BÁO CÁO THỰC HÀNH

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

**Lab 2: Triển khai Snort Inline**

*GVHD: Đỗ Hoàng Hiển*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT204.O21.ATCL.2- Nhóm 3

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Huỳnh Minh Tân Tiến | 21521520 | [21521520@gm.uit.edu.vn](mailto:21521520@gm.uit.edu.vn) |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | **Yêu cầu 1** | 100% |
| 2 | **Yêu cầu 2** | 100% |
| 3 | **Yêu cầu 3** | 100% |

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

BÁO CÁO CHI TIẾT

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

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

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

1.1a   
- Snort là một hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) và cũng có thể được cấu hình để hoạt động như một hệ thống phòng thủ xâm nhập (Intrusion Prevention System - IPS). Nó được sử dụng rộng rãi để phát hiện và ngăn chặn các cuộc tấn công mạng, bao gồm các loại tấn công từ từ chối dịch vụ (Denial of Service - DoS), tấn công mã độc (Malware), tấn công bằng buffer overflow, và nhiều hơn nữa.  
- Snort có thể hoạt động ở 3 chế độ:

+ Package sniffer: hiển thị thông tin header các gói tin

+ Package log: ghi lại các thông tin vào file log để xử lý sau này

+ IDS: phân tích các gói tin hoặc các luồng TCP, thực hiện các chức năng IDS theo cơ chế signature-based.

1.1b

Snort là một hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS) mã nguồn mở phổ biến được sử dụng rộng rãi để giám sát và bảo vệ các mạng máy tính. Dưới đây là một số tính năng chính của Snort:

* Phát hiện xâm nhập dựa trên chữ ký (Signature-based intrusion detection): Snort sử dụng cơ sở dữ liệu chữ ký để phát hiện các mẫu tấn công đã biết. Điều này bao gồm so sánh các luồng dữ liệu đến từ mạng với các quy tắc đã được định nghĩa trước.
* Phát hiện xâm nhập dựa trên quy tắc (Rule-based intrusion detection): Snort cho phép người quản trị xác định các quy tắc tùy chỉnh để phát hiện các hành vi không mong muốn hoặc đáng ngờ trong dữ liệu mạng.
* Phát hiện và chặn các loại tấn công phổ biến: Snort có thể phát hiện và ngăn chặn nhiều loại tấn công mạng, bao gồm những loại tấn công như port scanning, denial-of-service (DoS), buffer overflow, và SQL injection.
* Phân tích dữ liệu mạng đa dạng: Snort có thể phân tích nhiều loại dữ liệu mạng, bao gồm IPv4, IPv6, TCP, UDP, ICMP và các giao thức khác.
* Hỗ trợ logging và báo cáo: Snort có khả năng ghi lại các sự kiện phát hiện xâm nhập vào các tập tin log, cho phép người quản trị kiểm tra và phân tích sau này. Nó cũng có khả năng tạo các báo cáo tổng hợp về các mẫu tấn công và hành vi mạng.
* Hỗ trợ cho cộng đồng và cập nhật linh hoạt: Snort là một dự án mã nguồn mở, điều này có nghĩa là nó có sự hỗ trợ từ cộng đồng lớn các nhà phát triển và người dùng. Các quy tắc và cơ sở dữ liệu chữ ký có thể được cập nhật thường xuyên để phản ánh các mối đe dọa mới.
* Tính linh hoạt và mở rộng: Snort có thể được tùy chỉnh và mở rộng để phù hợp với nhu cầu cụ thể của môi trường mạng. Người dùng có thể thêm các plug-in và mở rộng tính năng của Snort thông qua các giao diện lập trình ứng dụng (API).
* Hỗ trợ nhiều môi trường: Snort có thể được triển khai trên nhiều nền tảng hệ điều hành, bao gồm Linux, Windows, và Unix, làm cho nó phù hợp với các môi trường mạng đa dạng.

