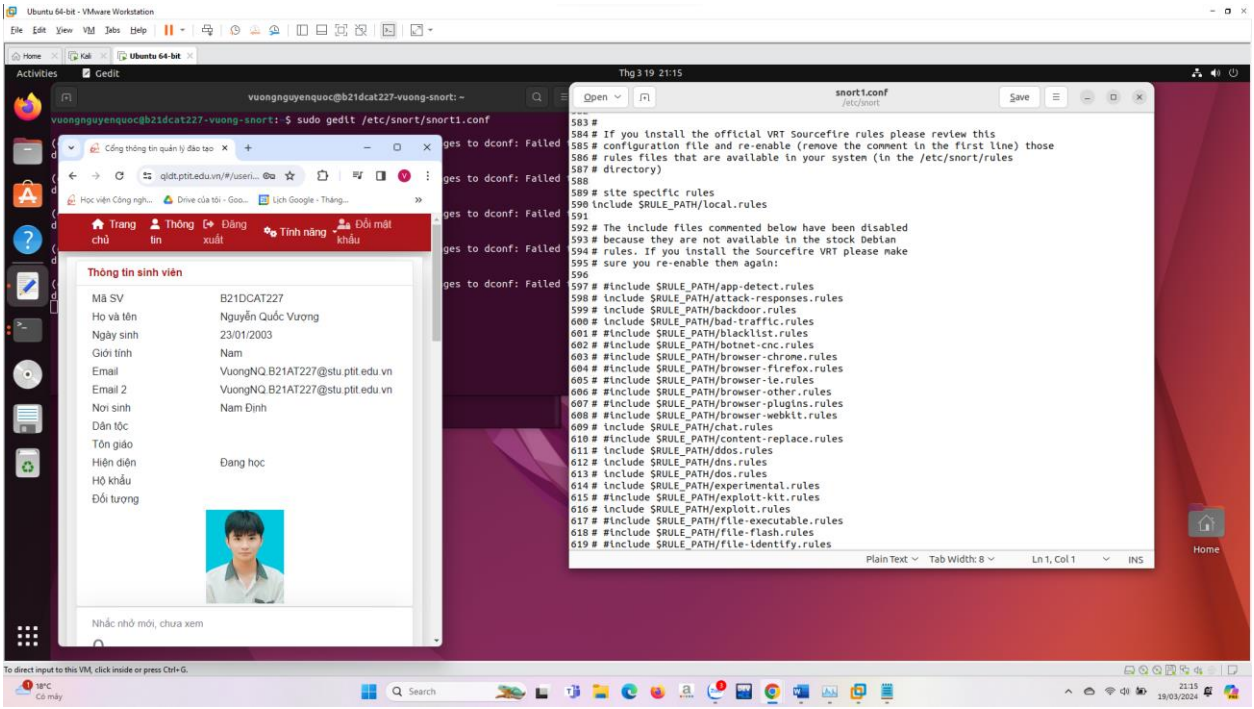


- Bước 2: Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.



