BÁO CÁO LAB 2

Môn: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

GVTH: ĐỖ HOÀNG HIỂN

Sinh viên thực hiện	**Sinh viên 1** MSSV: 21522573 Họ tên: Phạm Thanh Tâm **Sinh viên 2** MSSV: 21520514 Họ tên: Nguyễn Văn Anh Tú
Lớp	**NT204.O21.ATCL**
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc *(nếu là nhóm)*	**[Sinh viên 1]**: Yêu cầu 1,3 **[Sinh viên 2]**: Yêu cầu 2, 3
Link Video thực hiện *(nếu có yêu cầu)*	
Ý kiến *(nếu có)* *+ Khó khăn gặp phải* *+ Đề xuất, góp ý…*	
Điểm tự đánh giá *(bắt buộc)*	**10/10**

[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

BÁO CÁO CHI TIẾT

Yêu cầu 1: Sinh viên trả lời các câu hỏi bên dưới.

1.1a. Tìm hiểu về Snort? Snort cho phép chạy trên những chế độ (mode) nào?

- Snort là hệ thống ngăn chặn xâm nhập nguồn mở có khả năng phân tích lưu lượng truy cập và ghi nhật ký gói theo thời gian thực. Là hệ thống ngăn chặn xâm nhập mã nguồn mở hàng đầu thế giới. Snort sử dụng một loạt quy tắc giúp xác định hoạt động mạng độc hại và sử dụng các quy tắc đó để tìm các gói phù hợp với chúng và tạo cảnh báo cho người dùng.

- Snort chạy trên 3 mode:

+ Sniffer mode (chế độ ngầm): Trong chế độ này, Snort hoạt động như một công cụ giám sát mạng, chờ đợi và ghi lại các gói dữ liệu mạng mà nó nhận được. Chế độ này thường được sử dụng để xác định các vấn đề về bảo mật trong mạng, kiểm tra hoạt động mạng, và phát hiện xâm nhập.

+ Packet Logger Mode (Chế độ ghi gói dữ liệu): Trong chế độ này, Snort ghi lại toàn bộ hoặc một phần của các gói dữ liệu mạng mà nó nhận được vào một tập tin log. Thông thường, chế độ này được sử dụng để ghi lại lưu lượng mạng để phân tích sau này hoặc để duy trì một lịch sử hoạt động mạng.

+ Network Intrusion Detection System (NIDS) Mode (Chế độ phát hiện xâm nhập mạng): Đây là chế độ phổ biến nhất và mạnh mẽ nhất của Snort. Trong chế độ này, Snort sử dụng các quy tắc (rules) được định nghĩa trước để phát hiện các hoạt động không mong muốn hoặc các mẫu tấn công trong lưu lượng mạng. Khi Snort phát hiện một hoạt động không mong muốn, nó sẽ tạo ra cảnh báo để cảnh báo người quản trị hệ thống.

1.1b. Trình bày về những tính năng chính của Snort?

- Snort có ba mục đích sử dụng chính:

+ Là một thám thính gói như tcpdump, như một trình ghi nhật kí gói – rất hữu ích cho việc gỡ lỗi lưu lượng truy cập mạng hoặc có thể sử dụng như một hệ thống ngăn chặn xâm nhập mạng toàn diện.Snort có thể được tải xuống và cấu hình để sử dụng cho cá nhân và doanh nghiệp

+ Snort có khả năng phát hiện các mẫu tấn công dựa trên các quy tắc và chính sách được cấu hình trước. Khi phát hiện một mẫu tấn công, nó sẽ tạo ra các cảnh báo để cảnh báo người quản trị hệ thống.

+ Snort có thể kiểm tra tất cả các gói tin trên mạng, phân tích chúng và kiểm tra xem chúng có chứa các biểu hiện của các cuộc tấn công hay không. Snort sử dụng một ngôn ngữ quy tắc mạnh mẽ để định nghĩa các biểu hiện của các loại tấn công. Người dùng có thể tạo ra các quy tắc tùy chỉnh dựa trên nhu cầu cụ thể của họ.

+ Snort có khả năng phát hiện tấn công dựa trên các chữ ký của chúng. Nó sử dụng cơ sở dữ liệu chữ ký để so sánh các gói tin mạng và xác định xem chúng có tương tự với các mẫu tấn công đã biết hay không.

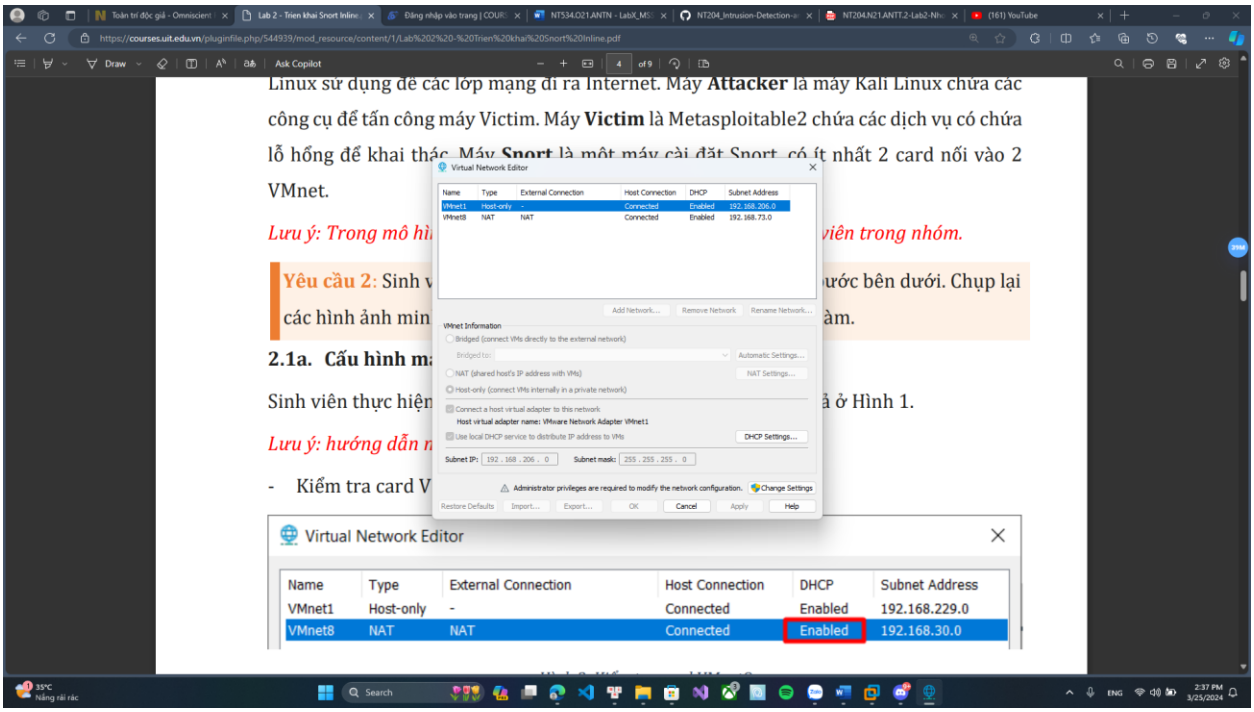
+ Snort không chỉ phát hiện tấn công dựa trên các chữ ký mẫu, mà còn dựa trên hành vi không bình thường của các gói tin mạng để xác định các mẫu tấn công mới hoặc không xác định trước. Snort cung cấp cơ chế cập nhật để cập nhật các quy tắc phát hiện mới và các chữ ký mới của các mẫu tấn công.

2. Cài đặt và cấu hình Snort để giám sát mạng

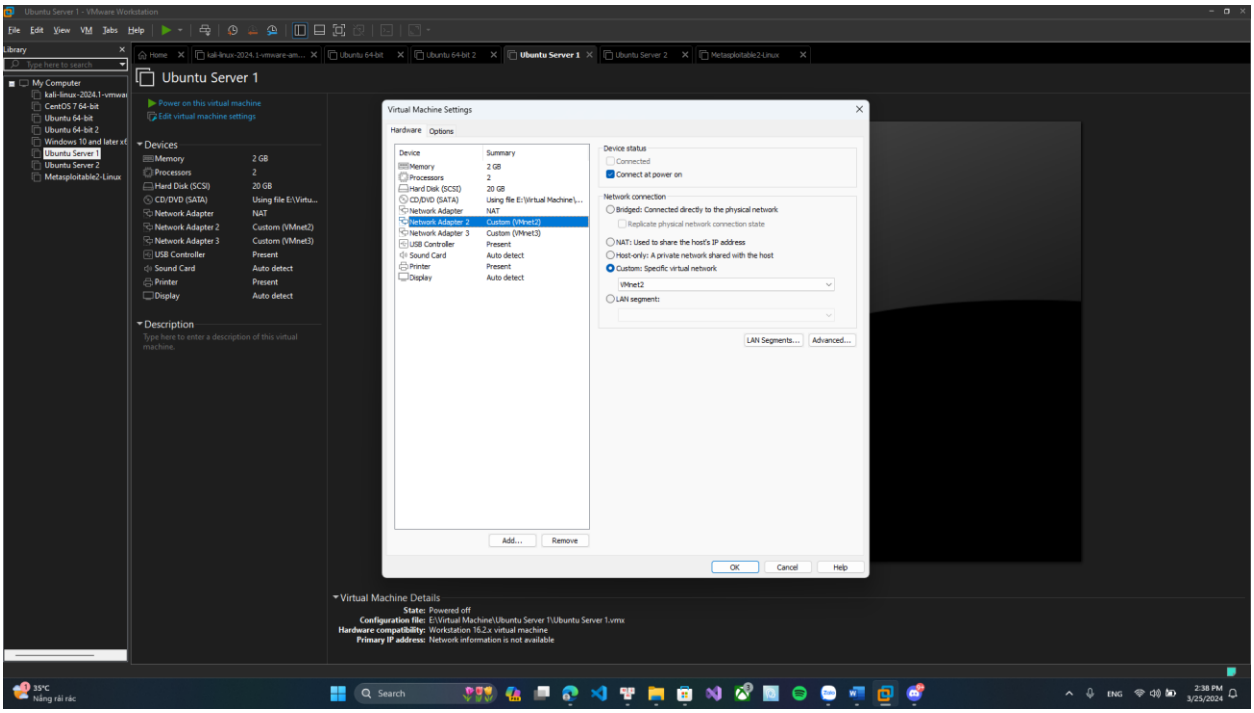
Yêu cầu 2: Sinh viên cài đặt và cấu hình Snort Inline theo các bước bên dưới. Chụp lại các hình ảnh minh chứng (chụp full màn hình) cho từng bước làm

