TRƯỜNG ĐẠI HỌC MỞ HÀ NỘI

**KHOA CÔNG NGHỆ THÔNG TIN**

--------------------------



**BÁO CÁO BÀI TẬP LỚN**

**Môn: An ninh mạng máy tính**

**Đề tài:**

**Giám sát và phát hiện tấn công sớm hệ thống mạng doanh nghiệp với giải pháp Site 24x7**

*Giảng viên hướng dẫn:***ThS. Lê Ngọc An**

*Sinh viên thực hiện:* Nguyễn Vũ Hoàng - 1910A

Nguyễn Trọng Hùng – 2210A05

***Hà Nội – 2024***

**MỤC LỤC**

[MỤC LỤC i](#_Toc180441954)

[PHÂN CÔNG CÔNG VIỆC iii](#_Toc180441955)

[DANH MỤC HÌNH ẢNH iii](#_Toc180441956)

[DANH MỤC BẢNG BIỂU iii](#_Toc180441957)

[CHƯƠNG 1: LÝ THUYẾT 3](#_Toc180441958)

[*1.1.* Thực trạng về an ninh mạng hiện nay 3](#_Toc180441959)

[1.1.1. Thực trạng về an ninh mạng thế giới 3](#_Toc180441960)

[1.1.2. Thực trạng về an ninh mạng tại việt Nam 3](#_Toc180441961)

[1.2. Tổng quan về tấn công mạng 4](#_Toc180441962)

[1.2.1. Tấn công mạng là gì ? 4](#_Toc180441963)

[1.2.2. Các hình thức tấn công mạng phổ biến 5](#_Toc180441964)

[1.3. Tổng quan về giám sát mạng 34](#_Toc180441965)

[1.3.1. Giám sát mạng là gì? 34](#_Toc180441966)

[1.3.2. Các thành phần của một hệ thống giám sát 34](#_Toc180441967)

[CHƯƠNG 2: GIẢI PHÁP 37](#_Toc180441968)

[2.1 Zabbix 37](#_Toc180441969)

[2.1.1. Chức năng chính của Zabbix: 37](#_Toc180441970)

[2.1.2. Kiến trúc của Zabbix: 38](#_Toc180441971)

[2.1.3. Các tính năng nổi bật của Zabbix: 39](#_Toc180441972)

[2.1.4. Lợi ích của Zabbix: 40](#_Toc180441973)

[2.1.5. Ứng dụng trong thực tế: 40](#_Toc180441974)

[2.2. Snort 40](#_Toc180441975)

[2.2.1. Chức năng chính của Snort: 41](#_Toc180441976)

[2.2.2. Các chế độ hoạt động của Snort: 41](#_Toc180441977)

[2.2.3. Kiến trúc của Snort: 42](#_Toc180441978)

[2.2.4. Cách thức hoạt động của Snort: 43](#_Toc180441979)

[2.2.5. Ưu điểm của Snort: 44](#_Toc180441980)

[2.2.6. Nhược điểm của Snort: 44](#_Toc180441981)

[2.3. Site24x7 45](#_Toc180441982)

[2.3.1. Các chức năng chính của Site24x7: 45](#_Toc180441983)

[2.3.2. So sánh Site24x7 với các công cụ Zabbix, Snort 46](#_Toc180441984)

[CHƯƠNG 3: TIẾN HÀNH TRIỂN KHAI VÀ THỬ NGHIỆM 47](#_Toc180441985)

[3.1. Kịch bản 47](#_Toc180441986)

[3.2. Triển khai tấn công lần 1 48](#_Toc180441987)

[3.3. Triển khai tấn công lần 2 52](#_Toc180441988)

# PHÂN CÔNG CÔNG VIỆC

|  |  |
| --- | --- |
| Nguyễn Vũ Hoàng | Tìm hiểu thực trạng an ninh thế giới và Việt Nam, so sánh các loại giải pháp, làm báo cáo. |
| Nguyễn Trọng Hùng | Tìm hiểu lý thuyết, dựng lab ảo hóa, cài đặt agent thêm thiết bị của Site24x7 làm báo cáo. |

# LÝ THUYẾT

## Thực trạng về an ninh mạng hiện nay

### Thực trạng về an ninh mạng thế giới

Theo một số nghiên cứu, có khoảng 30.000 cuộc tấn công mạng diễn ra mỗi ngày trên toàn thế giới, theo McAfee 390.000 mẫu mã độc mới được tạo ra mỗi ngày. Thống kê từ CVE trung bình có khoảng 20-30 lỗ hổng được phát hiện mỗi ngày.

Theo tạp chí Info Security quý 3 năm 2024:

* Lỗ hổng Log4Shell tàn phá suốt năm 2022 với xếp hạng quan trọng 10/10. Đã có 1,2 triệu cuộc tấn công trên toàn cầu một tuần sau khi Log4Shell được công khai
* Số lượng mối đe dọa an ninh mạng năm 2023 đã tăng 482% so với cùng kỳ năm trước.
* Năm 2023 đã có 867 mối đe dọa và 35.776 báo cáo về sự xâm phạm (IOC), tăng tương ứng 482% và 380% so với năm trước. Tổng cộng có 582 mối đe dọa đã được phát hiện, phân tích và báo cáo trong khoảng thời gian này, tăng 218% so với năm 2021
* Trí tuệ nhân tạo AI đã được áp dụng cả trong tấn công và phòng thủ. Sự gia tăng sử dụng AI trong các cuộc tấn công cho phép tin tặc tạo ra các chiến lược tinh vi hơn, khiến việc phát hiện trở nên khó khăn hơn.
* Trong Q4/2023, Stealers đã trở thành loại mã độc phổ biến nhất



Hình 1.1: Bxh các loại mã độc Q4 2023

* Nhóm phần mềm độc hại phổ biến nhất là Agent Tesla



Hình 1.2: Bxh các nhóm mã độc Q4 2023

Có thể kể đến vụ tấn công mạng phổ biến thế giới là :

* **Vụ SolarWinds (2020):** tấn công vào chuỗi cung ứng, được thực hiện do 1 nhóm hacker có liên quan đến chính phủ Nga tên là APT29 hoặc Cozy Bear. Đây là một trong những vụ an ninh mạng lớn nhất trong lịch sử, làm rung chuyển cả lĩnh vực an ninh mạng và quốc phòng trên toàn cầu. Gây hậu quả nghiêm trọng về an ninh quốc gia Mỹ, thiệt hại về niềm tin và kinh tế. Ước tính hơn 18000 khách hàng của SolarWinds bị ảnh hưởng bới bản vá chứa mã độc với tên gọi SunBurst.
* **Vụ Microsoft Exchange (2021):** do nhóm hacker có tên Hafnium có liên hệ với chính phủ Trung Quốc tiến hành, khai thác lỗ hổng Zero-Day để chiếm quyền kiểm soát hệ thống và đánh cắp dữ liệu từ Microsoft Exchange Server. Gây ảnh hưởng đến hàng trăm nghìn tổ chức trên thế giới, bao gồm: Các cơ quan chính phủ, các tổ chức tài chính, công công ty luật, y tế, giáo dục, …

### Thực trạng về an ninh mạng tại việt Nam

Theo ghi nhận của Bộ Công an trong năm 2023:

* Có tới 13.900 vụ tấn công an ninh mạng vào các hệ thống tại Việt Nam, tăng 9,5% so với năm 2022.
* 554 website của các cơ quan tổ chức chính phủ và giáo dục có tên miền .gov.vn; .edu.vn bị xâm nhập, chèn mã quảng cáo cờ bạc, cá độ.
* Hơn 83.000 máy tính, máy chủ bị mã độc mã hóa dữ liệu tống tiền tấn công, tăng 8,4% so với năm 2022
* Tháng 6/2024, hệ thống rà quét từ xa của trung tâm NCSC đã phát hiện hơn 1600 lỗ hổng, trên 5000 hệ thống đang mở công khai trên internet, 12 lỗ hổng mới được công bố có mức độ ảnh hưởng Nghiêm trong/Cao có thể bị lợi dụng để khai thác vào các hệ thống của các cơ quan, tổ chức



Hình 1.3: Các lỗ hổng đáng chú ý trong tháng 6/2024

## Tổng quan về tấn công mạng

### Tấn công mạng là gì ?

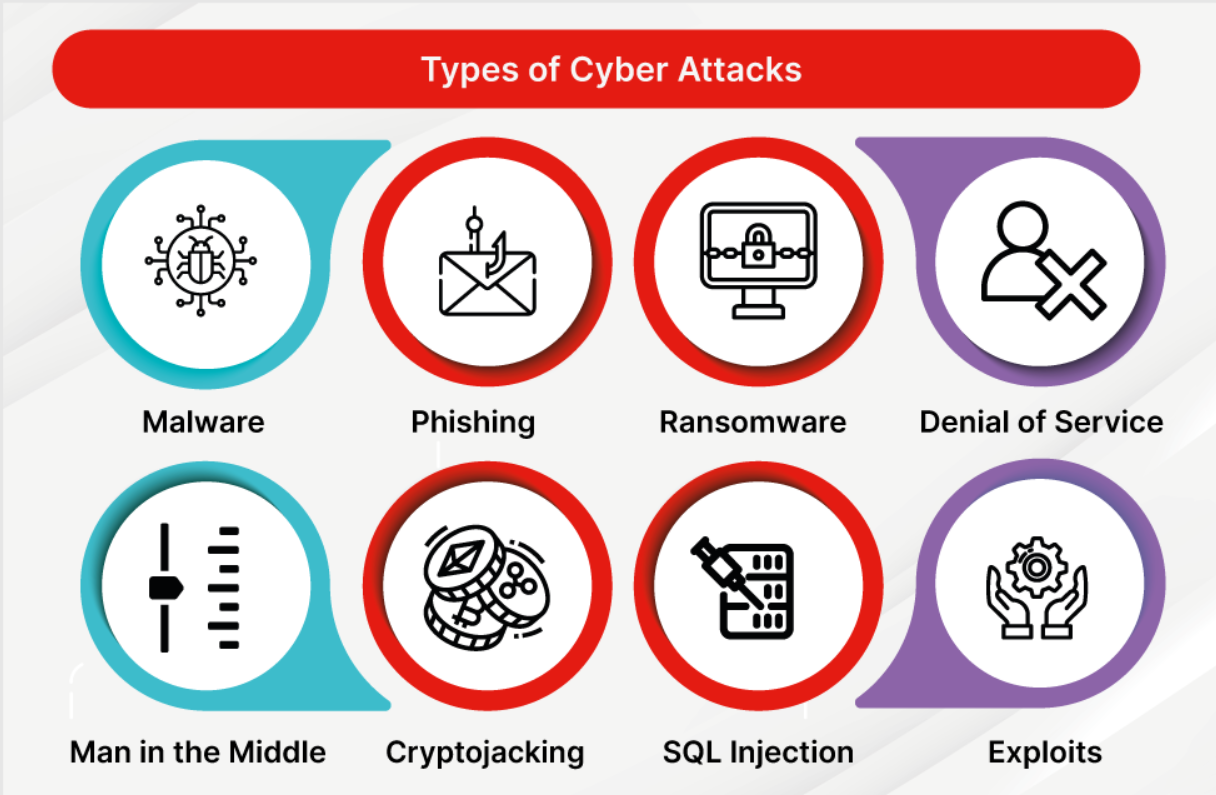
Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử (theo Luật An Ninh Mạng 2018).