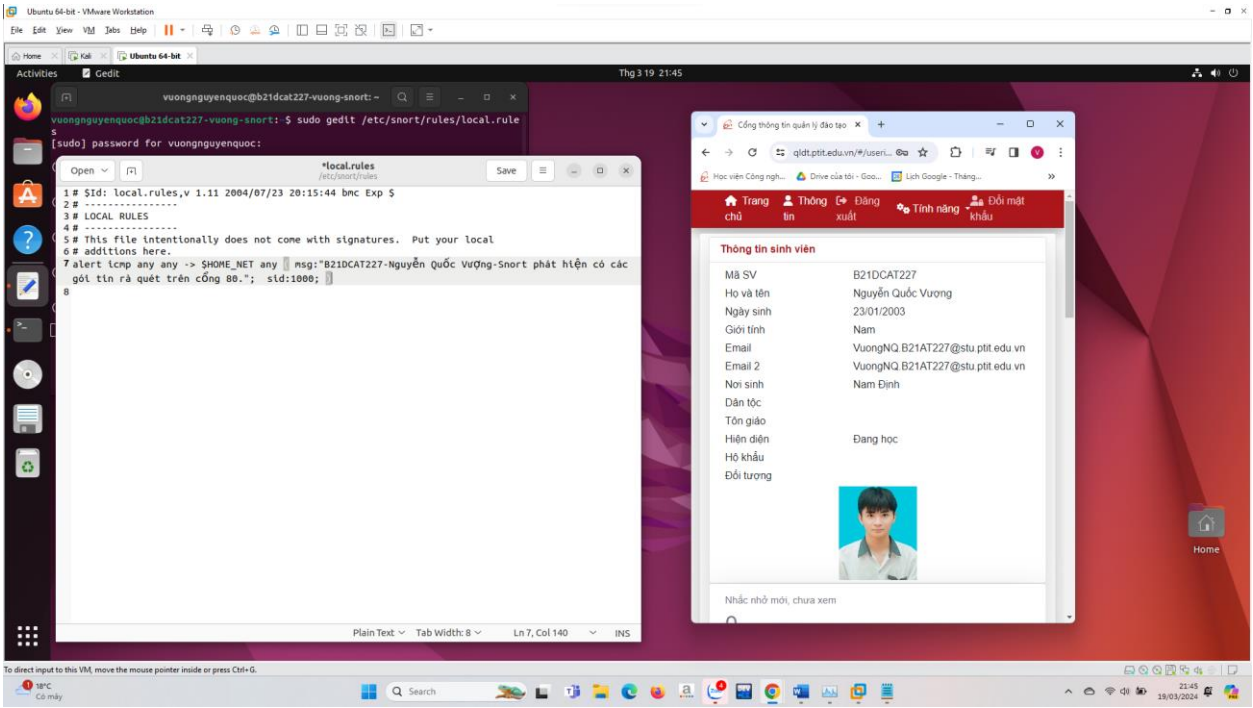
- Bước 3: Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống:
  + Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện có các gói Ping gửi đến.”

Tạo 1 file configuration chỉ sử dụng luật tự tạo:

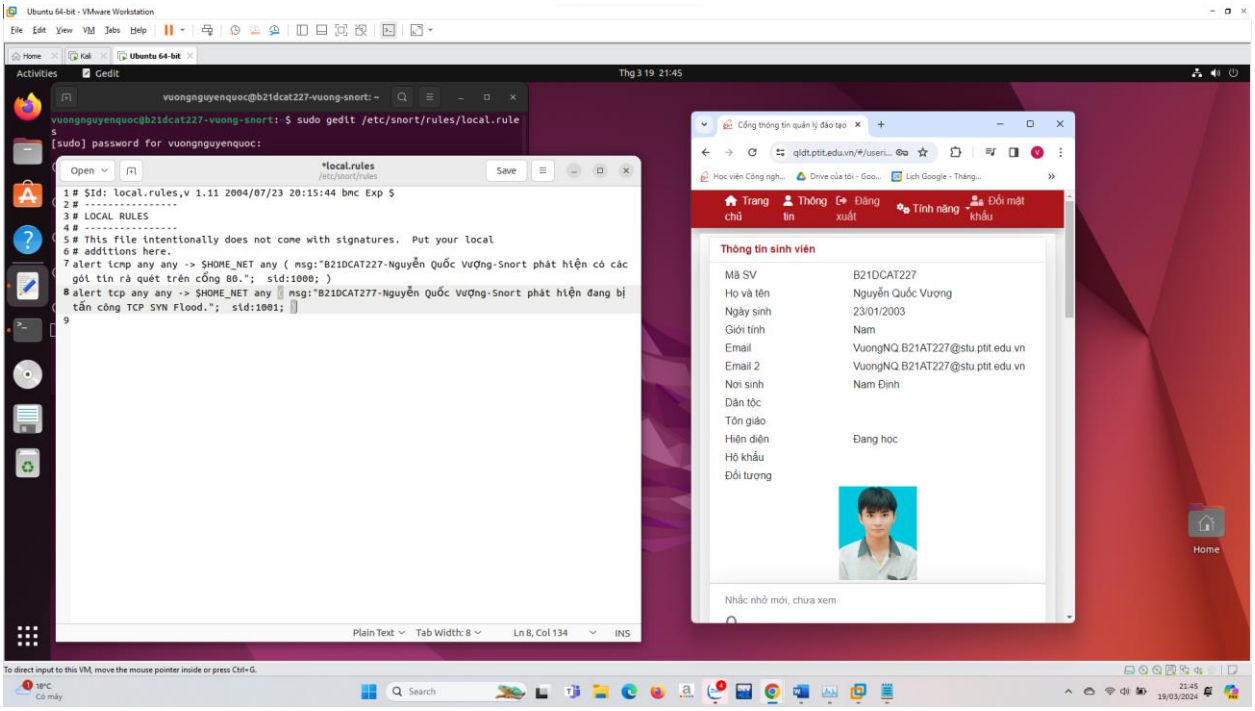


Sửa file Luật:

+ 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: “<Mã SV-Tên SV>-Snort phát hiện có các gói tin rà quét trên cổng 80.”

