**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**

[**I.** **Cơ sở lý thuyết** 4](#_Toc209696146)

[1. Network Security 4](#_Toc209696147)

[2. Intrusion detection systems (IDS) và Intrusion prevention systems (IPS) 4](#_Toc209696148)

[a. Hệ thống phát hiện xâm nhập (IDS) 4](#_Toc209696149)

[b. Hệ thống ngăn chặn xâm nhập (IPS) 4](#_Toc209696150)

[3. Snort 4](#_Toc209696151)

[a. Giới thiệu về Snort 4](#_Toc209696152)

[b. Các phiên bản Snort 4](#_Toc209696153)

[c. Snort rules và cú pháp viết lệnh Snort 4](#_Toc209696154)

[d. Cách hoạt động của Snort 4](#_Toc209696155)

[4. VirtualBox 4](#_Toc209696156)

[**II.** **Mô hình thí nghiệm** 4](#_Toc209696157)

[1. Mô hình thí nghiệm 4](#_Toc209696158)

[2. Cấu hình mạng 4](#_Toc209696159)

[**III.** **Cài đặt và cấu hình Snort** 4](#_Toc209696160)

[1. Cách tải và cài đặt Snort trên Ubuntu 4](#_Toc209696161)

[2. Giới thiệu về file cấu hình snort.conf 4](#_Toc209696162)

[3. Giới thiệu về cú pháp (syntax) trong Snort 4](#_Toc209696163)

[4. Cấu trúc file log mà Snort lưu trữ 4](#_Toc209696164)

[**IV.** **Thực nghiệm và kiểm thử** 5](#_Toc209696165)

[1. Thực hiện lệnh ping từ Kali → Metasploitable 2 5](#_Toc209696166)

[2. Quan sát và phân tích log Snort 5](#_Toc209696167)

[**V.** **Kết quả và minh họa** 5](#_Toc209696168)

[**VI.** **Kết luận** 5](#_Toc209696169)

[**VII.** **References** 5](#_Toc209696170)

# **Cơ sở lý thuyết**

## Network Security

An ninh mạng là việc bảo vệ hạ tầng mạng khỏi truy cập trái phép, lạm dụng hoặc đánh cắp. Nó tạo ra môi trường an toàn cho thiết bị, ứng dụng và người dùng, đồng thời sử dụng nhiều lớp phòng thủ với chính sách và kiểm soát để cho phép người dùng hợp pháp truy cập, còn kẻ tấn công thì bị ngăn chặn.

Trong thời đại số hóa, an ninh mạng rất quan trọng để các tổ chức bảo vệ dịch vụ, thông tin và uy tín của mình. Nó không chỉ giúp đáp ứng nhu cầu khách hàng và nhân viên mà còn ngăn chặn các cuộc tấn công, bảo vệ dữ liệu và duy trì danh tiếng.

Trong đó, có một số loại an ninh mạng sau:

* Tường lửa (Firewall): Giám sát, cho phép/chặn lưu lượng mạng dựa trên quy tắc.
* Workload security: Bảo vệ workload trên môi trường đám mây và hybrid.
* VPN: Mã hóa kết nối từ thiết bị đến mạng, thường dùng IPsec/SSL.
* Kiểm soát truy cập (Access control) là quá trình xác thực người dùng và thiết bị để áp dụng chính sách bảo mật, ngăn chặn hoặc hạn chế truy cập của các thiết bị không tuân thủ
* Antivirus/Antimalware: các phần mềm giúp phát hiện, ngăn chặn và loại bỏ mã độc như virus, trojan, spyware hay ransomware.

Ngoài ra, an ninh mạng còn bao gồm cơ chế phát hiện/phòng chống phần mềm độc hại, cũng như kiểm soát quyền truy cập để đảm bảo chỉ người dùng hợp lệ được sử dụng tài nguyên

## Intrusion detection systems (IDS) và Intrusion prevention systems (IPS)

### Hệ thống phát hiện xâm nhập (IDS)

IDS là một thiết bị hoặc phần mềm giám sát các hoạt động của mạng hoặc hệ thống để phát hiện hoạt động độc hại và tạo báo cáo trên hệ thống quản lý.

Đây là một dạng hệ thống quản lý bảo mật cho máy tính và mạng.

IDS thu thập và phân tích thông tin từ nhiều khu vực trong máy tính hoặc mạng để nhận diện mối đe dọa bảo mật.

Các chức năng chính gồm:

* Giám sát và phân tích hoạt động của người dùng và hệ thống
* Phân tích cấu hình và lỗ hổng hệ thống
* Đánh giá tính toàn vẹn của hệ thống và tệp tin
* Nhận diện mẫu tấn công
* Phân tích các hành vi bất thường
* Theo dõi vi phạm chính sách người dùng

Có hai loại hệ thống phát hiện xâm nhập (IDS):

* Hệ thống phát hiện xâm nhập dựa trên máy chủ (**Host-based IDS – HIDS**)
* Hệ thống phát hiện xâm nhập dựa trên mạng (**Network-based IDS – NIDS**)

|  |  |  |
| --- | --- | --- |
| **Tiêu chí** | **HIDS** | **NIDS** |
| Vị trí triển khai | Trên từng host/thiết bị riêng lẻ | Ở điểm chiến lược trong mạng (gần firewall, gateway) |
| Phạm vi giám sát | Hoạt động, log, file của host | Toàn bộ lưu lượng mạng đi qua subnet |
| Ưu điểm | - Xác minh tấn công có thành công hay không - Phát hiện thay đổi file, truy cập bất thường - Chi phí thấp | - Một số ít NIDS giám sát được mạng lớn - Ít gây ảnh hưởng, có thể ẩn khỏi attacker |
| Nhược điểm | - Khó quản lý, phải cài từng máy - Dễ bị tấn công hoặc vô hiệu hóa - Không phát hiện tốt quét mạng | - Khó xử lý khi mạng lớn/đông - Không phân tích được dữ liệu mã hóa - Không biết tấn công có thành công hay không |

Table 1. So sánh HIDS và NIDS

### Hệ thống ngăn chặn xâm nhập (IPS)

IPS là một thiết bị hoặc phần mềm bảo mật đặt trực tiếp trong luồng mạng, có khả năng giám sát, phát hiện và **ngăn chặn** các hoạt động độc hại theo thời gian thực.

Đây là một phần mở rộng của IDS, nhưng không chỉ cảnh báo mà còn chủ động chặn tấn công.

IPS phân tích lưu lượng mạng, so sánh với cơ sở dữ liệu chữ ký và hành vi để ngăn chặn mối đe dọa trước khi gây hại.

Các chức năng chính gồm:

* Giám sát và phân tích lưu lượng mạng theo thời gian thực
* Phát hiện và chặn các gói tin độc hại
* Phòng chống tấn công dựa trên chữ ký và hành vi
* Ngăn chặn tấn công từ chối dịch vụ (DoS/DDoS)
* Bảo vệ lỗ hổng chưa được vá (zero-day) thông qua phân tích bất thường
* Thực thi chính sách bảo mật của tổ chức

IDS thiên về giám sát và cảnh báo, IPS thiên về ngăn chặn và phản ứng chủ động.

## Snort

### Giới thiệu về Snort



Figure 1: Snort logo

Snort là hệ thống ngăn chặn xâm nhập (IDS/IPS) mã nguồn mở hàng đầu thế giới. Snort IPS sử dụng một tập hợp các quy tắc để xác định hoạt động mạng độc hại, tìm các gói tin phù hợp với những quy tắc đó và tạo cảnh báo cho người dùng.

Snort cũng có thể được triển khai **trực tiếp trong luồng mạng** để chặn trực tiếp các gói tin này. Snort có ba cách sử dụng chính:

1. Như một công cụ bắt gói tin (packet sniffer) giống tcpdump.
2. Như một công cụ ghi log gói tin — hữu ích cho việc gỡ lỗi lưu lượng mạng.
3. Như một hệ thống ngăn chặn xâm nhập mạng đầy đủ chức năng.

Snort được sử dụng rộng rãi trong nghiên cứu và doanh nghiệp do miễn phí, dễ cấu hình, và cộng đồng hỗ trợ lớn.

### Các phiên bản Snort

Snort được phát triển từ năm 1998 và hiện có 2 phiên bản: **Snort 2.x** (phiên bản chuẩn, phổ biến, có nhiều tài liệu và bộ quy tắc hỗ trợ) và **Snort 3.0** (phiên bản mới, cải thiện hiệu suất, khả năng mở rộng và tính dễ sử dụng). Trong thực tế, Snort 2.x vẫn được dùng nhiều nhất. Tuy nhiên, các rule viết cho Snort 2 cần được viết lại hoặc chuyển đổi để chạy trên Snort 3.

### Snort rules và cú pháp viết lệnh Snort

**Rule** trong Snort là tập hợp các quy tắc dùng để xác định hành vi đáng ngờ trong lưu lượng mạng. Mỗi rule mô tả điều kiện (ví dụ: địa chỉ IP, cổng, giao thức, mẫu dữ liệu trong gói tin) và hành động cần thực hiện (cảnh báo, ghi log, hoặc chặn). Nói ngắn gọn, rule chính là “luật lệ” mà Snort dựa vào để phát hiện và phản ứng với các mối đe dọa. Snort có 3 loại rule/rule-sets:

* Community rules: miễn phí, do cộng đồng Snort tạo.
* Registered rules: miễn phí, do Talos cung cấp, nhưng cần đăng ký tài khoản.
* Subscription-only rules: yêu cầu trả phí để sử dụng.

Ngoài ra, người dùng cũng có thể tự viết rule phù hợp với nhu cầu riêng.

Cú pháp rule tổng quan của các phiên bản Snort 2.x

Diagram

Description automatically generated

Figure 2: Cú pháp rule Snort 2.x

**Action**

* Hành động Snort thực hiện khi rule khớp.
* Ví dụ:
  + alert → tạo cảnh báo
  + log → ghi log
  + pass → bỏ qua
  + drop → chặn gói tin (khi chạy inline)

**Protocol**

* Giao thức áp dụng cho rule: tcp, udp, icmp, hoặc ip (mọi giao thức).

**Source IP / Source Port**

* Địa chỉ và cổng nguồn.
* Có thể là IP cụ thể (192.168.1.5), mạng (/24), hoặc any.

**Direction**

* Ký hiệu: -> (một chiều) hoặc <-> (hai chiều).

**Destination IP / Destination Port**

* Địa chỉ và cổng đích. Tương tự source.

**Options (trong ngoặc đơn)**

* Đây là phần quan trọng nhất, chứa điều kiện chi tiết.
* Ví dụ:
  + msg:"ICMP Packet Detected"; → thông báo khi rule khớp.
  + content:"badstring"; → tìm chuỗi trong payload.
  + sid:1000001; → ID của rule.
  + rev:1; → phiên bản rule.

### Cách hoạt động của Snort

Diagram

Description automatically generated

Figure 3: Mô hình hóa cách hoạt động của Snort

Quy trình hoạt động của Snort được thể hiện qua các bước sau. Đầu tiên, hệ thống tiến hành thu thập các gói tin từ hạ tầng mạng thông qua kỹ thuật sniffing. Các gói tin này sau đó được đưa vào bộ tiền xử lý (preprocessor) để chuẩn hóa và phát hiện những mẫu bất thường. Tiếp theo, Snort sử dụng các plugin và cơ chế giải mã gói tin, đồng thời có thể áp dụng thuật toán học máy nhằm phân loại lưu lượng. Tại Snort Detection Engine, các gói tin được đối chiếu với tập hợp rules (rule set) đã định nghĩa để phát hiện các hành vi tấn công. Khi phát hiện dấu hiệu xâm nhập, hệ thống sẽ ghi nhận cảnh báo vào log, từ đó phục vụ cho công tác giám sát và phân tích an ninh mạng.

1. Ví trí của Snort IDS/IPS

A diagram of a firewall

AI-generated content may be incorrect.

Figure 4: Vị trí của Snort IDS/IPS trong mô hình mạng

Vị trí của Snort IDS và Snort IPS trong mạng khác nhau vì mục tiêu của chúng khác:

* **Snort IDS** (Intrusion Detection System):
  + Đặt ở vị trí song song (out-of-band) với lưu lượng mạng.
  + Nó chỉ giám sát, phân tích gói tin đi qua và tạo cảnh báo khi phát hiện tấn công, không can thiệp trực tiếp vào luồng dữ liệu.
  + Thường đặt sau firewall hoặc tại các điểm chiến lược trong mạng để quan sát toàn bộ traffic.
* **Snort IPS** (Intrusion Prevention System):
  + Đặt trực tiếp (inline) trong luồng mạng, giữa thiết bị nguồn và đích.
  + Mọi gói tin đi qua đều được phân tích, nếu phát hiện độc hại thì sẽ bị chặn hoặc drop ngay lập tức.
  + Thường triển khai ở gateway hoặc giữa các vùng mạng quan trọng.

## VirtualBox

A blue and orange text

AI-generated content may be incorrect.

Figure 5: VirtualBox logo

Oracle VirtualBox là một ứng dụng ảo hóa đa nền tảng cho phép chạy nhiều hệ điều hành trong nhiều máy ảo trên cùng một máy tính. Nó hỗ trợ lưu, sao chép, xuất, chuyển máy ảo, cài đặt appliance sẵn cấu hình, và thậm chí chạy các hệ điều hành cũ nhờ khả năng cấu hình phần cứng ảo linh hoạt.

VirtualBox giúp tiết kiệm chi phí phần cứng và điện năng bằng cách gom nhiều máy ảo vào ít máy chủ mạnh, tránh lãng phí tài nguyên. Nó cũng là công cụ hữu ích cho phát triển và kiểm thử, đặc biệt trong việc xử lý sự cố cấu hình phần mềm hoặc mạng.

Trong bối cảnh nghiên cứu IDS/IPS, VirtualBox cho phép tạo mô hình mạng gồm máy tấn công, máy chạy IDS/IPS (Snort), và máy nạn nhân để mô phỏng các kịch bản tấn công.

# **Mô hình thí nghiệm**

## Mô hình thí nghiệm

A diagram of a network

AI-generated content may be incorrect.

Figure 6: 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 7: 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

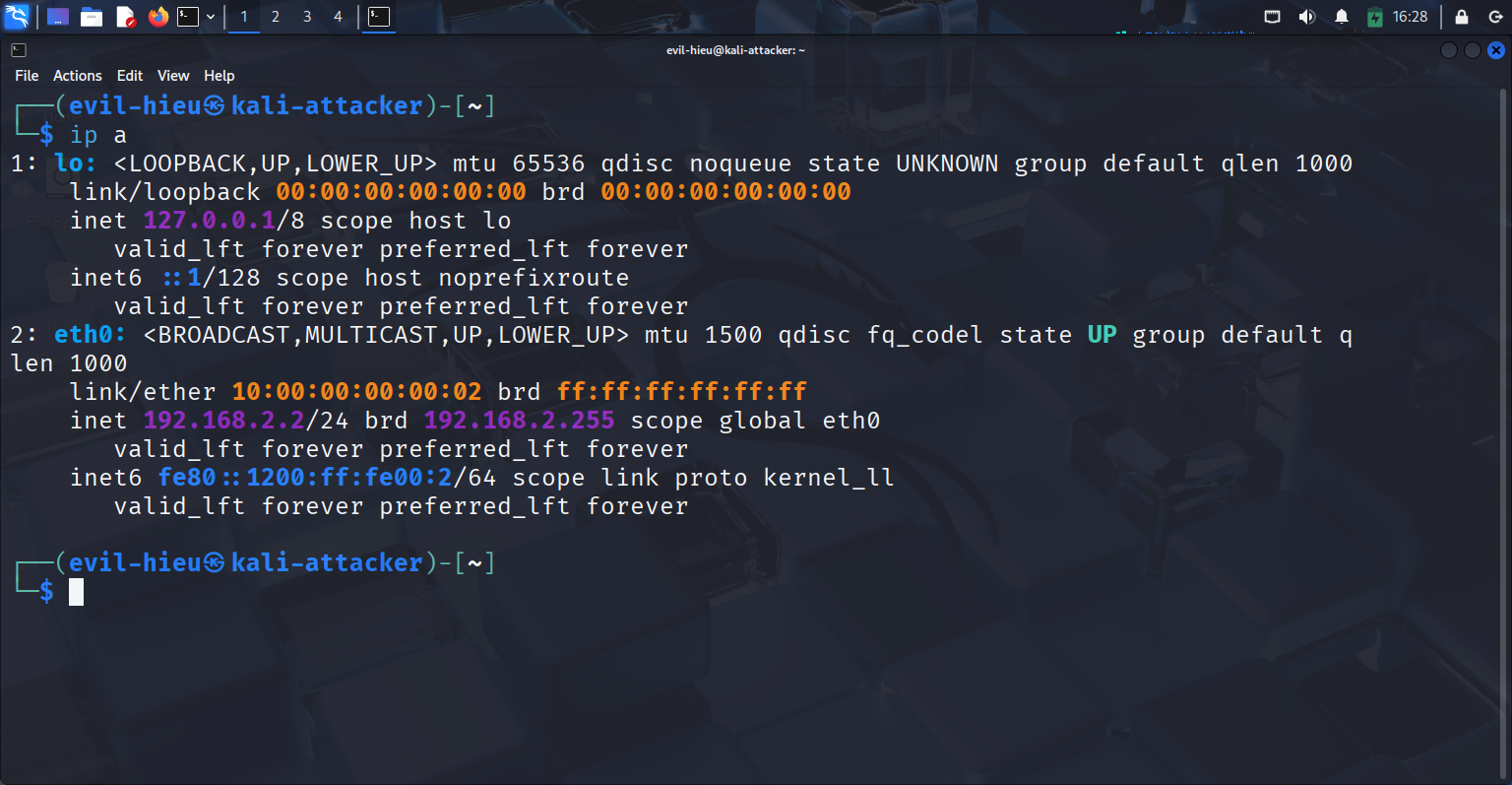


Figure 8: Cấu hình mạng của máy ảo Kali

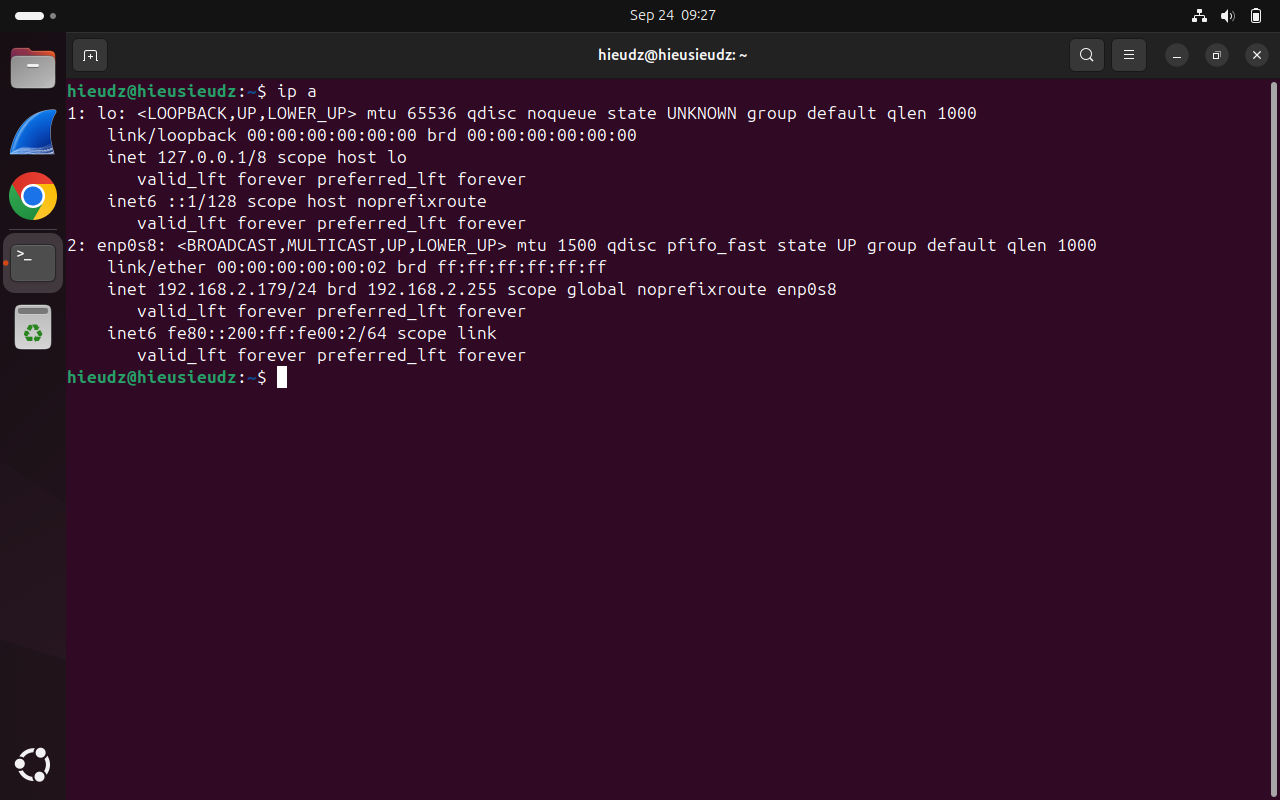


Figure 9: Cấu hình mạng của máy ảo Ubuntu

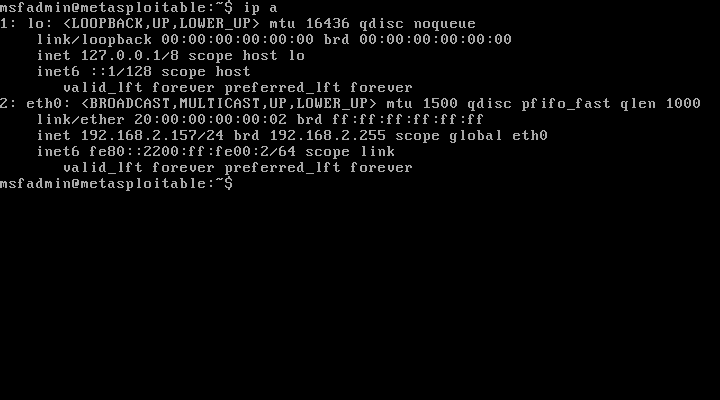


Figure 10: Cấu hình mạng của máy ảo Metasploitable 2

Ta kiểm tra kết nối giữa 3 máy bằng lệnh ping

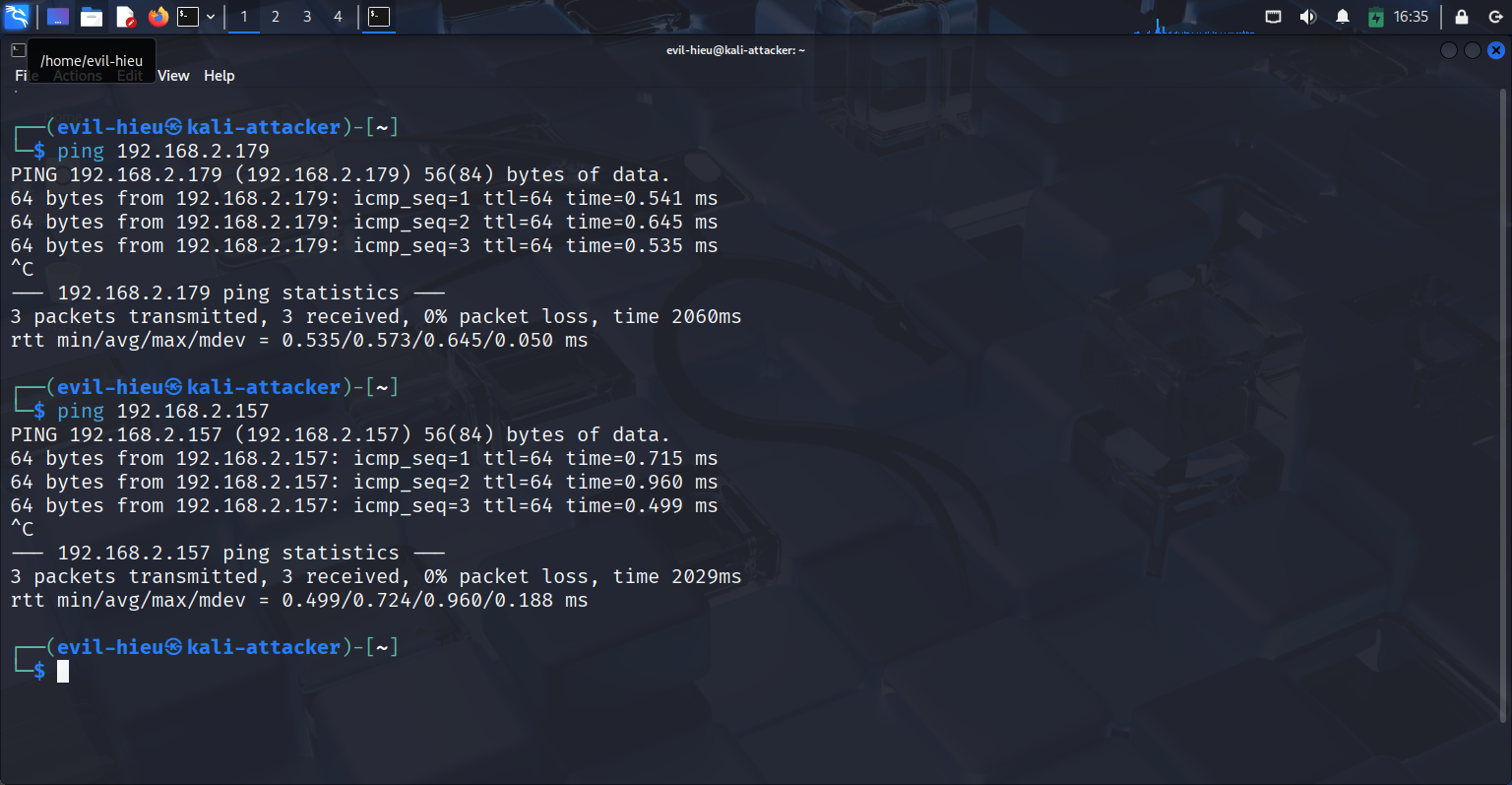


Figure 11: Máy ảo Kali ping

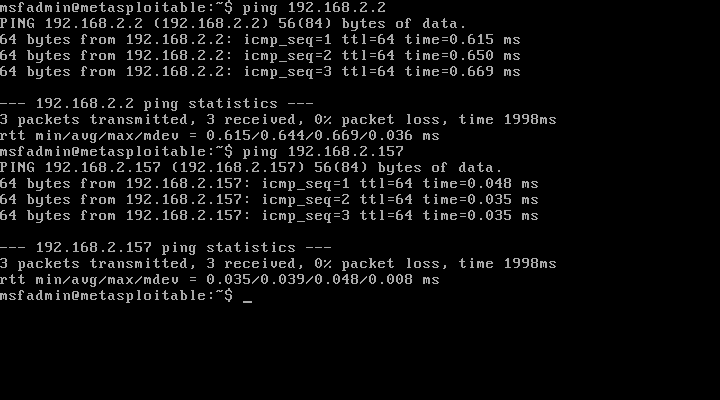


Figure 12: Máy ảo Metasploitable 2 ping

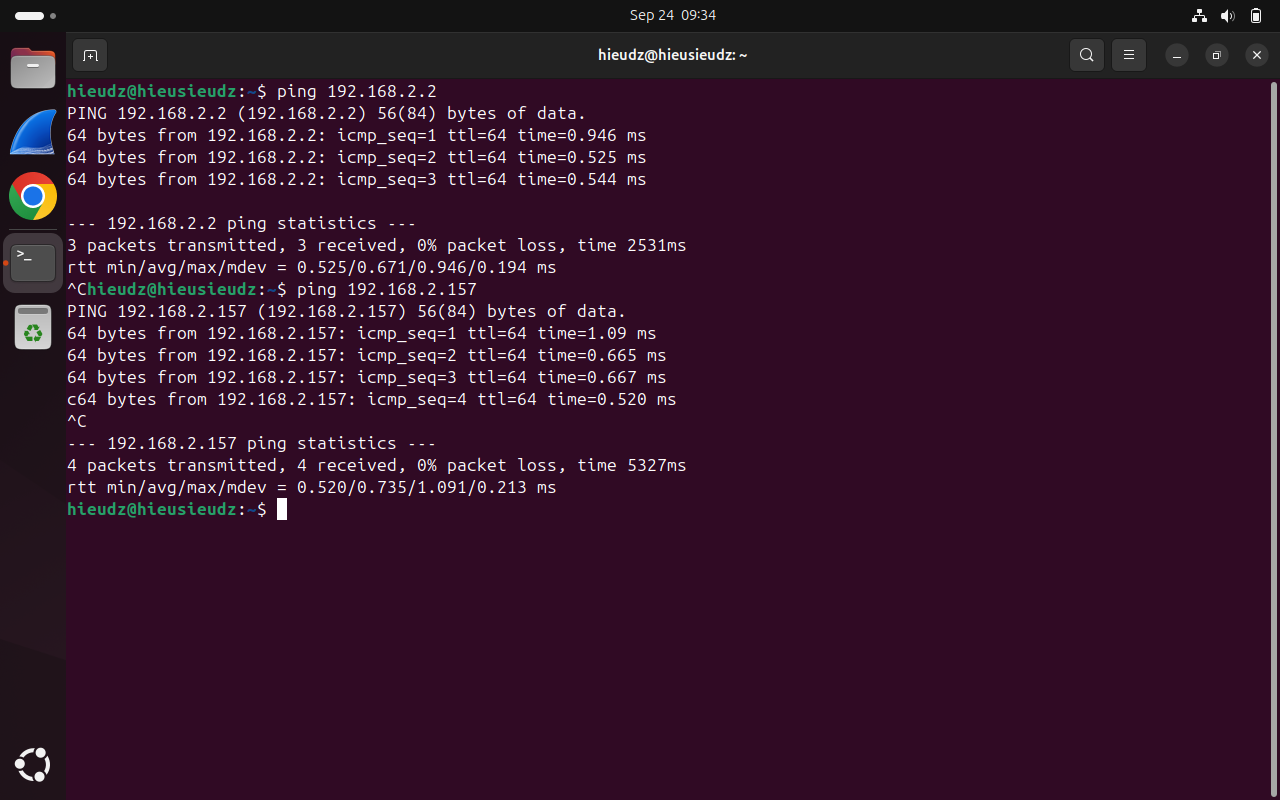


Figure 13: Máy ảo Ubuntu ping

# **Cài đặt và cấu hình Snort**

## Cách tải và cài đặt Snort trên Ubuntu

## Giới thiệu về file cấu hình snort.conf

## Giới thiệu về cú pháp (syntax) trong Snort

## Cấu trúc file log mà Snort lưu trữ

# **Thực nghiệm và kiểm thử**

## Thực hiện lệnh ping từ Kali → Metasploitable 2

## Quan sát và phân tích log Snort

# **Kết quả và minh họa**

# **Kết luận**

# **References**

<https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-security.html#tabs-9da71fbd27-item-1288c79d71-tab>

<https://vpmpce.wordpress.com/wp-content/uploads/2024/02/unit-4-network-security.pdf>

<https://www.snort.org/>

<https://hackersploit.academy/>

<https://www.virtualbox.org/>