Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

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

Kỳ báo cáo: Buổi 02

Tên chủ đề: Triển khai Snort Inline

GV: Đỗ Hoàng Hiển

Ngày báo cáo: 08/04/2023

Nhóm: 07

1. THÔNG TIN CHUNG:

Lớp: NT204.N21.ANTT

STT	Họ và tên	MSSV	Email
1	Phạm Phúc Đức	20520162	20520162@gm.uit.edu.vn
2	Lê Trần Thùy Trang	20520323	20520323@gm.uit.edu.vn
3	Nguyễn Đức Tấn	20520751	20520751@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Tìm hiểu và sử dụng Snort	100%	Trang, Tấn
2	Cài đặt và cấu hình Snort để giám sát mạng	100%	Đức, Trang
3	Viết rule cho Snort	100%	Đức, Tấn

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Tìm hiểu và sử dụng Snort

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

Snort là một hệ thống ngăn chặn xâm nhập mạng nguồn mở, có khả năng thực hiện phân tích lưu lượng truy cập thời gian thực và ghi nhật ký gói trên mạng IP. Nó có thể thực hiện phân tích giao thức, tìm kiếm/khớp nội dung và có thể được sử dụng để phát hiện nhiều cuộc tấn công và thăm dò khác nhau, chẳng hạn như tràn bộ đệm (buffer overflows), quét cổng ẩn (stealth port scans), tấn công CGI (CGI attacks), thăm dò (SMB probes), nỗ lực lấy dấu vân tay của hệ điều hành (OS fingerprinting attempts),...[2]

Snort cho phép chạy trên 3 mode[3]:

- Sniffer mode: Chỉ đơn giản là đọc các gói tin từ mạng và hiển thị chúng trên console (màn hình).
- Packet logger mode: Cho phép Snort ghi lại các gói tin truyền qua mạng vào một tập tin log để phân tích sau này.
- Network Intrusion Detection System (NIDS) mode: Cho phép Snort phát hiện các cuộc tấn công trên mạng bằng cách so sánh các gói tin mạng với các quy tắc (rules) được định nghĩa trước.

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

Các tính năng chính của Snort:

- Phát hiện tấn công: Snort có thể phát hiện nhiều loại tấn công khác nhau như DOS, remote attack,...
- Giám sát lưu lượng mạng: Snort giám sát lưu lượng trong thời gian thực, giúp việc phát hiện và bảo vệ hệ thống mạng một cách kịp thời.

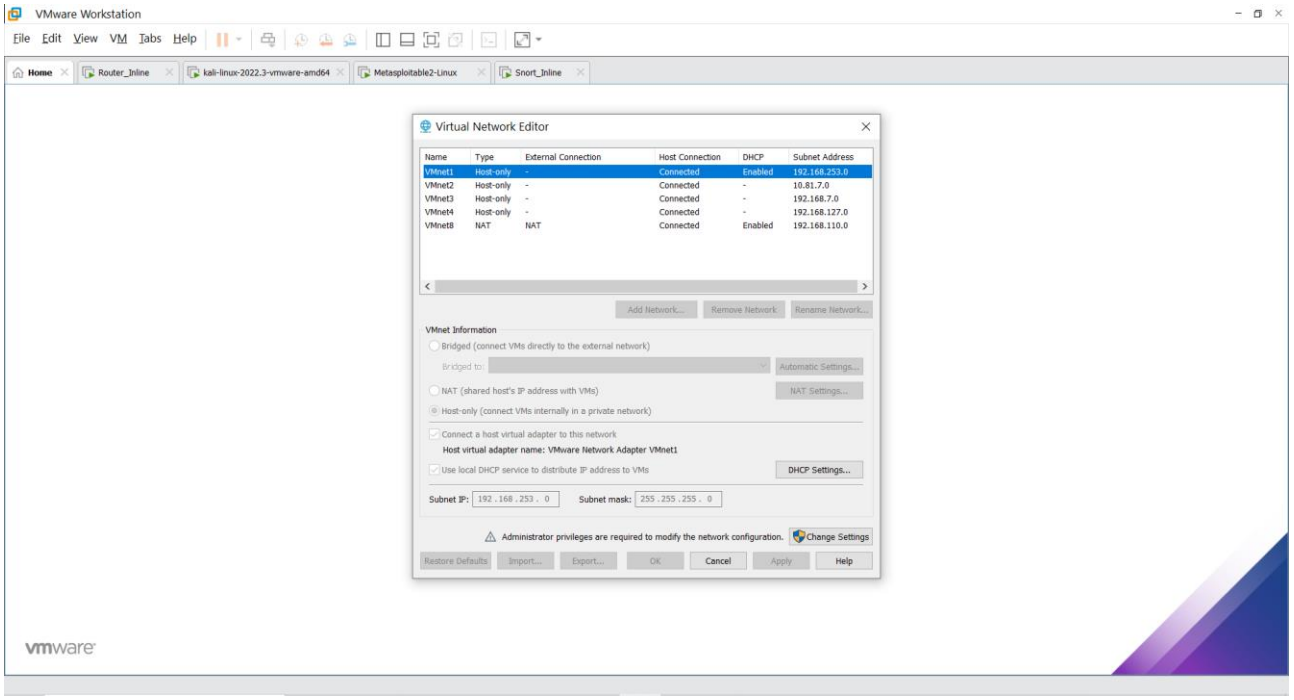
[2] Snort, "What is Snort" [Trực tuyến: What is Snort?] [Truy cập ngày 08/04/2023]
[3] "Getting Started" [Trực tuyến: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node3.html#:~:text=Sniffer%20mode%2C%20which%20simply%20reads,and%20analysis%20on%20network%20traffic] [Truy cập ngày 08/04/2023]

- Kiểm soát truy cập: Kiểm soát bằng cách cho phép hoặc chặn lưu lượng truy cập đi hoặc đến IP, port cụ thể.
- Tính khả dụng cao: Snort có thể triển khai được trên nhiều hệ thống nhau, bao gồm Linux, Windows và Unix.

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

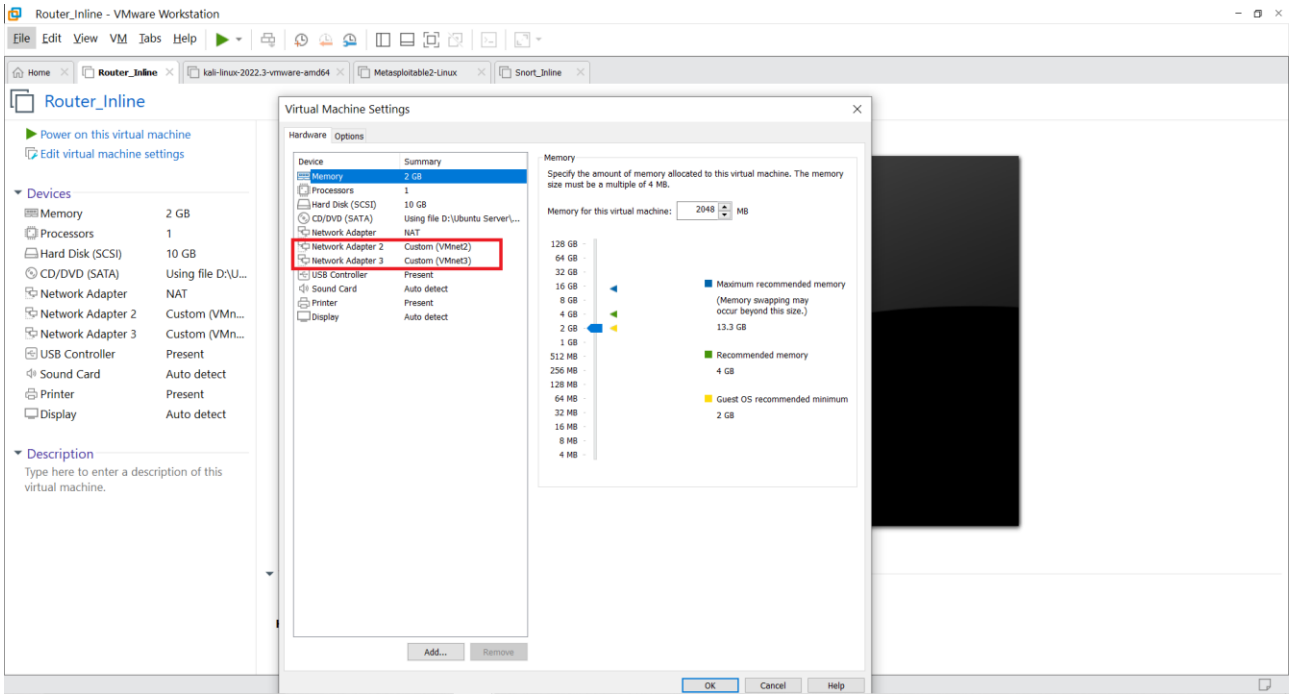
Yêu cầu 2: Cài đặt và cấu hình Snort Inline theo các bước

Bước 1: Thêm các card mạng cần sử dụng:



