Tìm hiểu về hệ thống phát hiện tấn công, đột nhập Suricata: kiến trúc, cài đặt, cấu hình, tạo luật; xây dựng 3 kịch bản phát hiện tấn công.

<https://docs.suricata.io/en/latest/> :Tài liệu

**MỤC LỤC**

1. **Lời mở đầu** ................................................................................... Trang 1
2. **Giới thiệu tổng quan về hệ thống IDS/IPS** ............................................ Trang 2
3. **Giới thiệu về Suricata** ...................................................................... Trang 3
4. **Kiến trúc của Suricata** ...................................................................... Trang 4
   * 4.1 Capture Engine
   * 4.2 Decode Engine
   * 4.3 Preprocessing Engine
   * 4.4 Rule Engine và Detection Engine
   * 4.5 Output và Logging
5. **Cài đặt và cấu hình Suricata** .............................................................. Trang 7
   * 5.1 Hướng dẫn cài đặt trên Ubuntu/Debian
   * 5.2 Hướng dẫn cài đặt trên CentOS/RHEL
   * 5.3 Cấu hình file suricata.yaml
6. **Tạo luật phát hiện tấn công trong Suricata** ............................................. Trang 9
   * 6.1 Cấu trúc cơ bản của luật
   * 6.2 Ví dụ thực tế
   * 6.3 Cập nhật và quản lý ruleset
7. **Xây dựng 3 kịch bản phát hiện tấn công** ................................................ Trang 11
   * 7.1 Kịch bản 1: Phát hiện Port Scanning
   * 7.2 Kịch bản 2: Phát hiện SQL Injection
   * 7.3 Kịch bản 3: Phát hiện Distributed Denial of Service (DDoS)
8. **Kết luận và hướng phát triển tương lai** ................................................ Trang 14
9. **Tài liệu tham khảo** .......................................................................... Trang 15

**1. LỜI MỞ ĐẦU**

Trong bối cảnh an ninh mạng ngày càng trở thành mối quan tâm hàng đầu của các tổ chức, việc triển khai các hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) là cực kỳ cần thiết để bảo vệ hệ thống mạng khỏi các cuộc tấn công.  
Báo cáo này tập trung nghiên cứu và triển khai Suricata – một trong những công cụ mã nguồn mở được sử dụng phổ biến trong việc giám sát, phát hiện và ngăn chặn tấn công mạng. Qua báo cáo, chúng ta sẽ đi sâu vào kiến trúc, quy trình cài đặt, cấu hình, tạo luật và xây dựng các kịch bản phát hiện tấn công thực tế, nhằm cung cấp cái nhìn toàn diện về khả năng của Suricata.

**2. GIỚI THIỆU TỔNG QUAN VỀ HỆ THỐNG IDS/IPS**

Hệ thống IDS (Intrusion Detection System) và IPS (Intrusion Prevention System) là những giải pháp an ninh mạng giúp:

* **Giám sát lưu lượng mạng:** Liên tục theo dõi các gói tin đi qua hệ thống.
* **Phát hiện hành vi bất thường:** So sánh các gói tin với các luật đã được cấu hình sẵn để phát hiện các dấu hiệu của tấn công.
* **Cảnh báo và/hoặc ngăn chặn:** Khi phát hiện mối đe dọa, hệ thống có thể cảnh báo cho quản trị viên hoặc trực tiếp ngăn chặn lưu lượng độc hại.

Với sự phát triển của các mối đe dọa mạng tinh vi, các hệ thống IDS/IPS ngày càng được cải tiến để đáp ứng nhu cầu bảo vệ hệ thống mạng một cách hiệu quả.

**3. GIỚI THIỆU VỀ SURICATA**

Suricata là một hệ thống IDS/IPS mã nguồn mở, được phát triển bởi Open Information Security Foundation (OISF).  
**Những ưu điểm nổi bật của Suricata:**

* **Hiệu suất cao:** Nhờ kiến trúc đa luồng, Suricata có khả năng xử lý lưu lượng mạng tốc độ cao.
* **Hỗ trợ đa dạng giao thức:** Phân tích và ghi log các giao thức như TCP, UDP, HTTP, DNS, TLS...
* **Tích hợp dễ dàng:** Có thể kết hợp với các công cụ giám sát và phân tích như Elastic Stack, Zeek, MISP.
* **Tính năng phong phú:** Hỗ trợ cả chế độ IDS (phát hiện) và IPS (ngăn chặn), cùng khả năng ghi log chi tiết giúp phục vụ việc phân tích sau sự cố.

