**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

-----

**Trần Đức Mạnh**

# NGHIÊN CỨU PHẦN MỀM SURICATA PHÁT HIỆN XÂM NHẬP TRONG MÔI TRƯỜNG MẠNG IOT CHO DOANH NGHIỆP VỪA VÀ NHỎ

**Chuyên ngành: Hệ thống thông tin**

**Mã số: 8.48.01.04**

**TÓM TẮT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ**

HÀ NỘI - 2025

Đề án tốt nghiệp được hoàn thành tại:

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

Người hướng dẫn khoa học: PGS. TSKH. Hoàng Đăng Hải

Phản biện 1:……

Phản biện 2:……

Đề án tốt nghiệp sẽ được bảo vệ trước Hội đồng chấm đề án tốt nghiệp thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: …….giờ…….ngày…….tháng……năm…….

Có thể tìm hiểu đề án tốt nghiệp tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn Thông

# MỞ ĐẦU

## 1. Lý do chọn đề tài

Ngày nay, công nghệ viễn thông đang phát triển rất nhanh. Internet băng thông rộng ngày càng phổ biến với giá thành, chi phí rẻ. Tất cả những điều đó đang tạo điều kiện hoàn hảo cho sự phát triển của Internet of Things (IoT – Internet vạn vật). Rất nhiều doanh nghiệp, công ty đã áp dụng mạng IoT để nâng cao hiệu quả sản xuất, kinh doanh. Không những các tập đoàn, công ty lớn mà ngay cả các doanh nghiệp vừa và nhỏ cũng đang từng bước triển khai sử dụng mạng IoT.

Tuy nhiên, đi kèm với sự bùng nổ của mạng IoT, những nguy cơ về bảo mật sẽ ngày càng lớn. Đối với các doanh nghiệp lớn, việc triển khai các hệ thống phát hiện xâm nhập mạng (IDS - Intrusion Detection System) đã là phổ biến. Nhưng mạng IoT trong các doanh nghiệp vừa và nhỏ thường được đầu tư với chi phí ít, hệ thống bảo vệ thường không đủ mạnh để đáp ứng các yêu cầu về bảo mật và an toàn thông tin. Do vậy, một yêu cầu thực tiễn đặt ra là cần xây dựng một hệ IDS cỡ nhỏ phù hợp với mạng IoT của các doanh nghiệp vừa và nhỏ.

Đề án này chọn doanh nghiệp vừa và nhỏ vì đây là những doanh nghiệp đang đóng một vai trò rất quan trọng trong phát triển kinh tế quốc gia. Tuy nhiên, các doanh nghiệp này còn có mức đầu tư vào an toàn bảo mật thông tin thấp, sẽ kéo theo các lỗ hổng bảo mật, mất nguy cơ an toàn thông tin rất lớn. Do vậy, một nhu cầu thực tế đặt ra là cần phát triển và triển khai các hệ thống IDS cỡ nhỏ song hiệu quả, phù hợp cho hệ thống mạng của các doanh nghiệp vừa và nhỏ.

Phần mềm Suricata là một hệ IDS cỡ nhỏ, là một phần mềm mã nguồn mở đa nền tảng song có hiệu suất cao, dễ dàng tương thích với các thành phần an ninh mạng hiện có. Kết quả thực hiện đề án tốt nghiệp là một giải pháp sử dụng mã nguồn mở, có chi phí đầu tư thấp nhưng đáp ứng được các yêu cầu, thách thức về bảo mật, an toàn thông tin cho môi trường mạng IoT tại doanh nghiệp vừa và nhỏ.

Nội dung của đề án được trình bày trong ba chương nội dung chính như sau:

**Chương 1: Mạng IoT trong doanh nghiệp vừa và nhỏ**

Giới thiệu về mạng IoT, các khái niệm và đặc trưng trong mạng này. Các thiết bị cơ bản có trong mạng IoT cho doanh nghiệp vừa và nhỏ, những liên kết, giao tiếp của thiết bị trong mạng, những tác nhân lỗ hổng và hạn chế hiện có trong mạng này..

**Chương 2: Hệ phát hiện xâm nhập và phần mềm Suricata**

Trình bày tổng quan về hệ phát hiện xâm nhập, phần mềm Suricata, các công nghệ được áp dụng, các luật trong Suricata.

**Chương 3: Xây dựng hệ IDS với Suricata cho mạng IoT trong doanh nghiệp vừa và nhỏ**

Chương này tập trung vào việc xây dựng một hệ thống IDS sử dụng Suricata nhằm tăng cường bảo mật cho mạng IoT của các doanh nghiệp vừa và nhỏ. Nội dung bao gồm các bước cài đặt, cấu hình, thử nghiệm và đánh giá hiệu quả của hệ thống, từ đó đề xuất các giải pháp tối ưu nhằm tăng cường bảo mật mạng IoT trong môi trường doanh nghiệp.

# CHƯƠNG 1. MẠNG IOT TRONG DOANH NGHIỆP VỪA VÀ NHỎ

## 1.1 Đặc trưng của doanh nghiệp vừa và nhỏ

Doanh nghiệp vừa và nhỏ đóng vai trò quan trọng trong nền kinh tế toàn cầu. Với quy mô giới hạn, các doanh nghiệp vừa và nhỏ thường có tính linh hoạt cao, dễ dàng thích ứng với các thay đổi của thị trường và ứng dụng công nghệ mới để nâng cao năng suất, trong đó Internet of Things (IoT) đóng vai trò quan trọng trong quá trình chuyển đổi số.

## 1.2 Khái quát về mạng IoT

### *1.2.1 Khái niệm*

Internet of Things (IoT) là một hệ thống các đối tượng vật lý được kết nối với nhau thông qua mạng Internet, cho phép chúng thu thập, truyền tải và trao đổi dữ liệu một cách tự động mà không cần sự can thiệp trực tiếp của con người.

### *1.2.2 Đặc trưng của mạng IoT*

- *Tính không đồng nhất*
- *Tính kết nối liên thông*
- *Khả năng thay đổi linh hoạt và tự động hoá*
- *Thu thập dữ liệu lớn*
- *Quy mô lớn và tính phân tán*
- *Tính mở rộng*
- *Bảo mật và quyền riêng tư*

### *1.2.3 Mạng IoT trong doanh nghiệp vừa và nhỏ*

*1.2.3.1 Kiến trúc và thiết bị*

- ***Tầng cảm biến (Sensing Layer)***
- ***Tầng mạng (Network Layer)***
- ***Tầng xử lý dữ liệu (Data Processing Layer)***
- ***Tầng ứng dụng (Application Layer)***

*1.2.3.2 Các giao tiếp, liên kết trong mạng IoT của doanh nghiệp vừa và nhỏ*

- ***Giao tiếp thiết bị - thiết bị (D2D - Device-to-Device):*** Cho phép các thiết bị IoT trao đổi dữ liệu trực tiếp với nhau mà không cần qua trung gian như gateway hoặc máy chủ đám mây.
- ***Giao tiếp Thiết bị - Gateway (D2G - Device-to-Gateway):*** Các thiết bị đầu cuối gửi dữ liệu đến một Gateway trung gian trước khi truyền tiếp lên hệ thống đám mây hoặc máy chủ xử lý.

- ***Giao tiếp Thiết bị - Đám mây (D2C - Device-to-Cloud):*** Các thiết bị IoT gửi dữ liệu trực tiếp lên nền tảng đám mây để lưu trữ, phân tích và xử lý.

## 1.3 Những nguy cơ an toàn thông tin trong mạng IoT của doanh nghiệp vừa và nhỏ

Các doanh nghiệp vừa và nhỏ thường thiếu nguồn lực tài chính, nhân sự chuyên môn và chiến lược bảo mật rõ ràng, điều này khiến họ dễ trở thành mục tiêu của các cuộc tấn công mạng.

### *1.3.1 Lỗ hổng bảo mật trên thiết bị IoT*

Các doanh nghiệp vừa và nhỏ cần lựa chọn thiết bị từ các nhà cung cấp uy tín, cập nhật firmware và thực hiện đánh giá bảo mật định kỳ.

### *1.3.2 Sử dụng mật khẩu mặc định hoặc mật khẩu yếu*

Trong các doanh nghiệp vừa và nhỏ khi việc quản lý bảo mật thường chưa được hệ thống hóa, thiếu chính sách kiểm soát truy cập và tiêu chuẩn hóa mật khẩu khiến hệ thống dễ bị tổn thương trước các hình thức tấn công.