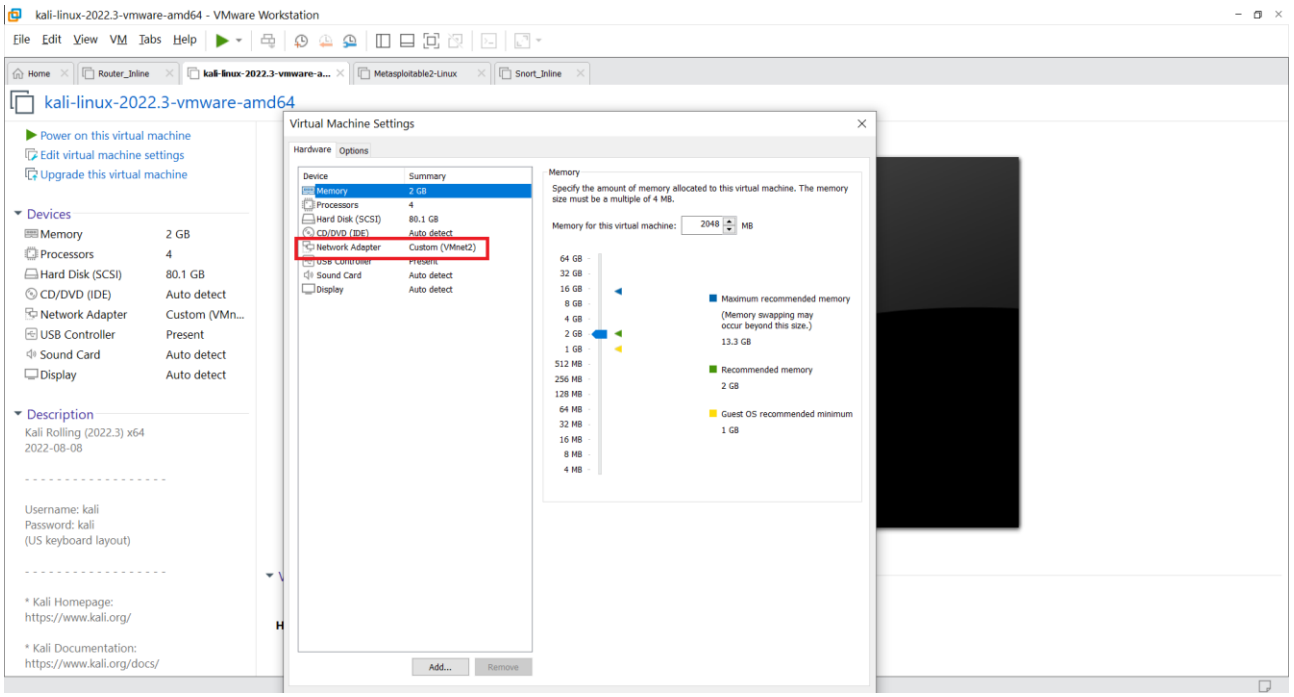
Hình 1: Tạo thêm các card mạng VMnet2/3/4

- Gán các card mạng cho máy **Router**:



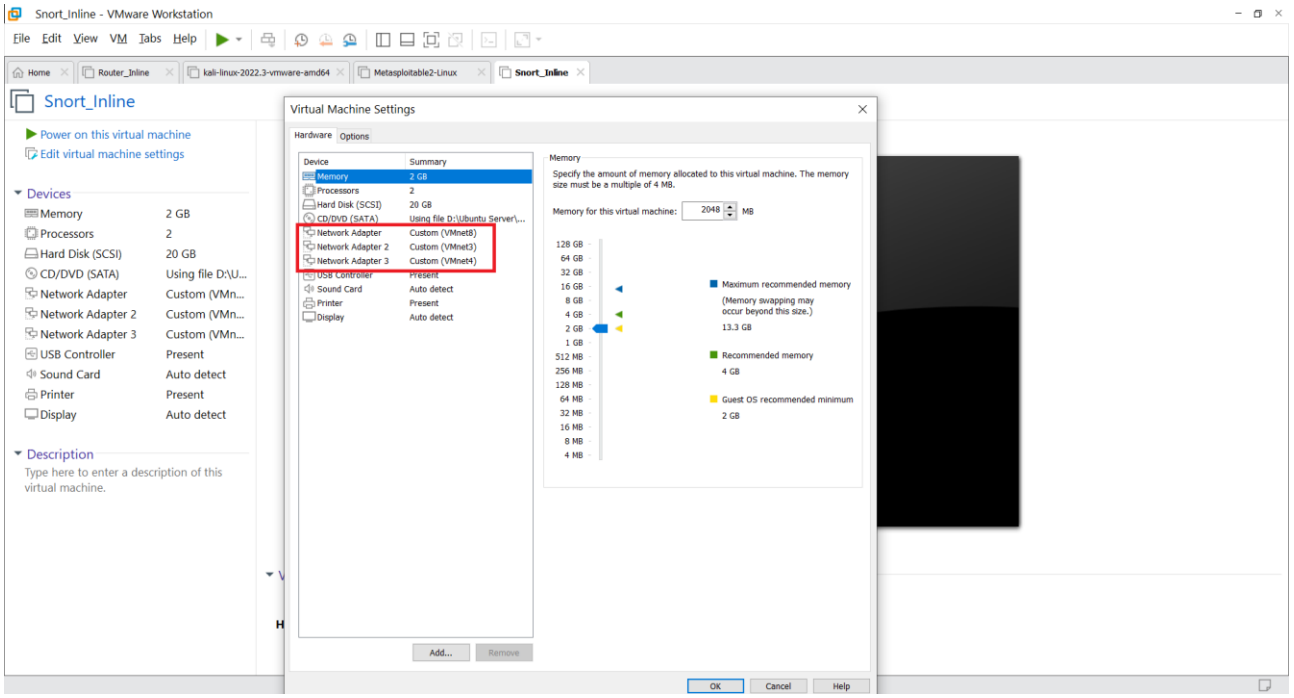
Hình 2: Gán card mạng cho Router

- Gán card mạng cho máy **Kali:**



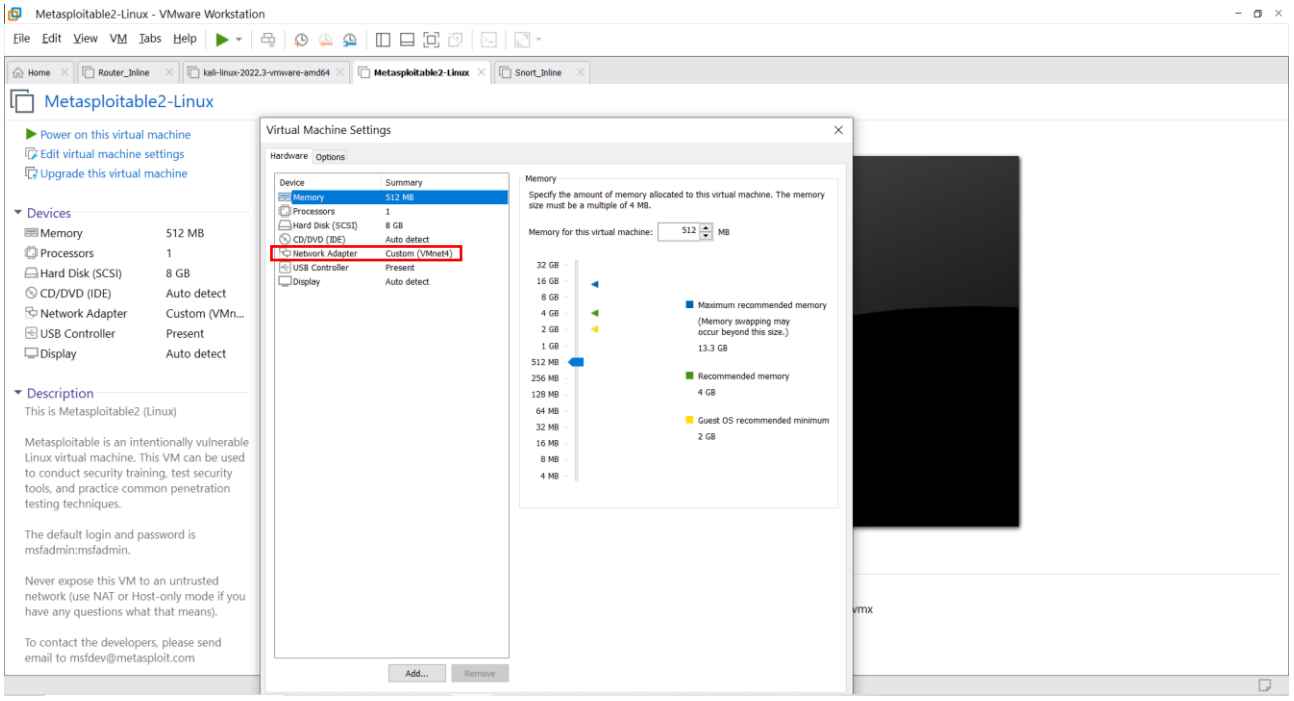
Hình 3: Gán card mạng cho Kali

- Gán card mạng cho máy **Snort:**



Hình 4: Gán card mạng cho Snort

- Gán card mạng cho máy **Victim:**



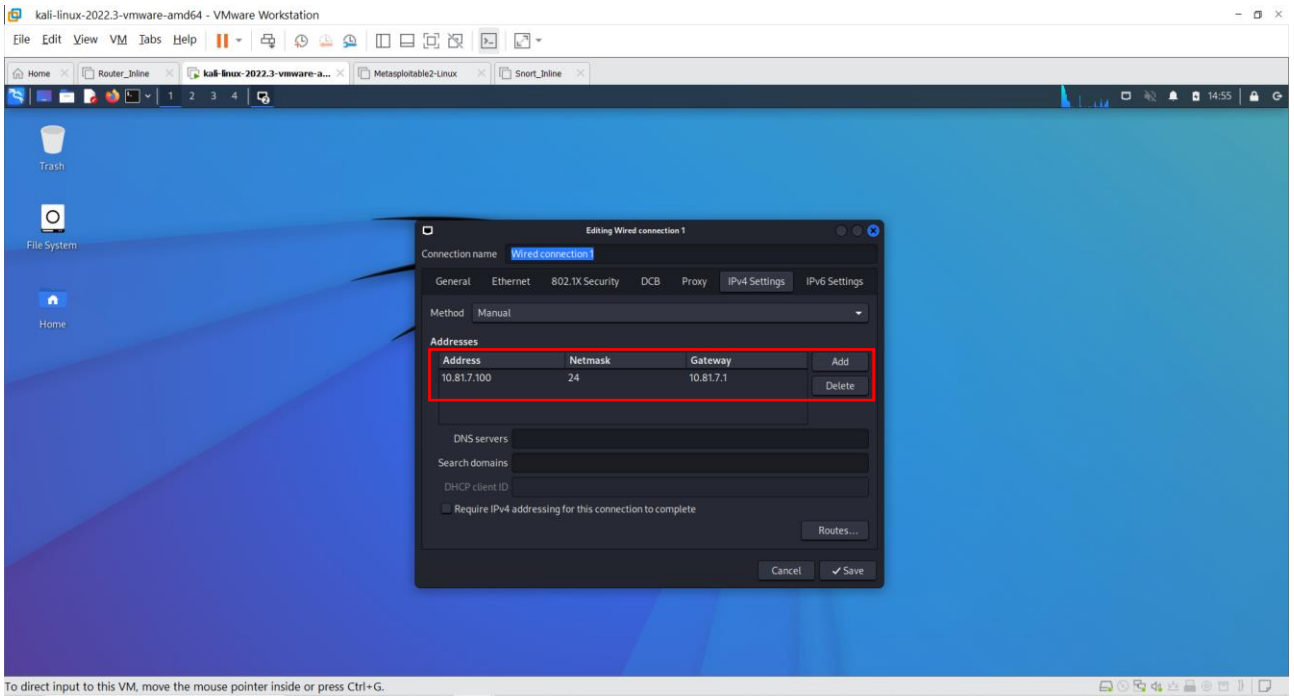
Hình 5: Gán card mạng cho Victim

Bước 2: Cấu hình ip cho các máy

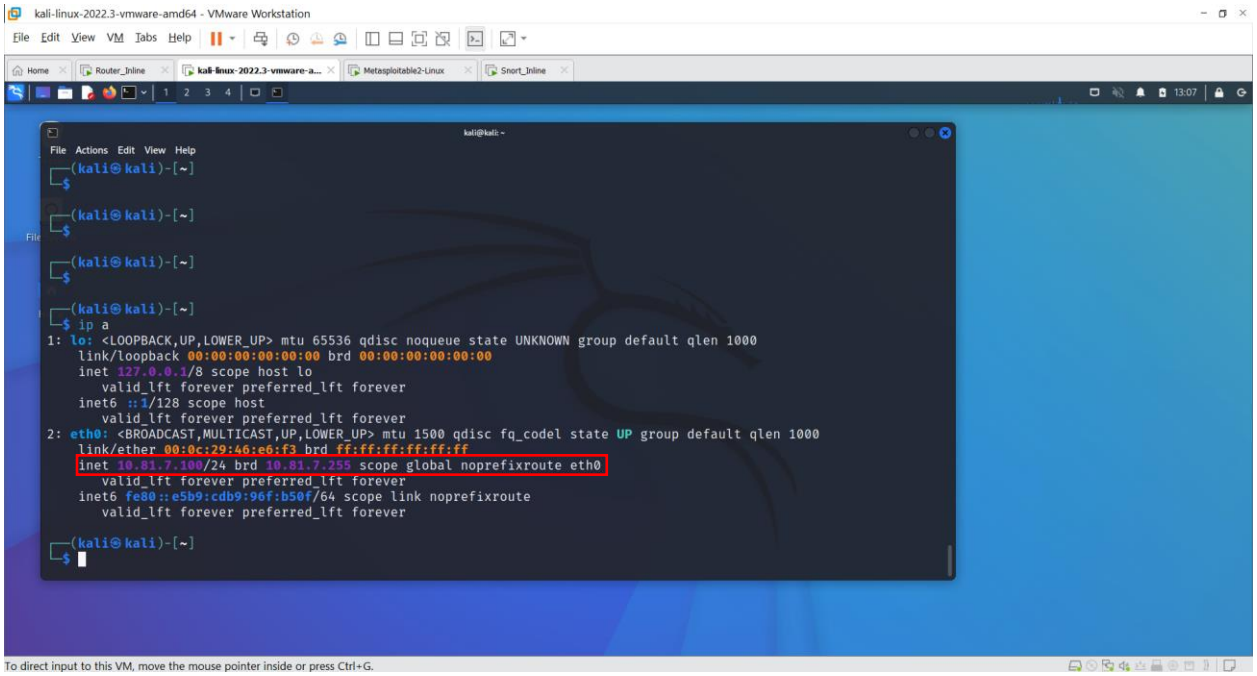
Attacker	10.81.7.100
Router	192.168.110.128 (ens33)

	10.81.7.1 (VMnet2 – ens37)
	192.168.7.1 (VMnet3 – ens38)
Snort	VMnet3 – ens38
	VMnet4 – ens37
Victim	192.168.7.200 (VMnet4 – eth0)

- Máy Attacker (Kali linux):

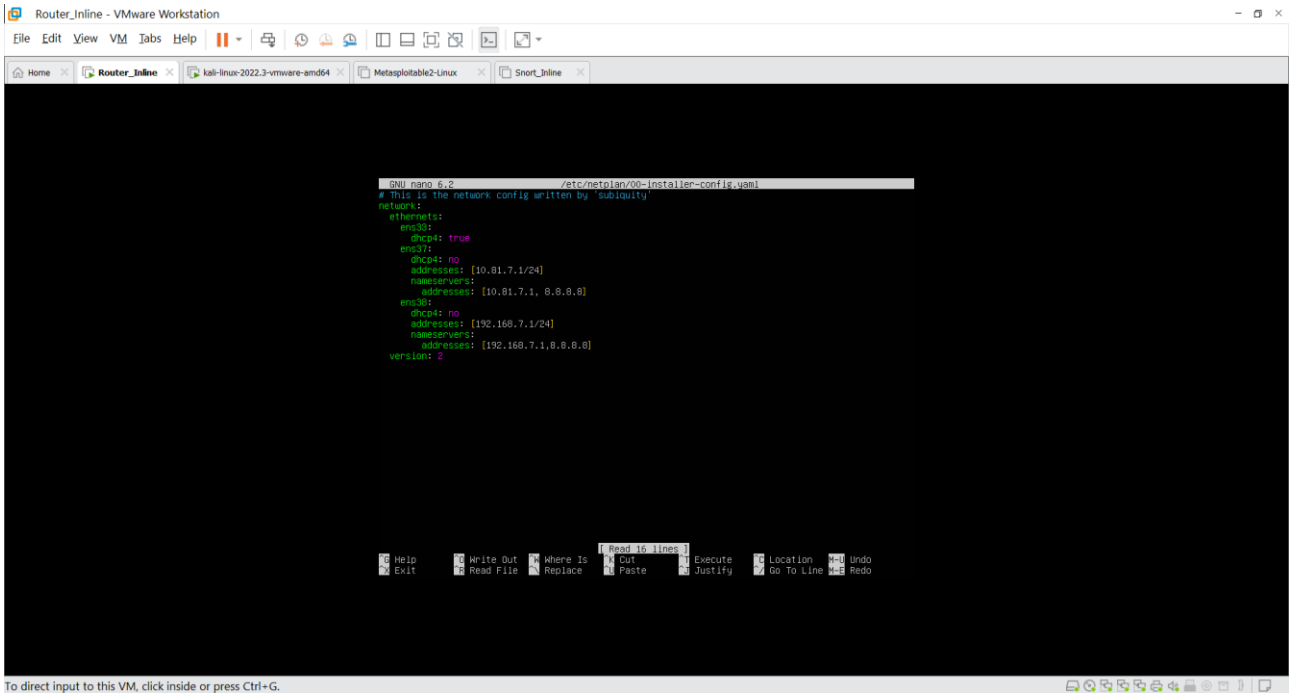


Hình 6: Thiết lập IP cho máy Attacker

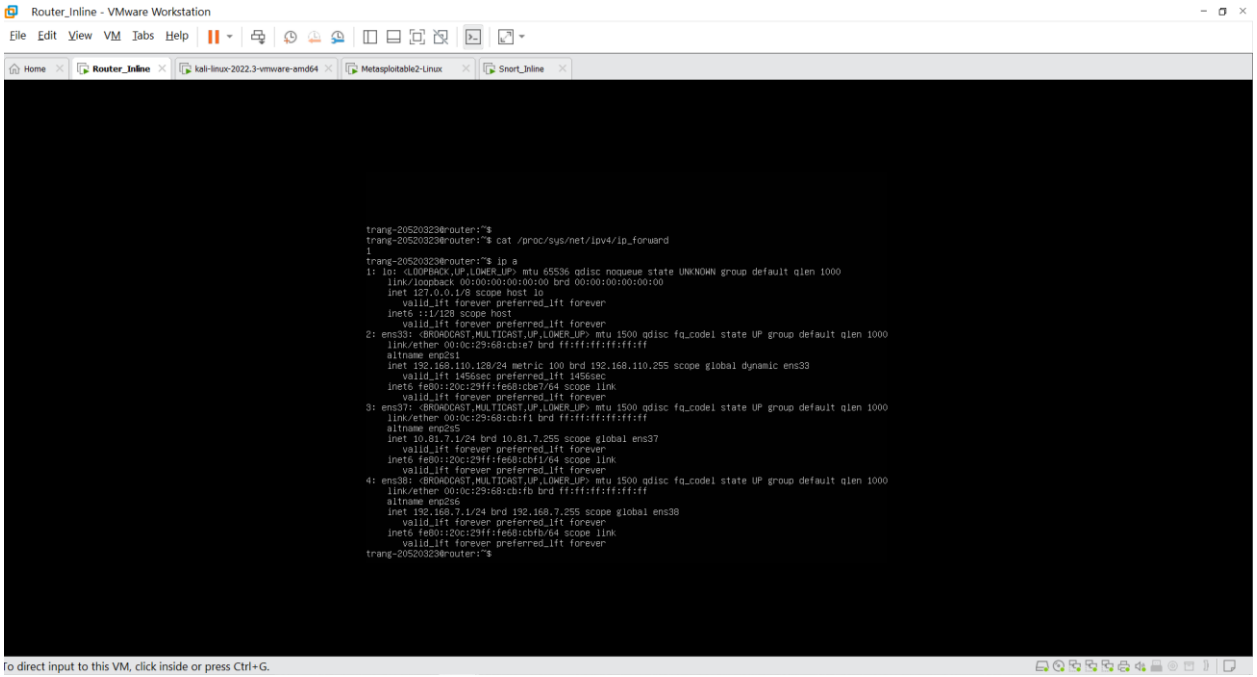


Hình 7: Máy Kali được thêm card mạng VMnet2

- Máy Router (Ubuntu Desktop):