### Các hình thức tấn công mạng phổ biến

Các hình thức tấn công mạng phổ biến bao gồm:

|  |  |
| --- | --- |
| 1- Malware | 5- Man in the Middle |
| 2- Phishing | 6- Cryptojacking |
| 3- Ransomware | 7- SQL Injection |
| 4- Denial of Service | 8- Exploits |

Bảng 1.4: Các hình thức tấn công mạng phổ biến



Hình 1.5: Các kiểu tấn công phổ biến

#### Malware Attack

* **Định nghĩa:**

**Malware** (viết tắt của **Malicious Software**) là một phần mềm độc hại được thiết kế để xâm nhập, làm hỏng hoặc đánh cắp thông tin từ các hệ thống máy tính. Malware bao gồm nhiều loại như virus, trojan, ransomware, spyware và worm. Những cuộc tấn công bằng malware có thể gây thiệt hại lớn về dữ liệu, làm gián đoạn hoạt động kinh doanh, và đe dọa bảo mật thông tin cá nhân.

* **Cơ chế hoạt động:**

Malware thường được phát tán thông qua nhiều cách khác nhau như email độc hại, tải xuống từ các trang web không an toàn, phần mềm lậu, hoặc cài đặt qua các thiết bị di động. Cơ chế hoạt động của malware có thể được chia thành các bước cơ bản:

1. Xâm nhập: Malware xâm nhập vào hệ thống thông qua một lỗ hổng bảo mật, một đường dẫn không an toàn hoặc do người dùng tự ý tải về.

2. Lây nhiễm: Khi malware đã vào hệ thống, nó sẽ bắt đầu lây lan sang các tập tin khác hoặc kết nối với các thiết bị khác trong mạng.

3. Thực thi: Malware thực hiện hành vi gây hại như đánh cắp thông tin, mã hóa dữ liệu, theo dõi hoạt động của người dùng hoặc phá hoại hệ thống.

4. Ẩn náu: Nhiều malware có khả năng tự ẩn mình để tránh bị phát hiện bởi các phần mềm diệt virus hoặc các biện pháp bảo mật.

* **Dấu hiệu nhận biết:**

Một số dấu hiệu thường gặp khi hệ thống bị malware tấn công:

* Hiệu suất chậm: Máy tính hoặc mạng chạy chậm đột ngột, khởi động lâu, hoặc thường xuyên bị treo.
* Xuất hiện quảng cáo không mong muốn: Những quảng cáo bật lên liên tục mà người dùng không truy cập vào.
* Mất quyền kiểm soát: Người dùng bị mất quyền kiểm soát các tài khoản hoặc không thể truy cập vào một số tệp tin quan trọng.
* Dữ liệu bị mã hóa: Ransomware sẽ mã hóa các tập tin và yêu cầu tiền chuộc để giải mã.
* Phần mềm không mong muốn: Xuất hiện các phần mềm lạ mà người dùng không cài đặt.
* **Các kiểu Malware:**

Malware có nhiều hình thức và mỗi loại có mục tiêu khác nhau:

1.Virus: Lây nhiễm vào tệp tin hoặc chương trình và tự nhân bản khi người dùng chạy chúng.

2. Worm: Tự lây lan qua mạng mà không cần sự can thiệp của người dùng, phá hoại toàn bộ hệ thống hoặc gây tắc nghẽn mạng.

3. Trojan: Giả mạo là phần mềm hợp pháp, sau đó mở cửa cho hacker kiểm soát từ xa hoặc đánh cắp dữ liệu.

4. Ransomware: Mã hóa dữ liệu của nạn nhân và yêu cầu tiền chuộc để mở khóa.

5. Spyware: Theo dõi hoạt động của người dùng và gửi thông tin này về hacker, thường được dùng để đánh cắp thông tin cá nhân.

6. Adware: Hiển thị quảng cáo không mong muốn và làm phiền người dùng, đồng thời có thể thu thập thông tin.

* **Phương pháp phòng chống cơ bản:**

Để phòng chống malware, người dùng và doanh nghiệp có thể áp dụng các phương pháp sau:

* Sử dụng phần mềm diệt virus: Cài đặt và cập nhật thường xuyên các phần mềm diệt virus để phát hiện và ngăn chặn malware.
* Cập nhật hệ điều hành và phần mềm: Liên tục cập nhật để vá các lỗ hổng bảo mật.
* Tránh tải xuống và cài đặt phần mềm không rõ nguồn gốc: Chỉ tải và cài đặt từ các nguồn uy tín.
* Sao lưu dữ liệu thường xuyên: Sao lưu định kỳ để tránh mất mát dữ liệu nếu bị tấn công bởi ransomware.
* Giáo dục nhận thức bảo mật: Người dùng cần được giáo dục về các dấu hiệu nhận biết malware và cách phòng tránh khi sử dụng internet và email.
* Sử dụng tường lửa và giải pháp bảo mật mạng: Tường lửa có thể giúp ngăn chặn lưu lượng không mong muốn và bảo vệ mạng nội bộ khỏi các cuộc tấn công.

Việc bảo vệ hệ thống khỏi malware yêu cầu một phương pháp toàn diện kết hợp nhiều biện pháp bảo mật và sự cảnh giác của người dùng.

#### Phishing Attack

* **Định nghĩa:**

**Phishing attack** là một hình thức tấn công mạng, trong đó kẻ tấn công giả mạo là một thực thể đáng tin cậy (như ngân hàng, công ty, hoặc tổ chức chính phủ) để lừa người dùng tiết lộ thông tin cá nhân nhạy cảm như tên đăng nhập, mật khẩu, số thẻ tín dụng, hoặc thông tin tài khoản ngân hàng. Kẻ tấn công thường sử dụng các phương pháp như email, tin nhắn SMS, trang web giả mạo, hoặc cuộc gọi điện thoại để đánh lừa nạn nhân. Phishing là một trong những phương thức tấn công phổ biến nhằm mục tiêu đánh cắp danh tính, tiền bạc, hoặc thực hiện các hành vi phạm pháp khác.

* **Cơ chế hoạt động:**

Cơ chế hoạt động của phishing tấn công thông qua các bước sau:

1. Tạo ra nội dung giả mạo: Hacker sẽ tạo ra email, trang web, hoặc thông điệp SMS có giao diện giống hệt với các nguồn đáng tin cậy như ngân hàng, dịch vụ trực tuyến hoặc tổ chức nổi tiếng.

2. Gửi lừa đảo: Hacker sẽ gửi email, tin nhắn, hoặc đăng tải thông điệp giả mạo đến nạn nhân. Thông điệp này thường chứa liên kết đến trang web giả mạo hoặc tệp tin độc hại.

3. Lừa nạn nhân cung cấp thông tin: Khi người dùng nhấp vào liên kết hoặc tải xuống tệp tin, họ có thể bị yêu cầu cung cấp thông tin nhạy cảm (như mật khẩu, số thẻ tín dụng) hoặc vô tình tải phần mềm độc hại.

4. Sử dụng thông tin: Sau khi hacker có được thông tin, họ sẽ sử dụng nó để đánh cắp tài khoản, tiền bạc, hoặc thực hiện các cuộc tấn công khác như lừa đảo tài chính.

* **Dấu hiệu nhận biết:**

Một số dấu hiệu có thể nhận biết được khi có cuộc tấn công phishing:

* Email/tin nhắn không chính thức: Địa chỉ email không khớp với tổ chức chính thức hoặc chứa lỗi chính tả, ngữ pháp kém.
* Liên kết đáng ngờ: Đường dẫn chứa ký tự lạ hoặc tên miền không chính xác, không khớp với trang web thực sự.
* Thông điệp khẩn cấp: Các email hoặc tin nhắn thường yêu cầu hành động khẩn cấp, như "Tài khoản của bạn sẽ bị khóa nếu bạn không phản hồi ngay lập tức".
* Yêu cầu thông tin cá nhân: Các tổ chức uy tín sẽ không yêu cầu thông tin nhạy cảm qua email hoặc tin nhắn.
* Tệp đính kèm đáng ngờ: Các tệp tin lạ hoặc không mong đợi thường đi kèm với mã độc.
* **Các kiểu tấn công Phishing:**

Có nhiều hình thức tấn công phishing, mỗi hình thức có phương pháp tiếp cận và mục tiêu khác nhau:

1. Email Phishing: Tấn công phổ biến nhất, trong đó kẻ xấu gửi email giả mạo từ các tổ chức đáng tin cậy để yêu cầu thông tin nhạy cảm hoặc phát tán malware.

2. Spear Phishing: Đây là một hình thức tấn công có mục tiêu cụ thể hơn, thường nhắm đến cá nhân hoặc tổ chức cụ thể. Hacker thu thập thông tin về nạn nhân và tạo ra email mang tính cá nhân hóa để tăng tính thuyết phục.

3. Whaling: Nhắm đến các cá nhân có quyền lực cao trong tổ chức như CEO, CFO, để đánh cắp thông tin quan trọng hoặc gây thiệt hại tài chính lớn.

4. Smishing và Vishing:

* Smishing: Tấn công qua tin nhắn SMS, hacker gửi tin nhắn lừa đảo với mục tiêu đánh cắp thông tin cá nhân hoặc lây nhiễm malware vào thiết bị di động.
* Vishing: Tấn công qua cuộc gọi điện thoại giả mạo, trong đó kẻ xấu giả danh các tổ chức để lừa người dùng cung cấp thông tin.

5. Clone Phishing: Hacker sao chép email hợp pháp trước đó từ một nguồn uy tín, sau đó chỉnh sửa nội dung và gửi lại với mục tiêu lừa đảo.

* **Phương pháp phòng chống cơ bản:**

Để phòng chống các cuộc tấn công phishing, người dùng có thể áp dụng các biện pháp sau:

* Cảnh giác với email và tin nhắn lạ: Kiểm tra kỹ địa chỉ email người gửi, không mở các liên kết hoặc tải tệp tin từ nguồn không rõ ràng.
* Không cung cấp thông tin cá nhân qua email hoặc tin nhắn: Không tổ chức uy tín nào yêu cầu cung cấp mật khẩu, số thẻ tín dụng qua email hoặc tin nhắn.
* Xác minh nguồn gửi: Luôn liên hệ trực tiếp với tổ chức thông qua kênh chính thức (như gọi điện thoại hoặc truy cập trang web chính thức) để xác minh thông tin.
* Cài đặt và cập nhật phần mềm bảo mật: Sử dụng phần mềm diệt virus và bảo mật đáng tin cậy, thường xuyên cập nhật hệ thống để vá các lỗ hổng.
* Kiểm tra URL trước khi nhập thông tin: Luôn kiểm tra đường dẫn của trang web trước khi nhập thông tin nhạy cảm. Trang web chính thức thường có giao thức bảo mật HTTPS.
* Kích hoạt xác thực hai yếu tố (2FA): Bật 2FA để tăng cường bảo mật cho các tài khoản trực tuyến.