Suricata không chỉ phát hiện các mối đe dọa theo luật định trước mà còn có khả năng phân tích dữ liệu dựa trên hành vi, từ đó nâng cao hiệu quả trong việc bảo vệ hệ thống mạng.

**4. KIẾN TRÚC CỦA SURICATA**

Suricata được xây dựng với cấu trúc phân tầng, mỗi tầng đảm nhiệm một chức năng cụ thể, giúp tối ưu hóa việc xử lý và phân tích lưu lượng mạng.

**4.1 Capture Engine**

Capture Engine là thành phần chịu trách nhiệm bắt các gói tin đi qua giao diện mạng.

* **Chức năng:** Sử dụng thư viện PCAP hoặc AF\_PACKET để thu thập dữ liệu.
* **Yêu cầu:** Đảm bảo có khả năng xử lý lưu lượng lớn mà không bị mất gói tin.

**4.2 Decode Engine**

Decode Engine giải mã các gói tin được thu thập, chuyển đổi chúng thành các thông tin có thể phân tích.

* **Chức năng:** Phân tích các giao thức và trích xuất thông tin cần thiết từ các gói tin.
* **Ưu điểm:** Hỗ trợ nhiều giao thức khác nhau, từ TCP/IP cho đến các giao thức ứng dụng như HTTP, SMTP,...

**4.3 Preprocessing Engine**

Preprocessing Engine xử lý trước các gói tin nhằm chuẩn bị cho quá trình phân tích chính.

* **Các tác vụ chính:**
  + Phân mảnh IP: Xử lý các gói tin bị phân mảnh.
  + Tái tạo luồng TCP: Gom các gói tin của cùng một kết nối để phân tích liên tục.
  + Loại bỏ các gói tin không cần thiết, giảm thiểu tải cho hệ thống phân tích.

**4.4 Rule Engine và Detection Engine**

Rule Engine chịu trách nhiệm so sánh các gói tin đã được xử lý với các luật (rules) đã được định nghĩa.

* **Cách hoạt động:** Khi một gói tin phù hợp với điều kiện của luật, hệ thống sẽ kích hoạt cảnh báo hoặc hành động ngăn chặn.
* **Detection Engine:** Xử lý các sự kiện phát sinh từ việc so sánh và quyết định mức độ nghiêm trọng của mối đe dọa.

**4.5 Output và Logging**

Suricata ghi nhận các sự kiện, cảnh báo và lưu log vào các file hoặc hệ thống quản lý log tập trung.

* **Các định dạng log:** JSON, fast.log, eve.json…
* **Ứng dụng:** Dễ dàng tích hợp với các công cụ phân tích như Elastic Stack để trực quan hóa và phân tích sâu hơn.

*Trang 4 kết thúc phần mô tả kiến trúc của Suricata.*

**5. CÀI ĐẶT VÀ CẤU HÌNH SURICATA**

Việc cài đặt và cấu hình Suricata là bước đầu tiên để triển khai hệ thống IDS/IPS hiệu quả. Dưới đây là hướng dẫn chi tiết cho các hệ điều hành phổ biến:

**5.1 Cài đặt trên Ubuntu/Debian**

**Bước 1:** Cập nhật hệ thống

bash

Sao chépChỉnh sửa

sudo apt update && sudo apt upgrade -y

**Bước 2:** Cài đặt Suricata

bash

Sao chépChỉnh sửa

sudo apt install suricata -y

**Bước 3:** Kiểm tra phiên bản cài đặt

bash

Sao chépChỉnh sửa

suricata --build-info

**5.2 Cài đặt trên CentOS/RHEL**

**Bước 1:** Cài đặt EPEL repository

bash

Sao chépChỉnh sửa

sudo yum install epel-release -y

**Bước 2:** Cài đặt Suricata

bash

Sao chépChỉnh sửa

sudo yum install suricata -y

**Bước 3:** Xác nhận cài đặt

bash

Sao chépChỉnh sửa

suricata --build-info

**5.3 Cấu hình file suricata.yaml**

File cấu hình chính của Suricata nằm ở /etc/suricata/suricata.yaml.  
**Một số điểm cần lưu ý:**