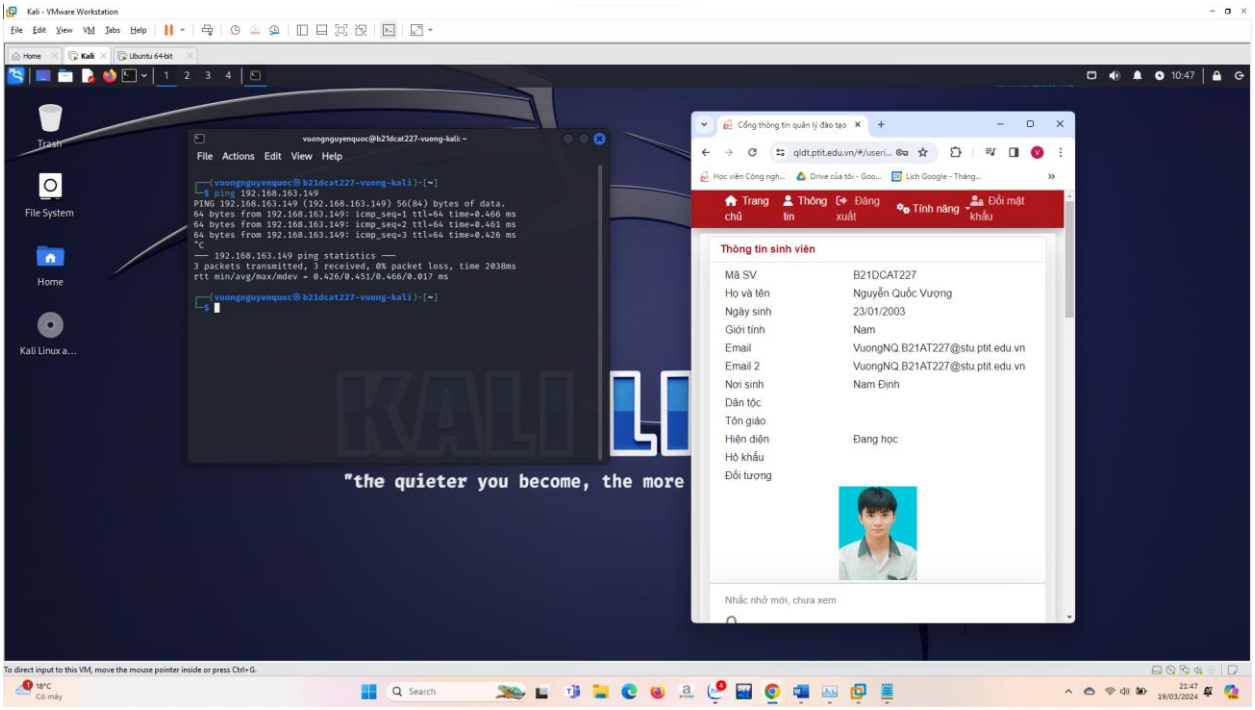


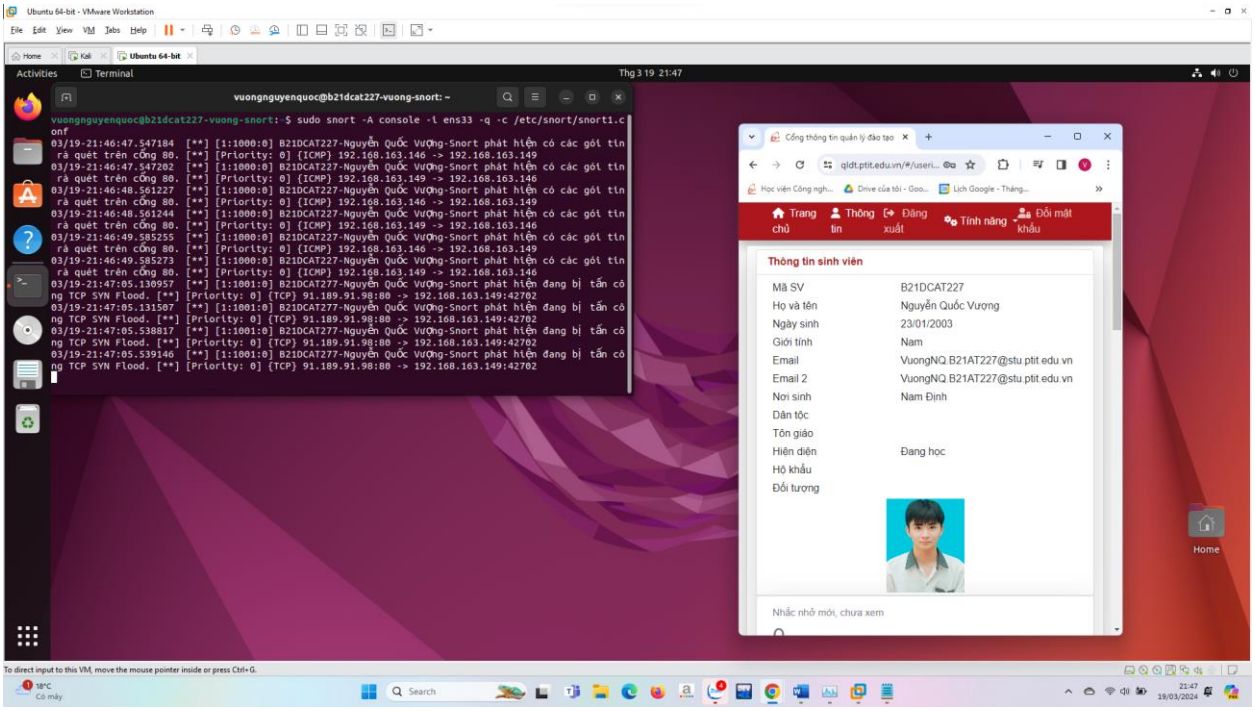
+ Phát hiện tấn công TCP SYN Flood từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện đang bị tấn công TCP SYN Flood.”