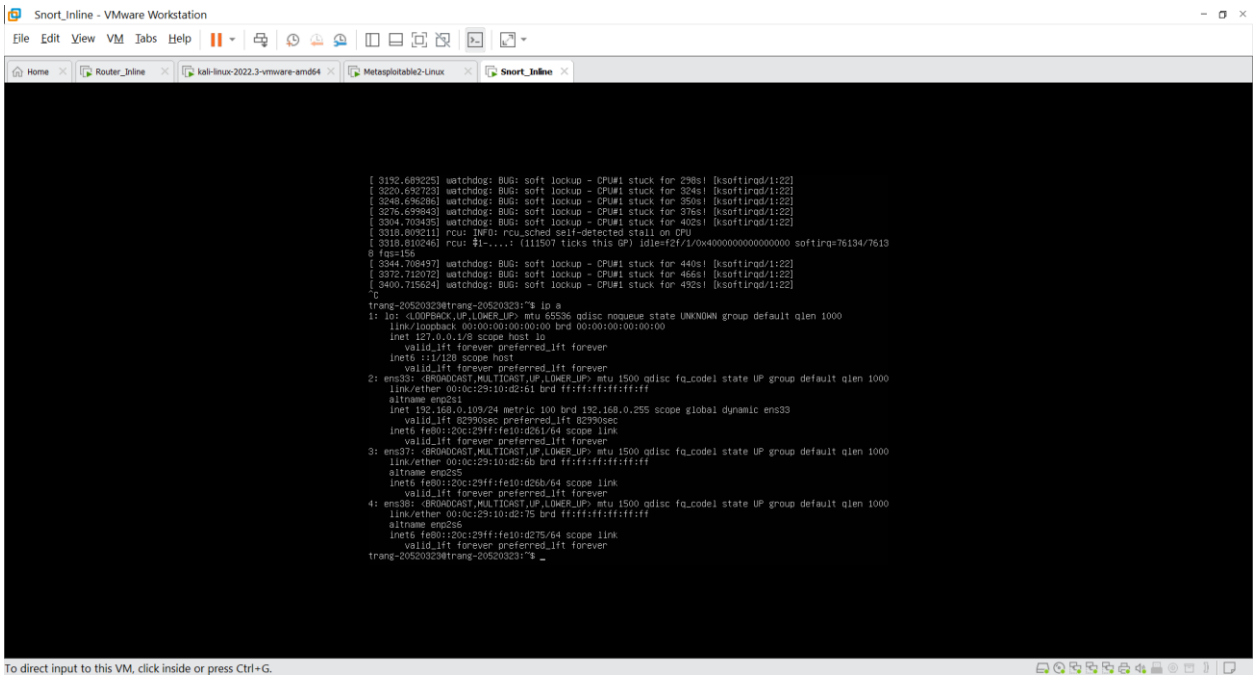


Hình 8: Thiết lập IP cho các interfaces của Router



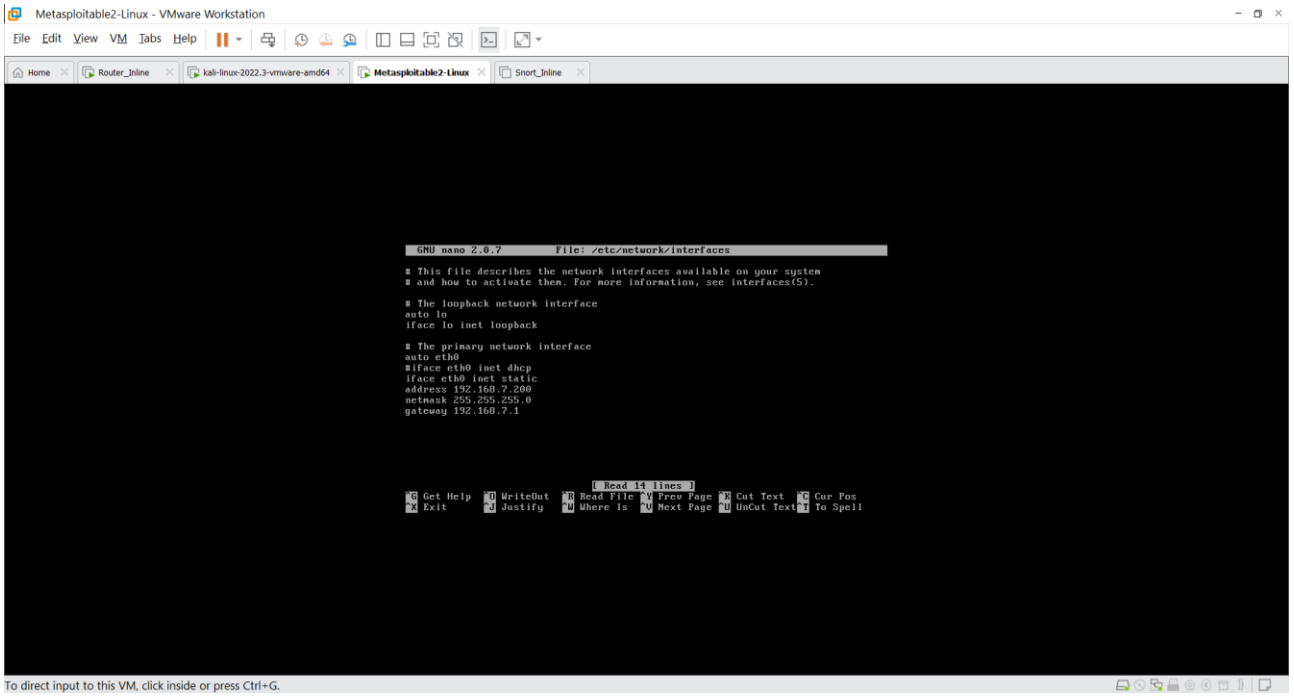
Hình 9: Ip máy Router

- Máy Snort:

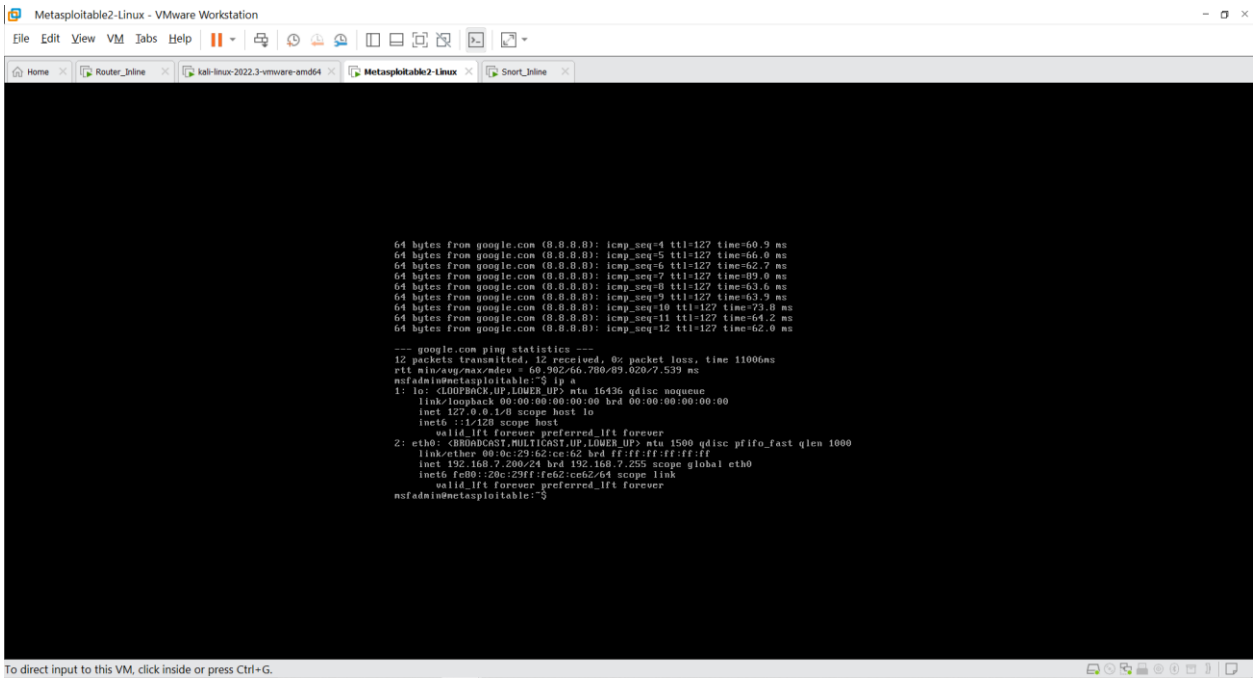


Hình 10: Cấu hình mạng cho máy Snort

- Máy victim (Metasploitable):