### *1.3.3 Thiếu khả năng cập nhật và vá lỗi bảo mật*

Phần lớn các thiết bị IoT phù hợp với các doanh nghiệp vừa và nhỏ, không hỗ trợ tính năng cập nhật hoặc nhà sản xuất ngừng cung cấp bản vá bảo mật sau một thời gian ngắn.

### *1.3.4 Tấn công bằng phần mềm độc hại*

Các doanh nghiệp vừa và nhỏ cần triển khai các giải pháp phòng chống mã độc, hệ thống giám sát an ninh mạng, phát hiện xâm nhập và sao lưu dữ liệu định kỳ.

### *1.3.5 Thiếu mã hóa dữ liệu trong truyền thông IoT*

Các doanh nghiệp nhỏ thường xem nhẹ vấn đề này, nên dễ bị lợi dụng để phá hoại hoặc cạnh tranh không lành mạnh. Việc sử dụng các giao thức mã hóa như là điều cần thiết.

### *1.3.6 Nhận thức bảo mật còn hạn chế*

Cần có các chương trình đào tạo nhận thức bảo mật định kỳ, đồng thời xây dựng văn hóa an toàn thông tin trong tổ chức.

### *1.3.7 Kết luận*

Hệ thống IoT trong doanh nghiệp vừa và nhỏ đang đối mặt với nhiều nguy cơ an toàn thông tin đến từ cả khía cạnh kỹ thuật và con người, cần triển khai chiến lược bảo mật toàn diện.

### 1.4 Nhu cầu triển khai hệ thống phát hiện xâm nhập trong mạng IoT của doanh nghiệp vừa và nhỏ

Việc triển khai mạng IoT trong các doanh nghiệp vừa và nhỏ cũng đồng thời mở rộng bề mặt tấn công của hệ thống. Nhu cầu phát hiện và cảnh báo các hành vi xâm nhập trái phép trở nên cấp thiết. Việc đầu tư vào IDS với mức độ phù hợp, có khả năng tùy biến và tích hợp cao sẽ đóng vai trò quan trọng trong việc đảm bảo tính an toàn, sẵn sàng và liên tục của hệ thống.

### 1.5 Kết luận chương

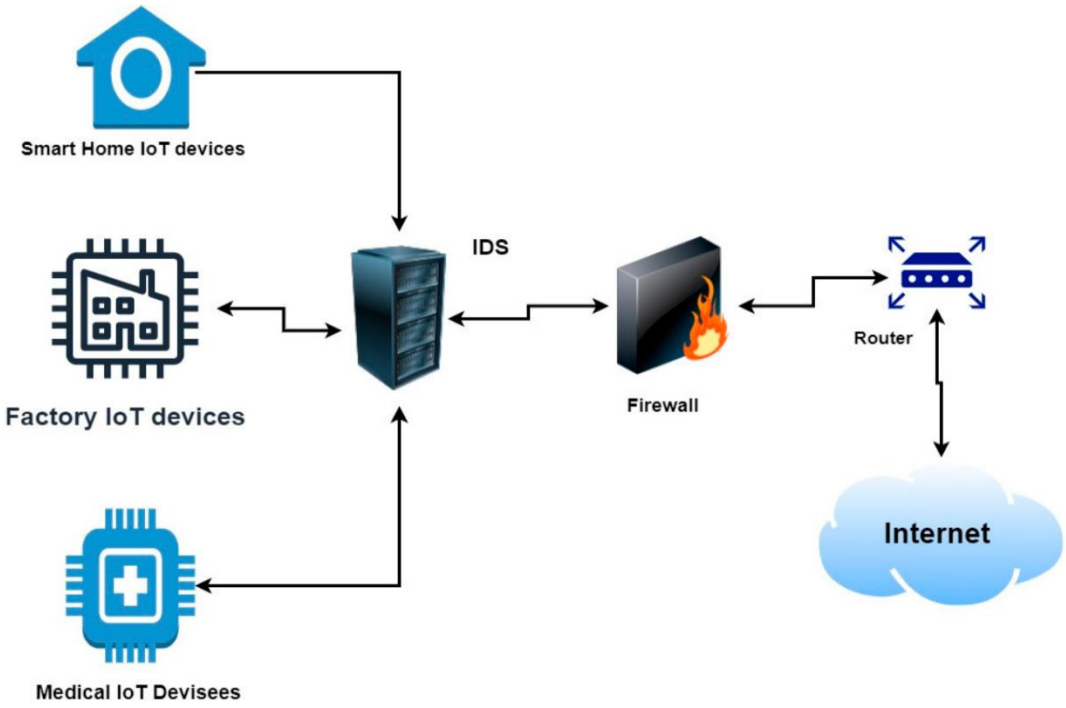
Chương này đã giới thiệu tổng quan về mạng IoT trong doanh nghiệp vừa và nhỏ, bao gồm các khái niệm cơ bản, đặc trưng của hệ thống IoT cũng như các nguy cơ về an toàn thông tin.

## CHƯƠNG 2. HỆ PHÁT HIỆN XÂM NHẬP VÀ PHẦN MỀM SURICATA

### 2.1 Tổng quan về hệ phát hiện xâm nhập

#### *2.1.1 Khái niệm*

Hệ thống phát hiện xâm nhập – IDS (Intrusion Detection System) là một hệ thống phần cứng hoặc phần mềm có nhiệm vụ giám sát các sự kiện đáng ngờ, những hành vi xâm nhập trái phép hay những hành động khai thác nguồn tài nguyên của hệ thống một cách bất hợp pháp.




*Hình 1: Mô hình IDS trong hệ thống mạng*

### *2.1.2 Các thành phần và chức năng*

Hệ thống phát hiện xâm nhập gồm 3 thành phần chính: Thành phần thu thập gói tin (Information Collection); Thành phần phát hiện tấn công (Detection); Thành phần phản hồi (Response)

### *2.1.3 Cơ chế hoạt động*

Hệ thống phát hiện xâm nhập hoạt động dựa trên việc giám sát lưu lượng mạng và phân tích dữ liệu để xác định các dấu hiệu xâm nhập hoặc hoạt động bất thường.

Quy trình hoạt động của IDS có thể được mô tả qua các bước sau:

***Bước 1: Thu thập gói tin***

Hệ thống IDS sử dụng các cảm biến được đặt tại các điểm chiến lược trong mạng để thu thập dữ liệu đảm bảo có thể giám sát toàn bộ lưu lượng mạng ra vào.

***Bước 2: Giải mã và phân tích gói tin***

IDS tiến hành giải mã và trích xuất các trường thông tin quan trọng của gói tin, sau đó được đối chiếu với các mẫu tấn công đã biết hoặc được đánh giá dựa trên hành vi bất thường để xác định nguy cơ xâm nhập.

***Bước 3: Phát hiện mối đe dọa***

IDS sử dụng hai phương pháp chính để xác định các cuộc tấn công:

*Phát hiện dựa trên dấu hiệu (Signature-based Detection):* Nếu phát hiện sự tương đồng giữa gói tin với một cơ sở dữ liệu chứa các mẫu tấn công đã biết (attack signatures), IDS sẽ tạo cảnh báo.

*Phát hiện dựa trên hành vi bất thường (Anomaly-based Detection): Nếu* lưu lượng mạng có sự sai lệch đáng kể so với một mô hình hành vi chuẩn (baseline model), IDS sẽ coi đó là một dấu hiệu xâm nhập và tạo cảnh báo.

***Bước 4: Tạo cảnh báo và thông báo sự cố***

Khi phát hiện dấu hiệu tấn công, IDS sẽ gửi cảnh báo đến hệ thống giám sát trung tâm.

***Bước 5: Phản hồi và lưu trữ dữ liệu sự cố***

Khi nhận được cảnh báo, hệ thống sẽ thực hiện các biện pháp phản hồi theo chính sách bảo mật đã được thiết lập.