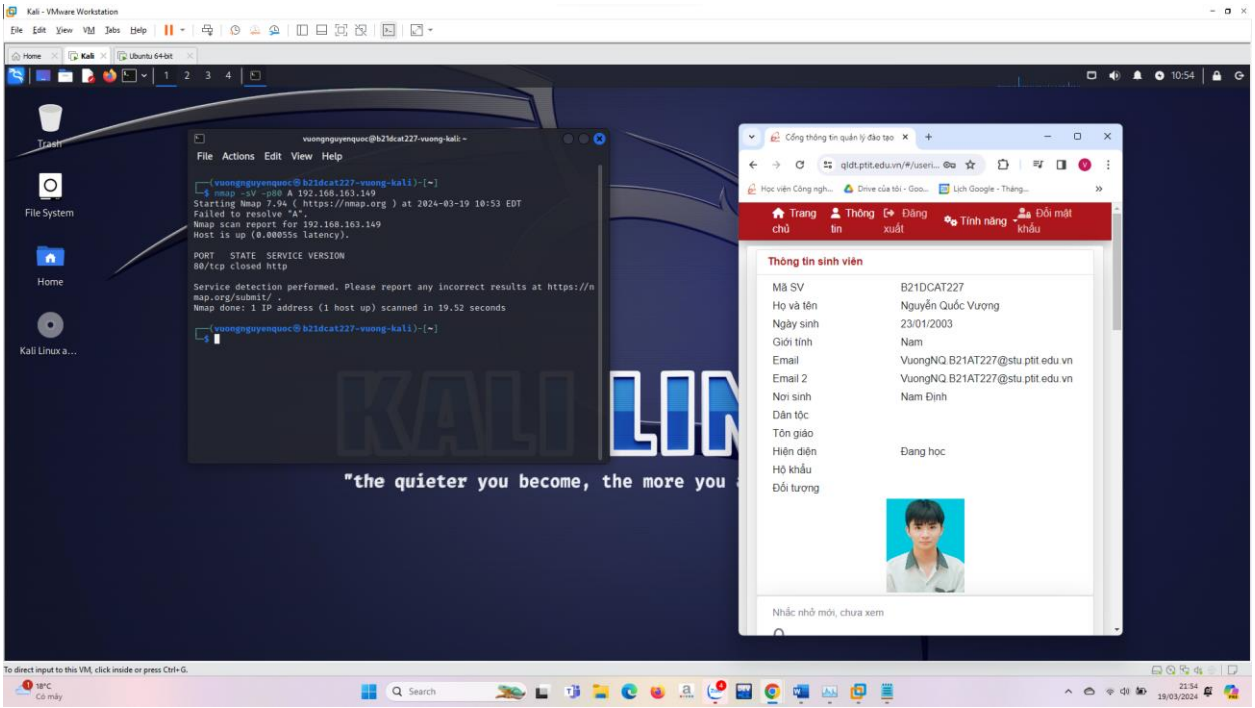
- Bước 4: thực thi tấn công và phát hiện sử dụng Snort