Phòng chống phishing đòi hỏi sự cảnh giác và ý thức bảo mật của người dùng để tránh trở thành nạn nhân của các cuộc tấn công lừa đảo.

#### Ransomeware Attack

* **Định nghĩa:**

**Ransomware** là một loại phần mềm độc hại (malware) được thiết kế để mã hóa dữ liệu hoặc khóa truy cập hệ thống của nạn nhân. Sau khi hệ thống hoặc dữ liệu bị khóa, kẻ tấn công sẽ yêu cầu một khoản tiền chuộc (thường bằng tiền mã hóa như Bitcoin) để cung cấp khóa giải mã hoặc khôi phục quyền truy cập. Nếu nạn nhân không trả tiền chuộc, dữ liệu có thể bị xóa hoặc mãi mãi không thể truy cập được

* **Cơ chế hoạt động:**

Ransomware hoạt động thông qua các bước sau:

1. Phát tán: Ransomware có thể lây nhiễm vào máy tính hoặc mạng thông qua email độc hại, trang web không an toàn, phần mềm lậu, hoặc lỗ hổng bảo mật.

2. Thực thi: Sau khi lây nhiễm, ransomware được kích hoạt và bắt đầu quét dữ liệu trong hệ thống.

3. Mã hóa dữ liệu: Ransomware sẽ mã hóa tất cả dữ liệu quan trọng của nạn nhân như tài liệu, hình ảnh, và cơ sở dữ liệu. Một số loại ransomware còn có khả năng khóa toàn bộ hệ thống.

4. Yêu cầu tiền chuộc: Sau khi mã hóa dữ liệu, ransomware hiển thị một thông báo yêu cầu nạn nhân phải trả tiền chuộc (thường bằng tiền điện tử) để có khóa giải mã.

5. Giao dịch chuộc: Nếu nạn nhân trả tiền, kẻ tấn công sẽ gửi khóa giải mã. Tuy nhiên, không có gì đảm bảo rằng nạn nhân sẽ nhận được khóa hoặc dữ liệu sẽ được khôi phục.

* Dấu hiệu nhận biết khi bị tấn công:

Khi bị tấn công bởi ransomware, nạn nhân có thể nhận thấy một số dấu hiệu sau:

* Tệp tin bị mã hóa: Các tệp quan trọng không thể mở được, và các tệp này thường có phần đuôi lạ như ".lock" hoặc ".encrypted".
* Thông báo yêu cầu tiền chuộc: Một thông điệp xuất hiện trên màn hình, thông báo rằng hệ thống hoặc tệp tin đã bị mã hóa và yêu cầu trả tiền chuộc để giải mã.
* Hiệu suất hệ thống bị giảm: Hệ thống có thể hoạt động chậm hoặc bị treo do quá trình mã hóa tốn nhiều tài nguyên.
* Các tệp và chương trình không hoạt động: Các tệp hoặc chương trình không phản hồi khi mở, hoặc bị khóa hoàn toàn.
* **Cách kiểu tấn công Ransomeware:**

Ransomware có nhiều loại khác nhau với mục tiêu và phương thức tấn công khác nhau:

**1. Crypto Ransomware:** Loại này mã hóa các tệp quan trọng của nạn nhân, yêu cầu trả tiền chuộc để nhận được khóa giải mã.

**2. Locker Ransomware:** Thay vì mã hóa dữ liệu, loại này khóa toàn bộ hệ thống của nạn nhân, làm cho họ không thể sử dụng máy tính. Dữ liệu không bị mã hóa, nhưng nạn nhân không thể truy cập vào hệ thống mà không trả tiền chuộc.

**3. Ransomware as a Service (RaaS):** Đây là mô hình ransomware mà hacker phát triển và bán hoặc cho thuê phần mềm ransomware cho những người muốn thực hiện tấn công nhưng không có kiến thức kỹ thuật.

**4. Scareware:** Loại ransomware này thường giả mạo là phần mềm bảo mật giả, hiển thị thông báo rằng máy tính của nạn nhân bị nhiễm virus và yêu cầu trả tiền để "khắc phục" vấn đề, dù không có mã hóa thực sự diễn ra.

**5. Doxware (Ransomware kết hợp với Doxing):** Ngoài mã hóa, kẻ tấn công đe dọa công khai dữ liệu nhạy cảm của nạn nhân nếu không trả tiền chuộc.

* **Các phương pháp phòng chống cơ bản:**

Để phòng chống ransomware, các cá nhân và tổ chức cần áp dụng các biện pháp bảo mật chặt chẽ:

* **Sao lưu dữ liệu thường xuyên:** Sao lưu dữ liệu định kỳ vào thiết bị ngoại vi hoặc lưu trữ đám mây để đảm bảo có thể khôi phục dữ liệu mà không cần trả tiền chuộc.
* **Cập nhật phần mềm và hệ điều hành:** Luôn giữ cho hệ điều hành, phần mềm và ứng dụng được cập nhật mới nhất để vá các lỗ hổng bảo mật.
* **Sử dụng phần mềm bảo mật và diệt virus:** Cài đặt và cập nhật thường xuyên các phần mềm bảo mật đáng tin cậy để phát hiện và ngăn chặn ransomware.
* **Cảnh giác với email và liên kết lạ:** Không mở các tệp đính kèm, đường dẫn từ email không rõ nguồn gốc, và tránh tải xuống phần mềm từ các nguồn không tin cậy.
* **Bật xác thực hai yếu tố (2FA):** Xác thực hai yếu tố giúp tăng cường bảo mật cho tài khoản trực tuyến, làm cho hacker khó có thể xâm nhập vào hệ thống hơn.
* **Giáo dục nhận thức bảo mật:** Đào tạo người dùng về các kỹ thuật lừa đảo và dấu hiệu nhận biết ransomware để giảm thiểu nguy cơ bị lừa đảo.

Bằng cách kết hợp các biện pháp phòng chống kỹ thuật và nhận thức người dùng, các cá nhân và tổ chức có thể giảm thiểu nguy cơ trở thành nạn nhân của các cuộc tấn công ransomware.

#### Denial of Service Attack

* **Định nghĩa:**

DoS (Denial of Service): là hình thức tấn công mà hacker tạo ra một lưu lượng truy cập vô cùng lớn ở cùng một thời điểm để làm hệ thống quá tải dẫn đến bị sập. Lúc đó người dùng không ai có thể truy cập được.

DDoS (Distributed Denial of Service): là hình thức biến thể của DoS. Theo đó, tin tặc sử dụng một mạng lưới các máy tính để tấn công. Sự nguy hiểm thể hiện ở chỗ chính các máy tính thuộc mạng lưới máy tính trên cũng không biết bản thân đang bị lợi dụng làm công cụ tấn công.

* **Cơ chế hoạt động:**

Tấn công DoS hoạt động bằng cách khai thác các tài nguyên hệ thống hoặc làm quá tải khả năng xử lý của mục tiêu:

1. Gửi yêu cầu ồ ạt: Kẻ tấn công gửi một lượng lớn các yêu cầu không hợp lệ hoặc vô nghĩa đến hệ thống mục tiêu (ví dụ: máy chủ web, máy chủ email).

2. Tài nguyên bị quá tải: Hệ thống không thể xử lý hết các yêu cầu và dẫn đến cạn kiệt tài nguyên như CPU, RAM, hoặc băng thông mạng.

3. Từ chối dịch vụ: Kết quả là hệ thống không thể xử lý các yêu cầu hợp lệ của người dùng bình thường, dẫn đến từ chối dịch vụ.

Trong DDoS, kẻ tấn công sử dụng nhiều thiết bị bị xâm nhập (botnet) để đồng thời gửi yêu cầu đến mục tiêu từ nhiều nguồn, làm tăng hiệu quả và độ khó trong việc phát hiện và ngăn chặn.

* **Dấu hiệu nhận biết khi bị tấn công:**

Một số dấu hiệu nhận biết khi một hệ thống bị tấn công DoS hoặc DDoS:

* Hiệu suất hệ thống chậm: Các dịch vụ hoặc ứng dụng chậm hoặc không thể truy cập.
* Tăng đột biến lưu lượng mạng: Lưu lượng truy cập mạng tăng đột biến bất thường từ một hoặc nhiều nguồn.
* Trang web hoặc dịch vụ không phản hồi: Trang web hoặc dịch vụ trở nên không thể truy cập đối với người dùng.
* Băng thông mạng bị tiêu thụ hết: Hệ thống bị cạn kiệt băng thông mạng khiến các dịch vụ mạng bị đình trệ.
* Sự tăng vọt trong yêu cầu đến từ địa chỉ IP hoặc địa điểm đáng ngờ: Tăng mạnh yêu cầu từ các địa chỉ IP không xác định hoặc từ nhiều quốc gia cùng một lúc.
* **Cách kiểu tấn công Ransomeware:**

1. Flood Attack: Kẻ tấn công gửi một lượng lớn các yêu cầu đến máy chủ, gây quá tải băng thông hoặc làm cạn kiệt tài nguyên hệ thống.

Ví dụ: HTTP Flood, SYN Flood, UDP Flood.

2. Ping of Death: Kẻ tấn công gửi một gói tin Ping có kích thước quá lớn, gây ra lỗi trong hệ thống đích và dẫn đến sự sụp đổ của hệ thống.

3. Buffer Overflow Attack: Tấn công làm đầy bộ đệm của hệ thống, khiến nó không thể tiếp tục xử lý các yêu cầu hợp lệ.

4. Teardrop Attack: Kẻ tấn công gửi các gói tin bị phân mảnh không hợp lệ đến hệ thống, làm hệ thống không thể ghép lại các gói tin này và dẫn đến sụp đổ.

5. DDoS (Distributed Denial of Service): Cuộc tấn công từ nhiều nguồn khác nhau, thường sử dụng botnet để tấn công đồng thời từ hàng nghìn hoặc hàng triệu thiết bị.

* **Các phương pháp phòng chống cơ bản:**
* **Sử dụng tường lửa (Firewall):** Cấu hình tường lửa để lọc lưu lượng độc hại và giới hạn số lượng yêu cầu từ các địa chỉ IP đáng ngờ.
* **Hệ thống phòng thủ DDoS chuyên dụng:** Sử dụng các giải pháp phòng chống DDoS từ các nhà cung cấp dịch vụ bảo mật hoặc đám mây để phân tích và lọc lưu lượng mạng đáng ngờ.
* **Giới hạn tốc độ yêu cầu**: Áp dụng giới hạn băng thông và số lượng yêu cầu từ mỗi nguồn để tránh các cuộc tấn công flood.
* **Cập nhật và vá lỗi hệ thống:** Đảm bảo hệ điều hành, ứng dụng và hệ thống mạng được cập nhật thường xuyên để vá các lỗ hổng có thể bị khai thác.
* **Sử dụng mạng phân phối nội dung (CDN):** CDN giúp phân tán lưu lượng truy cập và bảo vệ hệ thống khỏi bị quá tải bằng cách phục vụ nội dung từ nhiều máy chủ phân tán.
* **Giám sát lưu lượng mạng:** Liên tục theo dõi lưu lượng truy cập để phát hiện sớm các dấu hiệu tấn công và có biện pháp phòng chống kịp thời.