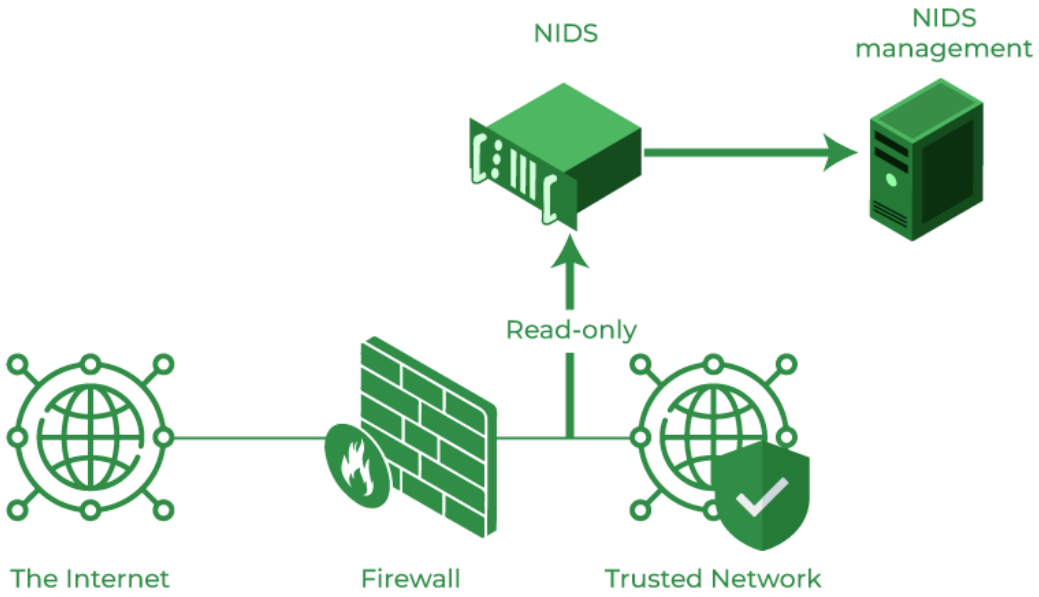
***Bước 6: Phân tích và đánh giá mối đe dọa***

IDS sẽ so sánh dữ liệu mới thu thập với các cuộc tấn công trước đó nhằm xác định liệu đây có phải là một cuộc tấn công thực sự hay chỉ là cảnh báo giả (false positive).

### *2.1.4 Phân loại*

*2.1.4.1 Hệ thống phát hiện xâm nhập dựa trên mạng – NIDS*

Là một giải pháp bảo mật được thiết kế để giám sát và phân tích lưu lượng mạng nhằm phát hiện phát hiện các hành vi xâm nhập trái phép hay các hoạt động độc hại tới hệ thống thông tin.




*Hình 2:Mô hình NIDS*

Hệ thống phát hiện xâm nhập dựa trên mạng có những ưu điểm sau:

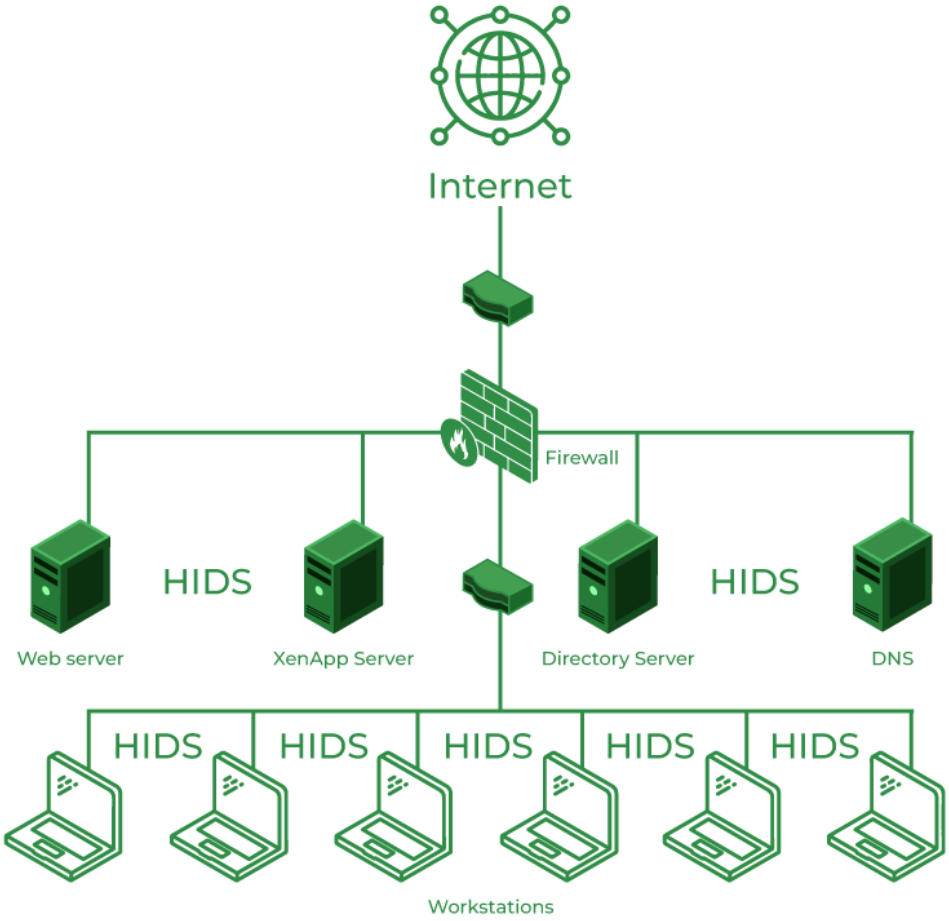
*Giám sát lưu lượng mạng theo thời gian thực*
*Bảo vệ nhiều thiết bị cùng lúc*
*Phát hiện tấn công từ bên ngoài*
*Không gây ảnh hưởng đến hiệu suất máy chủ*

Tuy nhiên, bên cạnh những ưu điểm, NIDS cũng tồn tại những hạn chế nhất định:

*Khó phát hiện tấn công từ bên trong*
*Không thể giám sát lưu lượng đã mã hóa*
*Dễ bị lách luật bởi các kỹ thuật tấn công nâng cao*
*Cần được cấu hình và cập nhật thường xuyên*

*2.1.4.2 Hệ thống phát hiện xâm nhập dựa trên máy chủ - HIDS*

Là một giải pháp bảo mật được thiết kế nhằm giám sát và phân tích các hoạt động diễn ra trên thiết bị đầu cuối để phát hiện và phản ứng kịp thời với các mối đe dọa an ninh mạng.




*Hình 3: Mô hình HIDS*

Hệ thống phát hiện xâm nhập dựa trên thiết bị đầu cuối có những ưu điểm nổi bật sau:

*Giám sát chi tiết từng thiết bị*
*Có khả năng phát hiện tấn công mã hóa*
*Phát hiện tấn công zero-day và các kỹ thuật lẩn tránh*
*Phân tích nhật ký hệ thống và hỗ trợ điều tra bảo mật*

Bên cạnh những ưu điểm, HIDS có những điểm hạn chế như sau:

*Không giám sát được toàn bộ hệ thống mạng*
*Tiêu tốn tài nguyên hệ thống*
*Dễ bị vô hiệu hóa bởi kẻ tấn công*