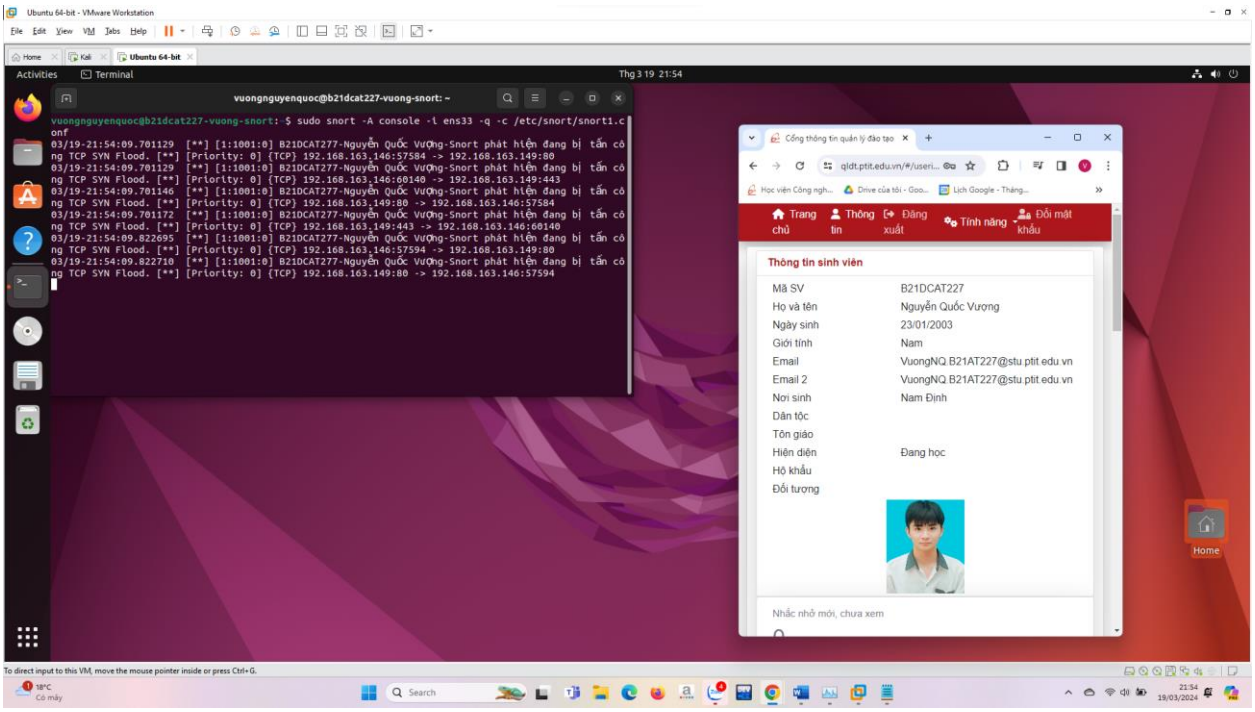
+ Từ máy Kali, sử dụng lệnh ping để ping máy Snort. Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.