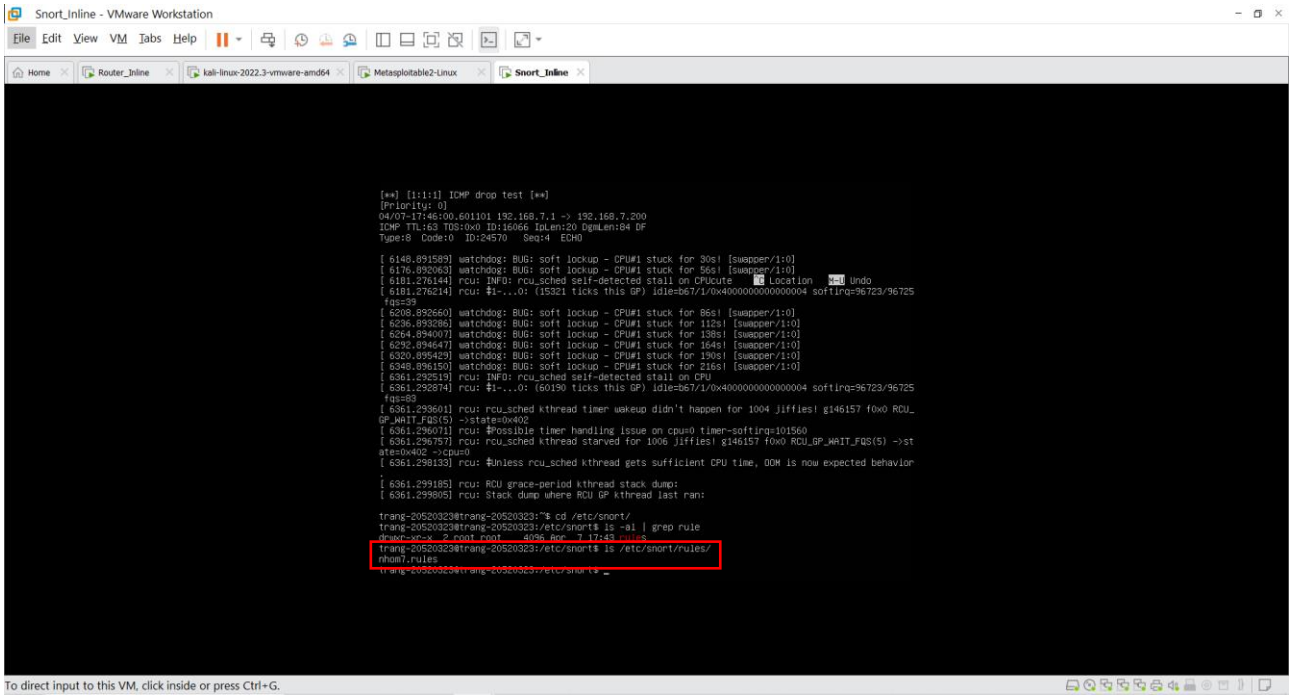
Hình 11: Thiết lập IP cho máy Victim



Hình 12: Thông tin cấu hình mạng của máy Victim

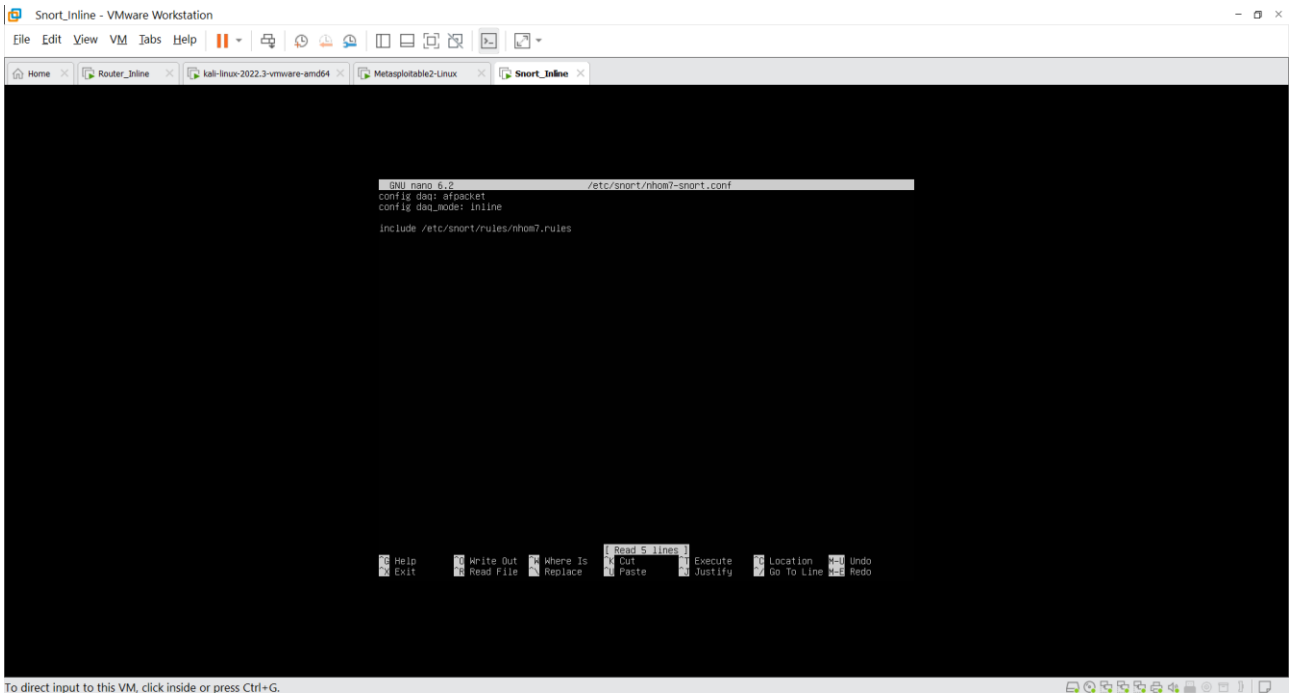
Bước 3: Cấu hình snort cho máy Snort:

Tạo file nhom7.rules và nhom7-snort.conf theo như yêu cầu:



Hình 13: Tạo các file theo yêu cầu

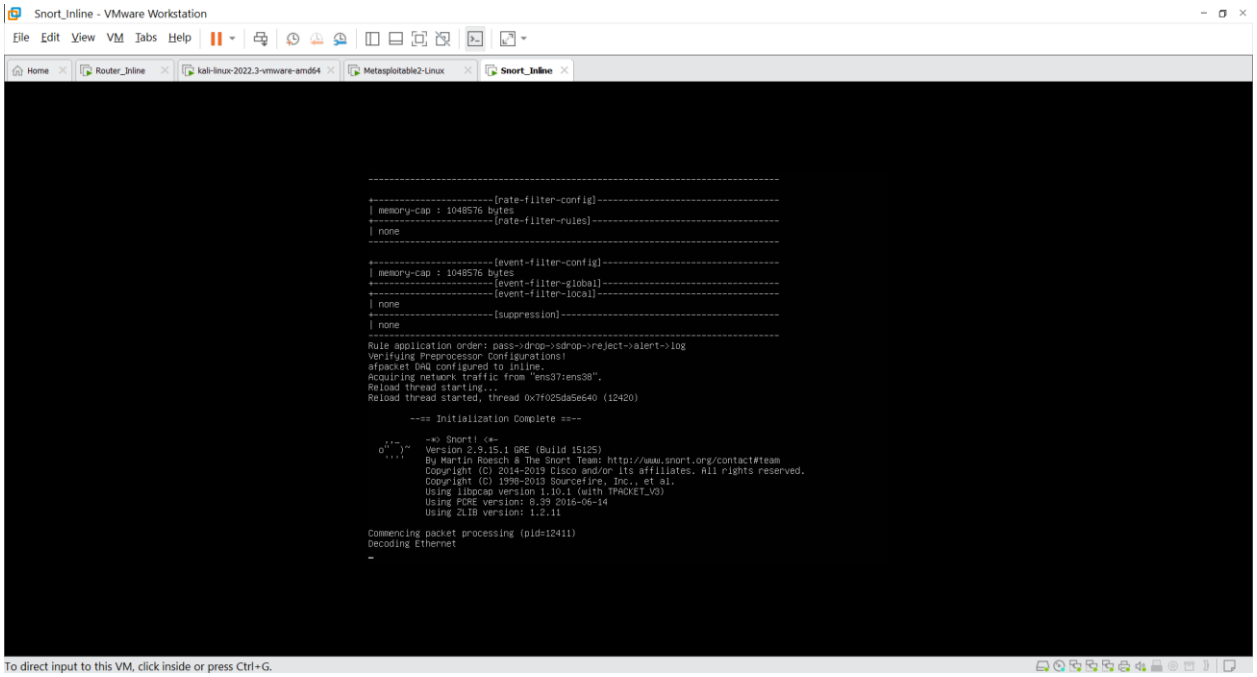
Thực hiện chỉnh sửa nội dung file nhom7-snort.conf:



Hình 14: Thêm nội dung vào file .conf

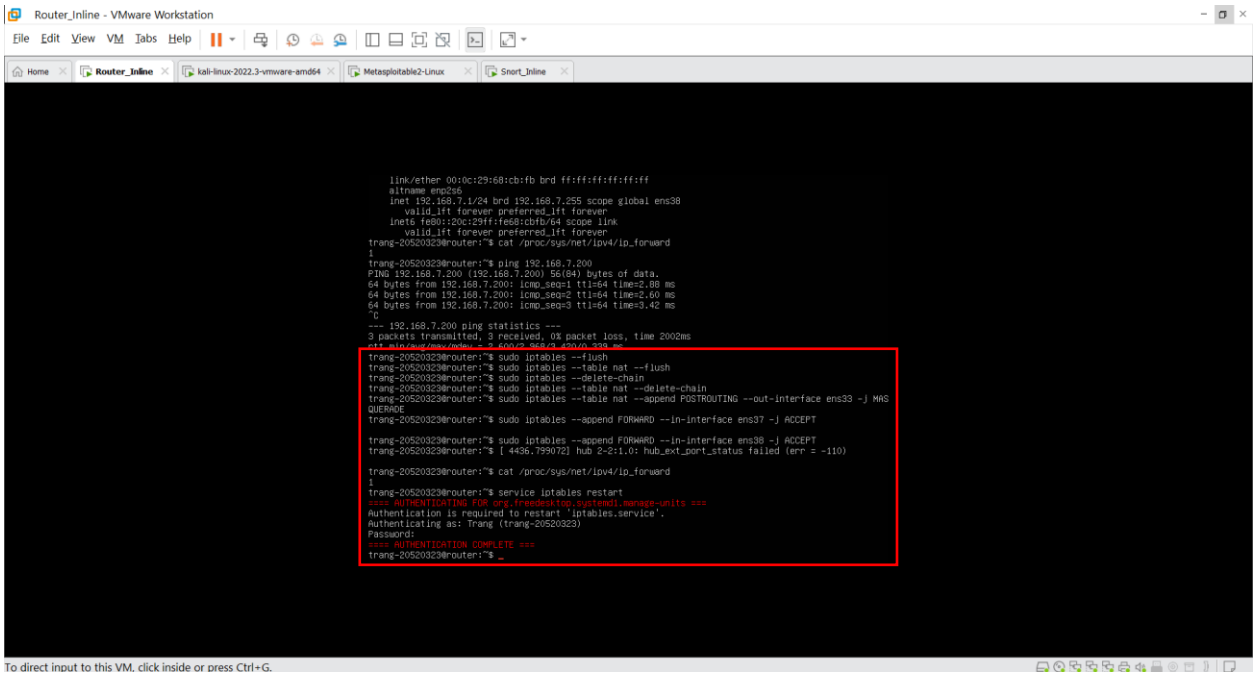
Cuối cùng chạy Snort trong inline mode bằng lệnh:

```
sudo snort -c /etc/snort/nhom7-snort.conf -Q -i ens38:ens37
```