*Yêu cầu cấu hình và quản lý chặt chẽ*

*2.1.4.3 So sánh*

*Bảng 1: Bảng so sánh NIDS và HIDS*

| Tiêu chí | NIDS (Network-based IDS) | HIDS (Host-based IDS) |
|---|---|---|
| Phạm vi giám sát | Giám sát toàn bộ lưu lượng mạng | Theo dõi hoạt động trên từng thiết bị |
| Cơ chế hoạt động | Phân tích các gói tin truyền qua mạng, phát hiện tấn công từ bên ngoài | Giám sát tệp tin, nhật ký hệ thống, quy trình chạy trên thiết bị |
| Phát hiện tấn công nội bộ | Không thể phát hiện các hành vi nguy hiểm từ người dùng hợp pháp hoặc tấn công nội bộ | Hiệu quả trong việc phát hiện hành vi đáng ngờ từ bên trong hệ thống |
| Phát hiện tấn công bên ngoài | Hiệu quả trong phát hiện tấn công từ mạng bên ngoài như DDoS, quét cổng, khai thác lỗ hổng | Hạn chế, chỉ phát hiện khi tấn công đã xâm nhập vào máy chủ |
| Ảnh hưởng đến hiệu suất hệ thống | Không ảnh hưởng đến hiệu suất máy chủ | Có thể tiêu tốn tài nguyên CPU, bộ nhớ của thiết bị giám sát |
| Khả năng bị tấn công | Có thể bị vượt qua bằng các kỹ thuật lẩn tránh (phân mảnh gói tin, tấn công băng thông thấp) | Có thể bị vô hiệu hóa nếu kẻ tấn công có quyền quản trị hệ thống |
| Phát hiện các cuộc tấn công Zero-day | Hạn chế trong việc phát hiện các cuộc tấn công chưa có dấu hiệu | Có khả năng phát hiện các hành vi bất thường, kể cả chưa có dấu hiệu |
| Khả năng cung cấp bằng chứng điều tra | Giới hạn, chỉ cung cấp thông tin về lưu lượng mạng | Giới hạn, chỉ cung cấp thông tin về lưu lượng mạng |

| | | |
|---|---|---|
| Cấu hình và bảo trì | Cần cập nhật danh sách dấu hiệu thường xuyên để duy trì hiệu quả phát hiện | Cần hiệu chỉnh cẩn thận để giảm thiểu cảnh báo sai |
| Tính phù hợp | Phù hợp với các tổ chức cần giám sát lưu lượng mạng trên diện rộng | Phù hợp với các hệ thống yêu cầu giám sát chi tiết trên từng thiết bị |

## 2.2 Phương pháp phát hiện xâm nhập

### *2.2.1 Khái niệm về xâm nhập mạng*

Xâm nhập mạng là hành vi truy cập trái phép vào hệ thống mạng.

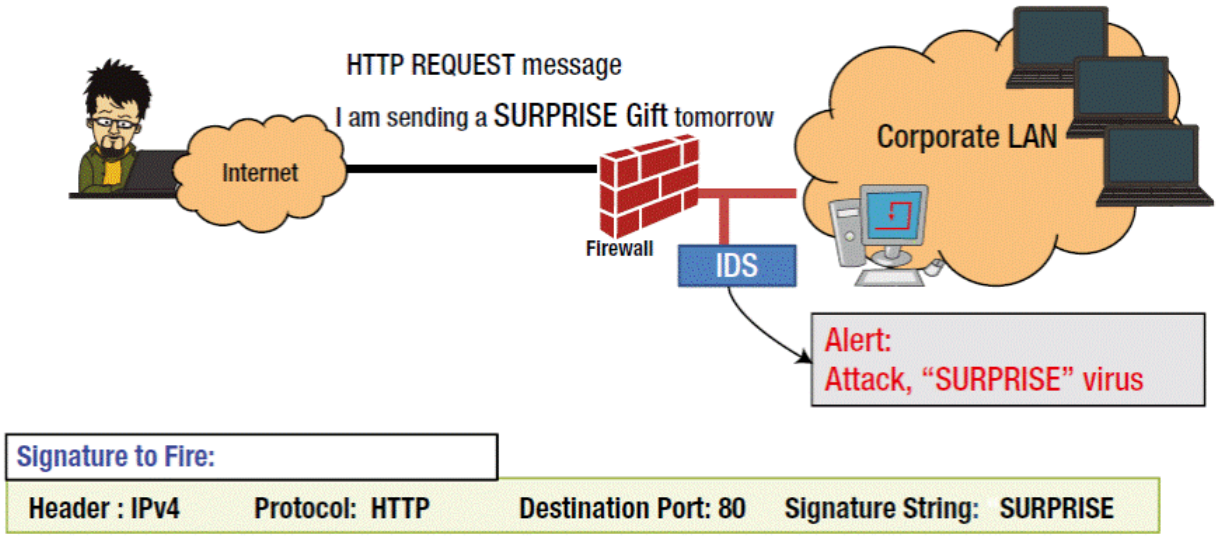
Việc triển khai các biện pháp bảo mật, kết hợp giữa phòng ngừa và phát hiện xâm nhập, là yếu tố quan trọng giúp các tổ chức bảo vệ hệ thống của mình trước những mối đe dọa ngày càng tinh vi.

### *2.2.2 Phát hiện xâm nhập mạng*

Phát hiện xâm nhập là quá trình giám sát, phân tích và nhận diện các hành vi truy cập bất thường hoặc trái phép trong hệ thống được phân loại thành hai nhóm chính.

#### *2.2.2.1 Phát hiện dựa trên dấu hiệu*

So sánh lưu lượng mạng với một tập hợp các mẫu tấn công đã biết được lưu trữ trong cơ sở dữ liệu dấu hiệu. Nếu trùng khớp với một mẫu tấn công sẽ đưa ra cảnh báo hoặc thực hiện các biện pháp ngăn chặn.




*Hình 4: Hình minh họa phát hiện xâm nhập dựa trên dấu hiệu*

Ưu điểm của phương pháp phát hiện dựa trên dấu hiệu:

*Độ chính xác cao với các mối đe dọa đã biết*
*Tỷ lệ cảnh báo sai thấp*
*Dễ triển khai và tối ưu hóa*

Hạn chế của phương pháp phát hiện dựa trên dấu hiệu:

*Không thể phát hiện các mối đe dọa chưa được ghi nhận*
*Dễ bị đánh lừa bởi các biến thể của tấn công*
*Phụ thuộc vào việc cập nhật cơ sở dữ liệu dấu hiệu*
*Giảm hiệu suất theo thời gian*

*2.2.2.2 Phát hiện dựa trên bất thường*

Nhận diện các mối đe dọa chưa từng được ghi nhận bằng cách xác định các hành vi bất thường trong hệ thống.

Ưu điểm của phương pháp phát hiện dựa trên bất thường:

*Phát hiện được các cuộc tấn công chưa từng được ghi nhận*
*Có khả năng giám sát hành vi trong thời gian thực*
*Không cần cập nhật dấu hiệu liên tục*

Hạn chế của phương pháp phát hiện dựa trên bất thường:

*Tỷ lệ báo động giả cao*
*Cần một giai đoạn học tập dài*
*Chi phí tính toán cao*

## 2.3 Phần mềm Suricata

### *2.3.1 So sánh một số công cụ phát hiện xâm nhập mạng*

Hiện nay, có nhiều công cụ IDS được phát triển để giám sát và ngăn chặn các cuộc tấn công mạng mã nguồn mở phổ biến nhất bao gồm: Snort, Zeek, Suricata

*Bảng 2: Bảng so sánh Snort, Suricata và Zeek*

| Tiêu chí | Snort | Suricata | Zeek |
|---|---|---|---|
| Phương pháp phát hiện | Dựa trên dấu hiệu | Dựa trên cả dấu hiệu và hành vi bất thường | Dựa trên hành vi bất thường |
| Hỗ trợ đa luồng | Không (Snort 2.x) | Có | Có |

| | | | |
|---|---|---|---|
| Hiệu suất xử lý | Trung bình | Cao | Cao nhưng yêu cầu CPU mạnh |
| Khả năng mở rộng | Tốt | Rất tốt | Rất tốt |
| Dễ cấu hình | Dễ dàng | Trung bình | Khó |
| Ghi nhật ký lưu lượng | Có nhưng hạn chế | Có | Rất mạnh |
| Trích xuất tệp từ lưu lượng | Không | Có | Có |
| Tích hợp với SIEM | Có nhưng giới hạn | Có | Rất tốt |
| Khả năng tùy chỉnh | Cao | Cao | Rất cao (hỗ trợ scripting) |
| Hỗ trợ giao thức IoT | Hạn chế | MQTT, CoAP, HTTP, TLS | Chỉ ghi log, không phân tích chuyên sâu |
| Kiểm tra gói sâu (Deep Packet Inspection) | Không | Có | Không |

Suricata là lựa chọn tối ưu.