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

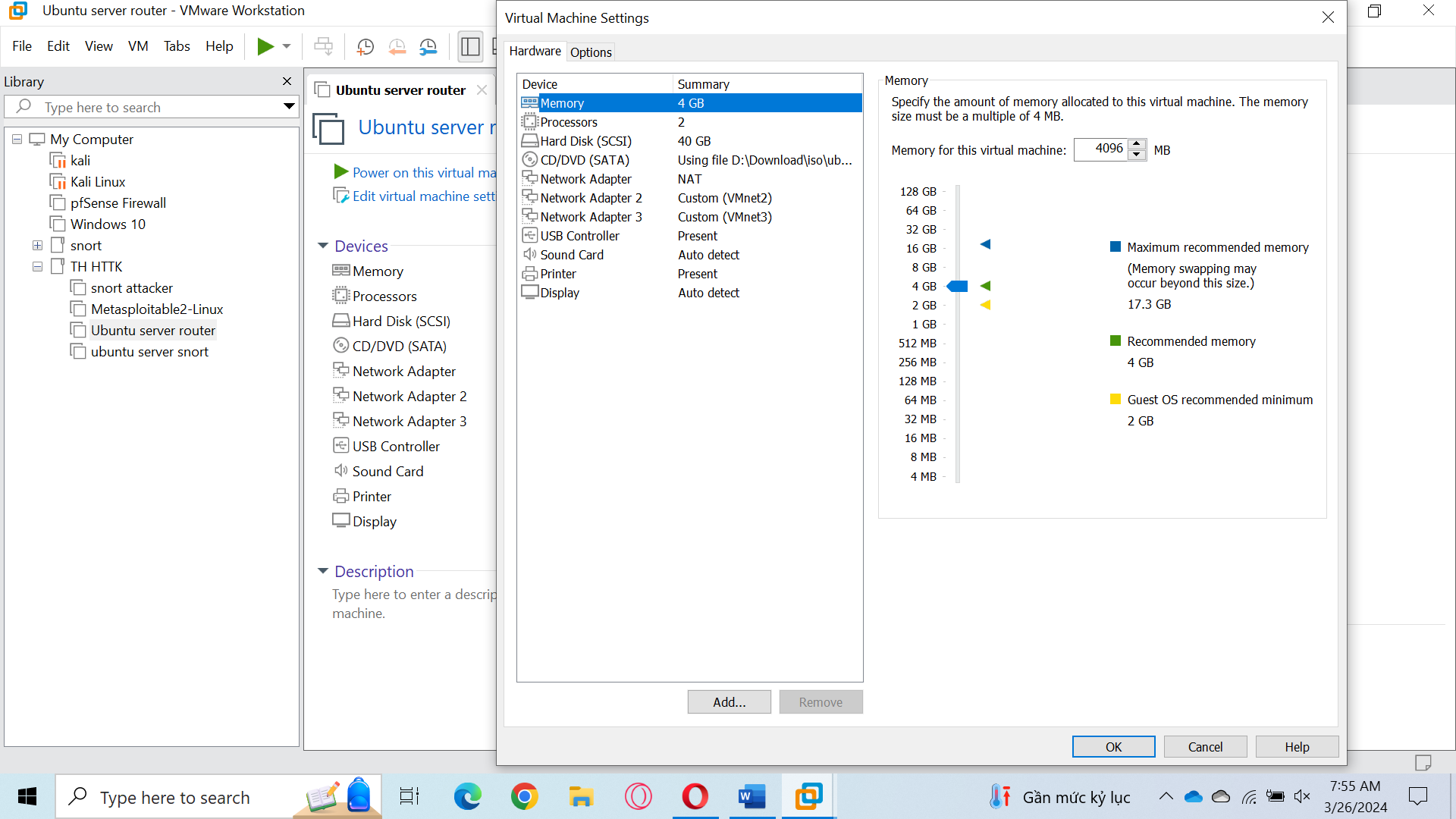
**Bước 1:** Cấu hình mạng cho các máy theo mô hình

- Kiểm tra card VMnet8 (NAT) đã tồn tại và được bật DHCP, và them những card mạng khác.