* **Giao diện mạng:** Xác định giao diện mà Suricata sẽ giám sát (ví dụ: eth0, ens33…).
* **Quy tắc (Rules):** Đường dẫn tới thư mục chứa các file rules.
* **Log & Output:** Cấu hình định dạng log (JSON, fast.log…) và các chế độ ghi log.
* **Chế độ hoạt động:** IDS hoặc IPS.
  + Ví dụ: Để chạy chế độ IDS, bạn sử dụng lệnh:

bash

Sao chépChỉnh sửa

sudo suricata -c /etc/suricata/suricata.yaml -i eth0

Việc cấu hình chính xác sẽ giúp Suricata vận hành ổn định và phát hiện các mối đe dọa một cách hiệu quả.

*Trang 7 kết thúc phần cài đặt và cấu hình Suricata.*

**6. TẠO LUẬT PHÁT HIỆN TẤN CÔNG TRONG SURICATA**

Một trong những ưu điểm lớn của Suricata là khả năng mở rộng và tùy chỉnh các luật phát hiện tấn công.  
Các luật này giúp xác định hành vi bất thường hoặc độc hại dựa trên các mẫu và dấu hiệu đã được định nghĩa.

**6.1 Cấu trúc cơ bản của một rule**

Một rule trong Suricata thường có cấu trúc như sau:

shell

Sao chépChỉnh sửa

alert <protocol> <source\_ip> <source\_port> -> <destination\_ip> <destination\_port> (msg:"Thông điệp cảnh báo"; sid:<ID>; rev:<revision>; ...)

**Ví dụ:**

shell

Sao chépChỉnh sửa

alert tcp any any -> any 80 (msg:"Phát hiện truy cập HTTP bất thường"; sid:1000001; rev:1;)

**6.2 Ví dụ thực tế**

Giả sử ta muốn phát hiện các kết nối HTTP với dấu hiệu bất thường, ta có thể tạo rule như:

shell

Sao chépChỉnh sửa

alert http any any -> any 80 (msg:"HTTP Request chứa từ khóa độc hại"; content:"<script>"; sid:1000002; rev:1;)

Trong rule trên:

* **alert http:** Kiểm tra lưu lượng giao thức HTTP.
* **any any -> any 80:** Áp dụng cho mọi kết nối từ bất kỳ IP và port nào đến cổng 80.
* **msg:** Thông điệp cảnh báo khi rule được kích hoạt.
* **content:** Điều kiện tìm kiếm nội dung trong gói tin.
* **sid:** Số định danh duy nhất cho rule.
* **rev:** Phiên bản của rule.

**6.3 Cập nhật và quản lý ruleset**

Suricata hỗ trợ cập nhật ruleset từ các nguồn bên ngoài như Emerging Threats.  
**Cập nhật tự động:**

bash

Sao chépChỉnh sửa

sudo suricata-update

Việc duy trì một ruleset cập nhật là yếu tố quan trọng giúp hệ thống luôn được bảo vệ trước các mối đe dọa mới.

*Trang 9 kết thúc phần tạo luật phát hiện tấn công.*

**7. XÂY DỰNG 3 KỊCH BẢN PHÁT HIỆN TẤN CÔNG**

Trong phần này, chúng ta xây dựng ba kịch bản cụ thể sử dụng Suricata để phát hiện các loại tấn công thường gặp.

**7.1 Kịch bản 1: Phát hiện Port Scanning**

**Mục tiêu:**  
Phát hiện hành vi quét cổng (port scanning) – một kỹ thuật phổ biến được kẻ tấn công sử dụng để tìm kiếm các cổng mở trên hệ thống.

**Cách thực hiện:**

* **Luật mẫu:**

alert tcp any any -> any any (msg:"Phát hiện Port Scanning"; detection\_filter: track by\_src, count 20, seconds 10; sid:2000001; rev:1;)

* **Giải thích:**
  + Luật này cảnh báo nếu từ một IP gửi 20 kết nối trong vòng 10 giây đến các cổng khác nhau.
  + Cấu hình detection\_filter giúp giảm số lượng cảnh báo giả và tập trung vào những hành vi quét nghiêm trọng.