### *2.3.2 Tóm tắt về phần mềm Suricata*

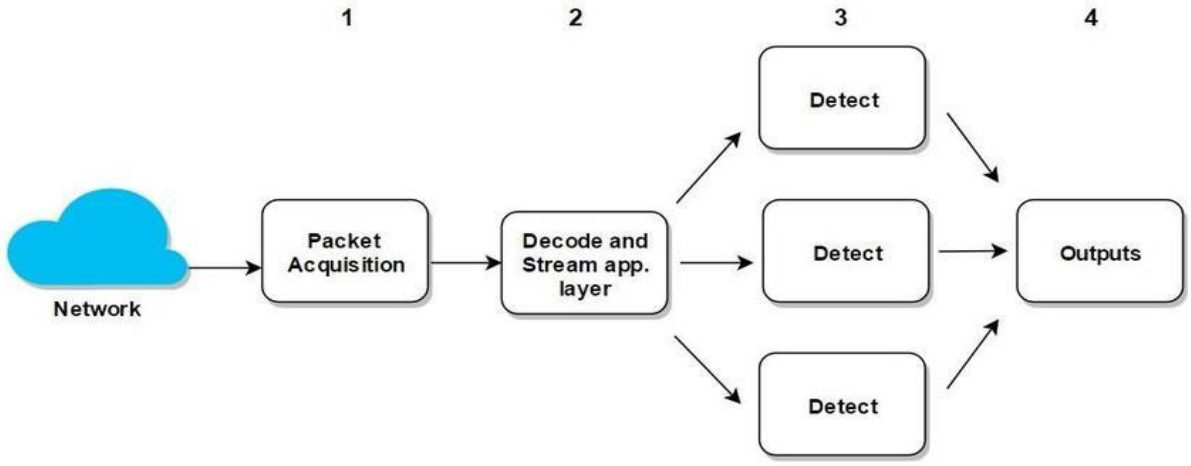
Suricata là một hệ thống phát hiện và ngăn chặn xâm nhập mạng (Network IDS/IPS) và công cụ giám sát an ninh mạng (Network Security Monitoring - NSM) hiệu suất cao. Các công nghệ chính bao gồm:

*Xử lý đa luồng (Multi-threading): T*ận dụng tối đa tài nguyên CPU để xử lý lưu lượng lớn theo thời gian thực.
*Deep Packet Inspection (DPI):* Khả năng phân tích sâu các gói tin.
*Hỗ trợ nhiều giao thức mạng:* Hoạt động trên các giao thức IP cơ bản, hỗ trợ HTTP, DNS, TLS, FTP, SSH, MQTT, CoAP và các giao thức IoT khác.
*Hỗ trợ GPU Acceleration:* Tận dụng GPU để tăng tốc xử lý gói tin, giảm tải cho CPU.
*Hệ thống phát hiện dựa trên dấu hiệu (Signature-based IDS):* Phát hiện các mối đe dọa đã biết.
*Phát hiện bất thường (Anomaly-based Detection):* Phân tích hành vi để phát hiện các cuộc tấn công chưa được biết trước.

*Tích hợp với hệ thống SIEM:* Hỗ trợ tích hợp với Elasticsearch, Logstash, Kibana (ELK Stack), Splunk, Wazuh.

### *2.3.3 Kiến trúc xử lý của Suricata*

Suricata được thiết kế với kiến trúc xử lý đa luồng.




*Hình 5: Kiến trúc xử lý đa luồng của Suricata*

Quy trình xử lý gói tin trong Suricata, bao gồm bốn giai đoạn chính:

- *Thu thập gói tin (Packet Acquisition)*
- *Giải mã và phân tích luồng ứng dụng (Decode & Stream Application Layer)*
- *Phát hiện mối đe dọa (Detection Engine)*
- *Xuất dữ liệu và cảnh báo (Output Processing)*

### *2.3.4 Tập luật của Suricata*

Tập luật của Suricata đóng vai trò quan trọng trong việc định nghĩa các loại lưu lượng mạng cần giám sát và quyết định hành động cần thực hiện khi phát hiện mối đe dọa.

***Hành động (Action)***

Xác định hành động khi một gói tin mạng khớp với các điều kiện được chỉ định trong rule.

***Tiêu đề (Header)***

Mô tả máy chủ, địa chỉ IP, cổng, giao thức và hướng lưu lượng (đến hoặc đi).

***Tùy chọn (Options)***

Mô tả chi tiết các đặc điểm của đối tượng.

## 2.4 Kết luận chương

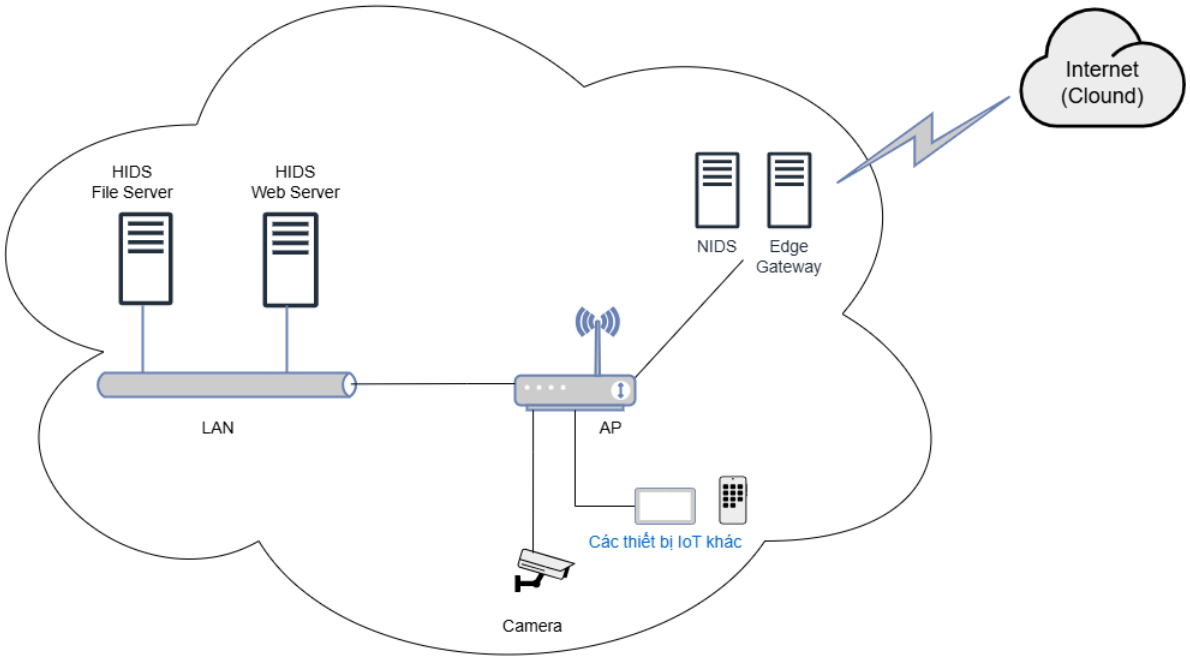
Chương 2 trình bày tổng quan về hệ thống phát hiện xâm nhập (IDS) và phần mềm Suricata, từ khái niệm, phân loại, phương pháp phát hiện đến kiến trúc xử lý và tập luật.

# CHƯƠNG 3. XÂY DỰNG HỆ IDS VỚI SURICATA CHO MẠNG IOT TRONG DOANH NGHIỆP VỪA VÀ NHỎ

## 3.1 Kiến trúc hệ IDS với Suricata

Kiến trúc của hệ thống phát hiện xâm nhập bao gồm các thành phần để thu thập, phân tích và cảnh báo các sự kiện an ninh mạng trong thời gian thực như: Các thiết bị IoT và hệ thống mạng, Máy chủ IDS với suricata.

Sơ đồ kiến trúc các IDS trên mạng doanh nghiệp vừa và nhỏ như trên hình sau:




*Hình 6: Sơ đồ kiến trúc các IDS trên mạng doanh nghiệp vừa và nhỏ*

## 3.2 Các thành phần chức năng của hệ IDS với Suricata

***Thu thập lưu lượng mạng***

Suricata sẽ giám sát tất cả các giao tiếp mạng giữa các thiết bị IoT với nhau và các thiết bị IoT với các thiết bị khác trong hệ thống.

***Phân tích gói tin và phát hiện tấn công***

Thực hiện phân tích các gói tin trong hệ thống mạng dựa trên các tập luật.

***Ghi lại dữ liệu và tạo cảnh báo***

Ghi lại các sự kiện bảo mật trong các tệp nhật ký, đặc tả chi tiết về cuộc tấn công, nguồn tấn công , loại tấn công, đặc trưng của cuộc tấn công.

## 3.3 Triển khai hệ IDS với Suricata

### *3.3.1 Cài đặt Suricata*

Thực hiện cài đặt suricata phiên bản 6.0.9 trên hệ điều hành Ubuntu Server.