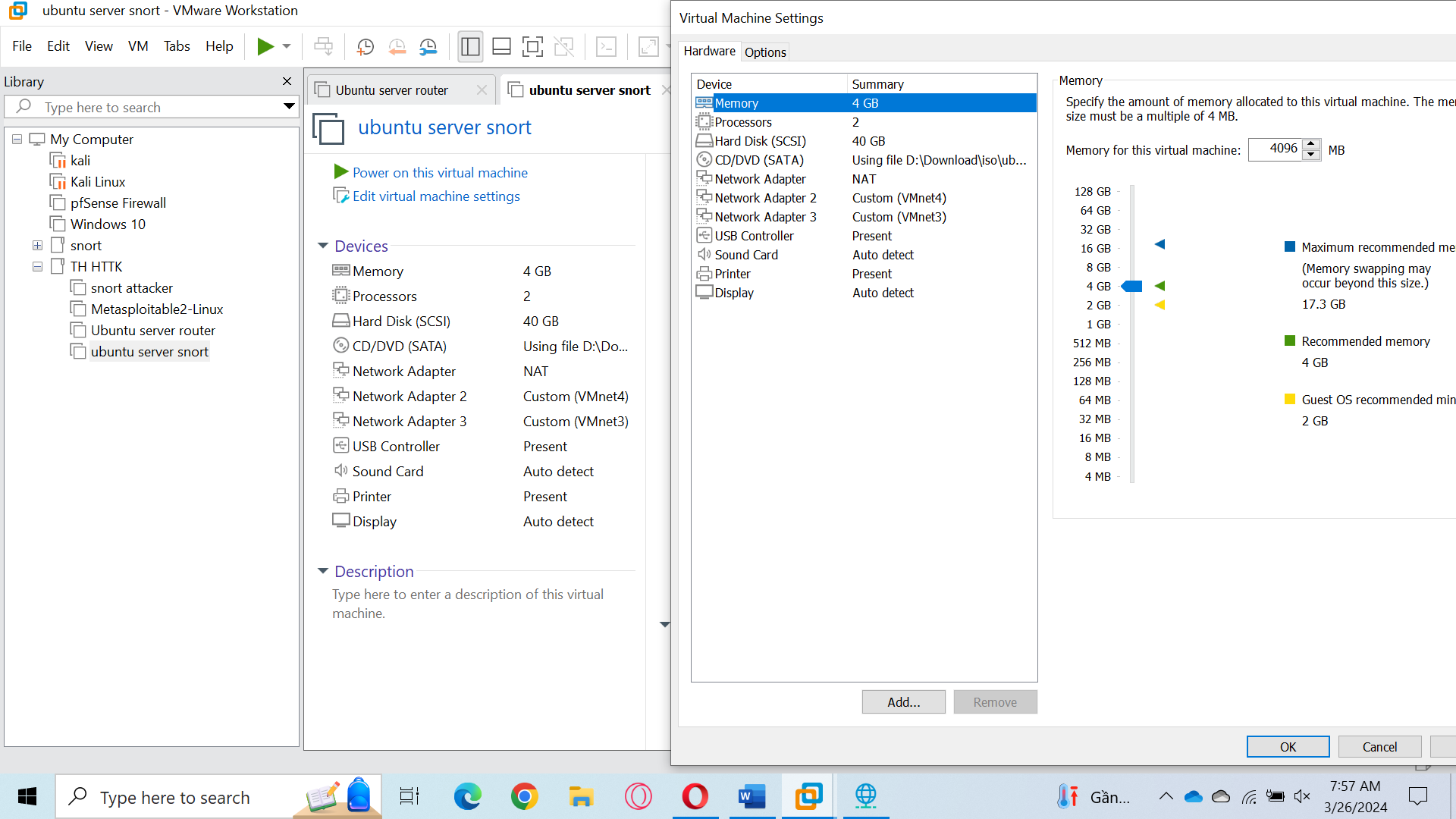
A screenshot of a computer

Description automatically generated

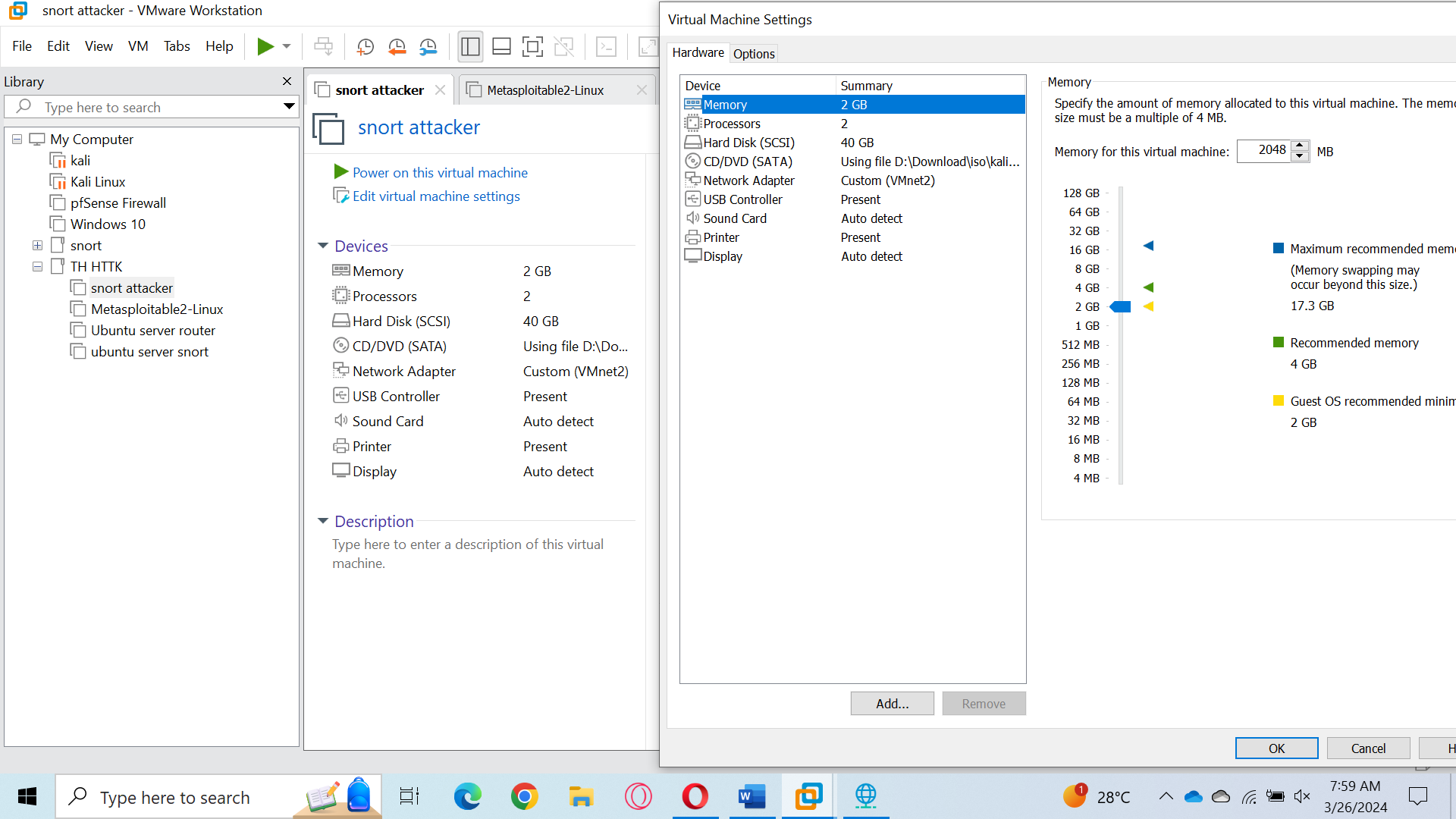
- Gán các card mạng cho máy Router.



- Gán card mạng cho máy Snort



- Gán card mạng cho máy Kali (Attacker)



- Gán card mạng cho máy Victim

A screenshot of a computer

Description automatically generated

**Bước 2:** Cấu hình địa chỉ ip cho các máy

|  |  |
| --- | --- |
| Attacker | 10.81.3.100 |
| Router | 192.168.30.129 (ens33) |
| 10.81.3.1 (VMnet2 - ens37) |
| 192.168.3.1 (VMnet3 - ens37) |
| Snort | VMnet4 – ens37 |
| VMnet3 – ens38 |
| Victim | 192.168.3.200 (VMnet4) |

- Đặt IP tĩnh cho máy Attacker

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Đặt IP tĩnh cho máy Victim

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Đặt IP cho các interfaces trên máy Router

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Cấu hình mạng cho Snort

A screenshot of a computer

Description automatically generated

**Bước 3:** Cấu hình NAT outbound cho máy router

A screenshot of a computer

Description automatically generated

- Các câu lệnh để cấu hình NAT:

* *iptables --flush*: Lệnh này xóa tất cả các quy tắc trong bảng mặc định, trong trường hợp này là bảng "filter".
* *iptables --table nat --flush*: Xóa tất cả các quy tắc trong bảng "nat". Bảng "nat" thường được sử dụng để thực hiện các chuyển đổi địa chỉ mạng (NAT) hoặc định tuyến dựa trên địa chỉ.
* *iptables --delete-chain*: Xóa tất cả các chuỗi (chains) trong bảng mặc định (trong trường hợp này là "filter"), ngoại trừ chuỗi mặc định.
* *iptables --table nat --delete-chain*: Tương tự như trên, lệnh này xóa tất cả các chuỗi trong bảng "nat", ngoại trừ chuỗi mặc định.
* *iptables --table nat --append POSTROUTING --out-interface ens33 -j MASQUERADE*: Thêm một quy tắc vào chuỗi "POSTROUTING" trong bảng "nat". Quy tắc này thực hiện việc "masquerade" (làm ẩn danh) các gói tin đi qua giao diện " ens33". Điều này thường được sử dụng để thực hiện NAT khi chia sẻ kết nối internet từ một máy tính có nhiều giao diện mạng.
* *iptables --append FORWARD --in-interface ens37/ens38 -j ACCEPT*: Thêm một quy tắc vào chuỗi "FORWARD" trong bảng mặc định (trong trường hợp này là "filter"). Quy tắc này cho phép tất cả các gói tin đi qua giao diện "ens37" hoặc ens38 để được chuyển tiếp (forward).
* *echo 1 > /proc/sys/net/ipv4/ip\_forward*: Bật tính năng chuyển tiếp gói tin trên kernel Linux. Nếu không bật tính năng này, hệ thống sẽ không chuyển tiếp các gói tin giữa các giao diện mạng.
* *service iptables restart*: Khởi động lại dịch vụ iptables để áp dụng các thay đổi cấu hình mới. Lưu ý rằng trong một số trường hợp, bạn có thể cần sử dụng "systemctl" thay vì "service" tùy thuộc vào phiên bản Linux bạn đang sử dụng.

- Máy Attacker ping được google.com

A computer screen shot of a computer screen

Description automatically generated

**Bước 4:** Cài đặt và cấu hình Snort

- Sau khi cài đặt, kiểm tra phiên bản Snort

A screenshot of a computer

Description automatically generated

- Kiểm tra afpacket DAQ đã phải được cài đặt để sử dụng được mode inline.

A screenshot of a computer

Description automatically generated

- Xóa tất cả các file rule mặc định của Snort. Tạo file rule của nhóm.

A screenshot of a computer

Description automatically generated

- Tạo file cấu hình snort của nhóm tại /etc/snort/nhom3-snort.conf.

A screenshot of a computer

Description automatically generated

- Kiểm tra file cấu hình snort bằng lệnh: sudo snort -T -c /etc/snort/nhom3-snort.conf -Q -i ens37:ens38

A screenshot of a computer

Description automatically generated

- Chạy Snort bằng lệnh: sudo snort -c /etc/snort/nhom3-snort.conf -Q -i ens37:ens38