**7.2 Kịch bản 2: Phát hiện SQL Injection**

**Mục tiêu:**  
Nhận diện các cuộc tấn công chèn SQL (SQL Injection) thông qua các yêu cầu HTTP độc hại.

**Cách thực hiện:**

* **Luật mẫu:**

alert http any any -> any 80 (msg:"Phát hiện SQL Injection"; flow: to\_server, established; content:"UNION SELECT"; nocase; pcre:"/(\%27)|(\')|(\-\-)|(\%23)|(#)/i"; sid:2000002; rev:1;)

* **Giải thích:**
  + Luật quét nội dung chứa từ khóa “UNION SELECT” và các ký tự đặc biệt thường dùng trong tấn công SQL Injection.
  + Sử dụng pcre (Regular Expression) để phát hiện các mẫu tấn công phức tạp hơn.

**7.3 Kịch bản 3: Phát hiện Distributed Denial of Service (DDoS)**

**Mục tiêu:**  
Nhận diện tình trạng tấn công DDoS khi lưu lượng mạng tăng đột biến từ nhiều nguồn khác nhau.

**Cách thực hiện:**

* **Luật mẫu:**

shell

Sao chépChỉnh sửa

alert ip any any -> any any (msg:"Phát hiện tấn công DDoS"; detection\_filter: track by\_dst, count 100, seconds 5; sid:2000003; rev:1;)

* **Giải thích:**
  + Luật này sẽ kích hoạt cảnh báo nếu đích nhận được hơn 100 gói tin trong vòng 5 giây.
  + Phương pháp detection\_filter theo dõi số lượng gói tin đến cùng một địa chỉ đích (by\_dst) để phát hiện tấn công từ nhiều nguồn.

*Trang 11 kết thúc phần xây dựng kịch bản phát hiện tấn công.*

**8. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN TƯƠNG LAI**

Qua báo cáo này, chúng ta đã có cái nhìn tổng quan và chi tiết về Suricata – từ kiến trúc, cài đặt, cấu hình, đến việc tạo luật và xây dựng các kịch bản phát hiện tấn công.  
**Một số kết luận chính:**

* Suricata là công cụ mạnh mẽ, hiệu quả với khả năng xử lý đa luồng và hỗ trợ nhiều giao thức.
* Việc cấu hình chính xác và duy trì ruleset cập nhật đóng vai trò then chốt trong việc đảm bảo hiệu quả phát hiện tấn công.
* Các kịch bản phát hiện tấn công như Port Scanning, SQL Injection và DDoS là những ví dụ cụ thể minh họa khả năng linh hoạt của Suricata.

**Hướng phát triển tương lai:**

* **Tích hợp với hệ thống giám sát tập trung:** Kết hợp với Elastic Stack, SIEM để thu thập, phân tích log và phản ứng kịp thời.
* **Nâng cao trí tuệ nhân tạo:** Sử dụng Machine Learning để tự động phát hiện các mẫu tấn công chưa được biết đến.
* **Cải tiến hiệu suất:** Tối ưu hóa quy trình xử lý dữ liệu cho lưu lượng mạng ngày càng tăng.

Suricata không chỉ là một công cụ IDS/IPS mạnh mẽ mà còn là nền tảng cho các giải pháp an ninh mạng tiên tiến trong tương lai.

*Trang 14 kết thúc phần kết luận và hướng phát triển.*

**9. TÀI LIỆU THAM KHẢO**

1. **Suricata Official Documentation:**  
   <https://suricata-ids.org/>
2. **Suricata User Guide và Wiki:**  
   <https://github.com/OISF/suricata>
3. **Emerging Threats Ruleset:**  
   https://rules.emergingthreats.net/
4. **Các bài viết chuyên sâu về IDS/IPS và Suricata trên AdminVietnam.org.**
5. **Slideshare và Studocu:** Các tài liệu tham khảo từ cộng đồng học thuật và chuyên gia bảo mật.

*Trang 15 kết thúc tài liệu tham khảo.*