#### Man in the Middle Attack

* **Định nghĩa:**

**Man-in-the-Middle (MitM) Attack** là một hình thức tấn công mạng trong đó kẻ tấn công âm thầm chặn, theo dõi hoặc can thiệp vào giao tiếp giữa hai bên (thường là giữa người dùng và máy chủ) mà hai bên không hay biết. Mục đích của tấn công MitM có thể là đánh cắp thông tin nhạy cảm, như thông tin đăng nhập, số thẻ tín dụng hoặc làm giả mạo nội dung giao tiếp.

* **Cơ chế hoạt động:**

MitM tấn công thường diễn ra qua nhiều bước:

1. Chặn đường truyền: Kẻ tấn công đứng giữa luồng giao tiếp giữa hai bên và giám sát tất cả dữ liệu trao đổi. Điều này có thể xảy ra thông qua nhiều phương pháp như:

* Nghe trộm Wi-Fi công cộng: Hacker có thể truy cập vào các mạng Wi-Fi không an toàn để theo dõi lưu lượng truy cập.
* DNS Spoofing: Kẻ tấn công làm giả địa chỉ DNS, chuyển hướng người dùng đến trang web độc hại thay vì trang web thực.
* ARP Spoofing: Kẻ tấn công giả mạo địa chỉ MAC trong mạng LAN để chặn lưu lượng mạng giữa hai thiết bị.

2. Giả mạo danh tính: Kẻ tấn công có thể đóng giả một bên trong giao tiếp để người dùng tin tưởng và cung cấp thông tin cá nhân hoặc nhạy cảm.

3. Chuyểntiếp hoặc thay đổi dữ liệu: Sau khi chặn thông tin, kẻ tấn công có thể chuyển tiếp hoặc sửa đổi nội dung tin nhắn, dữ liệu mà hai bên giao tiếp không phát hiện ra.

* **Dấu hiệu nhận biết khi bị tấn công:**

Tấn công MitM khó phát hiện do nó xảy ra trong thời gian thực mà không để lại dấu vết rõ ràng. Tuy nhiên, một số dấu hiệu có thể giúp nhận biết:

* Cảnh báo chứng chỉ SSL: Khi truy cập trang web và xuất hiện cảnh báo về chứng chỉ không hợp lệ hoặc kết nối không an toàn (HTTPS), có khả năng kẻ tấn công đang can thiệp vào kết nối.
* Hiệu suất mạng chậm: Kết nối internet hoặc mạng nội bộ chậm bất thường, có thể do kẻ tấn công đang chặn dữ liệu và gây tắc nghẽn.
* Chuyển hướng đến trang web lạ: Bạn bị chuyển hướng đến trang web không đúng địa chỉ mà bạn dự định truy cập.
* Yêu cầu thông tin lạ từ ứng dụng hoặc trang web: Các yêu cầu bất thường về thông tin cá nhân từ những nguồn đáng tin cậy có thể là dấu hiệu của việc tấn công MitM.
* **Cách kiểu tấn công MitM:**

**1. Wi-Fi Eavesdropping:** Kẻ tấn công kết nối vào mạng Wi-Fi công cộng không bảo mật để nghe trộm toàn bộ dữ liệu trao đổi.

**2. Session Hijacking**: Kẻ tấn công đánh cắp phiên làm việc của người dùng (cookie session) trên một trang web để chiếm quyền truy cập vào tài khoản của người đó mà không cần mật khẩu.

**3. DNS Spoofing:** Kẻ tấn công can thiệp vào hệ thống DNS, chuyển hướng người dùng đến trang web giả mạo khi họ nhập địa chỉ URL hợp lệ.

**4. HTTPS Spoofing:** Kẻ tấn công làm giả chứng chỉ SSL của các trang web để người dùng tin tưởng và nhập thông tin cá nhân trên trang web giả.

**5. Email Hijacking:** Kẻ tấn công chiếm quyền truy cập vào tài khoản email của người dùng và theo dõi hoặc thay đổi nội dung giao tiếp, ví dụ như các thông tin giao dịch tài chính.

* **Các phương pháp phòng chống cơ bản:**
* **Sử dụng mã hóa mạnh (SSL/TLS):** Luôn đảm bảo rằng các trang web và dịch vụ sử dụng giao thức bảo mật HTTPS (SSL/TLS) để mã hóa giao tiếp giữa trình duyệt và máy chủ.
* **Tránh sử dụng Wi-Fi công cộng không an toàn:** Không sử dụng mạng Wi-Fi công cộng mở hoặc không bảo mật để truy cập vào các trang web hoặc dịch vụ yêu cầu thông tin nhạy cảm.
* **Sử dụng VPN (Mạng riêng ảo):** VPN giúp mã hóa toàn bộ dữ liệu gửi và nhận qua internet, làm cho kẻ tấn công không thể theo dõi hoặc chặn dữ liệu.
* **Xác thực mạnh (Strong Authentication):** Sử dụng xác thực hai yếu tố (2FA) để tăng cường bảo mật cho các tài khoản trực tuyến, giúp hạn chế tấn công giả mạo danh tính.
* **Cảnh giác với các cảnh báo về chứng chỉ SSL:** Không truy cập vào các trang web xuất hiện cảnh báo về chứng chỉ không hợp lệ hoặc kết nối không an toàn.
* **Cập nhật phần mềm và hệ điều hành:** Luôn cập nhật phiên bản mới nhất của phần mềm, trình duyệt, và hệ điều hành để vá các lỗ hổng bảo mật có thể bị khai thác bởi kẻ tấn công.
* **Giám sát mạng liên tục:** Sử dụng các công cụ phát hiện xâm nhập (IDS) để theo dõi và phát hiện sớm các cuộc tấn công MitM.

#### Cryptojacking Attack

* **Định nghĩa:**

**Cryptojacking** là hình thức tấn công mạng trong đó kẻ tấn công chiếm quyền kiểm soát tài nguyên hệ thống của nạn nhân (máy tính, thiết bị di động, hoặc máy chủ) để khai thác tiền điện tử (cryptocurrency) mà không có sự cho phép. Nạn nhân có thể không biết rằng tài nguyên của họ đang bị sử dụng để phục vụ cho quá trình khai thác tiền điện tử. Điều này có thể xảy ra khi phần mềm độc hại được cài đặt trên thiết bị hoặc khi nạn nhân truy cập vào các trang web chứa mã khai thác tiền điện tử.

* **Cơ chế hoạt động:**

Cryptojacking hoạt động thông qua hai hình thức phổ biến:

1. Khai thác tiền điện tử dựa trên phần mềm độc hại (Malware-based Cryptojacking):

* Kẻ tấn công lây nhiễm phần mềm độc hại vào máy tính hoặc thiết bị của nạn nhân bằng cách gửi email độc hại, tải xuống phần mềm lậu, hoặc khai thác các lỗ hổng hệ thống. Phần mềm độc hại này sau đó âm thầm khai thác tiền điện tử bằng cách tận dụng CPU hoặc GPU của thiết bị.

2. Khai thác tiền điện tử dựa trên trình duyệt (Browser-based Cryptojacking):

* Kẻ tấn công nhúng mã JavaScript khai thác tiền điện tử vào một trang web. Khi người dùng truy cập trang web đó, mã JavaScript sẽ được chạy trên trình duyệt của người dùng và sử dụng tài nguyên máy tính của họ để khai thác tiền điện tử.
* **Dấu hiệu nhận biết khi bị tấn công:**
* Hiệu suất hệ thống chậm: Máy tính chạy chậm hoặc lag không rõ nguyên nhân, đặc biệt là khi truy cập vào một số trang web cụ thể.
* Quạt máy tính chạy liên tục: Hệ thống làm mát hoạt động mạnh, quạt CPU hoặc GPU chạy liên tục mà không có tác vụ nặng nào đang chạy.
* Nhiệt độ tăng cao: Thiết bị nóng hơn bình thường do việc sử dụng tài nguyên quá mức.
* Hóa đơn tiền điện tăng cao: Khai thác tiền mã hóa làm tăng lượng tiêu thụ điện năng một cách bất thường.
* Sử dụng CPU/GPU tăng đột ngột: Khi kiểm tra Task Manager hoặc Activity Monitor, bạn sẽ thấy mức sử dụng CPU hoặc GPU tăng cao ngay cả khi không chạy các chương trình nặng.
* **Cách kiểu tấn công Cryptojacking:**

1. Malware-based Cryptojacking: Sử dụng phần mềm độc hại để xâm nhập hệ thống và thực hiện việc đào tiền mã hóa.

2. Browser-based Cryptojacking: Chèn mã JavaScript vào trang web hoặc quảng cáo trực tuyến, tự động chạy khi người dùng truy cập và khai thác tài nguyên ngay trên trình duyệt.

3. Cloud-based Cryptojacking: Tấn công vào các nền tảng đám mây (cloud) để tận dụng tài nguyên mạnh mẽ từ các máy chủ cho việc khai thác tiền mã hóa.

* **Các phương pháp phòng chống cơ bản:**
* Cài đặt phần mềm diệt virus: Sử dụng các phần mềm bảo mật và diệt virus cập nhật để phát hiện và ngăn chặn mã độc.
* Sử dụng trình chặn mã độc: Các tiện ích mở rộng trình duyệt như NoScript hoặc MinerBlock giúp ngăn chặn mã JavaScript độc hại khai thác tài nguyên qua trình duyệt.
* Cập nhật phần mềm thường xuyên: Đảm bảo hệ điều hành, trình duyệt và các phần mềm khác được cập nhật để vá các lỗ hổng bảo mật.
* Giám sát hiệu suất hệ thống: Theo dõi hiệu suất CPU, GPU, và bộ nhớ để phát hiện sớm các dấu hiệu bất thường.
* Cấu hình bảo mật đám mây: Đối với các hệ thống trên nền tảng đám mây, cần đảm bảo rằng các biện pháp bảo mật và cấu hình xác thực được thiết lập đầy đủ

#### SQL Injection Attack

* **Định nghĩa:**

SQL Injection là một hình thức tấn công chèn mã SQL độc hại vào các truy vấn của cơ sở dữ liệu qua các điểm nhập liệu của ứng dụng web. Mục tiêu của tấn công này là truy xuất, thay đổi hoặc phá hủy dữ liệu trong cơ sở dữ liệu mà ứng dụng sử dụng, thậm chí là chiếm quyền điều khiển hệ thống.