2.1a. Cấu hình mạng cho các máy theo mô hình

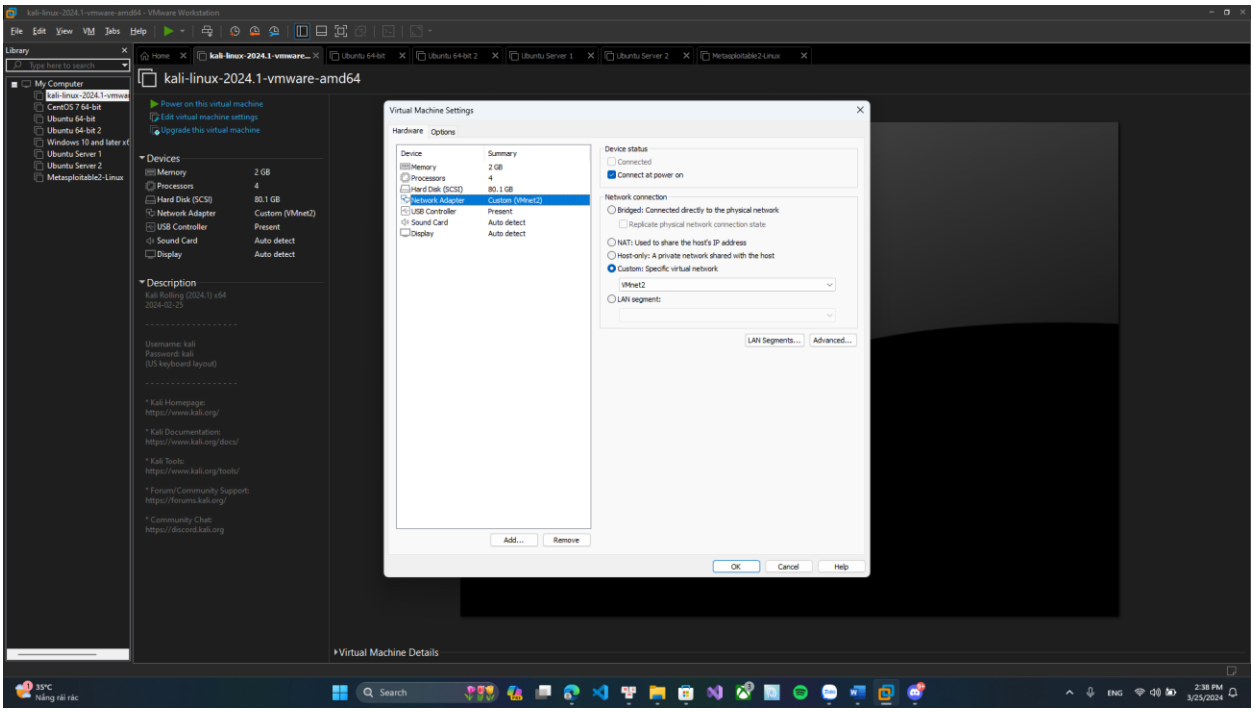
- Kiểm tra card VMnet8 (NAT) đã tồn tại và được bật DHCP



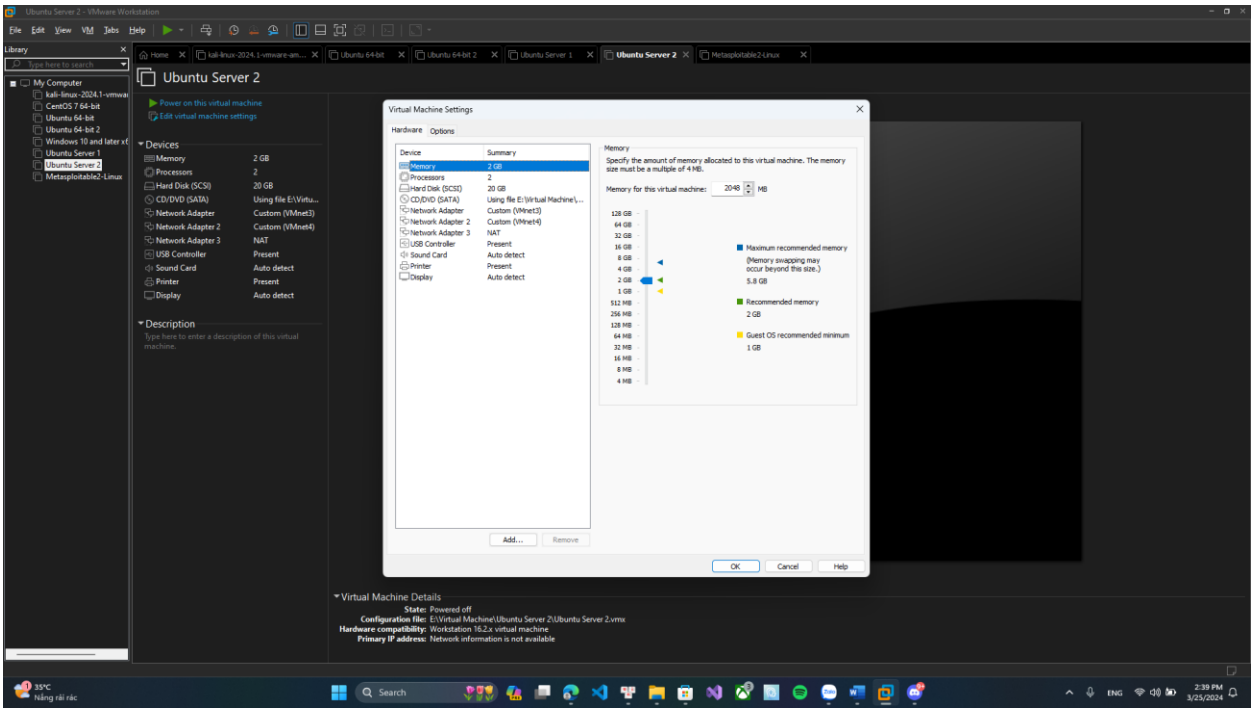
- Thêm card mạng cho Máy ảo Router:



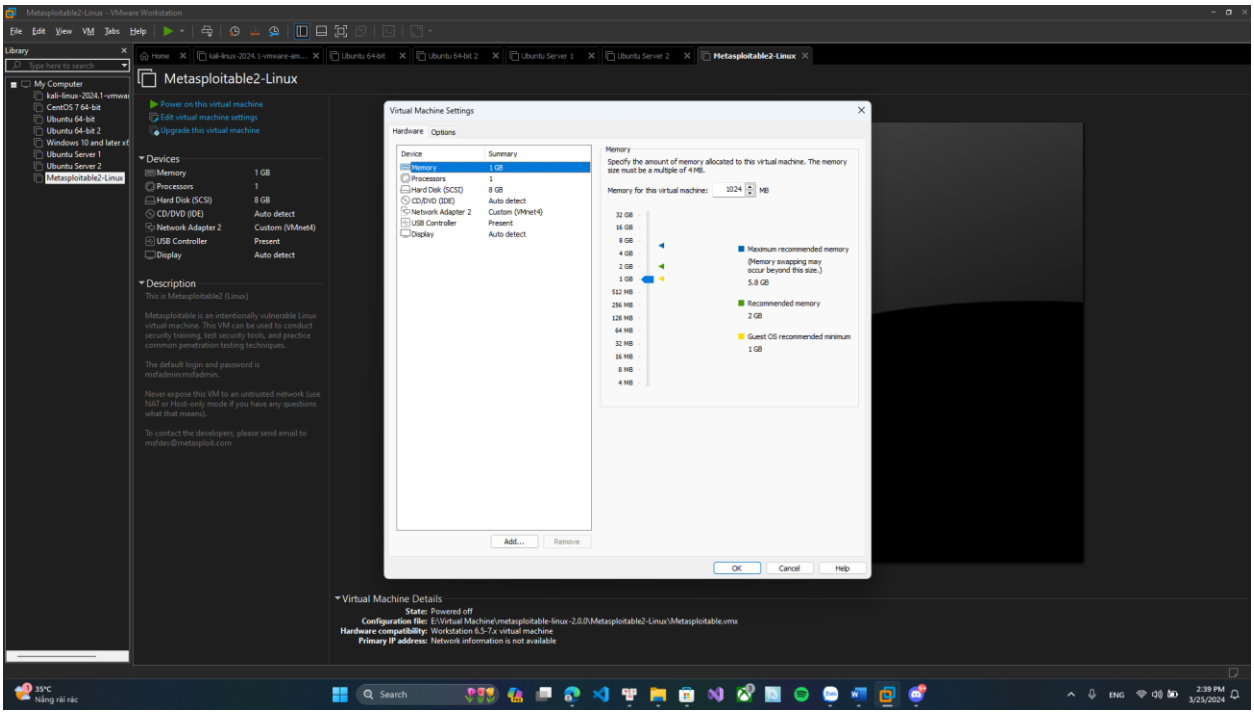
- Gán card mạng lên máy Kali:



- Gán card mạng lên máy ảo Snort:

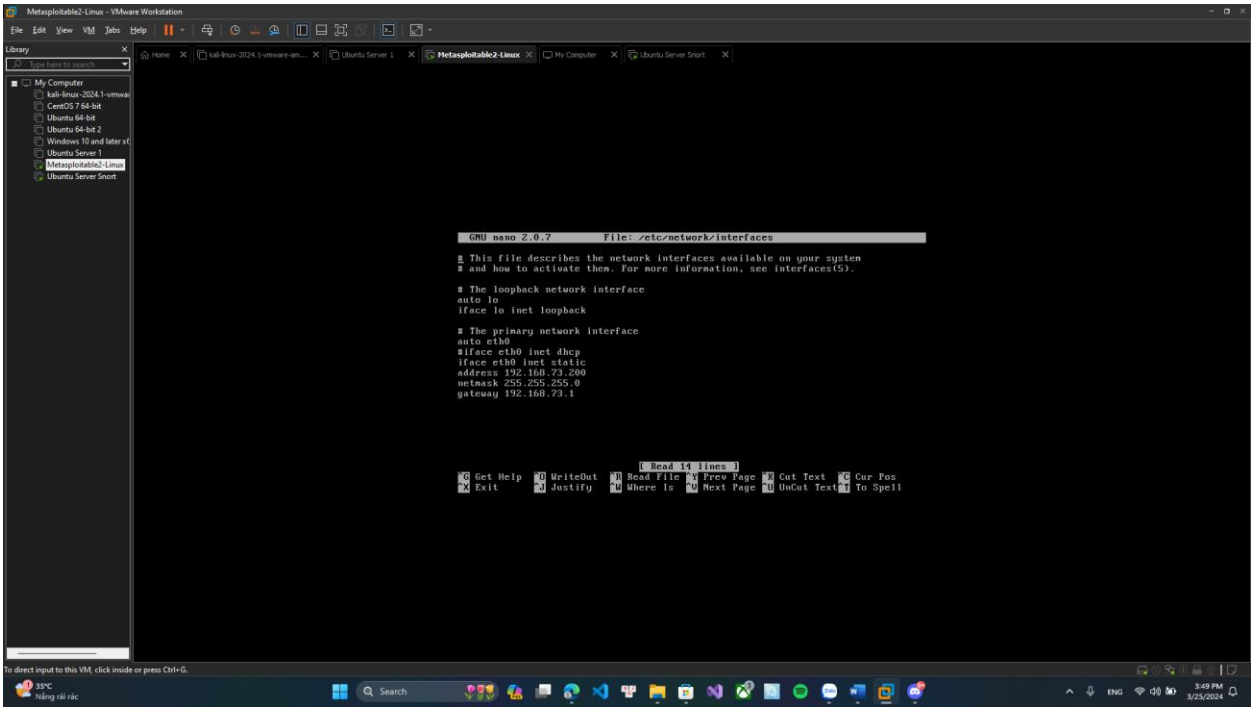


- Gán card mạng lên máy ảo Metasploitable 2 (Victim):

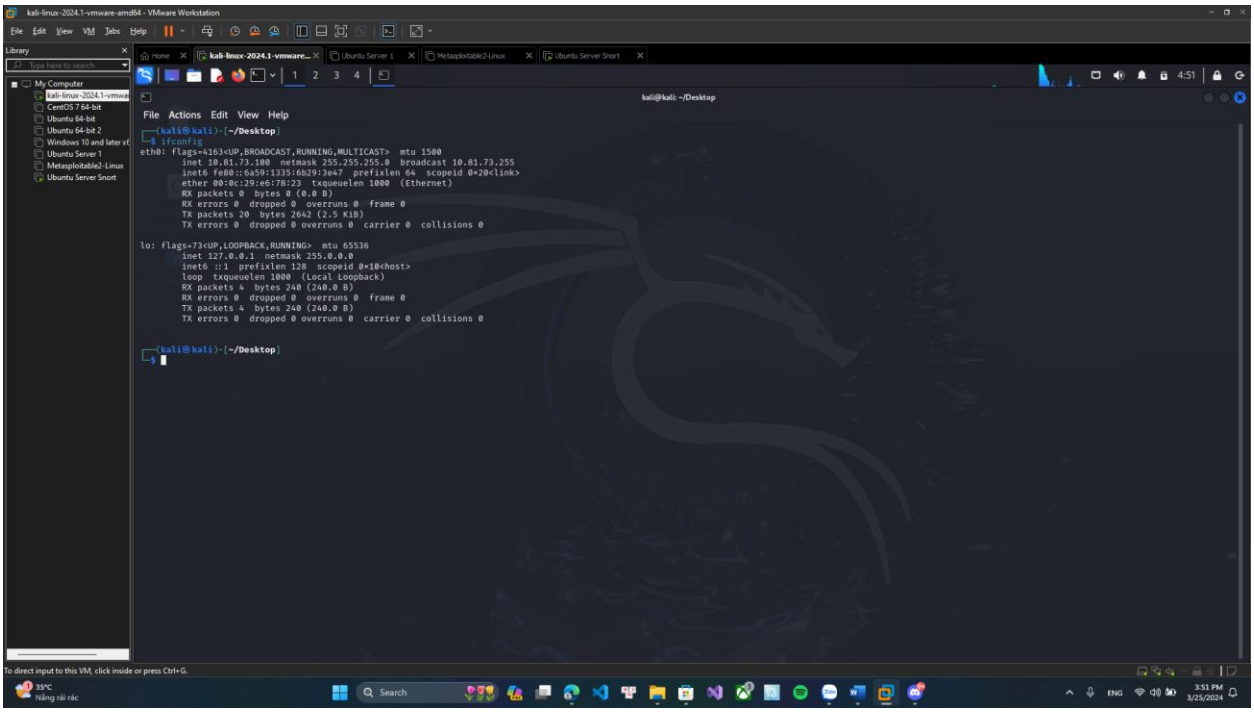


2.1b. Cấu hình địa chỉ ip cho các máy

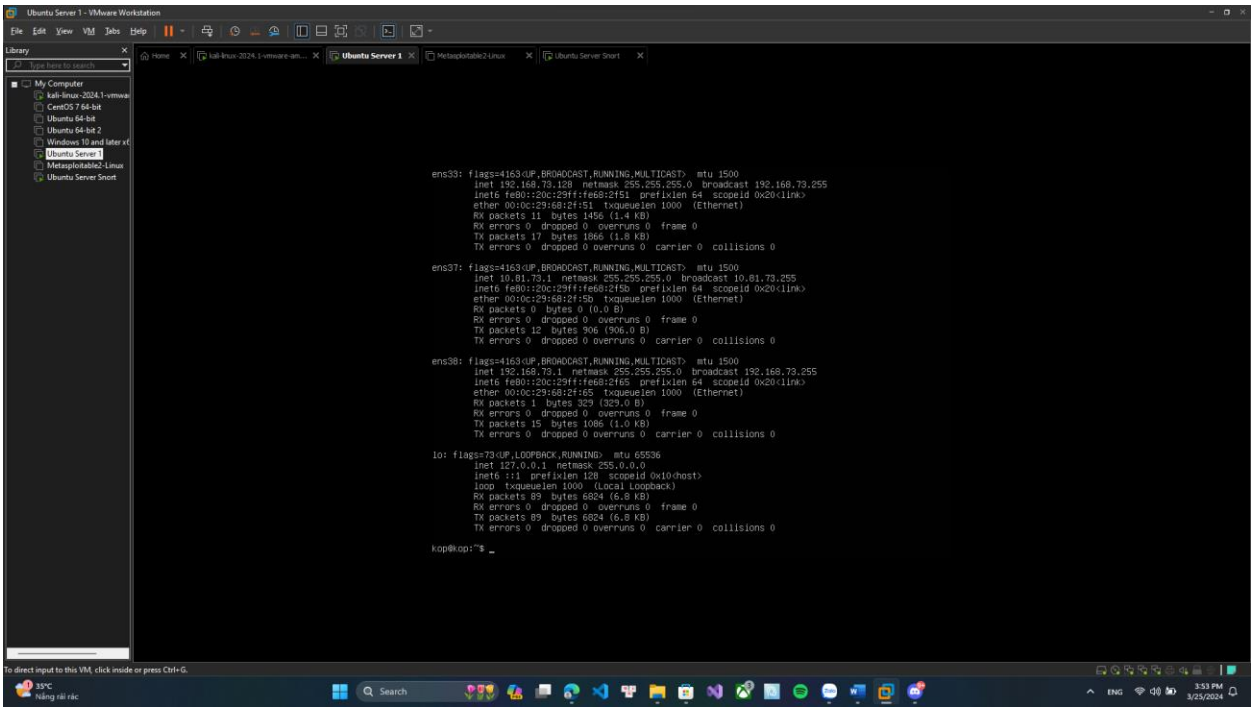
- Máy Victim:



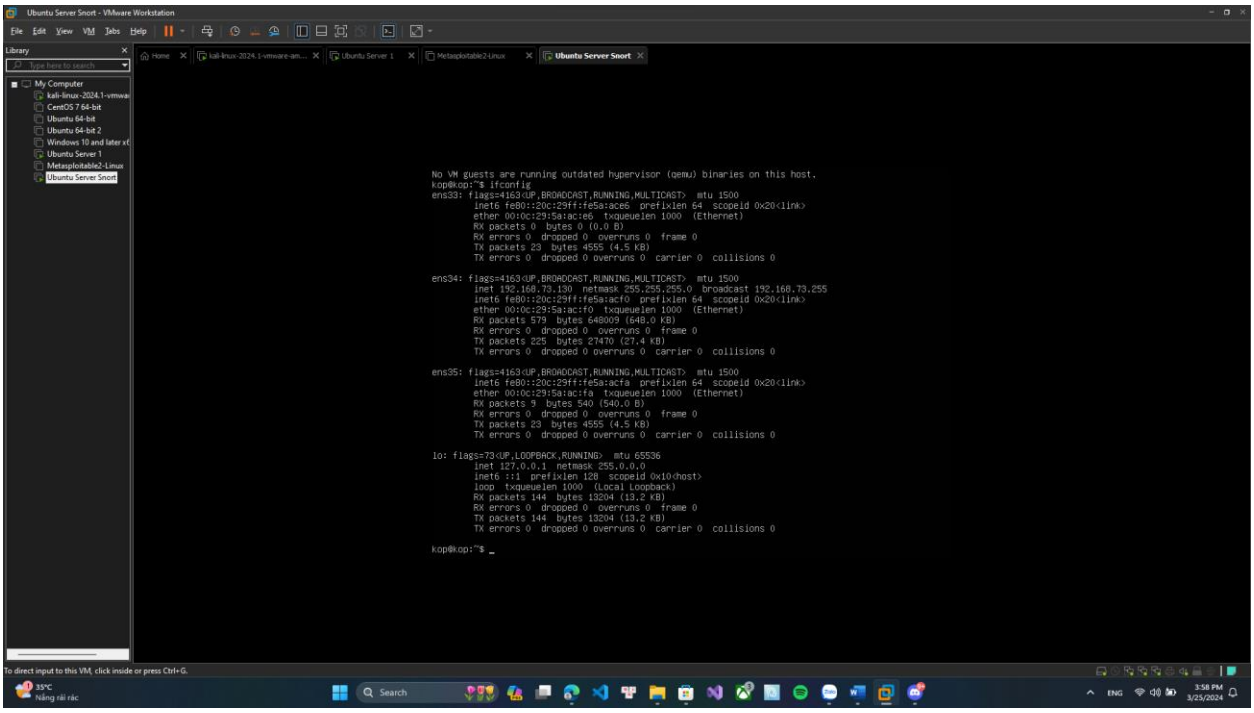
- Máy Attacker:



- Máy Router:

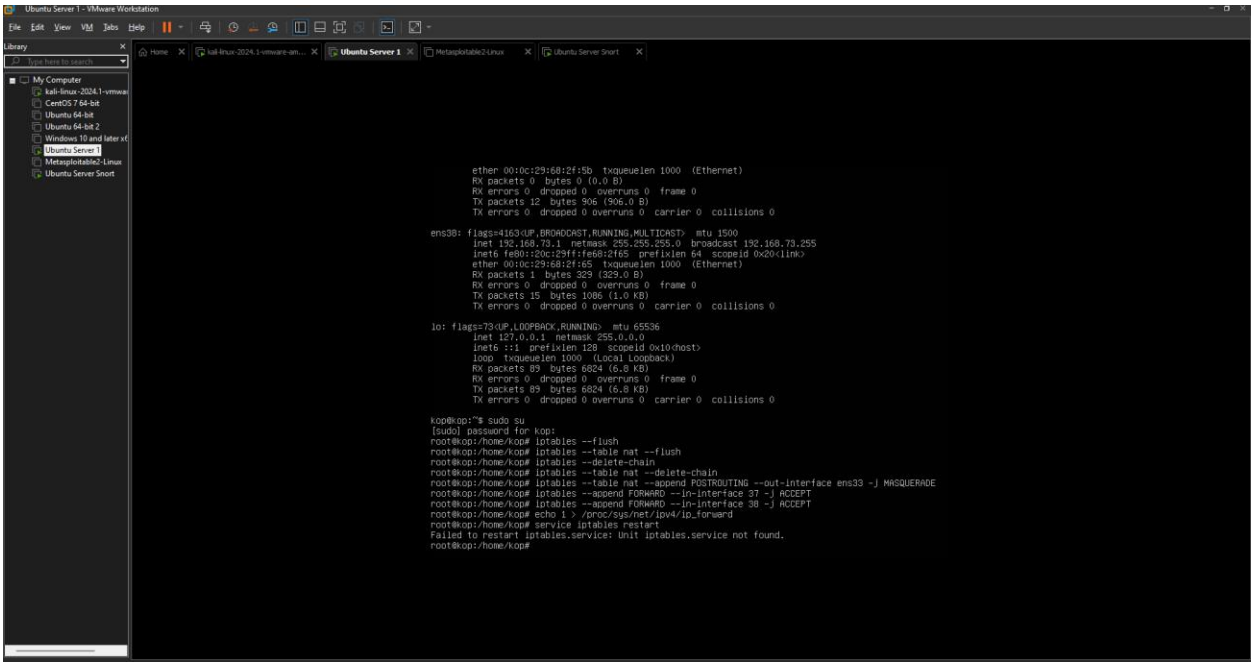


- Máy Snort:

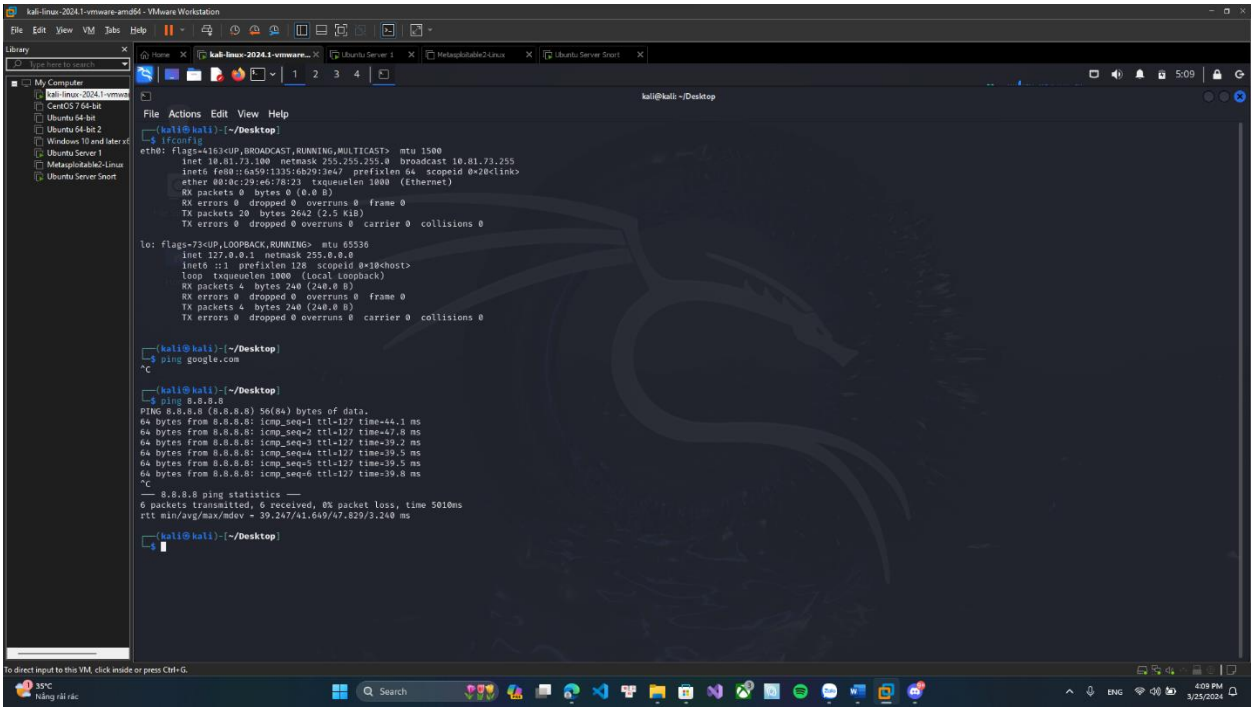


2.1c. Cấu hình NAT outbound cho máy router

- Set up Nat outbound:

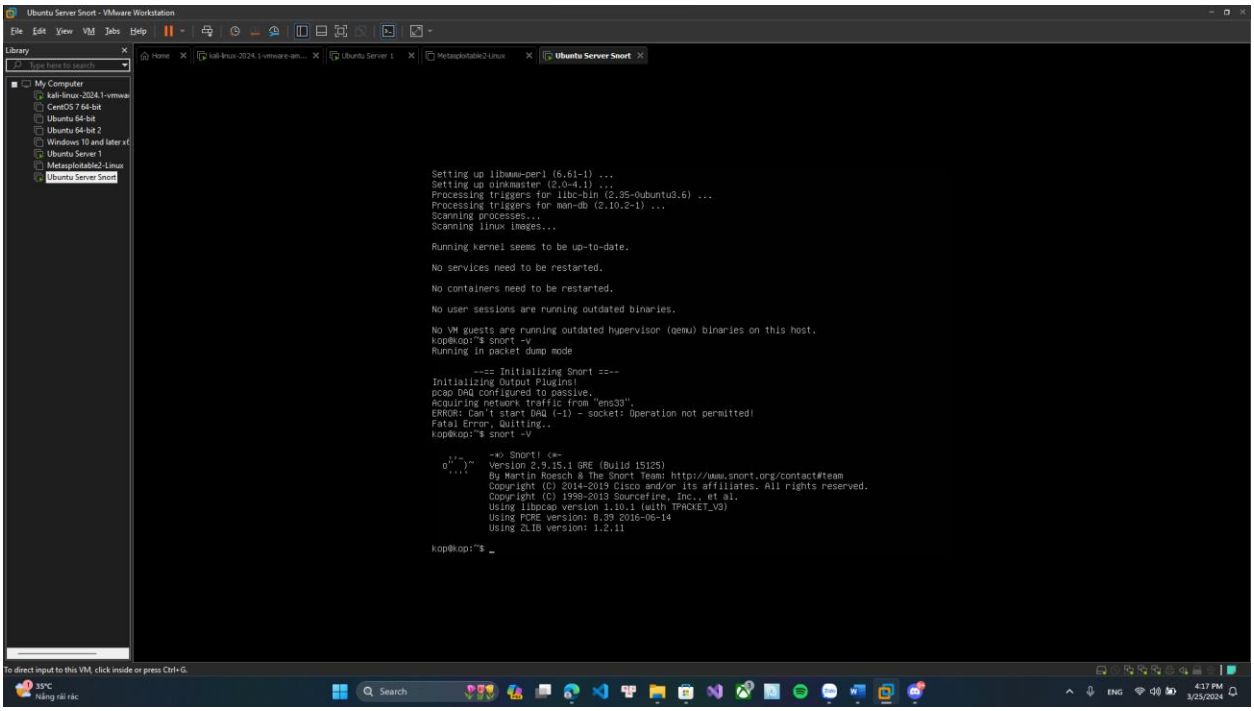


- Máy Kali (Attacker) đã ping được 8.8.8.8:

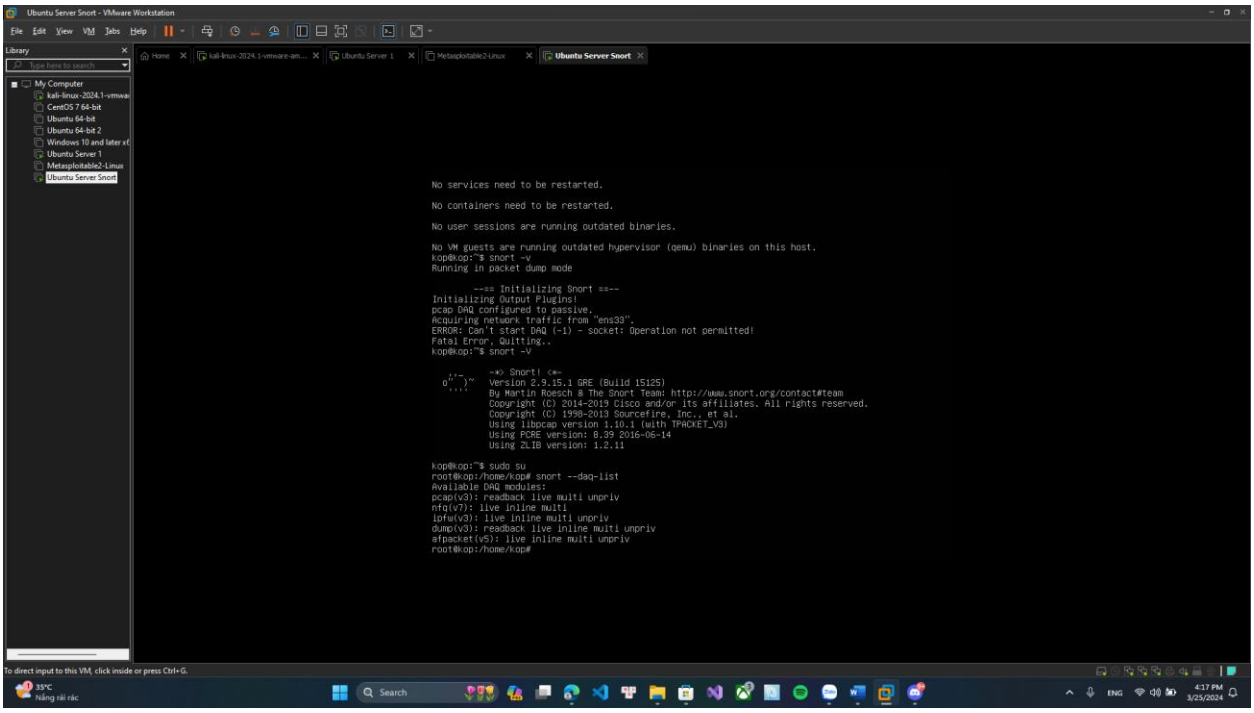


2.1d. Cài đặt và cấu hình Snort

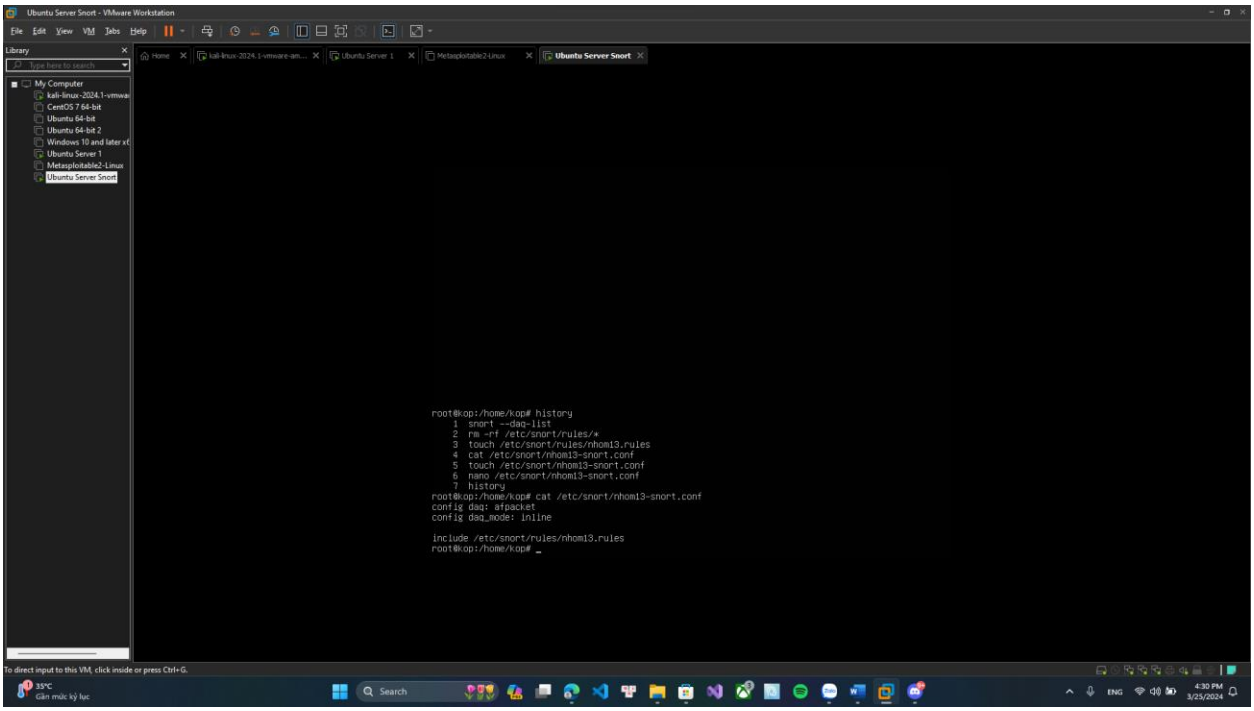
- Cài đặt Snort:



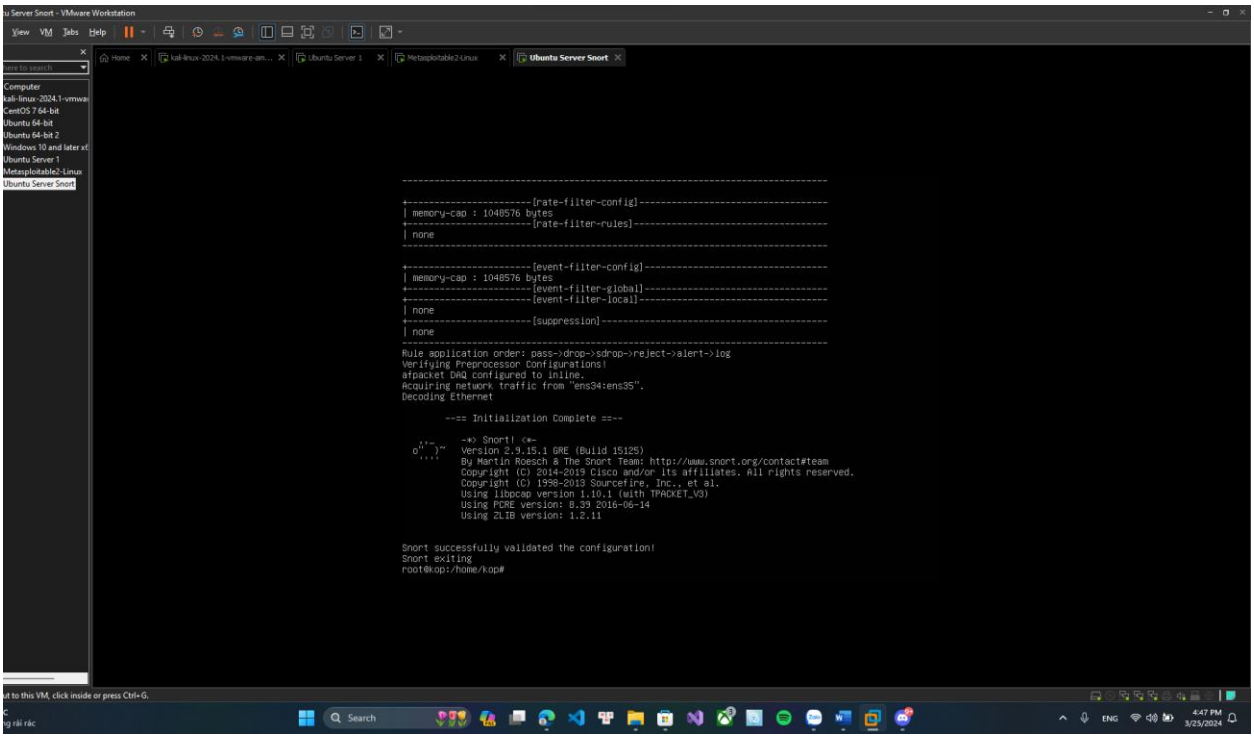
- Kiểm tra afpacket DAQ:



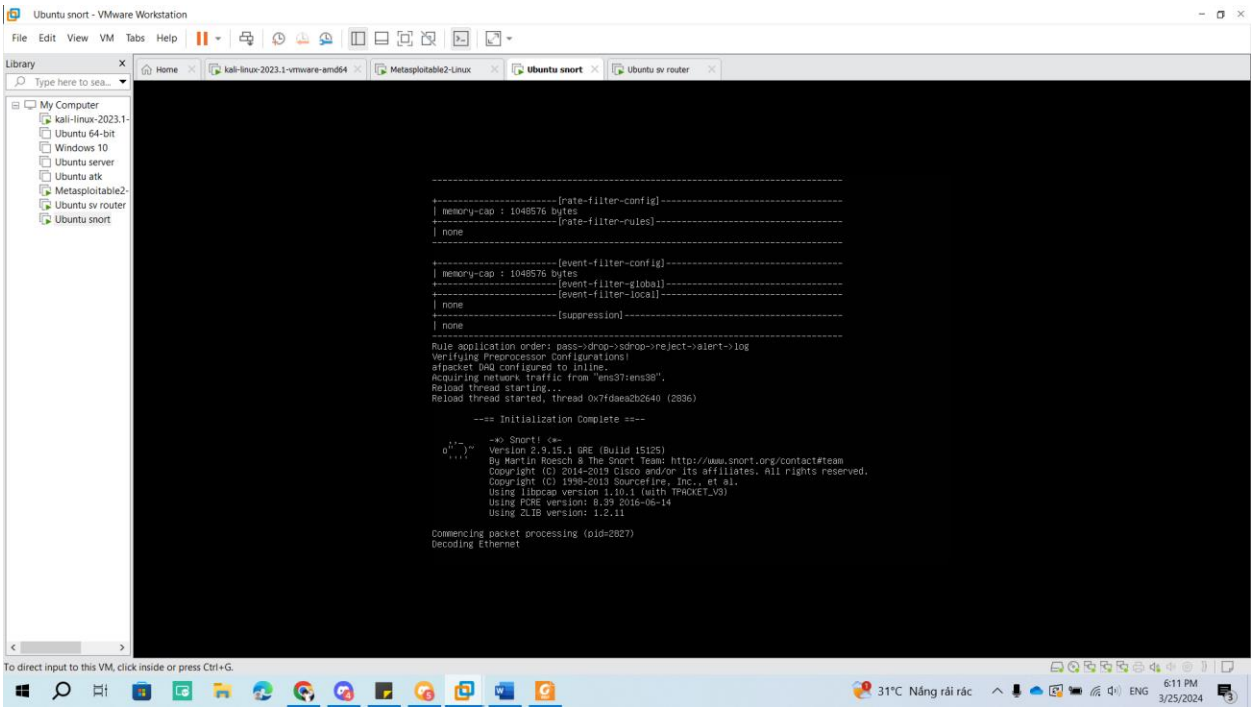
- Xóa file rule mặc định, tạo file rule mới và cấu hình snort:



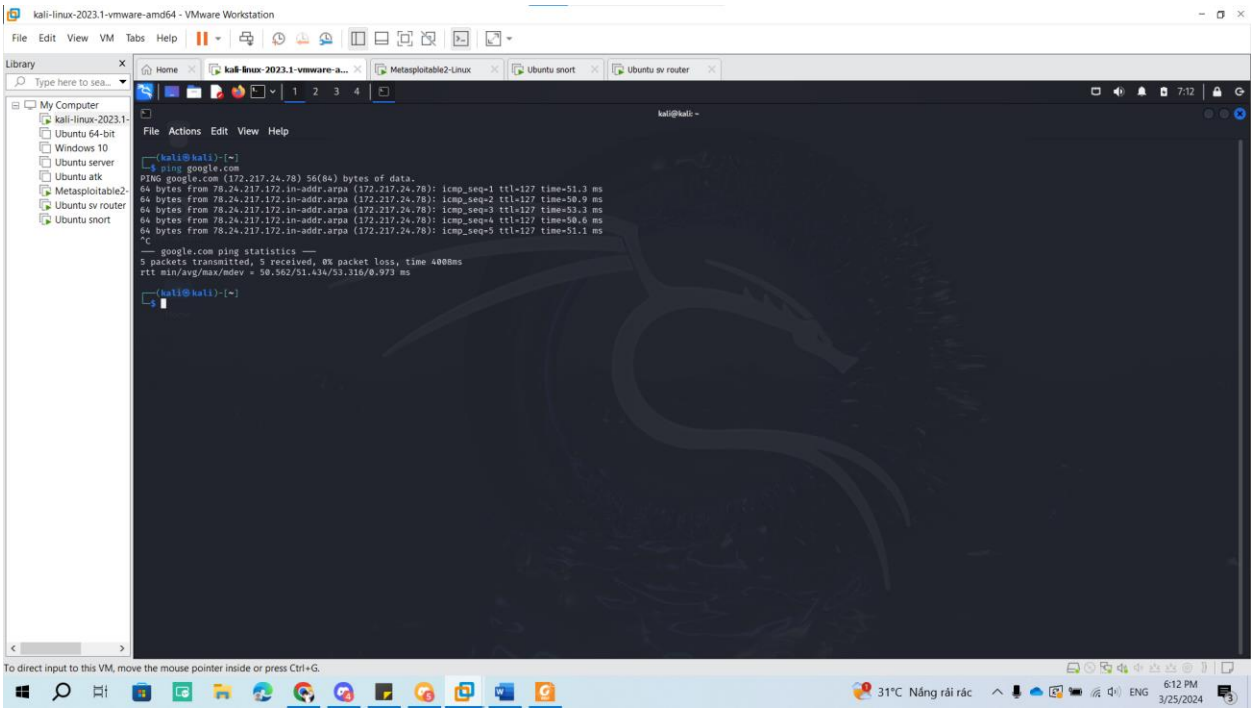
- Kiểm tra file cấu hình snort:



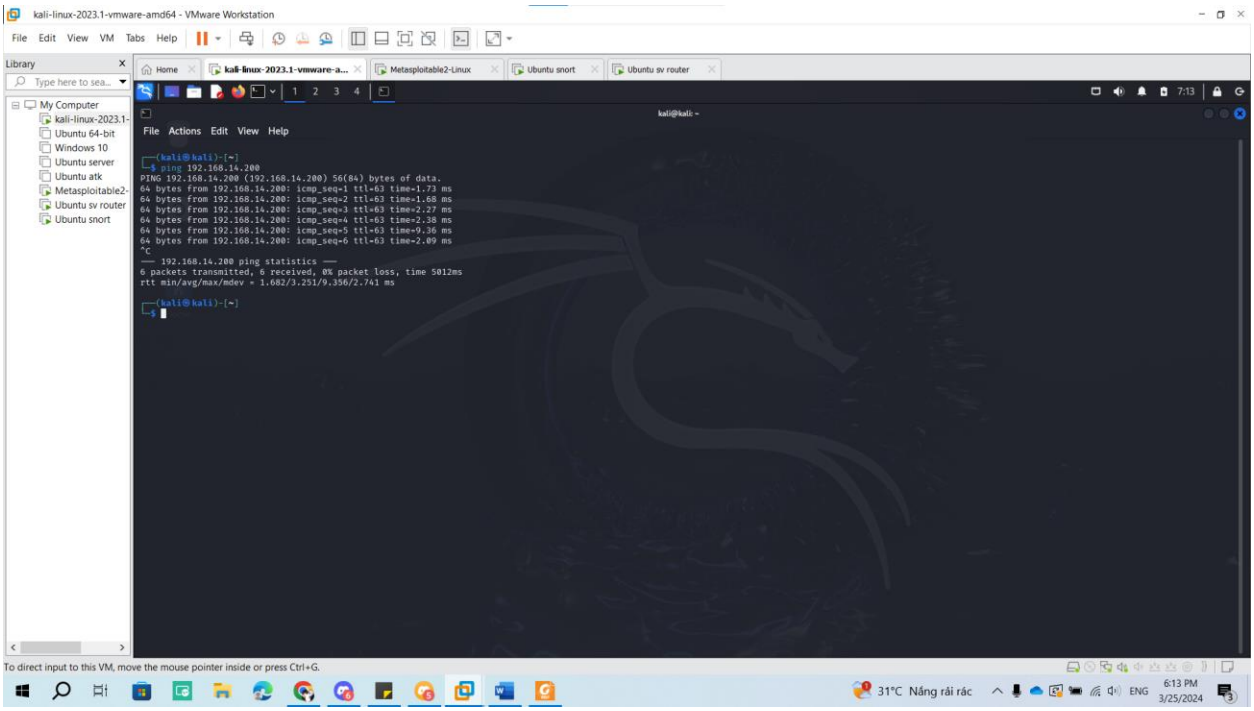
- Chạy Snort inline:



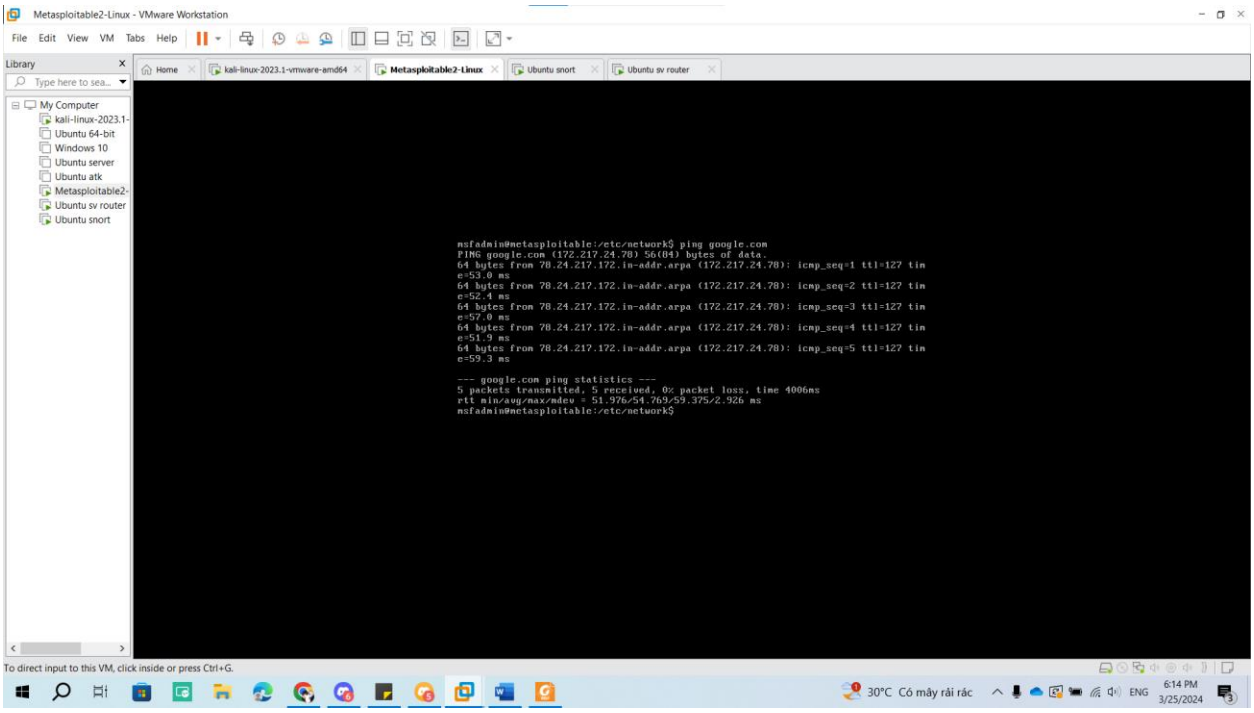
- Máy Kali ping google.com



- Máy Kali ping Victim

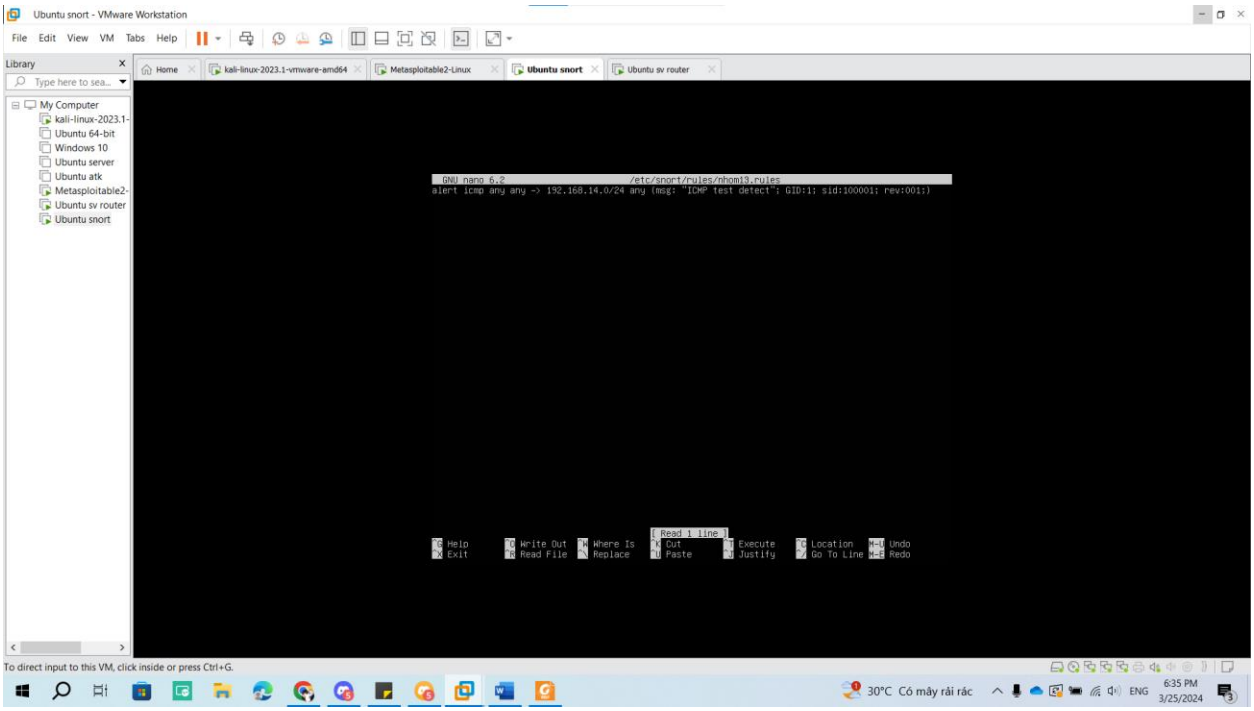


- Máy Victim ping google.com

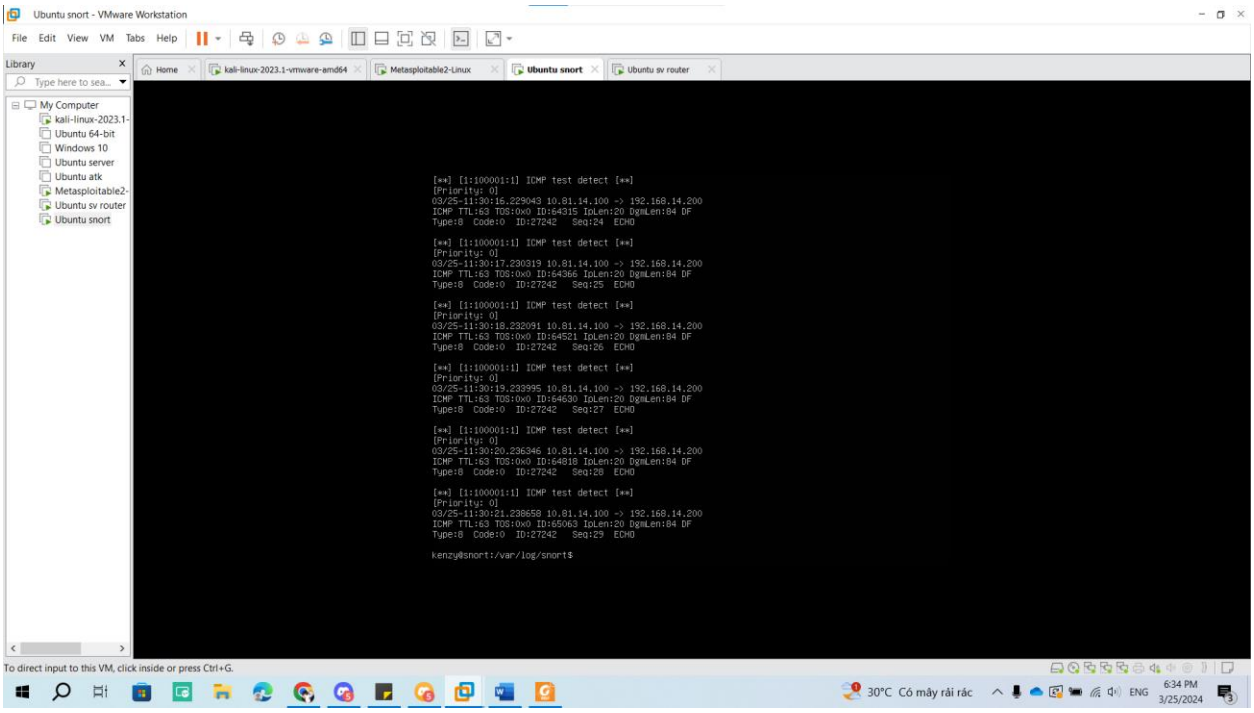


2.1e. Viết rule cho Snort

- Viết rule phát hiện gói ICMP gửi đến lớp mạng 192.168.x.0/24 trong file **/etc/snort/rules/nhom13.rules** như sau:



- Kiểm tra log của snort



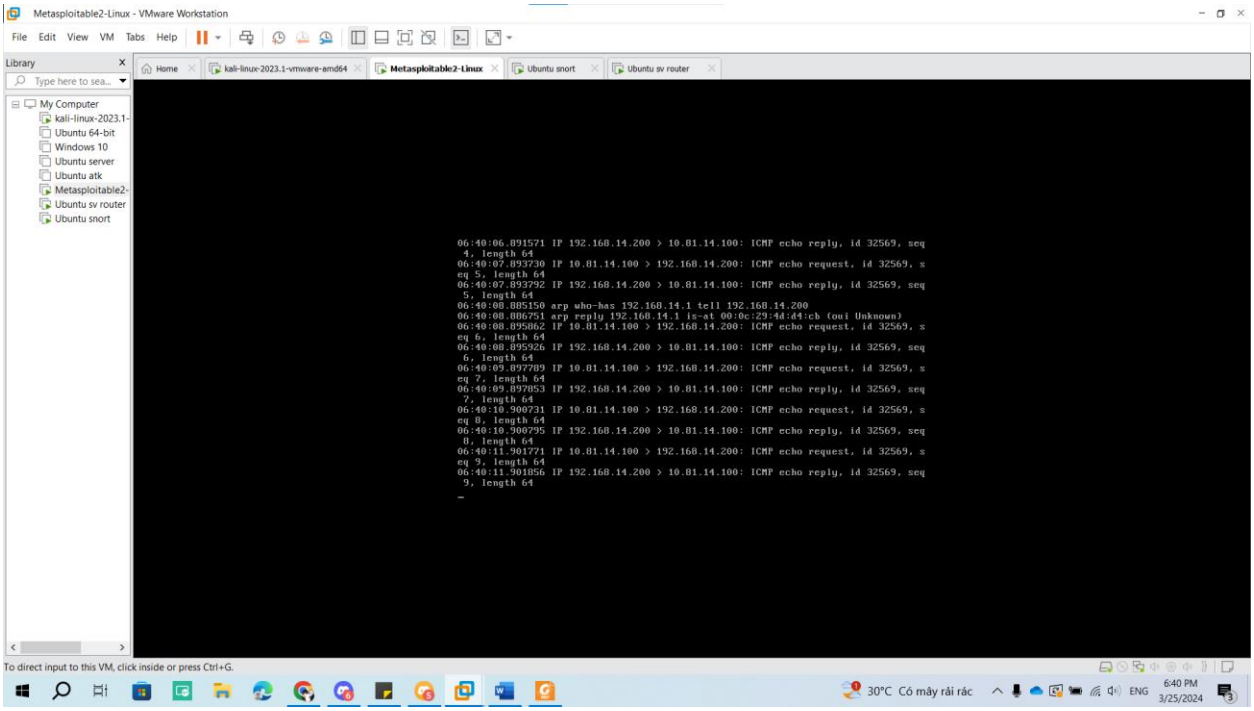
Yêu cầu 3: Sinh viên viết rule drop các gói ICMP đi đến máy Victim (rule #1) sử dụng tcmdump trên máy Victim kiểm tra các trường hợp sau:

- **Trước khi viết áp dụng rule #1**

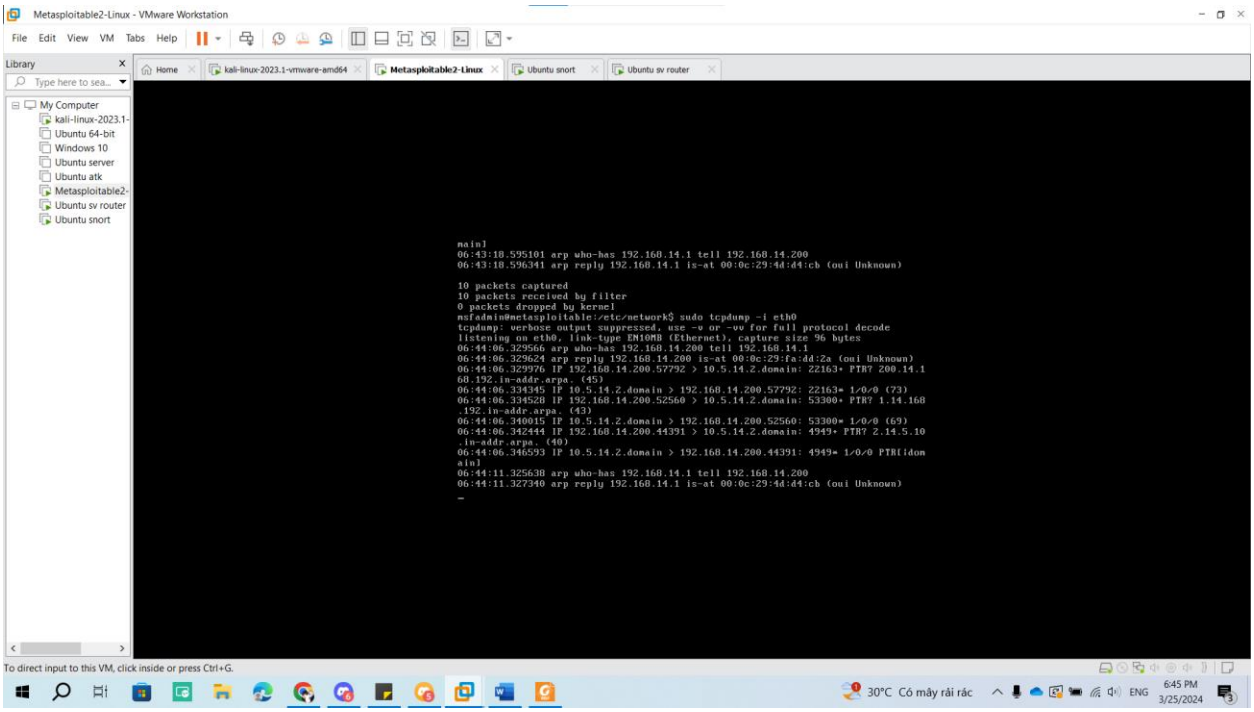
- **Sau khi áp dụng rule #1.**

Kiểm tra alert log của snort để xem kết quả

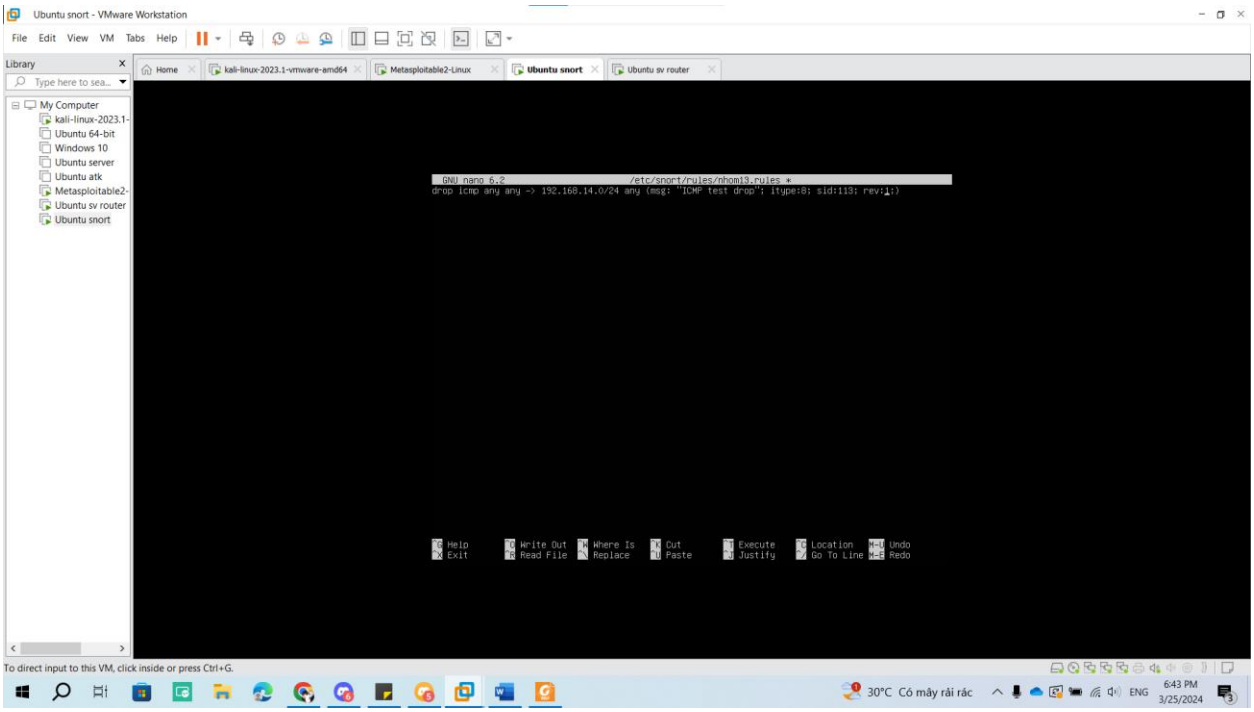
- Trước khi viết áp dụng rule #1



- Sau khi viết áp dụng rule #1



- Rule #1 drop các gói ICMP



- Alert log của Snort