
Hệ thống phát hiện
Xâm nhập SNORT IDS
Xâm nhập SNORT IDS
Nhóm 7

# NHÓM 7

## Tên Thành viên

- Trần Thị Linh Chi
- Vũ Nhật Hạ
- Nguyễn Khánh
- Nguyễn Trọng Nghĩa
- Lê Phan Bảo Trâm
- Đàm Như Vũ

# NỘI DUNG CHÍNH

01 HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS

02 HỆ THỐNG SNORT IDS

03 DEMO


HỆ THỐNG PHÁT HIỆN
XÂM NHẬP IDS
XÂM NHẬP IDS

# Giới thiệu IDS

Hệ thống phát hiện xâm nhập - IDS (Intrusion Detection Systems) là phần mềm hoặc công cụ giúp bảo mật hệ thống và cảnh báo lỗi khi có các hành vi đáng ngờ xâm nhập vào hệ thống.

# Chức năng IDS

## Giám sát

Giám sát lưu lượng mạng và các hoạt động khả nghi.

## Cảnh báo

Cảnh báo về tình trạng mạng cho hệ thống và nhà quản trị.

## Bảo vệ

Dùng những thiết lập mặc định và sử dụng cấu hình từ nhà quản trị mà có những hành động thiết thực chống lại kẻ xâm nhập và phá hoại.

# Phân loại IDS

NIDS (Network Intrusion Detection System) – Hệ thống phát hiện xâm nhập mạng, hệ thống sẽ tập hợp các gói tin để phân tích sâu bên trong nhằm xác định các mối đe dọa tiềm tàng mà không làm thay đổi cấu trúc của gói tin.

HIDS (Host-based Intrusion Detection System) – Hệ thống phát hiện xâm nhập dựa trên máy chủ, được cài đặt trực tiếp trên các máy tính cần theo dõi. HIDS giám sát lưu lượng đến và đi từ thiết bị để cảnh báo người dùng về những xâm nhập trái phép.


Hệ thống SNORT
IDS

# Giới thiệu về Snort

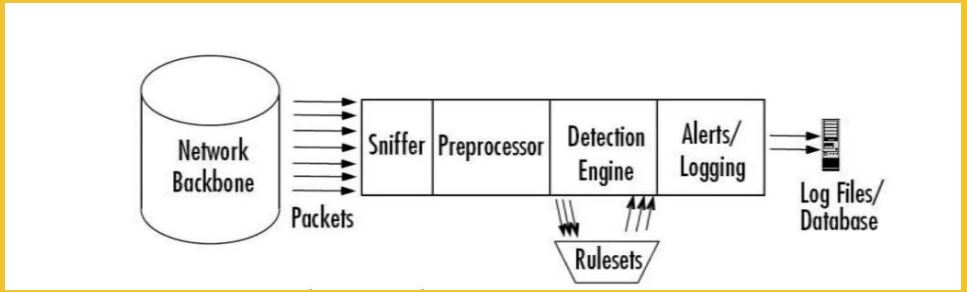
- Snort là phần mềm IDS được phát triển bởi Martin Roesh dưới dạng mã nguồn mở.
- Snort được đánh giá rất cao về khả năng phát hiện xâm nhập. Tuy snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời.
- Snort có thể chạy trên nhiều hệ thống như Windows, Linux, OpenBSD, FreeBSD, Solaris ...

# Kiến trúc của Snort

Snort gồm nhiều thành phần và mỗi phần có một chức năng riêng biệt:

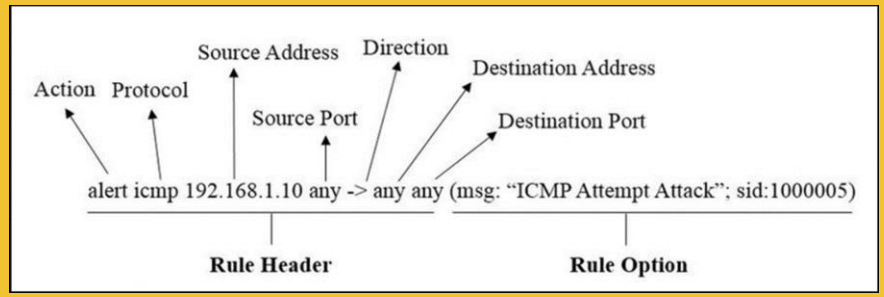
- Module giải mã gói tin (Packet Decoder)
- Module tiền xử lý (Preprocessors)
- Module phát hiện (Detection Engine)
- Module log và cảnh báo (Logging and Alerting System)
- Module kết xuất thông tin. (Output Module)

Mô hình của Snort



# Bộ Luật Snort

Cấu trúc luật (rule structure) trong hệ thống Snort IDS là một phần quan trọng để xác định và phát hiện các hoạt động xâm nhập trong mạng.




Cấu trúc của luật trong Snort được chia thành hai phần:

- Rule Header
- Rule Option

1. Phần Header

Chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa tiêu chuẩn để áp dụng luật với gói tin đó.

2. Phần Option

Chứa thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Nằm ngay sau phần Rule Header và được bọc bởi dấu ngoặc đơn "()".

# THANKS FOR LISTENING

listening