# CHƯƠNG 2 SNORT VÀ IPTABLES TRÊN HỆ ĐIỀU HÀNH LINUX

## 2.1. TỔNG QUAN VỀ SNORT

### 2.1.1. Giới thiệu về Snort

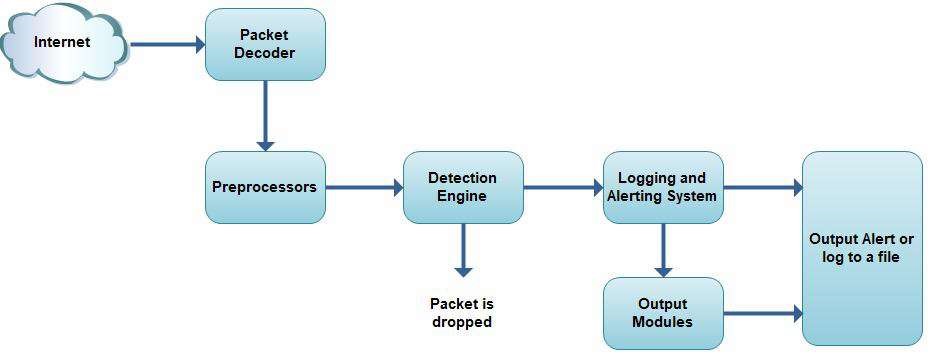
Snort là một hệ thống phát hiện xâm nhập mạng (Intrusion Detection System - IDS) mã nguồn mở, được sử dụng để giám sát và phát hiện các hoạt động không hợp lệ trên mạng. Nó có thể phát hiện các cuộc tấn công từ bên ngoài và bên trong mạng, cũng như các hoạt động bất thường trên hệ thống. Snort có thể được triển khai trên nhiều nền tảng hệ thống khác nhau và có khả năng tương thích với nhiều giao thức mạng. Nó được phát triển bởi Sourcefire và hiện nay là một sản phẩm phần mềm của Cisco.

### 2.1.2. Các thành phần của Snort

Snort bao gồm các thành phần chính sau đây:

* Packet Decoder
* Preprocessors
* Detection Engine
* Loging and alerting system
* Output Modules

Ở hình 2.1 cho thấy các thành phần này được sắp xếp. Bất kỳ dữ liệu nào đến từ internet đều đi vào packet decoder. Trên đường đi của nó với các module đầu ra, nó hoặc bị loại bỏ, ghi nhận hoặc một cảnh báo được tạo ra.



**Hình 2-1.** Các thành phần của Snort

#### 2.1.2.1. Packet Decoder (bộ phận giải mã gói tin)

Packet Decoder của Snort là một thành phần quan trọng trong hệ thống Snort, được sử dụng để giải mã các gói tin mạng và phân tích nội dung của chúng. Khi một gói tin mạng được nhận, Packet Decoder sẽ giải mã nó và phân tích các trường trong gói tin để xác định giao thức mạng được sử dụng, địa chỉ nguồn và đích, và các thông tin khác liên quan đến nội dung của gói tin.

Packet Decoder có thể giải mã nhiều loại giao thức mạng khác nhau, bao gồm các giao thức phổ biến như TCP, UDP, ICMP và cả các giao thức kết nối được sử dụng cho các ứng dụng web như HTTP và HTTPS. Khi phân tích các gói tin, Packet Decoder có thể áp dụng các quy tắc (rules) được cấu hình trước để xác định các hoạt động bất thường và phát hiện các cuộc tấn công từ bên ngoài hoặc bên trong mạng.