* **Cơ chế hoạt động:**

SQL Injection hoạt động dựa trên việc lợi dụng các lỗ hổng trong cách xử lý các câu lệnh SQL của ứng dụng web, khi không có biện pháp bảo mật để phân biệt dữ liệu hợp lệ và dữ liệu độc hại. Cụ thể:

1. Điểm nhập liệu không được kiểm tra kỹ: Kẻ tấn công chèn các mã SQL vào các trường nhập liệu như biểu mẫu (form), URL, hoặc cookie.

2. Chạy truy vấn độc hại: Mã SQL được chèn vào sau đó được thực thi bởi cơ sở dữ liệu của ứng dụng, dẫn đến việc lấy cắp, sửa đổi dữ liệu, hoặc thậm chí xóa bỏ cơ sở dữ liệu.

Ví dụ:

* Một truy vấn SQL hợp lệ: SELECT \* FROM tblUsers WHERE username = ‘admin’ AND password = ‘123’;
* Nếu ứng dụng không kiểm tra kỹ đầu vào, kể tấn công có thể nhập thành: SELECT \* FROM tblUsers WHERE username = ‘admin’ -- ‘ AND password = ‘123’;
* Phần sau dấu -- là chú thích trong SQL, khiến phần kiểm tra mật khẩu bị bỏ qua và kẻ tấn công có thể truy cập mà không cần mật khẩu.
* **Dấu hiệu nhận biết khi bị tấn công:**
* Truy vấn SQL bị lỗi: Nếu trang web hiển thị các thông báo lỗi cơ sở dữ liệu bất thường như "SQL syntax error", điều này có thể là dấu hiệu của SQL Injection.
* Dữ liệu không đúng: Các thay đổi dữ liệu hoặc hiển thị dữ liệu không mong muốn, ví dụ như việc dữ liệu bị rò rỉ hoặc hiển thị bất thường trên giao diện.
* Hoạt động không bình thường trong cơ sở dữ liệu: Các truy vấn cơ sở dữ liệu hoặc thao tác xuất hiện bất thường có thể là dấu hiệu của SQL Injection.
* **Cách kiểu tấn công SQLi:**

1. In-band SQLi: Đây là kiểu tấn công phổ biến nhất, kẻ tấn công có thể gửi truy vấn SQL độc hại và ngay lập tức nhận được phản hồi từ cơ sở dữ liệu.

* Error-based SQLi: Kẻ tấn công khai thác các thông báo lỗi để lấy thông tin chi tiết về cơ sở dữ liệu.
* Union-based SQLi: Sử dụng từ khóa UNION để kết hợp kết quả từ nhiều truy vấn, kẻ tấn công có thể trích xuất dữ liệu từ bảng khác.

2. Blind SQLi: Cơ sở dữ liệu không trả về lỗi hoặc thông tin trực tiếp, nhưng kẻ tấn công vẫn có thể suy đoán thông tin qua các phản hồi đúng/sai của ứng dụng.

* Boolean-based Blind SQLi: Thao tác dựa trên việc kiểm tra câu trả lời "đúng/sai" từ hệ thống để suy luận về cấu trúc và nội dung của cơ sở dữ liệu.
* Time-based Blind SQLi: Dựa trên độ trễ phản hồi của hệ thống khi thực thi các truy vấn để xác định thông tin.

3. Out-of-band SQLi: Sử dụng các kênh khác như DNS hoặc HTTP để gửi và nhận thông tin, hữu ích khi kênh chính không thể phản hồi ngay lập tức.

* **Các phương pháp phòng chống cơ bản:**
* **Sử dụng Prepared Statements (Truy vấn có chuẩn bị):** Các truy vấn SQL được xây dựng trước với các biến số, ngăn chặn việc chèn mã SQL vào.
* Ví dụ (PHP với PDO):

$stmt = $pdo->prepare("SELECT \* FROM users WHERE username = :username AND password = :password");

$stmt->execute(['username' => $username, 'password' => $password]);

* Chú giải:

‘$pdo’ là đối tượng PDO (PHP Data Object) được tạo ra để kết nối với cơ sở dữ liệu. Nó đại diện cho kết nối đên cơ sở dữ liệu và cung cấp các phương thức để thực thi các câu truy vấn SQL.

‘Prepare()’ là phương thức của đối tượng PDO được sử dụng để chuẩn bị một truy vấn SQL. Việc chuẩn bị truy vấn trước giúp ngăn chặn SQL Injection. Truy vấn không được thực thi ngay lập tức mà chỉ được ‘chuẩn bị’ để thực hiện sau khi các tham số cần thiết được cung cấp

‘:’ đây là các placeholder (biến tham số), thay vì truyền trực tiếp giá trị đầu vào vào trong câu lệnh SQL, những giá trị này sẽ được gán sau khi câu truy vấn đã được chuẩn bị. Điều này giúp câu truy vấn không bị tác động bởi giá trị dữ liệu do người dùng nhập vào

‘execute()’ là phương thức được dùng để thực thi câu truy vấn đã chuẩn bị với các giá trị cụ thể. Trong trường hợp này, phương thức này sẽ gán các giá trị thực tế cho các placeholder và rồi thực thi câu lệnh SQL với những giá trị này.

* ‘['username' => $username, 'password' => $password]’: Đây là một mảng kết hợp (associative array) trong PHP. Mảng này chỉ định các giá trị sẽ được gán vào các placeholder:

‘:username’ sẽ được thay thế bằng giá trị của biến $username (có thể là dữ liệu người dùng nhập vào).

‘:password’ sẽ được thay thế bằng giá trị của biến $password.

* **Sử dụng ORM (Object-Relational Mapping):** Các framework ORM như Hibernate, Django ORM, hoặc Entity Framework giúp trừu tượng hóa việc truy cập cơ sở dữ liệu và hạn chế nguy cơ SQL Injection.
* **Kiểm tra và lọc đầu vào:** Luôn xác thực và giới hạn dữ liệu nhập từ người dùng. Chỉ cho phép các ký tự hợp lệ và từ chối các ký tự đặc biệt.
* **Sử dụng WAF (Web Application Firewall):** Một số WAF có khả năng phát hiện và chặn các cuộc tấn công SQL Injection.
* **Ẩn thông tin lỗi:** Tránh hiển thị các thông báo lỗi SQL chi tiết cho người dùng, vì điều này có thể cung cấp manh mối cho kẻ tấn công.
* **Cập nhật phần mềm:** Thường xuyên cập nhật hệ thống, cơ sở dữ liệu và các framework web để vá các lỗ hổng bảo mật.

#### Exploits Attack

* **Định nghĩa:**

Exploits Attack là hình thức tấn công mạng trong đó kẻ tấn công lợi dụng các lỗ hổng bảo mật trong phần mềm, hệ điều hành, hoặc phần cứng để chiếm quyền điều khiển hệ thống, gây mất dữ liệu hoặc làm gián đoạn dịch vụ. **Exploit** là đoạn mã hoặc công cụ mà kẻ tấn công sử dụng để khai thác những lỗ hổng này.

* **Cơ chế hoạt động:**

1. Tìm kiếm lỗ hổng: Kẻ tấn công thường sử dụng các công cụ tự động hoặc khai thác thông tin từ các cơ sở dữ liệu công khai về lỗ hổng CVE để xác định các điểm yếu trong hệ thống.

2. Phát triển hoặc sử dụng mã khai thác (exploit): Sau khi phát hiện lỗ hổng, kẻ tấn công sẽ tạo ra hoặc sử dụng các mã khai thác có sẵn để tấn công mục tiêu.

3. Thực thi mã độc: Một khi đã khai thác thành công lỗ hổng, kẻ tấn công có thể thực hiện nhiều hoạt động khác nhau như chiếm quyền điều khiển hệ thống, đánh cắp dữ liệu, cài mã độc, hoặc phá hủy dữ liệu.

4. Khai thác liên tục: Một số exploit còn có khả năng duy trì quyền truy cập, cho phép kẻ tấn công tiếp tục kiểm soát hoặc quay lại tấn công hệ thống vào lúc khác.

* **Dấu hiệu nhận biết khi bị tấn công:**
* Hiệu suất hệ thống bất thường: Hệ thống trở nên chậm, ứng dụng ngưng hoạt động hoặc có hiện tượng hoạt động không bình thường.
* Thông báo lỗi không rõ nguyên nhân: Người dùng gặp phải các thông báo lỗi hoặc sự cố liên quan đến phần mềm hoặc hệ điều hành một cách đột ngột.
* Tập tin hoặc dữ liệu bị thay đổi hoặc mất: Một số dữ liệu có thể bị sửa đổi, mất, hoặc bị truy cập trái phép mà không có sự cho phép của người dùng hợp pháp.
* Hoạt động mạng bất thường: Tăng đột ngột trong lưu lượng mạng hoặc các kết nối đáng ngờ từ các IP không xác định.
* Hệ thống bảo mật bị vô hiệu hóa: Các phần mềm diệt virus, firewall hoặc công cụ bảo mật khác bị vô hiệu hóa mà không có sự can thiệp từ người dùng.
* **Cách kiểu tấn công Exploits:**

1. Buffer Overflow Exploid: Đây là dạng tấn công khai thác lỗ hổng khi một ứng dụng không kiểm soát được kích thước của dữ liệu được nhập vào bộ đệm (buffer), dẫn đến việc ghi đè lên các vùng bộ nhớ khác. Tin tặc có thể chèn mã độc vào vùng bộ nhớ bị ghi đè, từ đó thực thi mã này trên hệ thống.

2. Privilege Escalation Exploit: Tấn công này lợi dụng các lỗ hổng để kẻ tấn công có thể nâng quyền từ người dùng bình thường lên quyền quản trị hoặc hệ thống, từ đó có thể thực hiện các hành động mà họ không được phép thực hiện

3. Remote Code Execution (RCE): Đây là dạng tấn công lợi dụng lỗ hổng để thực thi mã độc từ xa mà không cần truy cập trực tiếp vào hệ thống. Điều này cho phép kẻ tấn công chạy bất kỳ lệnh nào trên máy nạn nhân.

