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

* Snort là một công cụ mã nguồn mở giám sát mạng và phát hiện xâm nhập. Nó được sử dụng để phát hiện các cuộc tấn công mạng bằng cách phân tích các gói tin được gửi và nhận trên một mạng. Snort có thể phát hiện các cuộc tấn công thông qua phân tích cú pháp, phân tích nội dung, phân tích hành vi và các kỹ thuật khác.
* Snort có thể chạy trên các chế độ sau:
  + **Sniffer mode**: Chế độ này cho phép Snort lắng nghe các gói tin trên một mạng và hiển thị chúng trên màn hình console. Chế độ này hữu ích để xem lưu lượng mạng đang truyền qua.
  + **Packet logger mode**: Chế độ này cho phép Snort lưu trữ các gói tin được nhận và gửi trên mạng vào một tập tin log. Chế độ này thường được sử dụng để thu thập thông tin cho mục đích phân tích.
  + **Intrusion Detection mode**: Chế độ này là chế độ chính của Snort và cho phép phát hiện các cuộc tấn công mạng. Khi Snort phát hiện một cuộc tấn công, nó có thể cảnh báo người quản trị mạng bằng cách gửi thông báo đến một hệ thống cảnh báo hoặc ghi lại các gói tin liên quan vào một tập tin log.
  + **Inline mode (prevention mode)**: Chế độ này cho phép Snort hoạt động như một thiết bị trung gian trên một mạng và có thể thực hiện các hành động như chặn các cuộc tấn công hoặc chuyển tiếp các gói tin đến một thiết bị khác. Tùy thuộc vào nhu cầu sử dụng, người dùng có thể chọn chế độ phù hợp để sử dụng Snort.

**1.1b. Trình bày những tính năng chính củà Snort?**

- Snort là một công cụ mã nguồn mở được sử dụng để giám sát mạng và phát hiện xâm nhập. Công cụ này có nhiều tính năng hữu ích để giúp người quản trị mạng phát hiện và ngăn chặn các cuộc tấn công mạng. Sau đây là một số tính năng chính của Snort:

1.**Giám sát liên tục**: Snort giám sát mạng liên tục và phát hiện các cuộc tấn công mạng ngay khi chúng xảy ra. Công cụ này có thể giúp người quản trị mạng phát hiện các mối đe dọa một cách nhanh chóng và hiệu quả.

2.**Phát hiện các cuộc tấn công bằng nhiều phương pháp**: Snort sử dụng nhiều kỹ thuật phân tích để phát hiện các cuộc tấn công mạng. Các phương pháp này bao gồm phân tích cú pháp, phân tích nội dung, phân tích hành vi, phân tích dựa trên chữ ký và các kỹ thuật khác.

3.**Hỗ trợ các cấu hình linh hoạt:** Snort có thể được cấu hình để phát hiện các cuộc tấn công cụ thể hoặc các mối đe dọa tiềm tàng khác trên mạng. Nó cũng có thể được cấu hình để phù hợp với mọi môi trường mạng.

4.**Cảnh báo ngay lập tức**: Khi phát hiện một cuộc tấn công, Snort có thể gửi một cảnh báo đến người quản trị mạng để cảnh báo về mối đe dọa.

5.**Hỗ trợ các tiêu chuẩn mở**: Snort hỗ trợ nhiều tiêu chuẩn mở như TCP/IP, HTTP, DNS và SMTP. Điều này giúp Snort tích hợp với các công nghệ khác trên mạng một cách dễ dàng.

6.**Hỗ trợ nhiều nền tảng**: Snort có thể chạy trên nhiều nền tảng khác nhau bao gồm Linux, Windows và MacOS. Tóm lại, Snort là một công cụ giám sát mạng và phát hiện xâm nhập mạnh mẽ và linh hoạt, có nhiều tính năng hữu ích để giúp người quản trị mạng phát hiện và ngăn chặn các cuộc tấn công mạng.

Gán card mạng cho máy Router.