A screenshot of a computer

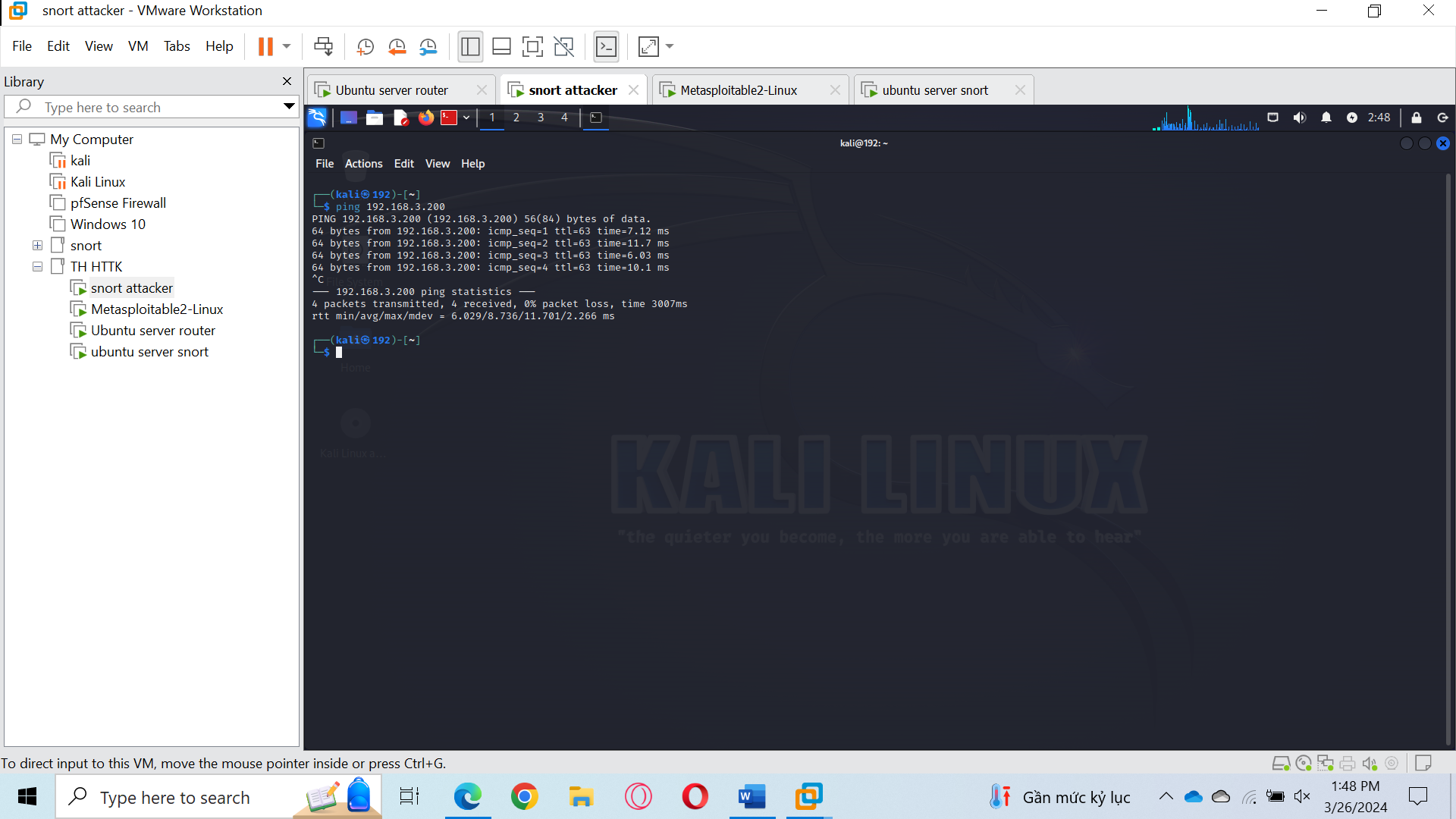
Description automatically generated

- Máy Victim ping được google.com

A screenshot of a computer

Description automatically generated

- Máy Attacker ping được máy Victim



**Bước 5:** Viết rule cho Snort

- Viết rule phát hiện gói ICMP gửi đến lớp mạng 192.168.3.0/24 trong file /etc/snort/rules/nhom3.rules

A computer screen shot of a black screen

Description automatically generated

- Kiểm tra log của snort trên console và /var/log/snort/alert.

A screenshot of a computer

Description automatically generated

**Yêu cầu 3: Sinh viên viết rule drop các gói ICMP đi đến máy Victim (rule #1). Sử dụng tcpdump 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 áp dụng rule#1:

* Trên máy Victim thực thi lệnh **tcpdump -i eth0**, sau đó thực hiện ping từ máy

kali tới máy victim (10.81.3.100 → 192.168.3.200), thì ta thấy các gói tin ICMP đến máy Victim như bình thường

A screenshot of a computer

Description automatically generated

* Thêm rule#1 trên vào file nhom3.rules:

*drop icmp any any -> 192.168.3.200 any (msg: "Drop ICMP"; itype:8; sid: 10; rev: 1;)*

Trong đó:

* drop: Đây là hành động được thực hiện bởi rule, nó sẽ drop (loại bỏ) các gói tin được kích hoạt bởi rule này.
* ICMP: Loại giao thức, trong trường hợp này, là ICMP.
* any any: Địa chỉ IP nguồn và đích, nghĩa là không giới hạn địa chỉ IP.
* 192.168.3.200: Địa chỉ IP đích mà rule sẽ áp dụng, trong trường hợp này là 192.168.3.200.
* msg: "Drop ICMP": Thông điệp được ghi log khi rule này được kích hoạt.
* itype: 8: Loại ICMP, trong trường hợp này là ICMP Echo Request (ping request).
* sid: 10: Số ID của rule, đây là một số duy nhất được sử dụng để xác định rule trong log.
* rev: 1: Số revision của rule.

A screenshot of a computer

Description automatically generated

* Sau đó, chạy lại Snort: *sudo snort -c /etc/snort/nhom3-snort.conf -Q -i ens37:ens38.*

Kết quả sau khi thêm rule#1:

* Trên máy Victim: Gói tin ICMP sẽ bị drop và không thể đến được máy Victim

A screenshot of a computer

Description automatically generated

* Trên máy Snort: Log thông báo gói ICMP bị drop

A screenshot of a computer

Description automatically generated