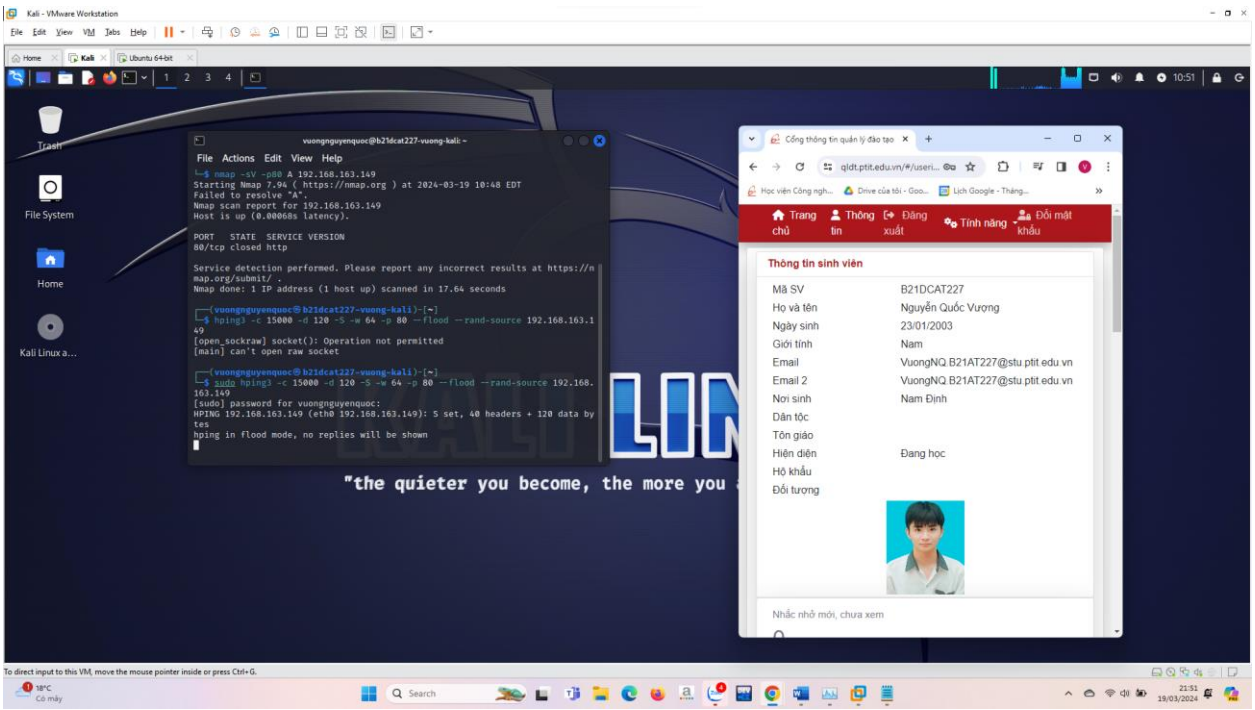


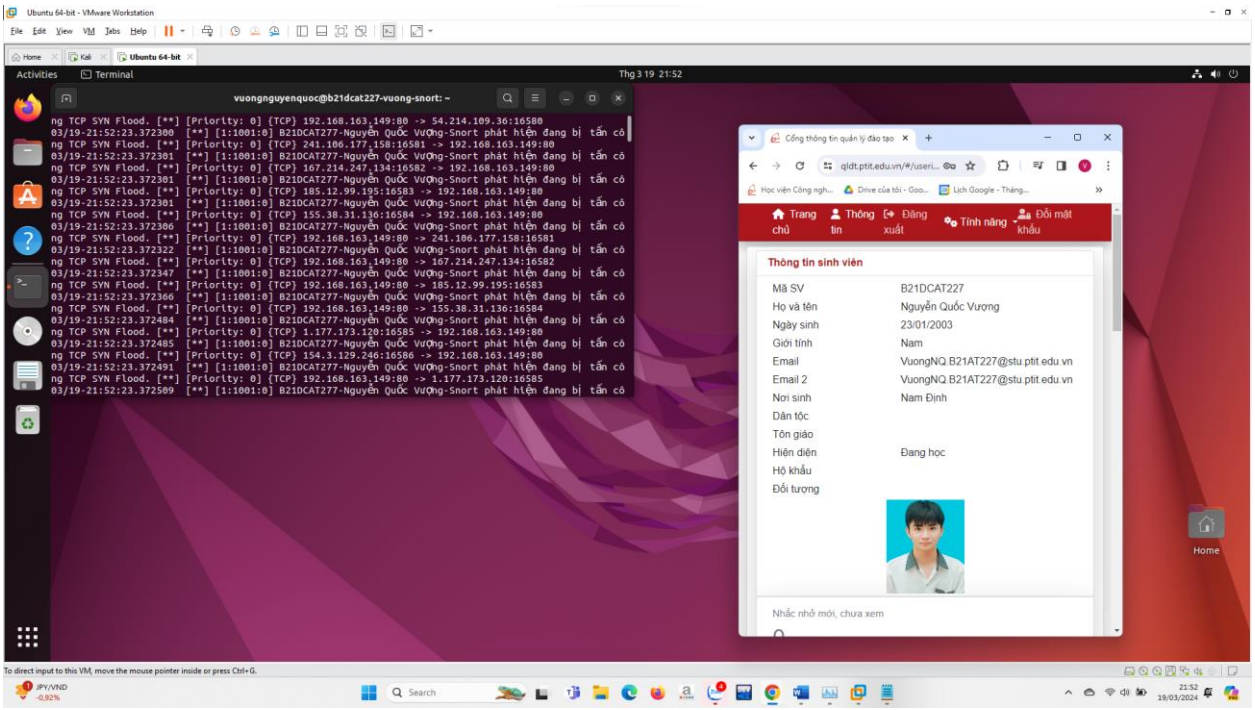
+ Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort (dùng lệnh: nmap -sV -p80 A <địa chỉ IP máy Snort>). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.





+ 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.





2.4 Kết quả cần đạt

- 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).