A picture containing chart

Description automatically generated

Gán càrd mạng cho máy Kali

Graphical user interface, text, application

Description automatically generated

Gán càrd mạng cho máy Snort

Graphical user interface, application, Word

Description automatically generated

Gán càrd mạng cho máy Victim

Text

Description automatically generated

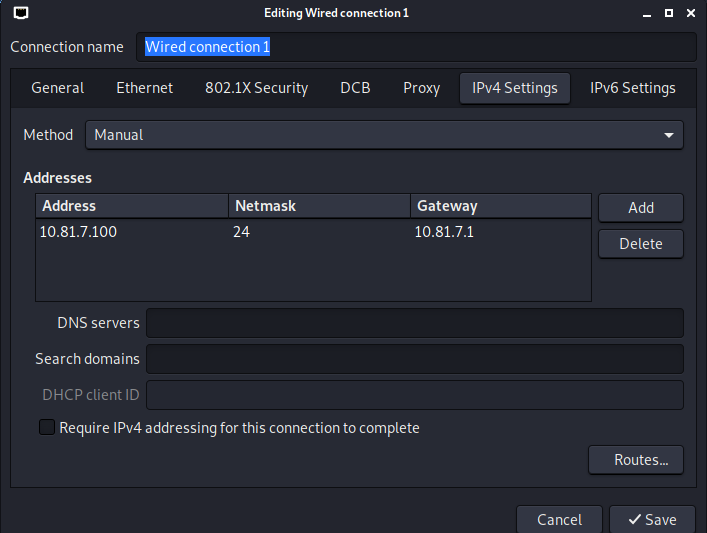
2.1b. Cấu hình địa chỉ ip cho các máy

Metasploitable2

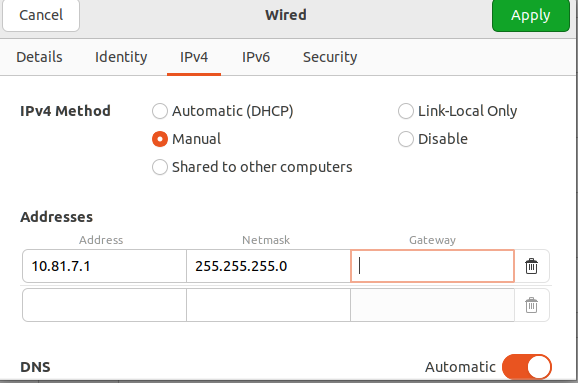
Text

Description automatically generated

KALI



Ubuntu



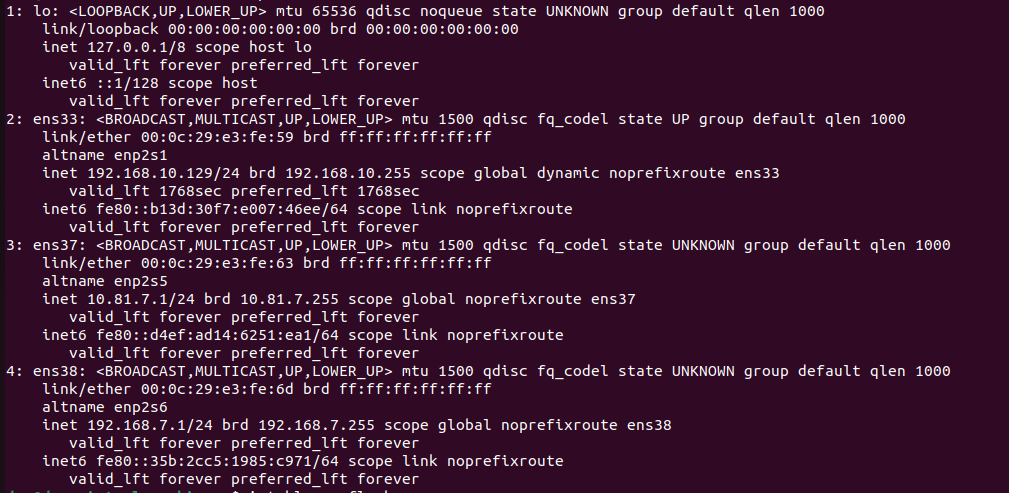
Graphical user interface, application

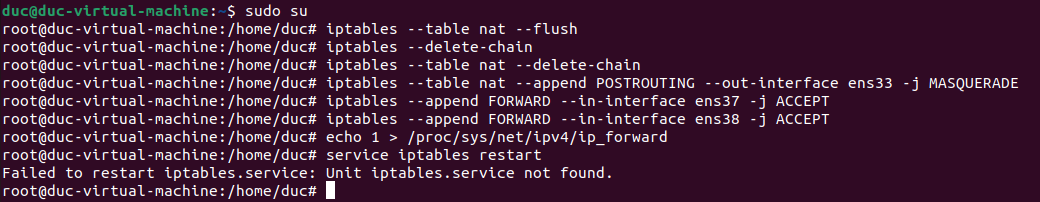
Description automatically generated

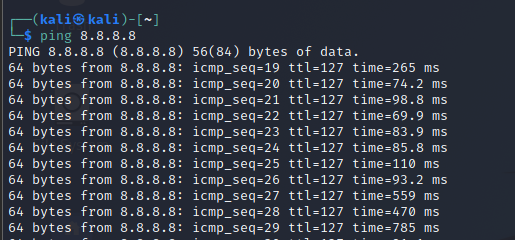
**2.1c. Cấu hình NAT outbound cho máy router**

A picture containing text

Description automatically generated

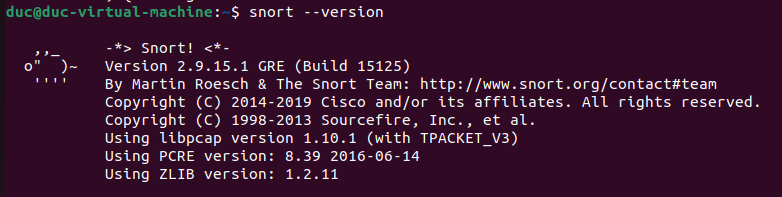






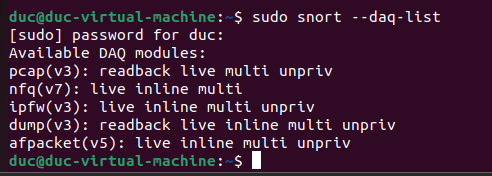
**2.1d. Cài đặt và cấu hình Snort**

**Sau khi cài đặt thành công, kiểm trà phiên bản Snort**



**- Kiểm tra packet DAQ đã phải đựợc cài đặt để sử dụng đựợc mode inline.**

Sudo snort –daq-list