4. Zero-Day Exploit: Đây là cuộc tấn công khai thác lỗ hổng chưa được biết đến hoặc chưa được vá bởi nhà cung cấp phần mềm. Vì lỗ hổng chưa được công bố hoặc chưa có bản vá, các hệ thống dễ dàng bị tấn công nếu bị khai thác

5. Cross-Site Scripting (XSS) Exploit: Đây là dạng tấn công khai thác lỗ hổng trong ứng dụng web, trong đó kẻ tấn công có thể chèn mã javascript độc hại vào trang web và mã này sẽ được thực thi trong trình duyệt của người khác

6. Denial of Service (DoS) Exploit: Tấn công này khai thác lỗ hổng trong hệ thống hoặc ứng dụng, khiến nó không thể cung cấp dịch vụ bình thường cho người dùng hợp pháp

7. Heap Spray Exploit: Đây là dạng tấn công khai thác lỗ hổng bộ nhớ động (heap) bằng cách cố tình làm đầy bộ nhớ với dữ liệu độc hại, sau đó kích hoạt khai thác tại vị trí bộ nhớ chứa mã độc để thực thi mã

* **Các phương pháp phòng chống cơ bản:**
* Cập nhật và vá lỗi phần mềm:
* Đảm bảo rằng hệ thống, phần mềm, và các ứng dụng đều được cập nhật thường xuyên để vá các lỗ hổng bảo mật. Các nhà phát triển liên tục phát hành các bản vá để sửa các lỗ hổng được phát hiện.Ví dụ: Sử dụng hệ thống quản lý bản vá (patch management) để tự động cập nhật các bản vá bảo mật cho hệ điều hành và phần mềm.
* Sử dụng cơ chế ASLR (Address Space Layout Randomization):
* ASLR là một cơ chế bảo mật giúp ngẫu nhiên hóa vị trí bộ nhớ của các đối tượng trong hệ thống, làm giảm hiệu quả của các cuộc tấn công khai thác dựa trên bộ nhớ như Buffer Overflow hoặc Heap Spray.Ví dụ: Kích hoạt ASLR trên các hệ điều hành như Linux hoặc Windows.
* Sử dụng DEP (Data Execution Prevention):
* DEP ngăn chặn các cuộc tấn công bằng cách đánh dấu các vùng bộ nhớ không thể thực thi được, ngăn chặn việc mã độc được thực thi từ các vùng bộ nhớ không hợp lệ. Ví dụ: Kích hoạt DEP trên các hệ điều hành để bảo vệ khỏi tấn công Buffer Overflow.
* Kiểm tra và lọc dữ liệu đầu vào:
* Các lỗ hổng như SQL Injection hay XSS thường xảy ra do việc không kiểm tra hoặc không lọc đúng dữ liệu đầu vào từ người dùng. Luôn xác thực và giới hạn dữ liệu nhập vào để ngăn chặn việc chèn mã độc. Ví dụ: Sử dụng các thư viện lọc đầu vào và cơ chế "prepared statements" trong SQL để tránh SQL Injection.
* Sử dụng hệ thống phát hiện và ngăn chặn tấn công (IDS/IPS):
* Hệ thống IDS/IPS có thể giúp phát hiện các cuộc tấn công đang xảy ra bằng cách giám sát các hoạt động mạng và hệ thống. Khi phát hiện một cuộc tấn công, hệ thống có thể chặn hoặc cảnh báo. Ví dụ: Sử dụng Snort hoặc Suricata để giám sát và phát hiện các hành vi khai thác lỗ hổng.
* Tường lửa ứng dụng web (WAF):
* WAF giúp lọc và giám sát lưu lượng HTTP, ngăn chặn các cuộc tấn công dựa trên web như SQL Injection hoặc Cross-Site Scripting (XSS). Ví dụ: Sử dụng WAF như ModSecurity để bảo vệ các ứng dụng web khỏi các lỗ hổng bảo mật phổ biến.
* Sao lưu dữ liệu thường xuyên:
* Để đối phó với các cuộc tấn công ransomware hoặc các dạng khai thác có thể làm mất dữ liệu, việc sao lưu dữ liệu thường xuyên là rất quan trọng. Ví dụ: Thiết lập quy trình sao lưu dữ liệu hàng ngày hoặc hàng tuần và lưu trữ tại các vị trí an toàn.
* Đào tạo nhận thức bảo mật cho nhân viên:
* Đào tạo cho người dùng và nhân viên cách nhận biết các cuộc tấn công như phishing hoặc cách nhận dạng các tệp đính kèm hoặc liên kết đáng ngờ. Ví dụ: Thực hiện các chương trình đào tạo bảo mật định kỳ, tăng cường nhận thức về cách phòng tránh và đối phó với các cuộc tấn công khai thác lỗ hổng.
* Sử dụng phần mềm diệt virus và các công cụ bảo mật khác:
* Phần mềm diệt virus và các công cụ bảo mật khác có thể giúp phát hiện các mã độc hoặc khai thác lỗ hổng trước khi chúng gây hại cho hệ thống. Ví dụ: Sử dụng các phần mềm bảo mật như Kaspersky, Norton hoặc Bitdefender để giám sát và bảo vệ hệ thống.

## Tổng quan về giám sát mạng

### Giám sát mạng là gì?

Giám sát mạng (Network Monitoring): tập trung vào việc theo dõi và quản lý hiệu suất, lưu lượng mạng, giám sát các thiết bị mạng (router, switch, firewall, máy chủ,…) và phát hiện lỗi, các sự cố xảy ra, vấn đề về kết nối hoặc suy giám hiệu suất

### Các thành phần của một hệ thống giám sát

Một hệ thống quản trị giám sát gồm có nhiều thành phần:

1. **Máy trinh sát (Sensor):** làm nhiệm vụ tiếp cận, tương tác với các hệ thống và dịch vụ cần giám sát để nhận biết trạng thái của những dịch vụ đó. Trong quá trình triển khai hệ thống, thành phần này sẽ được phân tán nằm rải rác nhiều nơi trên mạng để thu nhập thông tin từ những nguồn khác nhau như router, tường lửa, file nhật ký, …

2. **Máy thu thập (Collector):** Do các hệ thống, dịch vụ cần giám sát trong một hệ thống mạng có thể khác nhau vậy nên, để có thể lấy được thông tin một cách đồng nhất nhằm mục đích xử lý và thống kê, cần có một thành phần làm nhiệm vụ chuẩn hóa thông tin. Máy thu thập sẽ đọc những thông tin thu được từ các máy trinh sát và chuẩn hóa thông tin dựa trên những quy tắc biết trước. Thông tin đầu ra sẽ có định dạng giống nhau và được lưu vào cơ sở dữ liệu trung tâm.

3. **Cơ sở dữ liệu trung tâm:** Là nơi lưu trữ dữ liệu của toàn bộ hệ thống quản trị giám sát. Các dữ liệu ở đây đã được chuẩn hóa nên có thể sử dụng để tính toán các số liệu thống kê trên toàn hệ thống.

4. **Công cụ phân tích (Analysis tool):** Thành phần này sẽ đọc các dữ liệu từ cơ sở dữ liệu trung tâm và tính toán để tạo ra bản báo cáo số liệu thống kê trên toàn hệ thống.

Cơ chế hoạt động:

**Mỗi máy trinh sát** sẽ có một danh sách những đối tượng (nhật ký hoạt động, thành phần báo cáo trạng thái của router/tường lửa) mà **máy trinh sát** đó cần giám sát, dựa vào danh sách này **máy trinh sát** sẽ gửi truy vấn đến những đối tượng đó để lấy thông tin. Thông tin thu được sẽ gửi đến **máy thu thập** để chuẩn hóa rồi mới lưu trữ vào **cơ sở dữ liệu trung tâm**. Tùy theo thiết kế của hệ thống, nếu thông tin mà **máy trinh sát** thu được có định dáng giống nhau thì sẽ không cần đến **máy thu thập**.

Các **máy trinh sát** cũng có thể kiêm luôn **máy thu thập** thực hiện chuẩn hóa dữ liệu trong một số trường hợp. Thông tin được lưu trữ trong **cơ sở dữ liệu trung tâm** đã có định dạng rõ ràng, **bộ phân tích** sẽ đọc để xử lý và đưa ra số liệu thống kê tạo thành một bản báo cáo hoàn chỉnh rồi gửi báo cáo này cho quản trị viên. Trong một số hệ thống, **bộ phân tích** có thể thêm chức năng phát hiện dấu hiệu xác định trước(Ví dụ: Đăng nhập sai liên tiếp 3 lần trong 5 phút) để phát ra cảnh báo tới quản trị viên, cảnh báo có thể là SMS, Email,…

Thu thập dữ liệu chính là việc lấy các thông tin liên quan đến tình trạng hoạt động của các thiết bị trong hệ thống mạng, trong những hệ thống lớn, các thiết bị, dịch vụ sẽ nằm trên các máy chủ, các hệ thống con riêng biệt nhau, các thành phần của hệ thống cũng hoạt động trên các nền tảng khác nhau. Có 2 phương pháp để thu thập dữ liệu:

* Phương pháp đẩy (Push Method): Các thông tin từ các thiết bị, dịch vụ cần theo dõi sẽ tự động đẩy về các **máy thu thập** theo một lịch trình hoặc khi có sự kiện xảy ra.
* Phương pháp kéo (Pull Method): Các **máy thu thập** chủ động gửi yêu cầu kéo dữ liệu từ các thiết bị, dịch vụ đang giám sát về theo lịch trình cố định.

Sau khi thông tin đã được thu thập về hệ thống thì tiếp theo đến việc phân tích, cụ thể là sắp xếp dữ liệu, phát hiện bất thường, những mối đe dọa dựa trên thông tin về lưu lượng truy cập, trạng thái truy cập, định dạng request,…

Phân tích dữ liệu xong sẽ đến việc thực hiện đánh giá, đưa thông tin cảnh báo tới quản trị viên và hiện phản ứng, hành động chống lại các mối đe dọa, khắc phục sự cố có thể xảy ra nếu có.



Hình 2.4: Cơ chế hoạt động cơ bản của một hệ thống giám sát

# GIẢI PHÁP

## 2.1 Zabbix

**Zabbix** là một phần mềm mã nguồn mở mạnh mẽ dùng để giám sát hiệu năng và tính khả dụng của các hệ thống IT, bao gồm máy chủ, thiết bị mạng, ứng dụng và dịch vụ. Được thiết kế cho các doanh nghiệp vừa và lớn, Zabbix cung cấp khả năng giám sát tập trung với nhiều tính năng tiên tiến. Dưới đây là một số điểm nổi bật về Zabbix:

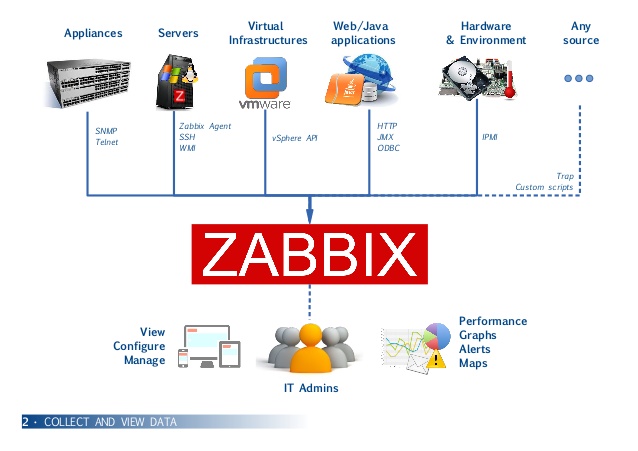
### Chức năng chính của Zabbix:

* **Giám sát tài nguyên hệ thống:** Theo dõi hiệu suất của CPU, bộ nhớ, đĩa cứng, lưu lượng mạng và nhiều tài nguyên khác.
* **Giám sát ứng dụng:** Zabbix có thể giám sát trạng thái và hiệu suất của các ứng dụng doanh nghiệp như cơ sở dữ liệu (MySQL, PostgreSQL), ứng dụng web, dịch vụ email và nhiều ứng dụng khác.
* **Cảnh báo và thông báo:** Hệ thống cảnh báo được cấu hình linh hoạt, có thể gửi thông báo qua email, SMS, hoặc các phương tiện khác khi một sự cố xảy ra.
* **Khả năng mở rộng:** Zabbix hỗ trợ các môi trường từ nhỏ đến rất lớn, cho phép giám sát hàng ngàn thiết bị.
* **Báo cáo và biểu đồ:** Cung cấp báo cáo chi tiết và biểu đồ thời gian thực giúp người quản trị dễ dàng theo dõi tình hình hệ thống.
* **Tùy biến linh hoạt:** Hỗ trợ tạo các trigger (điều kiện kích hoạt cảnh báo) và biểu đồ tùy chỉnh theo nhu cầu của người dùng.