#### 2.1.2.2. Preprocessor (bộ phận tiền xử lý)

Các Preprocessor là những thành phần hoặc plug-in có thể sử dụng cho Snort để sắp xếp, chỉnh sửa các gói dữ liệu trước khi bộ phần Detection Engine làm việc với chúng. Preprocessor có thể được sử dụng để giải mã các giao thức mạng phức tạp như IPv6, ICMPv6, SSL và SSH. Nó cũng có thể được sử dụng để loại bỏ các gói tin mạng giả mạo hoặc lừa đảo (spoofed packets), các gói tin tấn công từ bên ngoài và các gói tin có chứa các ký tự đặc biệt hoặc mã độc. Preprocessor cũng có khả năng giúp giảm bớt tình trạng báo động giả (false positives) trong hệ thống phát hiện xâm nhập.

Preprocessor còn dùng để tái hợp gói tin cho các gói tin có kích thước lớn. Ngoài ra nó còn giải mã các gói tin đã được mã hóa trước khi chuyển đến bộ phận Detection Engine.

#### 2.1.2.3. Detection Engine (bộ phận kiểm tra)

Detection Engine của Snort được sử dụng để phân tích các gói tin mạng và xác định xem chúng có chứa các đặc điểm của các cuộc tấn công hay không. Detection Engine sử dụng các quy tắc (rules) được cấu hình trước để phát hiện các cuộc tấn công mạng và các hoạt động bất thường khác.

Detection Engine có thể được cấu hình để phát hiện nhiều loại cuộc tấn công mạng khác nhau, bao gồm các cuộc tấn công từ bên ngoài, từ bên trong mạng và các cuộc tấn công chủ động. Nó cũng có thể được cấu hình để phát hiện các hoạt động bất thường trên mạng, như tải lên hoặc tải xuống dữ liệu lớn hoặc truy cập vào các tài nguyên mạng không được phép.

Detection Engine sử dụng một loạt các kỹ thuật phân tích dữ liệu để phát hiện các cuộc tấn công mạng, bao gồm phân tích đặc điểm của gói tin mạng, phát hiện các hoạt động không hợp lệ, phân tích các tập tin đính kèm và phát hiện các dấu vết của mã độc. Nó cũng có thể được cấu hình để phát hiện các cuộc tấn công mới và chưa biết trước đó, thông qua việc sử dụng các kỹ thuật như Machine Learning hay Deep Learning.

#### 2.1.2.4. Logging and Alerting System (Bộ phận ghi nhận và thông báo)

Logging and Alerting System của Snort được sử dụng để ghi lại các hoạt động trên mạng và cảnh báo người quản trị hệ thống khi phát hiện các cuộc tấn công mạng hoặc các hoạt động bất thường trên mạng.

Logging System của Snort sẽ ghi lại các thông tin về các gói tin mạng đã được phân tích bởi Detection Engine, bao gồm các thông tin như địa chỉ IP nguồn và đích, các thông tin về các giao thức mạng và các tập tin đính kèm, và các thông tin chi tiết về các cuộc tấn công mạng được phát hiện. Logging System cung cấp cho người quản trị hệ thống một bản sao của các hoạt động trên mạng và cung cấp dữ liệu để phân tích và tìm hiểu về các hoạt động trên mạng.

Alerting System của Snort sẽ cảnh báo người quản trị hệ thống khi phát hiện các cuộc tấn công mạng hoặc các hoạt động bất thường trên mạng. Alerting System cung cấp các thông báo cảnh báo về các cuộc tấn công mạng và các hoạt động bất thường trên mạng, bao gồm các chi tiết về các cuộc tấn công mạng được phát hiện. Các thông báo cảnh báo này sẽ giúp người quản trị hệ thống có thể nhanh chóng đưa ra các biện pháp phòng ngừa và bảo vệ hệ thống mạng của mình.

#### 2.1.2.5. Output Modules (bộ phận đầu ra)

Output Modules có thể đưa ra các kết quả phân tích của Snort dưới dạng các bản ghi định dạng ASCII hoặc các bản ghi định dạng binary được gửi đến các thiết bị khác để xử lý hoặc lưu trữ. Các Output Modules phổ biến của Snort bao gồm:

- Unified Output: cho phép Snort gửi các bản ghi định dạng binary đến các thiết bị khác trong hệ thống mạng để xử lý và lưu trữ.

- Syslog Output: cho phép Snort ghi các bản ghi định dạng ASCII vào các hệ thống log syslog.

- Database Output: cho phép Snort gửi các bản ghi định dạng ASCII hoặc binary vào cơ sở dữ liệu để lưu trữ và xử lý các thông tin về các cuộc tấn công mạng và các hoạt động bất thường trên mạng.

- Alert Fast Output: cho phép Snort gửi các bản ghi định dạng ASCII vào các thiết bị khác trong hệ thống mạng để cảnh báo người quản trị hệ thống khi phát hiện các cuộc tấn công mạng hoặc các hoạt động bất thường trên mạng.

- ASCII Output: cho phép Snort ghi các bản ghi định dạng ASCII vào các tập tin để lưu trữ và phân tích các thông tin về các cuộc tấn công mạng và các hoạt động bất thường trên mạng.

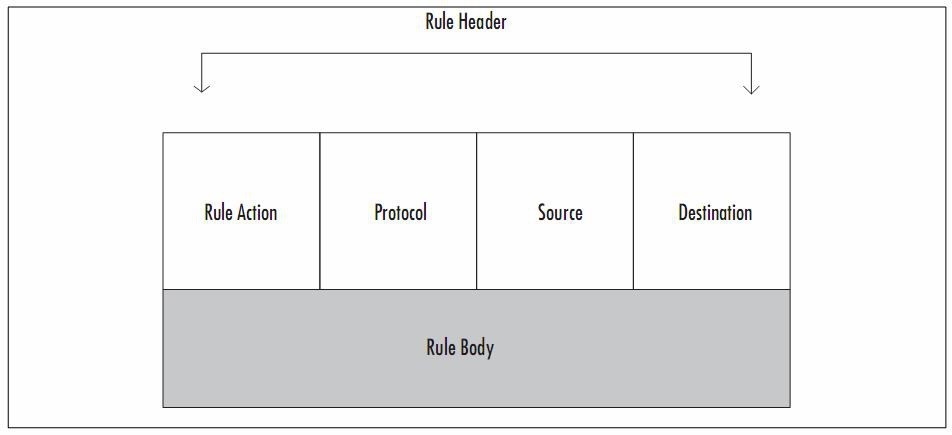
### 2.1.3. Cấu trúc của Rules

Một trong những chức năng được đánh giá cao nhất của Snort là cho phép người sử dụng tự viết các rule của riêng mình. Ngoài số lượng lớn các rule đi kèm với Snort, người quản trị có thể vận dụng khả năng của mình để phát triển ra các rule riêng thay vì phụ thuộc vào các cơ quan, tổ chức bên ngoài.

Rule là tập hợp các qui tắc để lựa chọn các traffic mạng phù hợp với một mô hình định trước. Rule Snort được chia làm hai phần: *rule header* và *rule options*.

#### 2.1.3.1. Rule header

Rule header chứa thông tin để xác định một packet cũng như tất cả những gì cần thực hiện với tất cả các thuộc tính chỉ định trong rule. Rule header bao gồm các phần sau: *Rule actions, protocol, IP address, port number, Direction operator*.



**Hình 2-2.** Cấu trúc của rule header

##### a. Rule action

Rule action là một phần của header trong một rule của Snort và xác định hành động sẽ được thực hiện bởi Snort khi phát hiện một luồng dữ liệu khớp với rule đó. Rule action có thể là một trong các giá trị sau:

- alert: tạo ra một cảnh báo và ghi lại thông tin về sự kiện vào log file.

- log: ghi lại thông tin về sự kiện vào log file mà không tạo ra cảnh báo.

- pass: bỏ qua luồng dữ liệu phù hợp với rule đó và không thực hiện bất kỳ hành động nào.

