

# **BÁO CÁO MÔN HỌC AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI:**

**TÌM HIỂU VÀ THỬ NGHIỆM PHÒNG CHỐNG  
TẤN CÔNG DOS DỰA TRÊN ỨNG DỤNG IPFIRE**

**SVTH: Nhóm 5**

**Nguyễn Hữu Nghĩa - 2124802050013**

**Lục Tấn Khoa - 2124802050022**

**GVHD: Ths. Lê Từ Minh Trí**



# Nội dung

## 01

**Tổng quan về tấn công DoS**

## 02

**Tổng quan về IPFire**

## 03

**Sơ đồ mô phỏng tấn công  
DoS và phòng chống dựa  
trên ứng dụng IPFire**



# 01

# Tổng quan về tấn công DoS

---



# Khái niệm

Tấn công DoS (Denial of Service) là một kiểu tấn công mạng với mục đích làm gián đoạn hoặc ngăn chặn người dùng hợp lệ truy cập vào tài nguyên hoặc dịch vụ của một hệ thống, máy chủ, hoặc mạng



# Mục tiêu của tấn công DoS



**Làm quá tải hệ thống**



**Làm gián đoạn dịch vụ**



**Tạo cơ hội cho kẻ tấn  
công thực hiện các  
hành động độc khác**

# Các loại hình tấn công DoS phổ biến



**Tấn công dựa  
trên lưu lượng  
(Flooding  
Attack):**

**ICMP Flood**

UDP Flood

TCP SYN Flood



**Tấn công ở lớp  
ứng dụng  
(Application  
Layer Attack):**

**HTTP Flood**

Slowloris



**Tấn công khai  
thác lỗ hổng:**

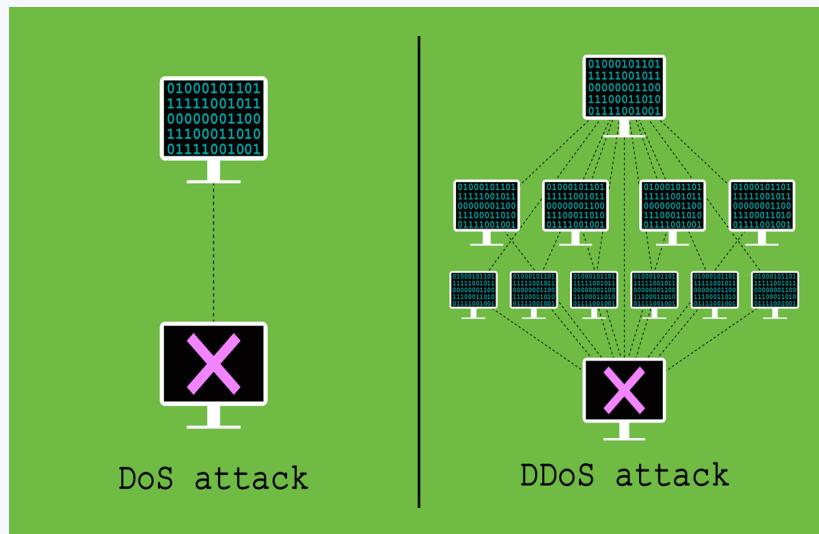
Ping of Death

Teardrop Attack

# Phân biệt Dos và Ddos

**DoS (Denial of Service):** Tấn công từ một nguồn duy nhất.

**DDoS (Distributed Denial of Service):** Tấn công từ nhiều nguồn, sử dụng nhiều nguồn tấn công đồng thời, thường là một mạng botnet với hàng ngàn thiết bị bị kiểm soát.





02

# Tổng quan về IPFire

---





# Khái niệm

IPFire là một hệ điều hành bảo mật mã nguồn mở được thiết kế dành riêng để bảo vệ mạng. Nó chủ yếu hoạt động như một firewall (tường lửa) và có thể được mở rộng để cung cấp các chức năng như VPN, lọc nội dung web, quản lý mạng, và phát hiện xâm nhập (IDS/IPS). IPFire được xây dựng trên nền tảng Linux và được tối ưu hóa để dễ dàng cấu hình, bảo trì và nâng cấp.



# Các tính năng bảo mật của IPFire



**Tường lửa (FireWall)**



**Hệ thống phát  
hiện và ngăn chặn  
xâm nhập (IPS)**



**Quản lý chất  
lượng dịch vụ  
(Qos)**

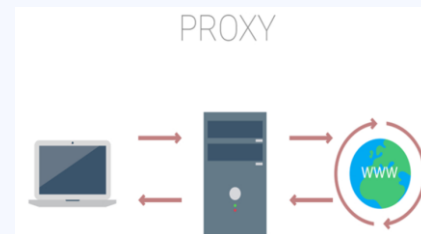
# Các tính năng bảo mật của IPFire



**Virtual Private  
Network (VPN)**



**Giám sát mạng  
(Monitoring and  
Logging)**



**Proxy và lọc nội  
dung**

# Kiến trúc mạng trong IPFire

## **RED (WAN)**

**Vùng kết nối trực tiếp với Internet**

## **GREEN (LAN)**

**Mạng nội bộ an toàn**

## **ORANGE (DMZ - Demilitarized Zone)**

**Khu vực cách ly cho các máy chủ truy cập từ Internet**

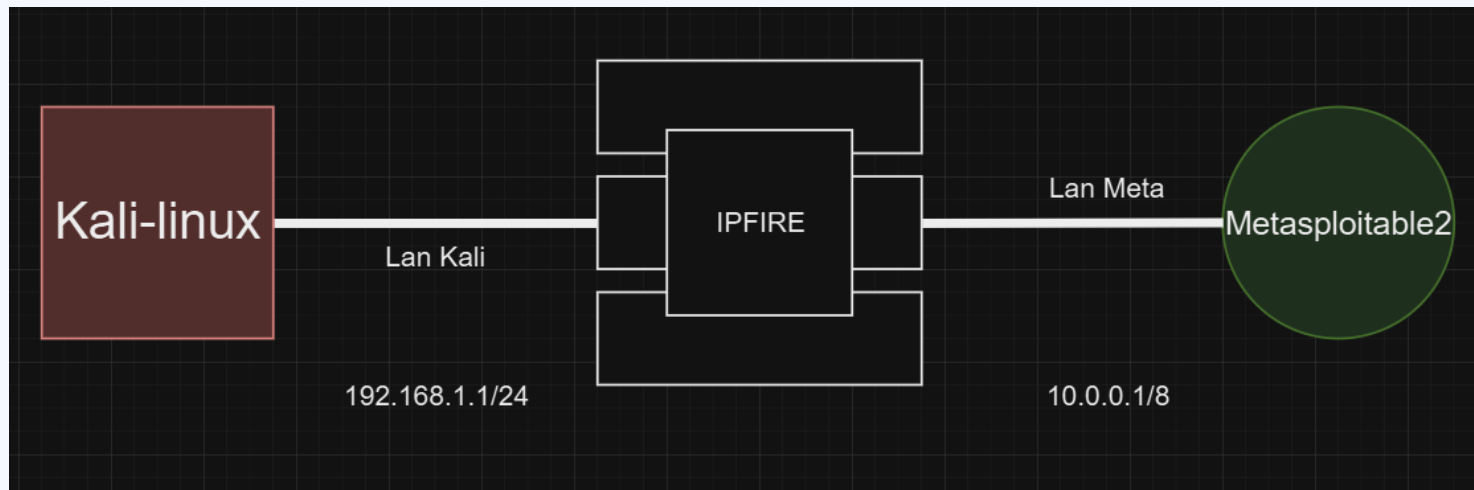
## **BLUE (Wireless)**

**Khu vực dành riêng cho kết nối Wi-Fi**

# 03

## Sơ đồ mô phỏng tấn công DoS và phòng chống dựa trên ứng dụng IPFire

# Sơ đồ cấu trúc mạng



The slide features decorative circuit-like patterns in the corners. The top-left corner has purple and orange lines with dots. The top-right corner has a grid of dots with purple and orange lines and circles. The bottom-right corner has a grid of dots with an orange line and a circle. The word "Thanks !" is centered in a large, bold, blue font.

# Thanks !