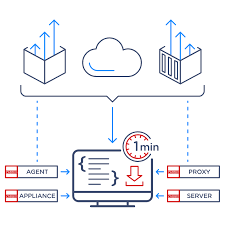
### Kiến trúc của Zabbix:

Zabbix có kiến trúc client-server, bao gồm các thành phần chính:

* **Zabbix Server:** Là thành phần trung tâm, nhận dữ liệu từ các Zabbix Agent hoặc các nguồn giám sát khác.



* **Zabbix Agent:** Được cài đặt trên các máy chủ và thiết bị cần giám sát để thu thập dữ liệu và gửi về cho Zabbix Server.



* **Zabbix Proxy:** Một thành phần trung gian giúp thu thập dữ liệu từ các môi trường giám sát từ xa và gửi về Zabbix Server.
* **Cơ sở dữ liệu:** Zabbix sử dụng cơ sở dữ liệu để lưu trữ thông tin cấu hình, dữ liệu giám sát và lịch sử.
* **Web Interface:** Giao diện web cho phép quản lý và theo dõi dữ liệu giám sát.

### Các tính năng nổi bật của Zabbix:

* **Hỗ trợ nhiều nền tảng:** Zabbix Agent có thể cài đặt trên nhiều hệ điều hành như Linux, Windows, macOS, Solaris và FreeBSD.
* **Khả năng mở rộng:** Có thể dễ dàng mở rộng hệ thống giám sát theo nhu cầu tăng trưởng của doanh nghiệp.
* **Hỗ trợ SNMP và IPMI:** Cho phép giám sát các thiết bị mạng và máy chủ thông qua các giao thức phổ biến như SNMP (Simple Network Management Protocol) và IPMI (Intelligent Platform Management Interface).
* **Tự động khám phá:** Zabbix có khả năng tự động phát hiện các thiết bị mới trong mạng.
* **Tích hợp API:** Zabbix cung cấp API cho phép tích hợp với các hệ thống quản lý và công cụ khác.
* **Bảo mật:** Hỗ trợ mã hóa dữ liệu giữa các thành phần để đảm bảo an toàn thông tin.

### Lợi ích của Zabbix:

* **Tiết kiệm chi phí:** Zabbix là mã nguồn mở và miễn phí, không yêu cầu chi phí giấy phép.
* **Khả năng mở rộng và tùy biến cao:** Dễ dàng tùy chỉnh để phù hợp với nhu cầu của từng tổ chức.
* **Cộng đồng hỗ trợ mạnh mẽ:** Do là phần mềm mã nguồn mở, Zabbix có một cộng đồng lớn hỗ trợ và phát triển.

### Ứng dụng trong thực tế:

* **Doanh nghiệp lớn:** Zabbix thường được sử dụng để giám sát hạ tầng IT phức tạp với hàng ngàn thiết bị và dịch vụ.
* **Nhà cung cấp dịch vụ:** Các nhà cung cấp dịch vụ sử dụng Zabbix để giám sát hiệu suất dịch vụ, đảm bảo chất lượng.
* **Tổ chức giáo dục:** Zabbix cũng được dùng trong các môi trường học thuật để quản lý và giám sát hạ tầng IT.

## Snort

**Snort** là một hệ thống phát hiện xâm nhập (IDS - Intrusion Detection System) mã nguồn mở, do công ty **Sourcefire** phát triển và hiện được duy trì bởi **Cisco Systems**. Snort có thể hoạt động như một IDS hoặc một hệ thống ngăn chặn xâm nhập (IPS - Intrusion Prevention System) để giám sát, phân tích lưu lượng mạng và bảo vệ mạng khỏi các cuộc tấn công bảo mật.

### Chức năng chính của Snort:

* **Phân tích và ghi lại lưu lượng mạng theo thời gian thực:** Snort giám sát lưu lượng mạng đi qua các giao diện mạng và phân tích dữ liệu đó dựa trên các quy tắc được định nghĩa.
* **Phát hiện xâm nhập:** Phát hiện các cuộc tấn công mạng và các hoạt động bất thường bằng cách kiểm tra các gói dữ liệu và so sánh chúng với cơ sở dữ liệu các dấu hiệu tấn công (signature-based detection).
* **Ngăn chặn tấn công (IPS):** Ngoài khả năng phát hiện, Snort cũng có thể ngăn chặn các tấn công bằng cách chặn hoặc loại bỏ các gói dữ liệu có vấn đề (tính năng IPS).
* **Phân tích lưu lượng mạng:** Snort cung cấp khả năng phân tích lưu lượng mạng để phát hiện các lỗ hổng bảo mật, quét cổng (port scanning), các cuộc tấn công từ chối dịch vụ (DoS), và nhiều loại tấn công khác.
* **Ghi lại dữ liệu:** Snort có thể ghi lại các gói tin để phân tích sau hoặc lưu giữ hồ sơ cho mục đích điều tra sau này.

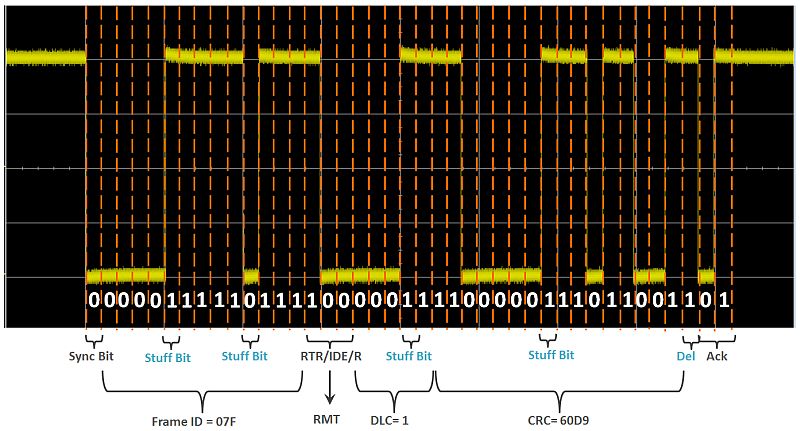
### Các chế độ hoạt động của Snort:

* **Sniffer Mode (Chế độ nghe lén):** Trong chế độ này, Snort chỉ đơn giản là đọc các gói tin mạng và hiển thị nội dung của chúng trên màn hình.
* **Packet Logger Mode (Chế độ ghi gói tin):** Snort ghi lại lưu lượng mạng vào một tệp nhật ký để phân tích sau này.
* **Network Intrusion Detection System (NIDS):** Trong chế độ này, Snort phân tích lưu lượng mạng theo thời gian thực và phát hiện các hành vi nguy hiểm dựa trên các dấu hiệu tấn công.
* **Intrusion Prevention System (IPS):** Snort không chỉ phát hiện mà còn có thể ngăn chặn các cuộc tấn công bằng cách loại bỏ hoặc thay đổi các gói tin độc hại.

### Kiến trúc của Snort:

Snort có kiến trúc module, bao gồm các thành phần chính:

* **Packet Decoder (Bộ giải mã gói tin):** Giải mã và xử lý các gói tin mạng để chuẩn bị cho việc phân tích.

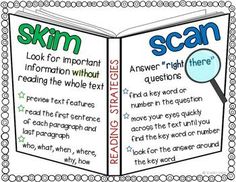


* **Preprocessors (Các bộ xử lý trước):** Thực hiện các bước xử lý và chỉnh sửa các gói tin trước khi chúng được đưa vào phân tích. Ví dụ, xử lý gói tin phân mảnh hoặc mã hóa.
* **Detection Engine (Bộ phát hiện):** Phần quan trọng nhất của Snort, thực hiện so khớp các gói tin với các quy tắc để phát hiện các mối đe dọa. Quy tắc này có thể là dấu hiệu của một cuộc tấn công hoặc một hành vi bất thường trong lưu lượng mạng.
* **Logging and Alerting System (Hệ thống ghi nhật ký và cảnh báo):** Sau khi phát hiện một cuộc tấn công, Snort sẽ ghi lại thông tin hoặc gửi cảnh báo đến người quản trị.
* **Output Modules (Các mô-đun xuất):** Xử lý và định dạng các kết quả ghi nhận để dễ dàng theo dõi hoặc tích hợp với các hệ thống giám sát khác.

### Cách thức hoạt động của Snort:

Snort sử dụng các **quy tắc (rules)** để xác định các mối đe dọa. Mỗi quy tắc là một mẫu để kiểm tra các gói tin nhằm phát hiện hành vi độc hại. Các quy tắc này có thể được chia thành nhiều nhóm như:

* **Attack Rules (Quy tắc tấn công):** Xác định các cuộc tấn công đã biết như SQL Injection, tấn công DDoS, hay tấn công buffer overflow.
* **Exploit Rules (Quy tắc khai thác lỗ hổng):** Xác định các nỗ lực khai thác lỗ hổng bảo mật đã được công bố.
* **Scan Rules (Quy tắc quét):** Phát hiện các hoạt động quét cổng (port scanning), một bước phổ biến trong các cuộc tấn công mạng.



Người dùng cũng có thể tùy chỉnh và thêm các quy tắc của riêng mình dựa trên nhu cầu cụ thể của hệ thống hoặc mạng.

### Ưu điểm của Snort:

* **Mã nguồn mở và miễn phí:** Snort là phần mềm mã nguồn mở và có sẵn miễn phí, điều này giúp doanh nghiệp tiết kiệm chi phí.
* **Dễ dàng triển khai:** Cài đặt và cấu hình Snort khá dễ dàng so với các hệ thống IDS/IPS khác.
* **Cộng đồng mạnh mẽ:** Vì là một phần mềm mã nguồn mở, Snort có một cộng đồng lớn hỗ trợ và đóng góp vào việc phát triển, bao gồm việc tạo ra các quy tắc phát hiện mới.
* **Khả năng tùy biến cao:** Người dùng có thể tạo và cấu hình các quy tắc phát hiện tùy chỉnh dựa trên nhu cầu bảo mật của hệ thống.
* **Khả năng phát hiện và phản ứng linh hoạt:** Snort có thể hoạt động như một hệ thống phát hiện xâm nhập (IDS) hoặc một hệ thống ngăn chặn xâm nhập (IPS) tùy thuộc vào cấu hình.