**- Xóa tất cả các file rule mặc định củà Snort**

sudo rm -rf /etc/snort/rules/\*



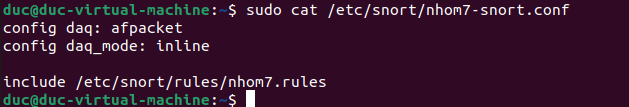
**- Tạo file rule củà nhóm định nghĩà. Ví dụ ở đây là nhóm 0**

/etc/snort/rules/nhom7.rules



**- Tạo file cấu hình snort củà nhóm tại /etc/snort/nhom7-snort.conf với nội dung như bên dưới để bật mode inline**

/etc/snort/nhom7-snort.conf



**- Kiểm tra file cấu hình snort bằng lệnh sau :**

**Sudo snort -T -c /etc/snort/nhom7-snort.conf -Q -i ens37:ens38**

Text

Description automatically generated

**- Chạy snort trong mode inline với dòng lệnh** :

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

Text

Description automatically generated

Graphical user interface, text

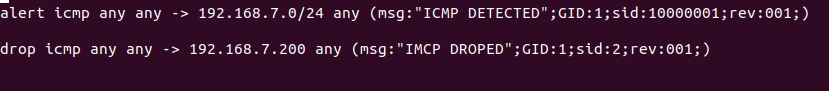
Description automatically generated

Trước khi viết rule

Text

Description automatically generated

Sau khi viết rule



Text

Description automatically generated

Text

Description automatically generated