Hình 15: Kết quả hạy snort

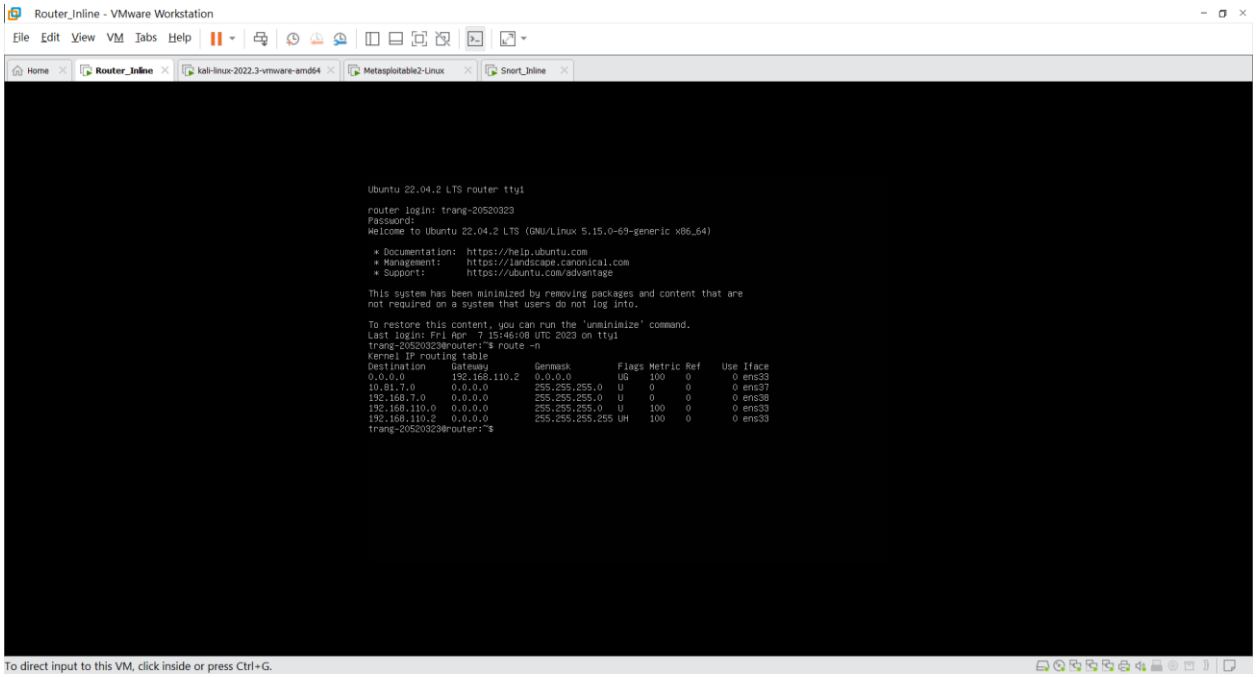
Bước 4: Cấu hình NAT outbound trên máy Router:



Hình 16: Cấu hình iptables trên máy Router

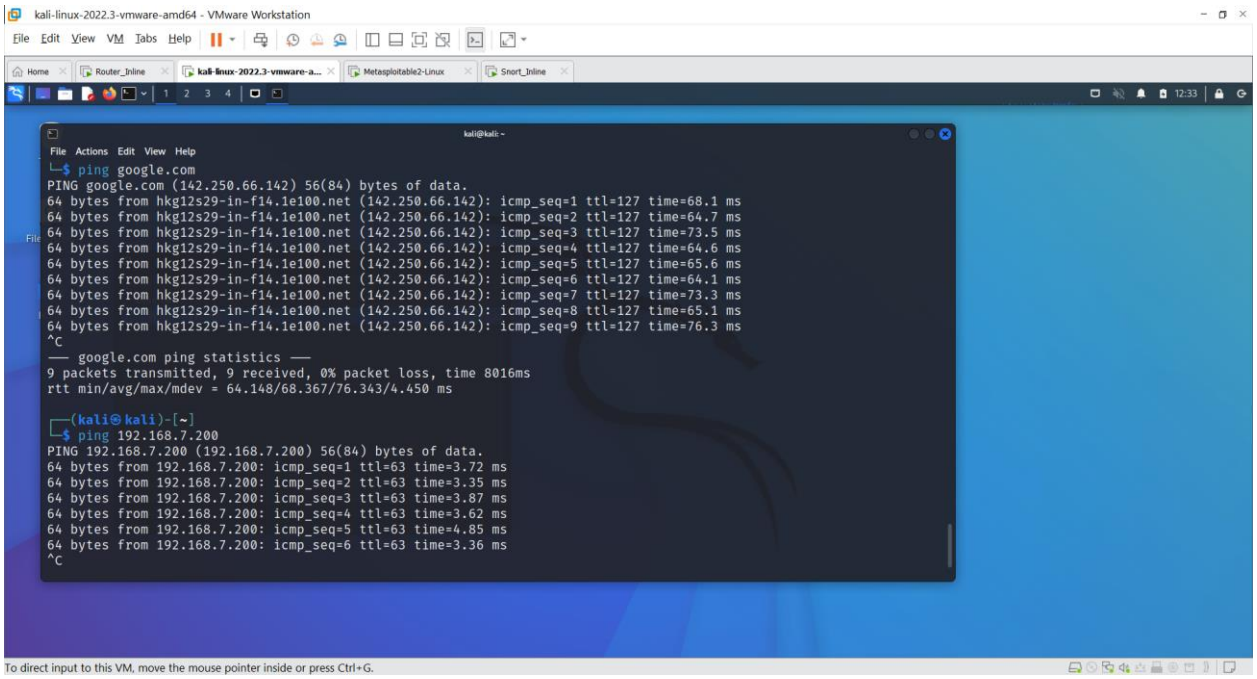
Câu lệnh	Ý nghĩa
iptables --flush	Xóa tất cả các rule trong bộ lọc và bảng nat

iptables --table nat --flush	Xóa tất cả các rule trong bảng NAT của iptables
iptables --delete-chain	Xóa một chain (chuỗi) cụ thể trong bảng mặc định của iptables.
iptables --table nat --delete-chain	Xóa tất cả các chuỗi không có trong bảng nat và bộ lọc mặc định.
iptables --table nat --append POSTROUTING --out-interface ens33 -j MASQUERADE	"--table nat": xác định bảng NAT của iptables sẽ được sử dụng để thực hiện chức năng chuyển đổi địa chỉ IP hoặc cổng cho các gói tin đi qua NAT. "--append POSTROUTING": thêm một rule vào chain POSTROUTING trong bảng NAT của iptables. "--out-interface ens33": chỉ định giao diện mạng ens33 là giao diện đầu ra của gói tin sẽ được thực hiện chuyển đổi địa chỉ IP. "-j MASQUERADE": sử dụng target MASQUERADE để thực hiện chuyển đổi địa chỉ IP của các gói tin đi qua NAT.
iptables --append FORWARD --in-interface ens37/ens38 -j ACCEPT	"--append FORWARD": thêm một rule vào chain FORWARD trong bảng filter của iptables. "--in-interface ens37/ens38": chỉ định giao diện mạng ens37/ens38 là giao diện đầu vào của các gói tin sẽ được cho phép đi qua. "-j ACCEPT": sử dụng target ACCEPT để cho phép các gói tin đi qua tường lửa.
echo 1 > /proc/sys/net/ipv4/ip_forward	Cho phép chuyển tiếp gói bằng kernel
service iptables restart	Áp dụng cấu hình



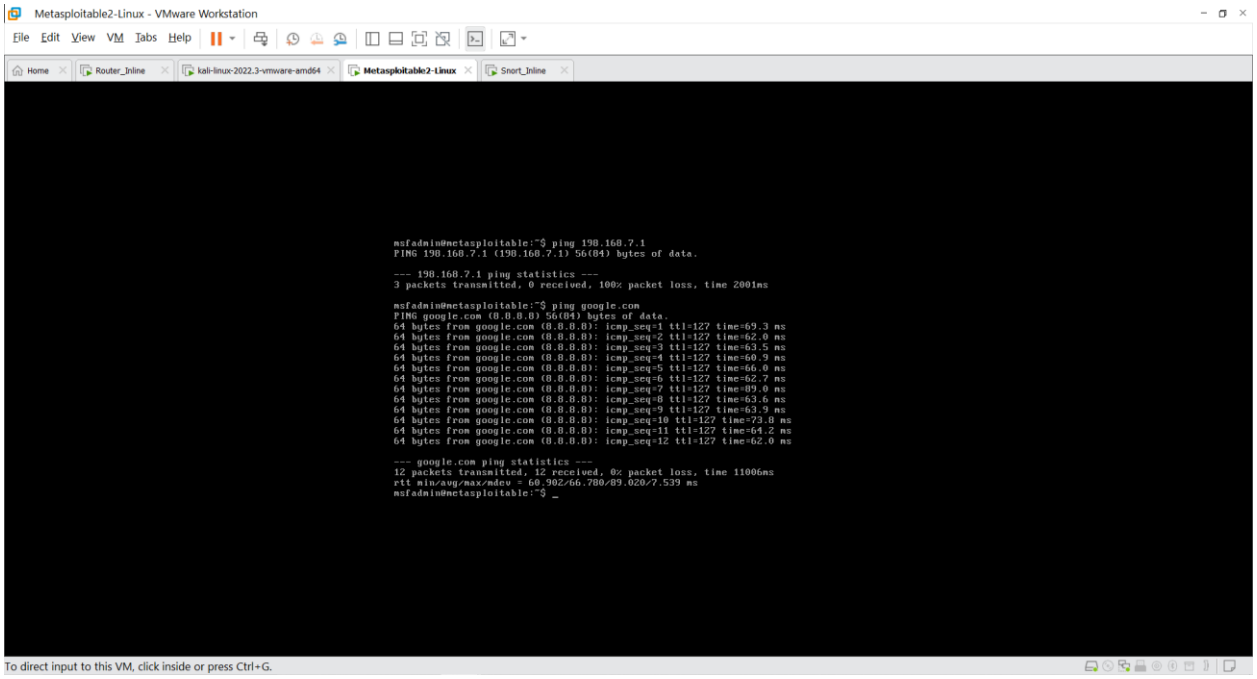
Hình 17: Thông tin bảng định tuyến

Kết quả trên máy Attacker:



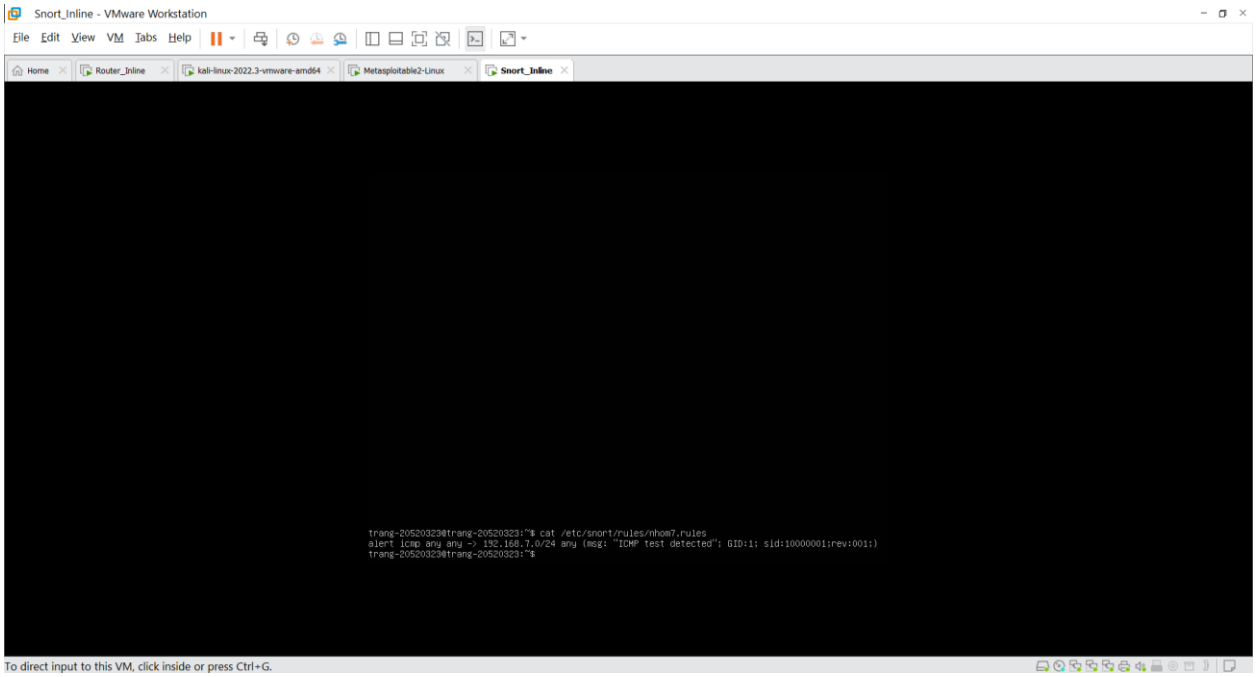
Hình 18: Ping tới google và máy Victim

Kết quả trên máy Victim khi thực hiện ping tới google.com (8.8.8.8):



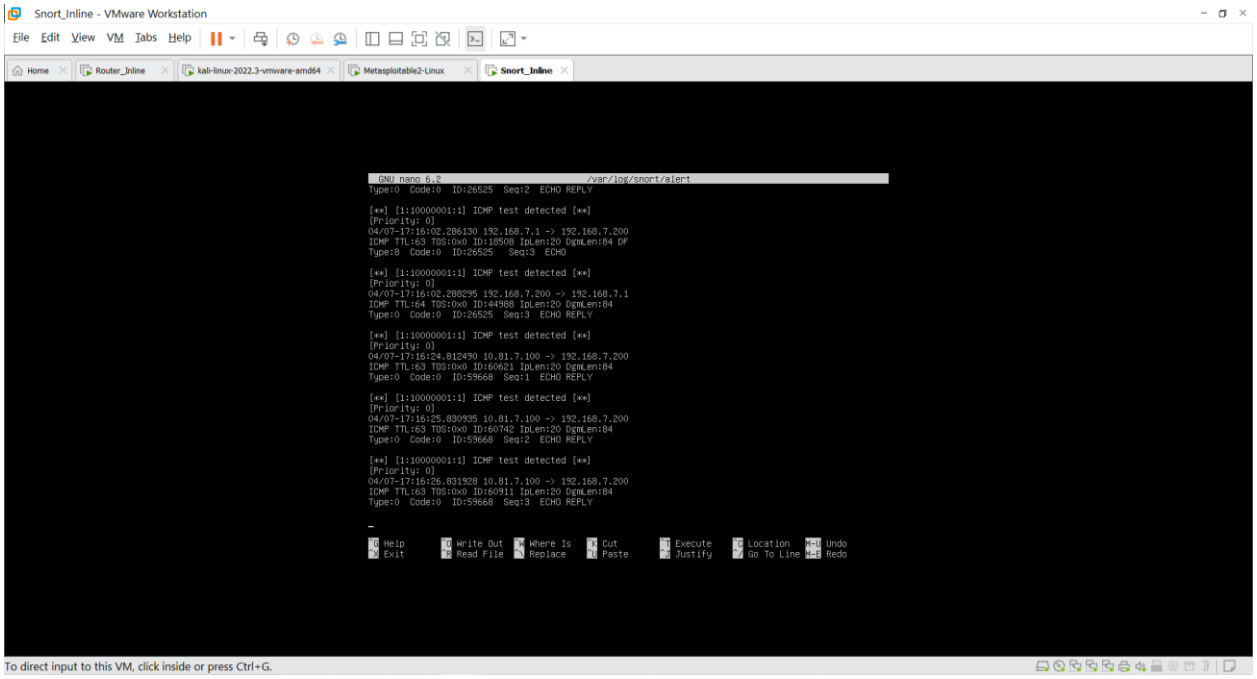
Hình 19: Ping tới google.com

Bước 5: Viết rule phát hiện gói ICMP gửi đến lớp mạng 192.168.7.0/24



Hình 20: Rule phát hiện gói IMCP

Kiểm tra log của snort trên **/var/log/snort/alert**.



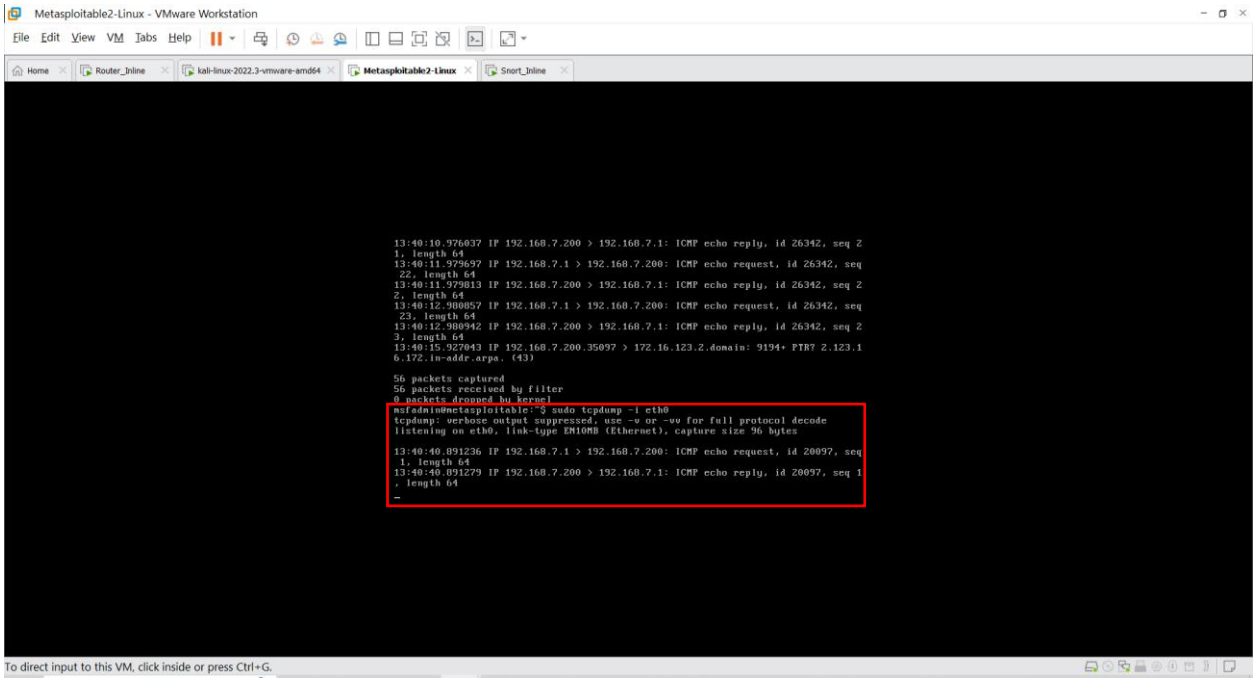
Hình 21: Log phát hiện gói IMCP

3. Viết rule cho Snort

Yêu cầu 3: viết rule drop các gói ICMP đi đến máy Victim:

Trước khi áp dụng rule#1:

- Trên máy Victim thực thi lệnh **tcpdump -i eth0**, sau đó thực hiện ping từ máy kali tới máy victim (10.81.7.100 → 192.168.7.200)



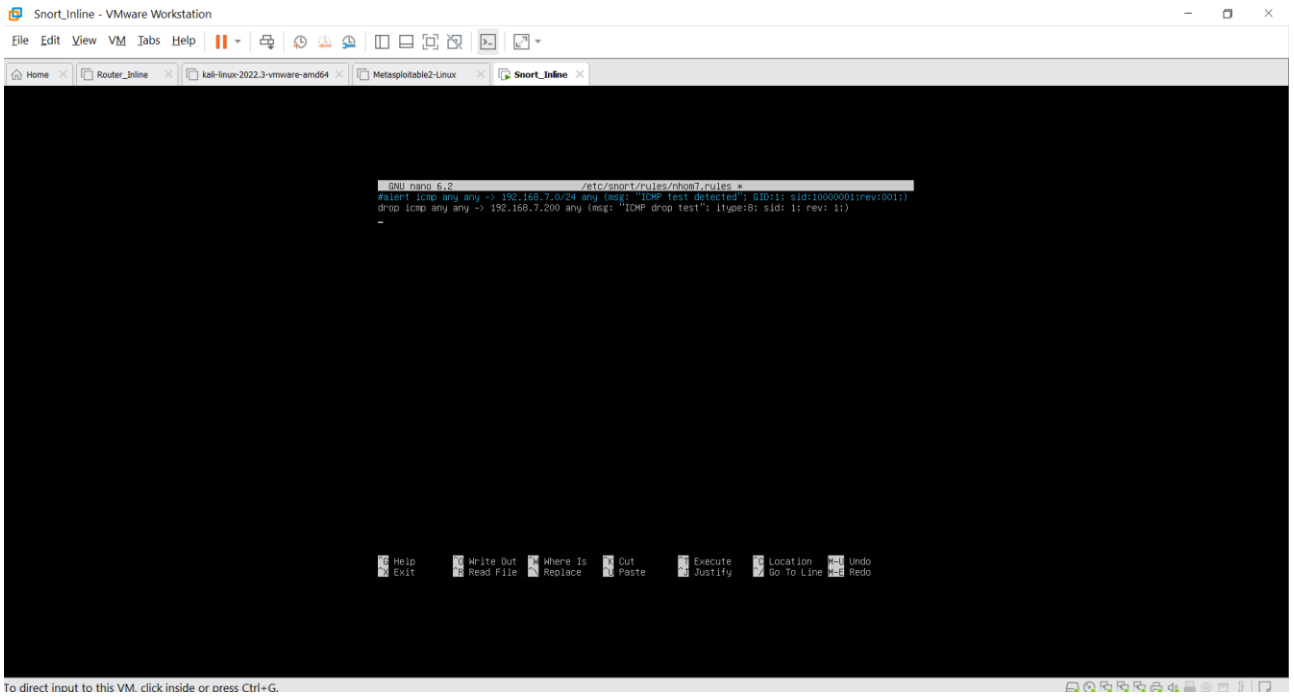
Hình 22: Các gói tin ICMP đến máy victim như bình thường

Thêm rule#1 trên vào file nhom7.rules:

```
drop ICMP any any -> 192.168.7.200 any (msg: "ICMP drop test"; itype: 8; sid: 1; rev: 1;)
```

Trong đó:

- **drop ICMP any any**: chặn tất cả các gói tin ICMP từ bất kỳ nguồn nào.
- **-> 192.168.7.200 any**: đến địa chỉ IP 192.168.7.200 trên bất kỳ cổng nào.
- **msg: "ICMP drop test":** hiển thị thông báo là "ICMP drop test"
- **itype: 8** để chỉ ra loại gói tin ICMP là Echo Request (ping).
- **sid: 1** để định danh cho rule.
- **rev: 1** để chỉ ra phiên bản của rule.



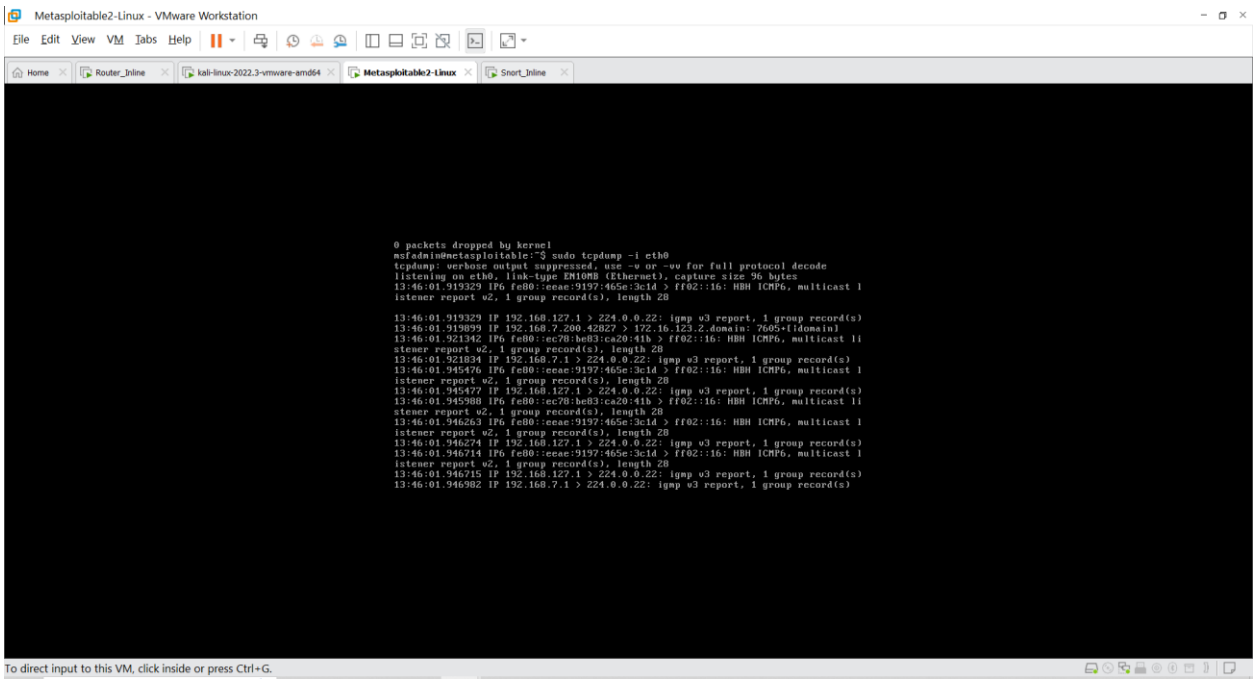
Hình 23: Thêm rule#1 vào file rules

Sau đó khởi chạy lại Snort:

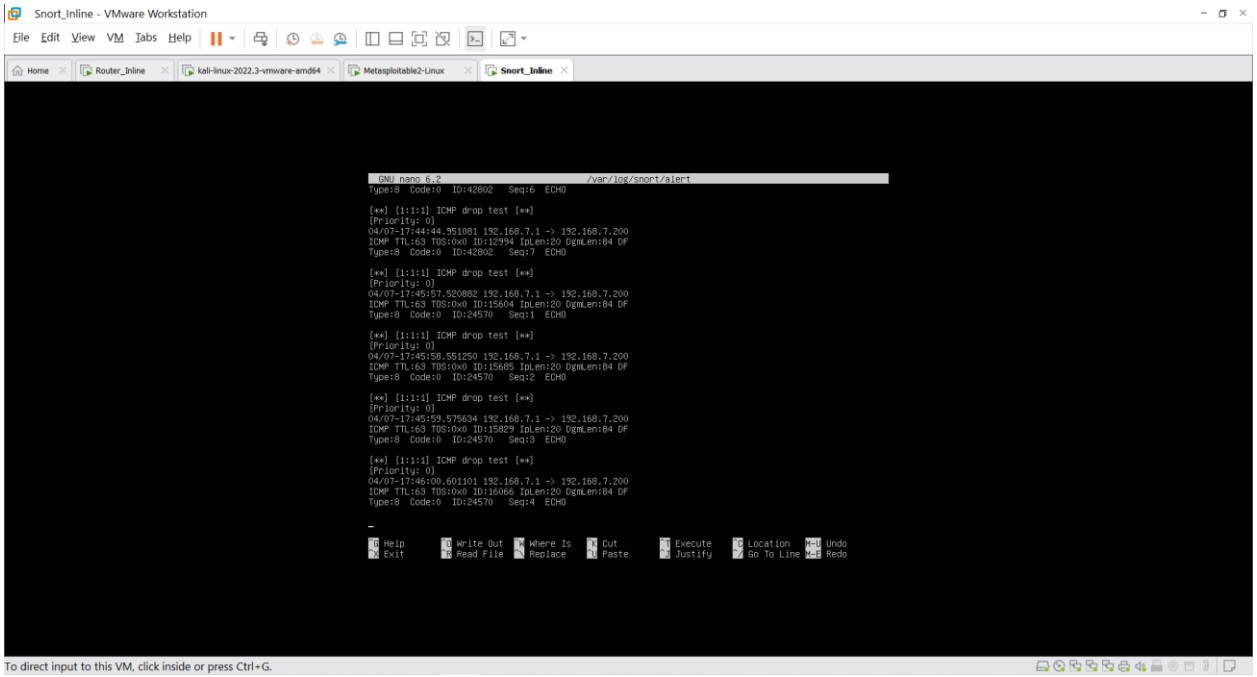
```
sudo snort -c /etc/snort/nhom7-snort.conf -Q -i ens38:ens37
```

Kết quả sau khi thêm rule#1:

- Trên máy Victim:



Hình 24: Gói tin ICMP sẽ bị drop và không thể đến được máy Victim



Hình 25: Log thông báo gói ICMP bị drop

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT