**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**─────── \* ───────**

****

**BÁO CÁO TUẦN 1**

Môn học: Project II (IT - 3931)

Đề tài: Network Security with IDS/IPS: Detection and Prevention of Network Attacks in a Virtualized Environment

|  |  |
| --- | --- |
| **Sinh viên thực hiện:** | **Ngô Trung Hiếu - 20225316**  **Kỹ thuật máy tính 04 – K67** |
| **Giảng viên hướng dẫn:** | **Nguyễn Quốc Khánh** |

**Hà Nội – 2025**

**Mục lục**

**No table of contents entries found.**

# **Cơ sở lý thuyết**

## Network Security

## IDS/IPS

## Snort

## VirtualBox

# **Mô hình thí nghiệm**

## Mô hình thí nghiệm

A diagram of a network

AI-generated content may be incorrect.

Figure 1: Mô hình thí nghiệm

Mô hình đơn giản này thí nghiệm khả năng ghi lại các gói tin và thông báo của Snort trong mạng nội bộ, với các gói tin có IP Des không nhất thiết là máy sử dụng Snort. Các node của mô hình và vai trò tương ứng bao gồm:

* Kali: attacker
* Ubuntu: chạy Snort
* Metasploitable 2: victim

Lý do sử dụng 3 distro khác nhau là vì mỗi máy có mục đích khác nhau, và mỗi distro được tối ưu sẵn cho mục đích đó. Dùng một distro (ví dụ Ubuntu cho cả ba) vẫn chạy được thí nghiệm, nhưng có lợi hại khác nhau.

## Cấu hình mạng

Cả 3 máy được cấu hình mạng **Internal Network** được đặt tên là **labnet** để có thể test Snort một cách đơn giản. Riêng máy Ubuntu sẽ phải chọn **Promiscuous Mode** thành **Allow All** cho phép máy ảo nhìn và bắt toàn bộ gói tin đi qua mạng, không chỉ gói gửi/nhận của chính nó.

A computer screen shot of a computer

AI-generated content may be incorrect.

Figure 2: Cấu hình mạng của máy ảo Ubuntu

Địa chỉ IP của 3 máy ảo Kali, Ubuntu, Metasploitable 2 lần lượt:

* Kali: 192.168.2.2/24
* Ubuntu: 192.168.2.179/24
* Metasploitable 2: 192.168.2.157/24

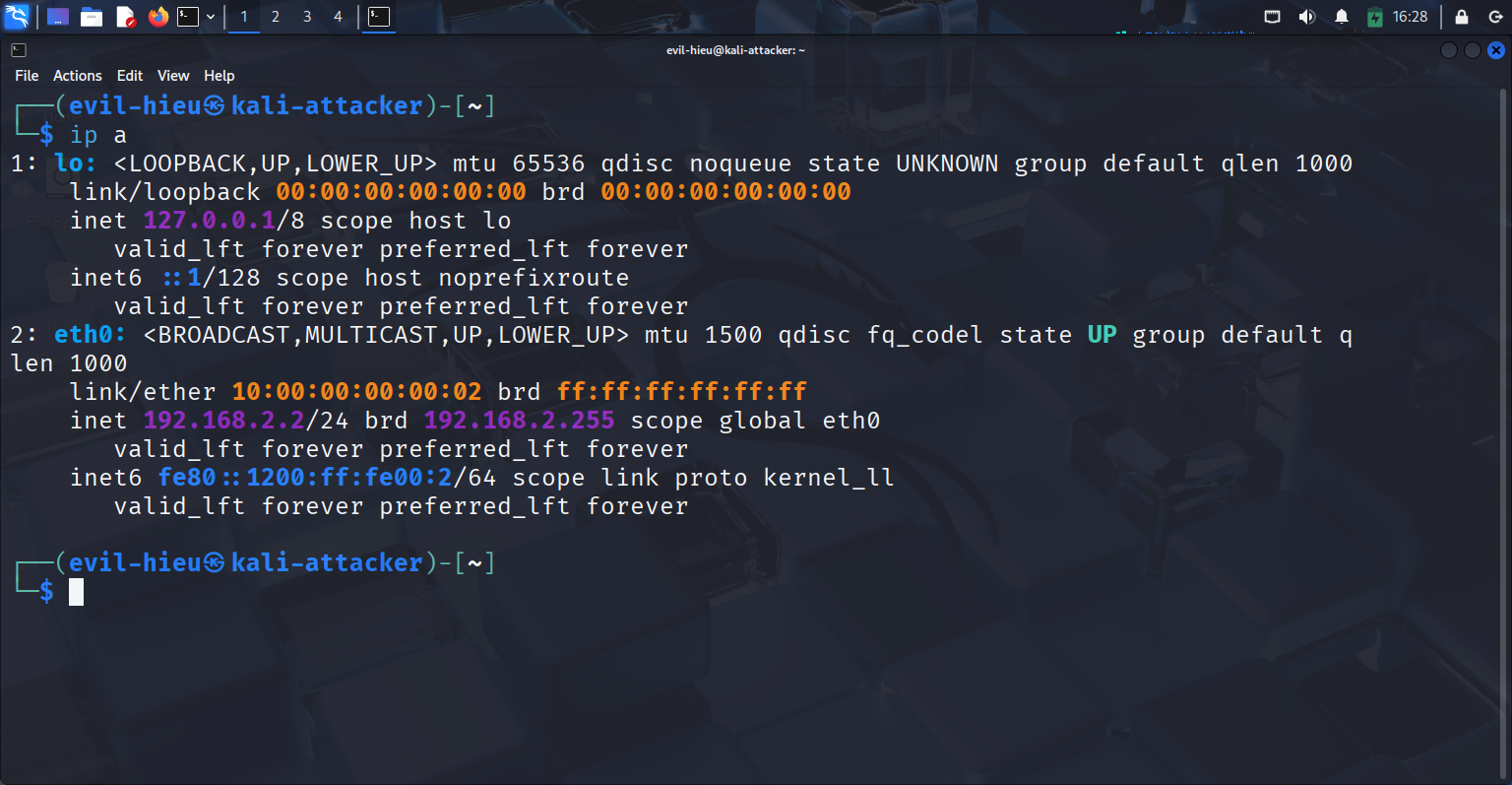


Figure 3: Cấu hình mạng của máy ảo Kali

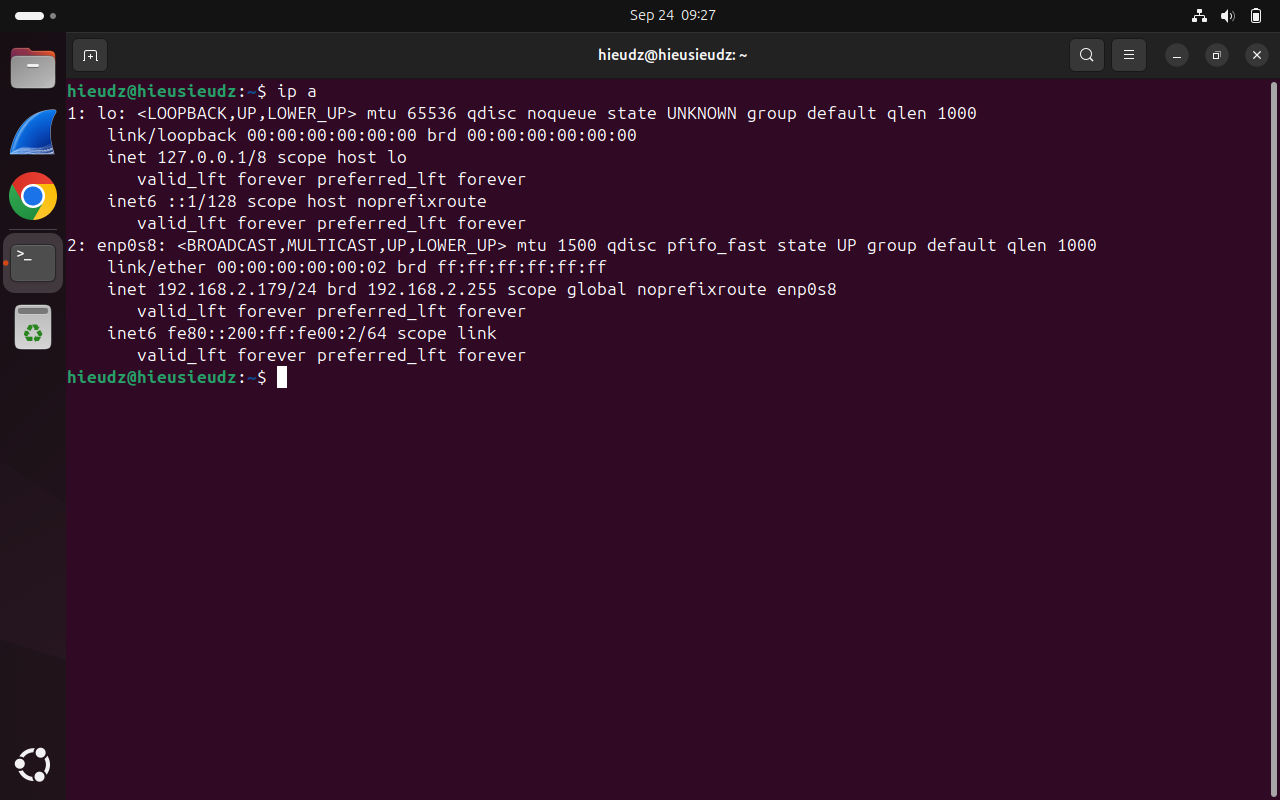


Figure 4: Cấu hình mạng của máy ảo Ubuntu

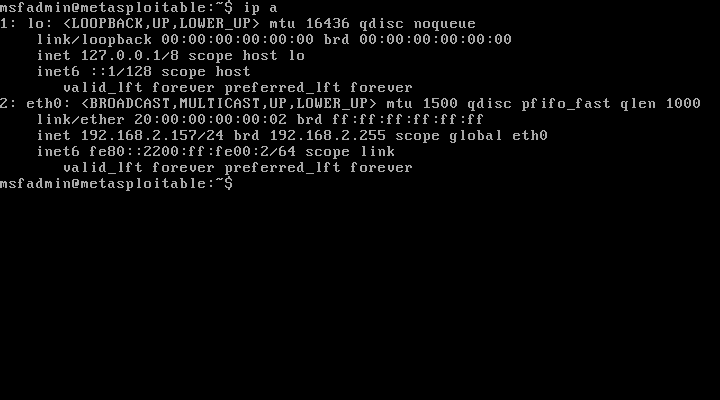


Figure 5: Cấu hình mạng của máy ảo Metasploitable 2

Ta kiểm tra kết nối giữa 3 máy bằng lệnh ping

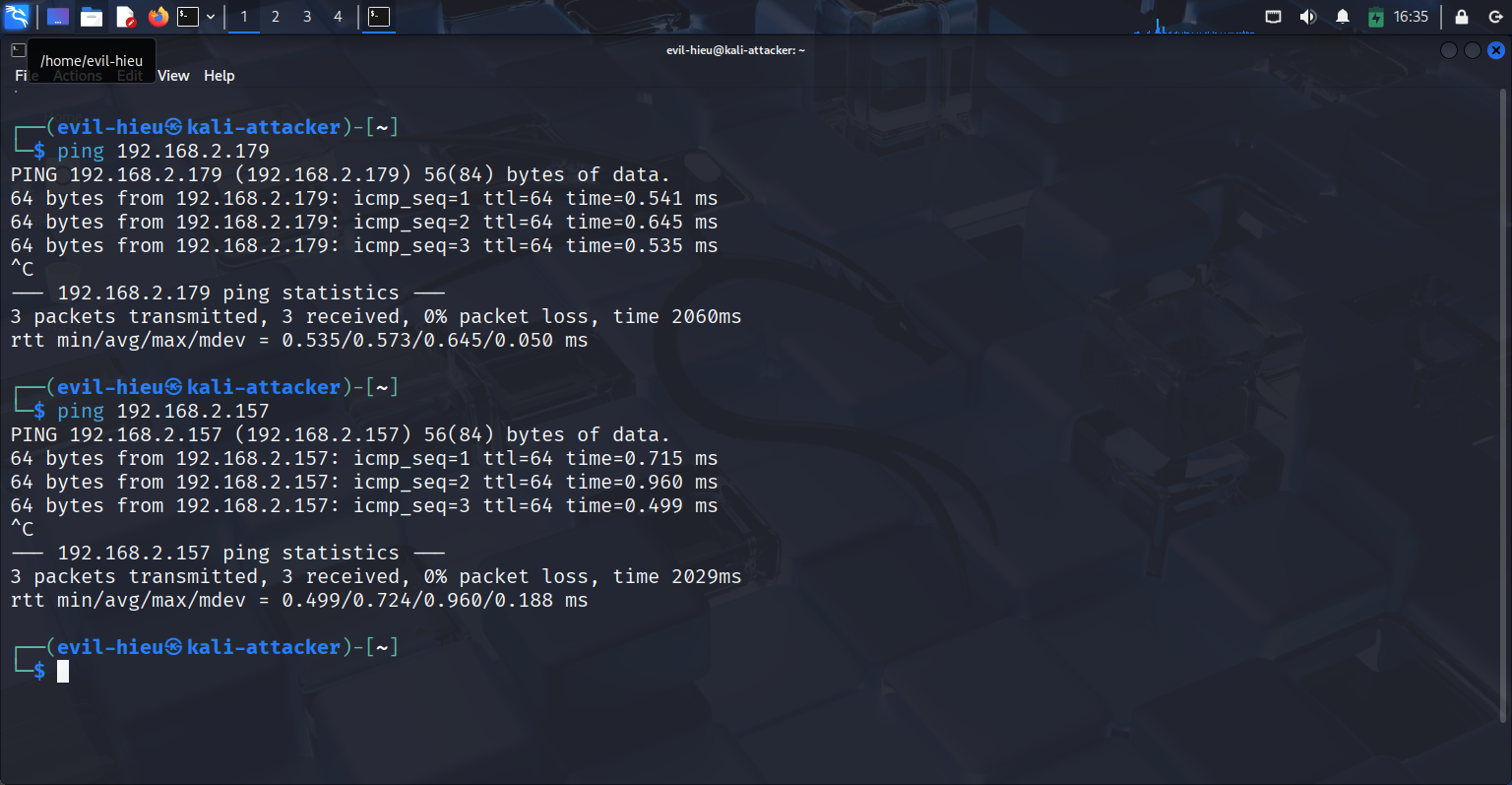


Figure 6: Máy ảo Kali ping

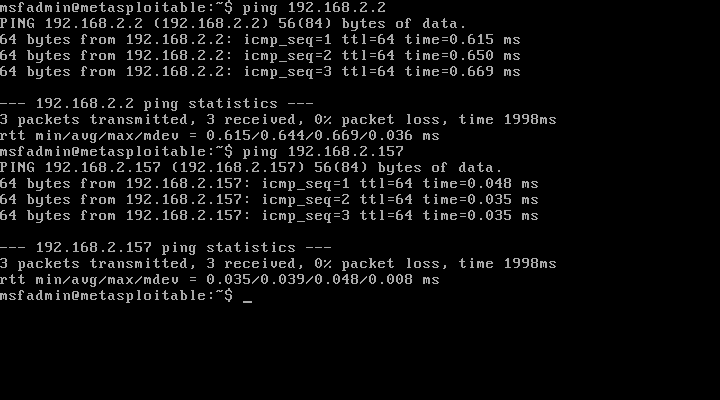


Figure 7: Máy ảo Metasploitable 2 ping

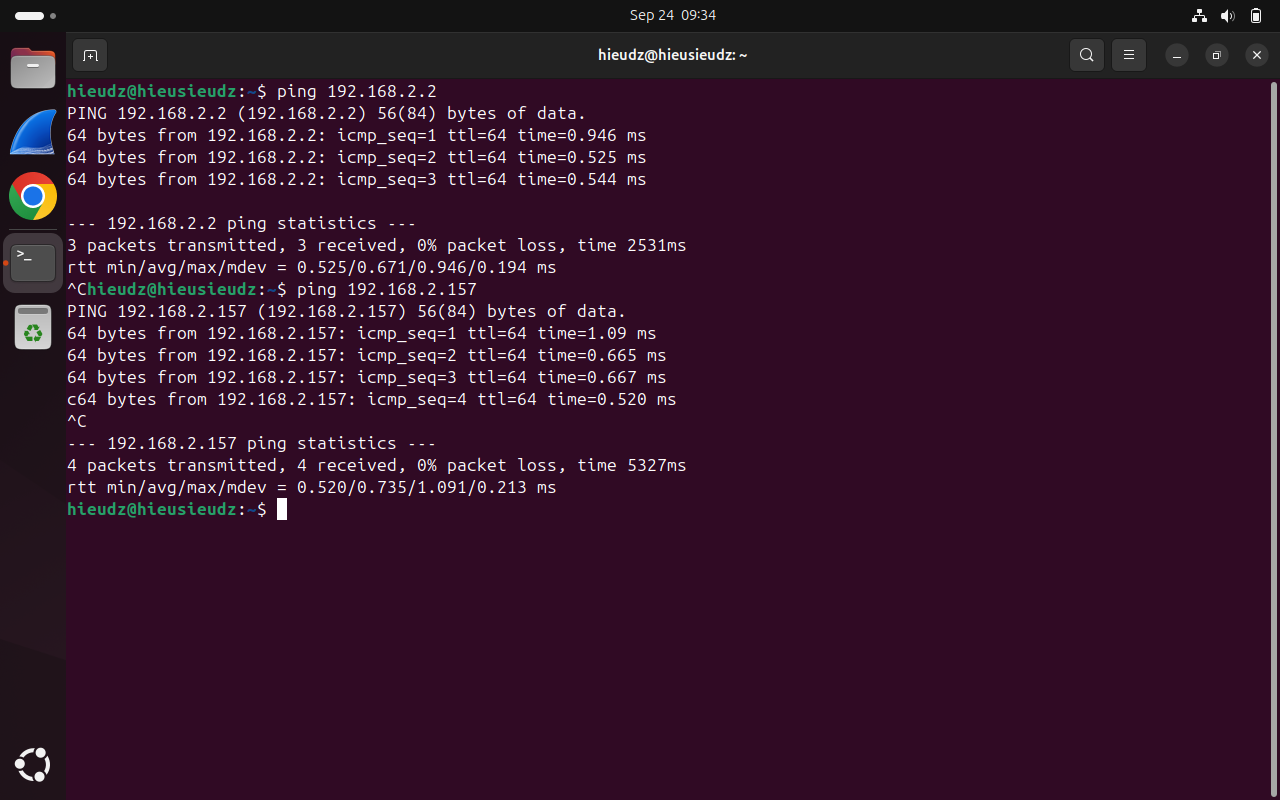


Figure 8: Máy ảo Ubuntu ping

# **Cài đặt và cấu hình Snort**

# **Thực nghiệm và kiểm thử**

# **Kết quả và minh họa**

# **Kết luận**

# **References**