***Cài đặt Suricata bằng APT repository của Ubuntu***

***Cấu hình suricata***

```
address-groups:
  HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
  #HOME_NET: "[192.168.0.0/16]"
  #HOME_NET: "[10.0.0.0/8]"
  #HOME_NET: "[172.16.0.0/12]"
  #HOME_NET: "any"

  EXTERNAL_NET: "!$HOME_NET"
  #EXTERNAL_NET: "any"
```

*Hình 7: Cấu hình dải mạng của doanh nghiệp, tổ chức*

```
  HTTP_SERVERS: "$HOME_NET"
  SMTP_SERVERS: "$HOME_NET"
  SQL_SERVERS: "$HOME_NET"
  DNS_SERVERS: "$HOME_NET"
  TELNET_SERVERS: "$HOME_NET"
  AIM_SERVERS: "$EXTERNAL_NET"
  DC_SERVERS: "$HOME_NET"
  DNP3_SERVER: "$HOME_NET"
  DNP3_CLIENT: "$HOME_NET"
  MODBUS_CLIENT: "$HOME_NET"
  MODBUS_SERVER: "$HOME_NET"
  ENIP_CLIENT: "$HOME_NET"
  ENIP_SERVER: "$HOME_NET"

port-groups:
  HTTP_PORTS: "80,8080"
  SHELLCODE_PORTS: "!80"
  ORACLE_PORTS: 1521
  SSH_PORTS: 22
  DNP3_PORTS: 20000
  MODBUS_PORTS: 502
  FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"
  FTP_PORTS: 21
  GENEVE_PORTS: 6081
  VXLAN_PORTS: 4789
  TEREDO_PORTS: 3544
```

*Hình 8: Cấu hình các dải mạng cho các giao thức và ports*

```
# Linux high speed capture support
af-packet:
  - interface: ens33
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
```

*Hình 9: Cấu hình interface thu thập lưu lượng mạng*

```
default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - custom.rules
```

*Hình 10: Cấu hình đường dẫn và tập luật*

```
 GNU nano 7.2                                                /etc/suricata/surica
    modbus:
      # How many unanswered Modbus requests are considered a flood.
      # If the limit is reached, the app-layer-event:modbus.flooded; will match.
      #request-flood: 500

      enabled: yes
      detection-ports:
        dp: 502
      # According to MODBUS Messaging on TCP/IP Implementation Guide V1.0b, it
      # is recommended to keep the TCP connection opened with a remote device
      # and not to open and close it for each MODBUS/TCP transaction. In that
      # case, it is important to set the depth of the stream reassembling as
      # unlimited (stream.reassembly.depth: 0)

      # Stream reassembly size for modbus. By default track it completely.
      stream-depth: 0

    # DNP3
    dnp3:
      enabled: yes
      detection-ports:
        dp: 20000

    # SCADA EtherNet/IP and CIP protocol support
    enip:
      enabled: yes

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

*Hình 11: Cấu hình các giao thức trong IoT*

```
root@castrol:~/suricata-6.0.9# sudo suricata -T -c /etc/suricata/suricata.yaml -v
11/2/2025 -- 19:27:21 - <Info> - Running suricata under test mode
11/2/2025 -- 19:27:21 - <Notice> - This is Suricata version 6.0.9 RELEASE running in SYSTEM mode
11/2/2025 -- 19:27:28 - <Notice> - Configuration provided was successfully loaded. Exiting.
root@castrol:~/suricata-6.0.9#
```

*Hình 12: Kiểm tra tệp cấu hình thành công*

```
root@castrol:~/suricata-6.0.9# sudo nano /etc/systemd/system/suricata.service
root@castrol:~/suricata-6.0.9# sudo systemctl enable suricata.service
Created symlink /etc/systemd/system/default.target.wants/suricata.service → /etc/systemd/system/suricata.service.
root@castrol:~/suricata-6.0.9# sudo systemctl start suricata.service
root@castrol:~/suricata-6.0.9# sudo systemctl status suricata.service
● suricata.service - Suricata IDS/IPS
     Loaded: loaded (/etc/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-02-11 19:31:37 UTC; 6s ago
   Main PID: 24880 (Suricata-Main)
      Tasks: 2 (limit: 2218)
     Memory: 835.3M (peak: 883.8M)
        CPU: 6.097s
     CGroup: /system.slice/suricata.service
             └─24880 /usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens33