- drop: loại bỏ luồng dữ liệu phù hợp với rule đó.

- reject: loại bỏ luồng dữ liệu phù hợp với rule đó và gửi một gói tin ICMP Unreachable cho người gửi dữ liệu.

- sdrop: tương tự như drop, nhưng sẽ không ghi lại thông tin về sự kiện vào log file.

Quản trị viên có thể chọn hành động phù hợp với từng rule để đáp ứng các yêu cầu bảo mật và đáp ứng với mức độ nguy hiểm của các cuộc tấn công mạng. Ví dụ, một số rule có thể được cấu hình để tạo ra cảnh báo để giúp quản trị viên kiểm tra sự cố, trong khi các rule khác có thể được cấu hình để loại bỏ luồng dữ liệu độc hại ngay lập tức.

##### b. Protocols

Trường tiếp theo của rule là protocol. Hiện nay Snort chỉ hỗ trợ bốn giao thức sau: TCP, UDP, ICMP, IP. Trong tương lai có thể hỗ trợ thêm các giao thức khác như: ARP, IGRP, GRE, OSPF, RIP…

##### c. IP address

Các địa chỉ IP được hình thành bởi dạng thập phân: xxxx.xxxx.xxxx.xxxx và một CIDR. Snort không cung cấp cơ chế tra cứu tên host tương ứng với địa chỉ IP.

##### d. Port number

Port number có thể được xác định gồm:

- Any ports: Có nghĩa là bất kỳ port nào.

- Static port: là chỉ định một port duy nhất, như: 80 (web), 21 (telnet).

- Ranger: phạm vi các port có thể được áp dụng.

##### e. Direction Operator

Chỉ ra hướng đi của rule, có hai loại đó là:

→ : chỉ ra hướng của rule bắt nguồn từ địa chỉ IP và port bến trái .

↔ : Hướng của rule này là hai chiều, điều này sẽ thuận lợi cho việc phân tích cả hai mặt của một traffic, như là telnet hoặc POP3…

##### f. Active/ Dynamic rules

Active/ Dynamic rules cung cấp cho snort những tính năng mạnh mẽ. Có một rule khác khi hành động được thực hiện với một số gói tin. Điều nay rất hữu ích cho snort để thực hiện ghi lại một số rule cụ thể.

#### 2.1.3.2. Rule Options

Đây chính là trái tim chính của Snort, có 4 loại rule options chính: *general, Payload, Non-Payload, Post- detections.*

##### a. General options

Cung cấp thông tin về rule nhưng không gây ra bất kỳ ảnh hưởng nào đến quá trình phát hiện packet.

Ví dụ:

**Định dạng:** gid: <generator id>;

alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

##### b. Payload Detection Rule Options

Tìm kiếm thông tin trong phần payload của packet. Phần này gồm các từ khóa như: content, nocase, rawbytes, depth, offset, distance, within, http client body, http cookie, http header, http method, http uri, fast pattern, uricontent, urilent, isdataat, pcre, byte test, byte jump, ftpbuonce, asn1, cvs.

Ví dụ:

**Định dạng:** depth :<number>;

alert tcp any any -> any 80 (content: "cgi-bin/phf"; offset:4; depth:20;)

##### c. Non-Payload Detection Rule Options

Tìm kiếm thông tin trong phần non-payload của packet, bao gồm các từ khóa: frag ,offset, ttl, tos, id, ipopts, fragbits, dsize, flags, flow, flowbits, seq, ack, window, itype, icode, icmp id, icmp seq, rpc, ip proto, sameip, stream size.

Ví dụ:

**Định dạng:** flags:[!|\*|+]<FSRPAU120>[,<FSRPAU120>];

alert tcp any any -> any any (flags:SF,12;)

##### d. Post-Detection Rule Options

Xảy ra khi một rule được kích hoạt, gồm các từ khóa: *logto, session, resp, react, tag, activated by, count.*