Feb 11 19:31:37 castrol systemd[1]: Started suricata.service - Suricata IDS/IPS.
Feb 11 19:31:37 castrol suricata[24880]: 11/2/2025 -- 19:31:37 - <Notice> - This is Suricata version 6.0.9 RELEASE r
Feb 11 19:31:43 castrol suricata[24880]: 11/2/2025 -- 19:31:43 - <Notice> - all 2 packet processing threads, 4 manag
root@castrol:~/suricata-6.0.9#
```

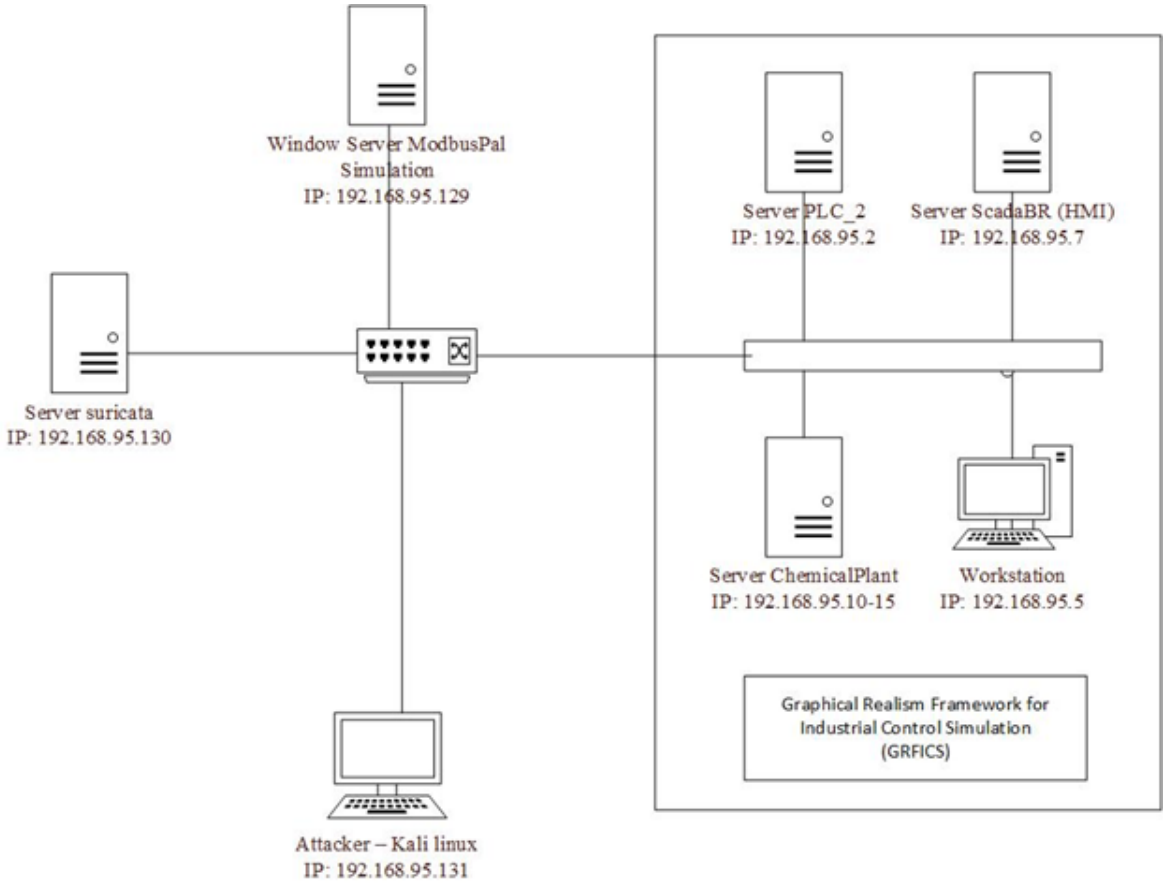
*Hình 13: Trạng thái của suricata khi khởi chạy thành công*

### *3.3.2 Cấu hình các luật của Suricata áp dụng vào môi trường mạng IoT cho doanh nghiệp*

Thêm đường dẫn của tập luật vào tệp cấu hình của suricat nằm tại đường dẫn /etc/suricata/suricata.yaml.

## 3.4 Thử nghiệm phát hiện tấn công với hệ IDS đã tạo lập

### *3.4.1 Mô hình thử nghiệm*



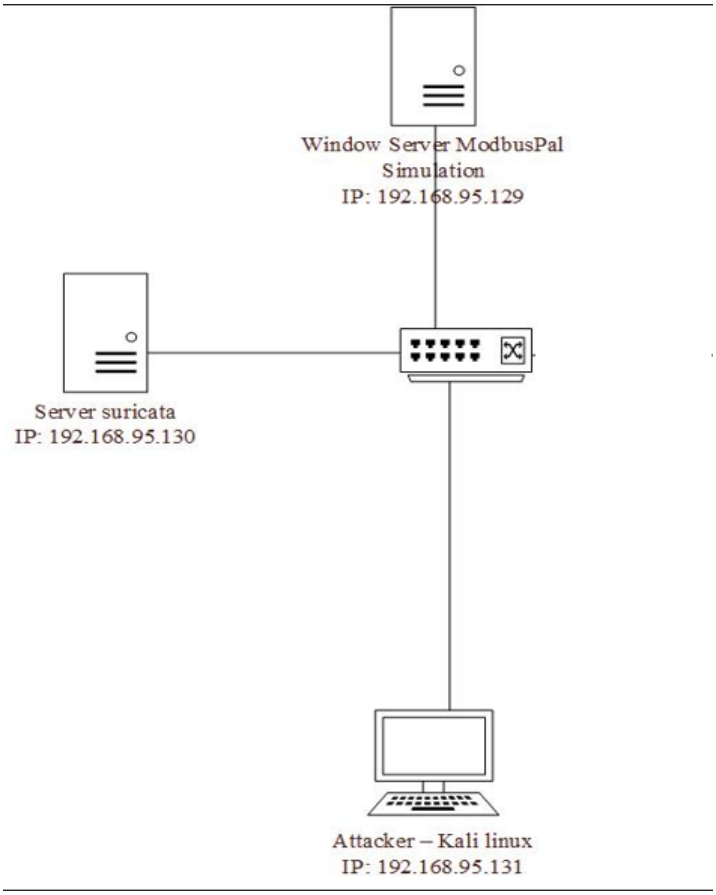

*Hình 14: Mô hình topo mạng mô phỏng kịch bản tấn công*

Mô phỏng mạng IoT bao gồm 2 thành phần giả lập sử dụng giao thức IoT là Modbuspal và Graphical Realism Framework for Industrial Control Simulation (GRFICS) version 2.

### *3.4.2 Xây dựng kịch bản tấn công xâm nhập mạng đối với hai mô hình doanh nghiệp vừa và nhỏ*

***Kịch bản 1:***

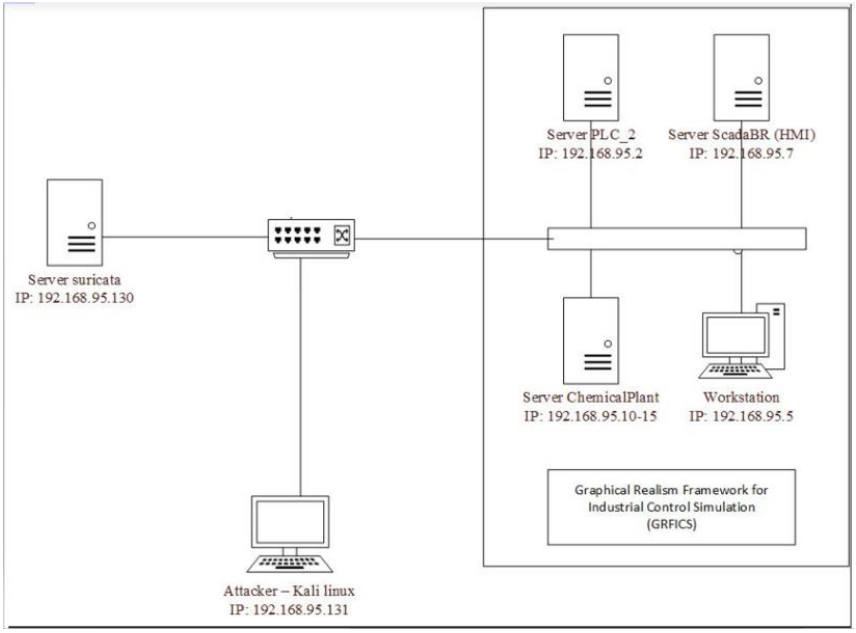
Thực hiện đọc và sửa giá trị của thanh ghi.




*Hình 15: Mô hình kịch bản 1*

***Kịch bản 2:***

Thực hiện khai thác vào thành phần PLC

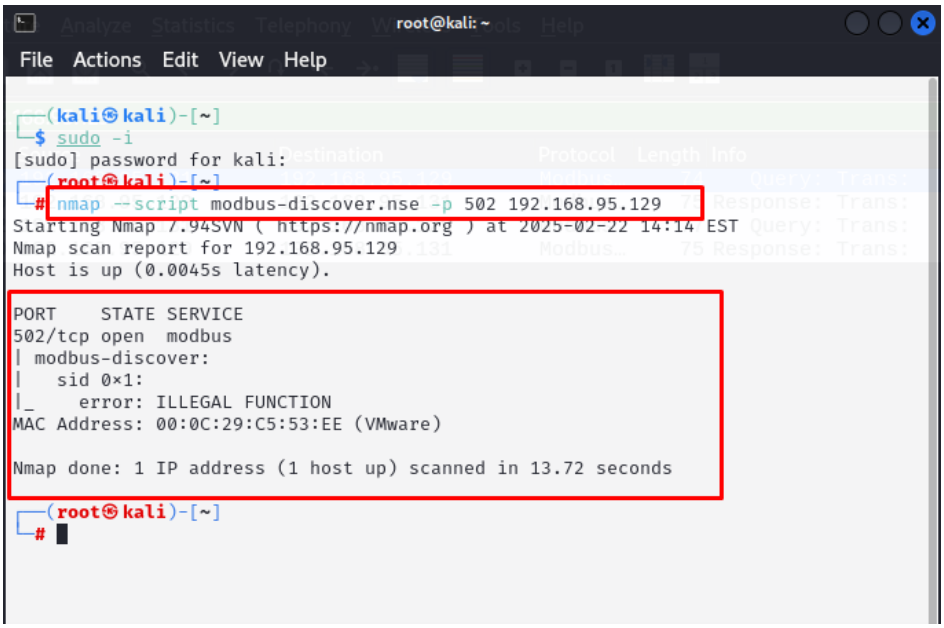



*Hình 16: Mô hình kịch bản 2*

### *3.4.3 Thực hiện thử nghiệm*

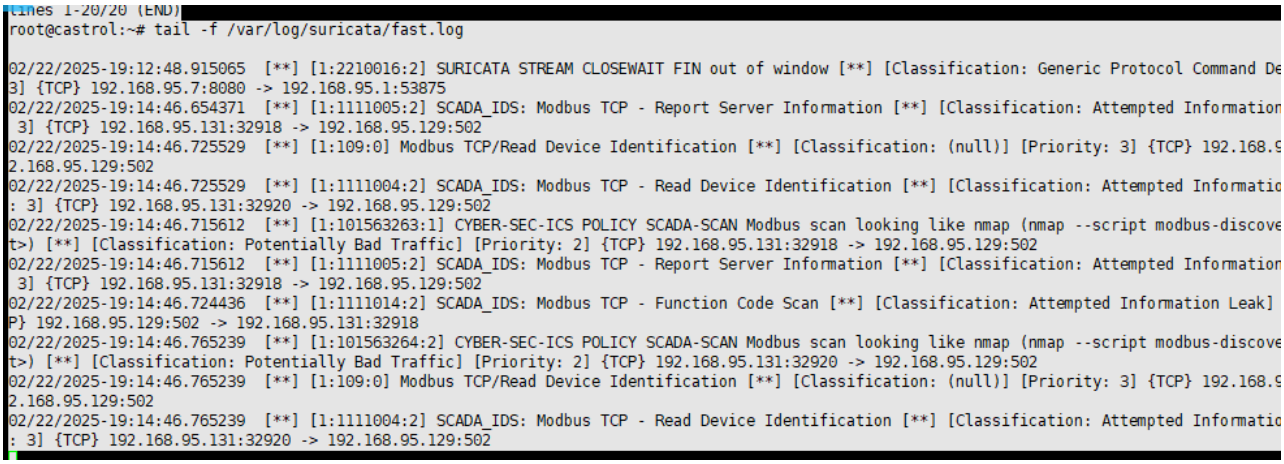
#### *3.4.3.1 Kịch bản 1*

Trên máy kẻ tấn công thực hiện scan ports 502 với options script (.nse)



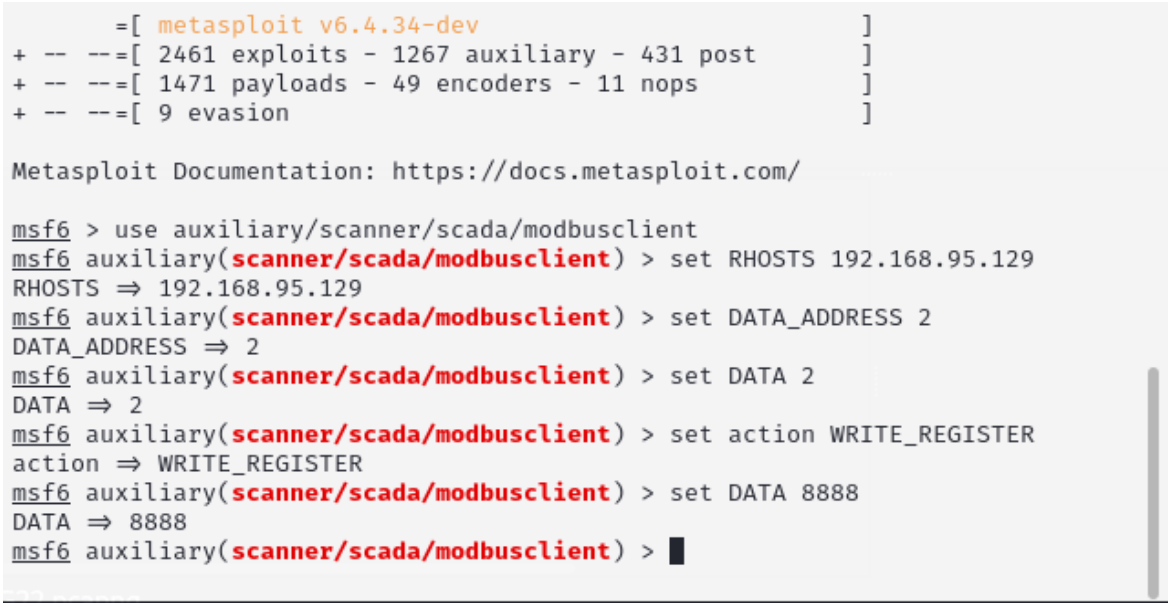

*Hình 17: Thực hiện quét cổng 502*

Máy chủ suricata sẽ đưa ra cảnh báo phát hiện hành vi dò quét và thu thập thông tin máy chủ.



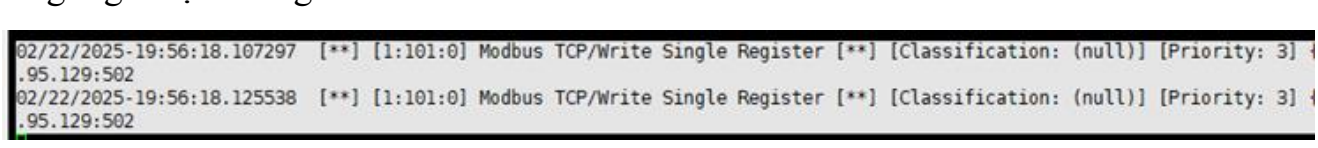

*Hình 18: Cảnh báo phát hiện hành vi rà quét cổng bằng nmap*

Thực hiện sửa giá trị thanh ghi.




*Hình 19: Đặt các giá trị*

Máy chủ suricata sẽ phát sinh cảnh báo cho thấy có một hành vi sử dụng modbus để ghi giá trị thanh ghi.




*Hình 20: Cảnh báo phát sinh trên suricata*

### *3.4.3.2 Kịch bản 2*

Thực hiện tấn công thay đổi giá trị thanh ghi coils

```
msf6 > use auxiliary/scanner/scada/modbusclient
msf6 auxiliary(scanner/scada/modbusclient) > set RHOSTS 192.168.95.2
RHOSTS ⇒ 192.168.95.2
msf6 auxiliary(scanner/scada/modbusclient) > set action WRITE_COIL
set action WRITE_COIL   set action WRITE_COILS
msf6 auxiliary(scanner/scada/modbusclient) > set action WRITE_COILS
action ⇒ WRITE_COILS
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 40
DATA_ADDRESS ⇒ 40
msf6 auxiliary(scanner/scada/modbusclient) > set number 1
number ⇒ 1
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_COILS 1
DATA_COILS ⇒ 1
msf6 auxiliary(scanner/scada/modbusclient) >
```

*Hình 21: Đặt các giá trị ghi vào write_coils*

Cảnh báo suricata phát hiện được cuộc tấn công

```
1 suricata
root@castrol:~# tail -f /var/log/suricata/fast.log
02/23/2025-19:00:29.441839  [**] [1:104:0] Modbus TCP/Write Multiple Coils [**] [Classification: (null)] [Priority: 3]
2:502
02/23/2025-19:00:29.445050  [**] [1:104:0] Modbus TCP/Write Multiple Coils [**] [Classification: (null)] [Priority: 3]
95.2:502
```

*Hình 22: Cảnh báo phát sinh trên suricata*

### *3.4.4 Đánh giá khả năng phát hiện tấn công của Suricata đối với hai kịch bản tấn công trên*

***Đối với kịch bản 1***

Khi thực hiện bước rà soát và tấn công khai thác, Suricata đều phát hiện tấn công với các thông tin cụ thể như thời gian phát hiện tấn công, mã luật dùng để phát hiện (sid), thông tin phương thức tấn công, địa chỉ và ports nguồn/đích trong cuộc tấn công.

***Đối với kịch bản 2***

Khi thực hiện thay đổi giá trị thanh ghi coils. Suricata đã cảnh báo các thông tin cụ thể như thời gian phát hiện tấn công, mã luật dùng để phát hiện (sid), thông tin phương thức tấn công, địa chỉ và ports nguồn/đích trong cuộc tấn công.

## 3.5 Kết luận chương

Thông qua hai kịch giả lập tấn công vào hệ thống IoT có thể thấy rằng giải pháp Suricata hiệu quả trong quá trình phát hiện tấn công.

# KẾT LUẬN

Đề án này nghiên cứu, triển khai và đánh giá hiệu quả của hệ thống phát hiện xâm nhập (IDS) cài đặt công cụ nguồn mở Suricata trong giám sát an toàn mạng IoT cho môi trường doanh nghiệp vừa và nhỏ.

Các kết quả chính đạt được trong bài gồm:

- Hiểu được khái quát các đặc trưng, cấu trúc các thành phần trong mạng IoT áp dụng trong mạng của doanh nghiệp vừa và nhỏ.
- Nghiên cứu tìm hiểu về những đặc trưng của mạng IoT trong doanh nghiệp vừa và nhỏ, những vấn đề về tấn công mạng IoT.
- Phân tích về hệ phát hiện xâm nhập và một số công cụ, từ đó đưa ra kiến trúc một hệ NIDS đặt tại Edge Gateway của doanh nghiệp vừa và nhỏ.
- Thực hiện xây dựng và cấu hình các luật phù hợp của Suricata áp dụng vào môi trường mạng IoT cho doanh nghiệp.

Có thể phát triển tiếp đề tài nghiên cứu theo hai hướng:

- Nghiên cứu tích hợp NIDS ở lớp biên với các HIDS hoặc NIDS phân tán khác trong mạng.
- Nghiên cứu khả năng áp dụng các mô hình học máy/học sâu và AI hạng nhẹ áp dụng được trên các thiết bị IoT nhỏ gọn.