### Nhược điểm của Snort:

* **Phát hiện dựa trên signature:** Vì chủ yếu dựa trên các dấu hiệu (signature-based detection), Snort có thể không phát hiện được các cuộc tấn công chưa biết hoặc tấn công zero-day.
* **Khả năng mở rộng hạn chế:** Khi triển khai trong các môi trường mạng lớn, Snort có thể gặp vấn đề với hiệu suất và cần tối ưu hóa cẩn thận.
* **Ứng dụng thực tiễn của Snort:**
* **Doanh nghiệp:** Snort thường được các doanh nghiệp sử dụng để bảo vệ mạng khỏi các cuộc tấn công và giám sát lưu lượng mạng.
* **Tổ chức giáo dục:** Các trường đại học và tổ chức học thuật sử dụng Snort để nghiên cứu và bảo vệ hạ tầng mạng của họ.
* **Nhà cung cấp dịch vụ:** Snort được các nhà cung cấp dịch vụ mạng sử dụng để bảo vệ mạng của khách hàng khỏi các mối đe dọa.

## Site24x7

Site24x7 là một nền tảng giám sát dựa trên đám mây toàn diện, cung cấp các công cụ giám sát hiệu suất cho các hệ thống CNTT, bao gồm trang web, ứng dụng, máy chủ, mạng và trải nghiệm người dùng cuối. Được phát triển bởi Zoho Corporation, Site24x7 tập trung vào việc cung cấp giải pháp giám sát dễ sử dụng, có khả năng mở rộng và đáp ứng cho các tổ chức, doanh nghiệp vừa và nhỏ, cũng như các tổ chức lớn.

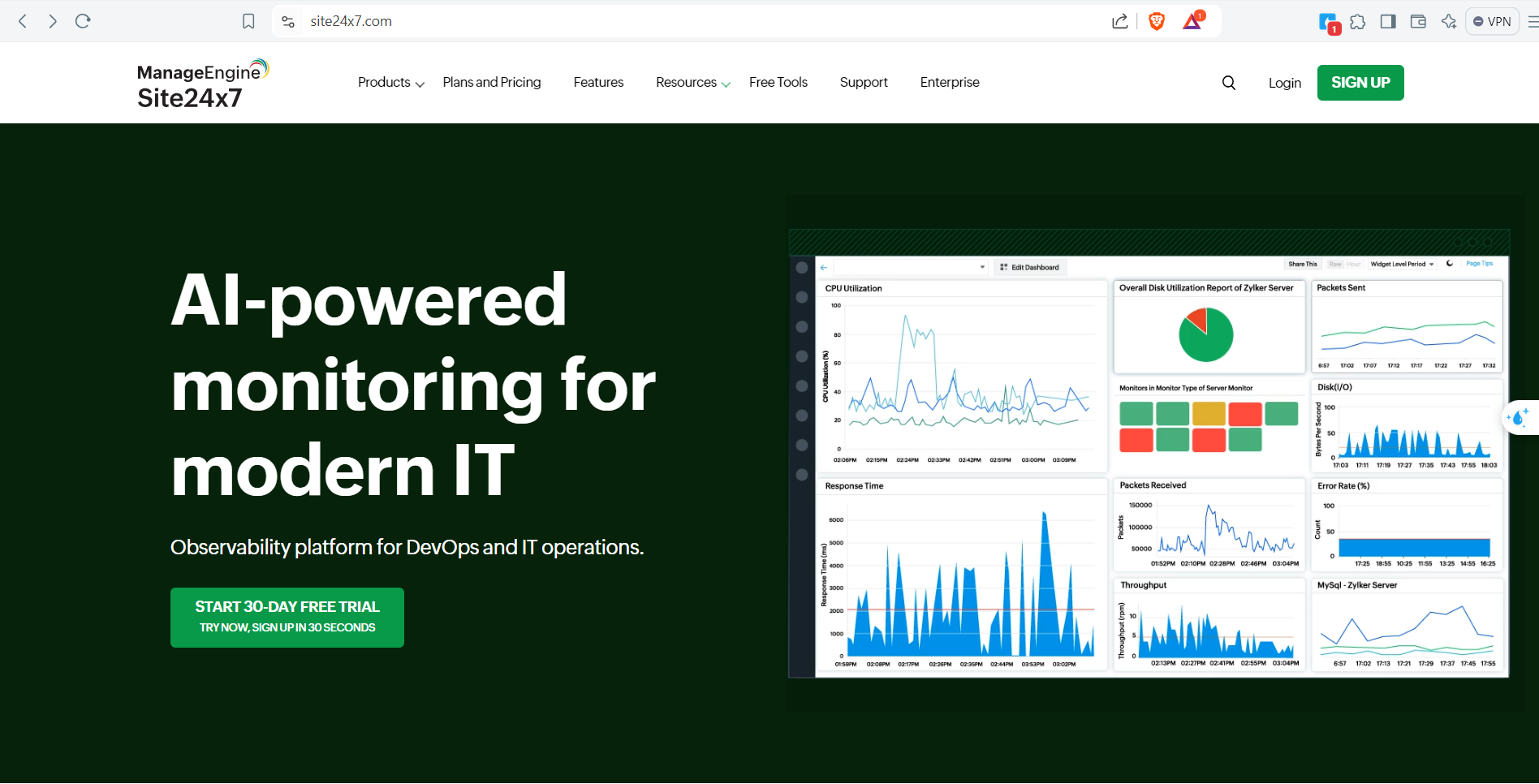
### Các chức năng chính của Site24x7:

* **Giám sát trang web:** Giám sát thời gian hoạt động (uptime), hiệu suất và thời gian phản hồi của các trang web từ nhiều vị trí trên thế giới, giúp đảm bảo trang web luôn hoạt động mượt mà.
* **Giám sát ứng dụng**: Theo dõi hiệu suất của các ứng dụng web và ứng dụng di động, bao gồm việc theo dõi các giao dịch, thời gian phản hồi và trải nghiệm người dùng cuối.
* **Giám sát máy chủ:** Giám sát tài nguyên hệ thống như CPU, bộ nhớ, ổ đĩa và mạng của máy chủ trên các hệ điều hành như Windows, Linux, Unix và FreeBSD.
* **Giám sát mạng**: Kiểm tra hiệu suất mạng thông qua việc giám sát các thiết bị mạng như bộ định tuyến, switch, và tường lửa bằng giao thức SNMP (Simple Network Management Protocol).
* **Giám sát trải nghiệm người dùng**: Dựa trên các giao dịch người dùng thực (RUM - Real User Monitoring), Site24x7 theo dõi trải nghiệm của người dùng cuối từ nhiều địa điểm khác nhau trên thế giới.
* **Quản lý nhật ký (Log Management**): Thu thập và phân tích nhật ký từ các ứng dụng, hệ thống và thiết bị mạng để phát hiện các vấn đề và giải quyết sự cố nhanh chóng.
* **Giám sát đám mây**: Hỗ trợ giám sát các dịch vụ đám mây như AWS, Microsoft Azure, và Google Cloud, bao gồm việc giám sát tài nguyên, dịch vụ và hiệu suất tổng thể.

### Hướng dẫn cài đặt

* B1: Đăng ký sử dụng

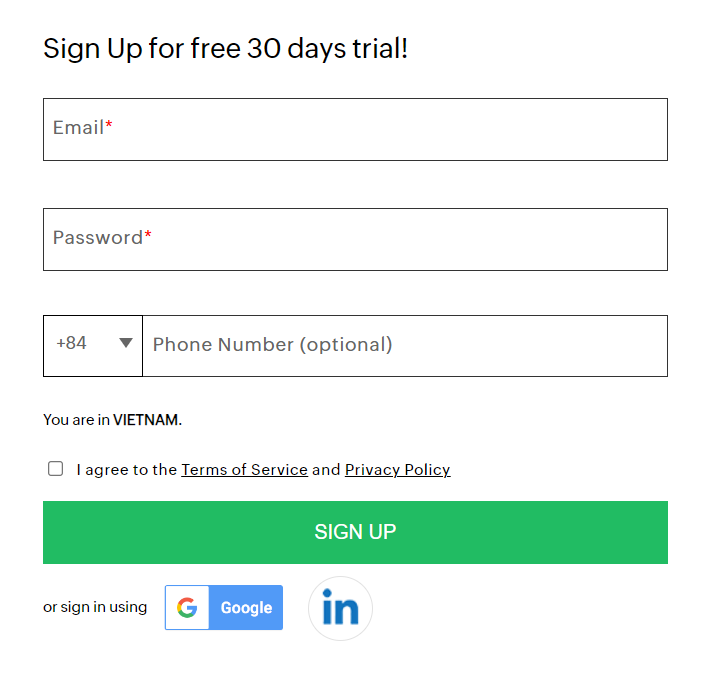
Truy cập đường dẫn [**https://www.site24x7.com/**](https://www.site24x7.com/)



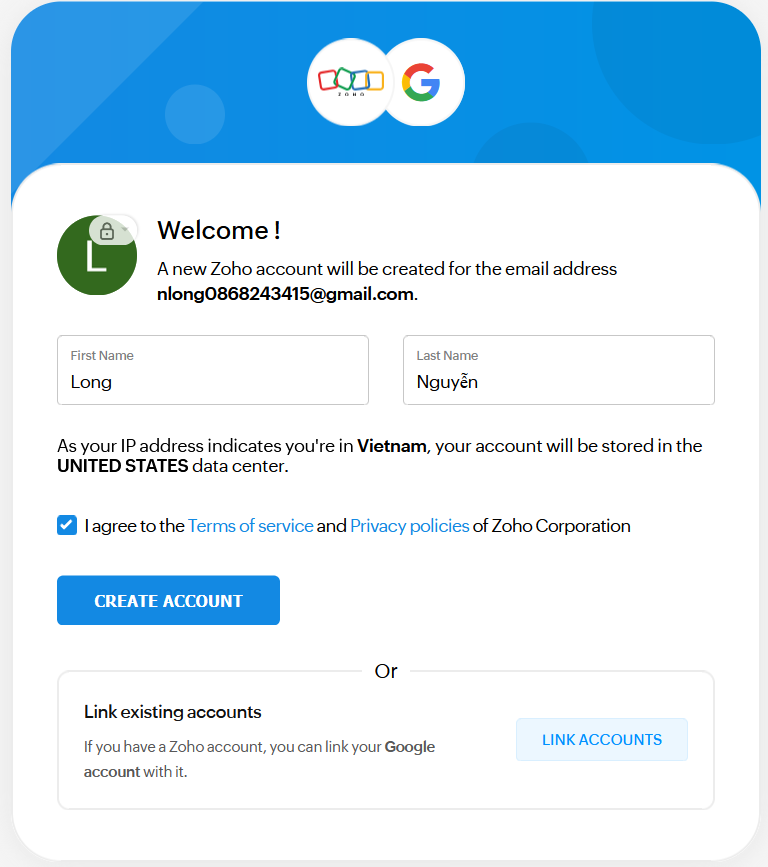
* Nhấn vào nút START 30-DAY FREE TRIAL

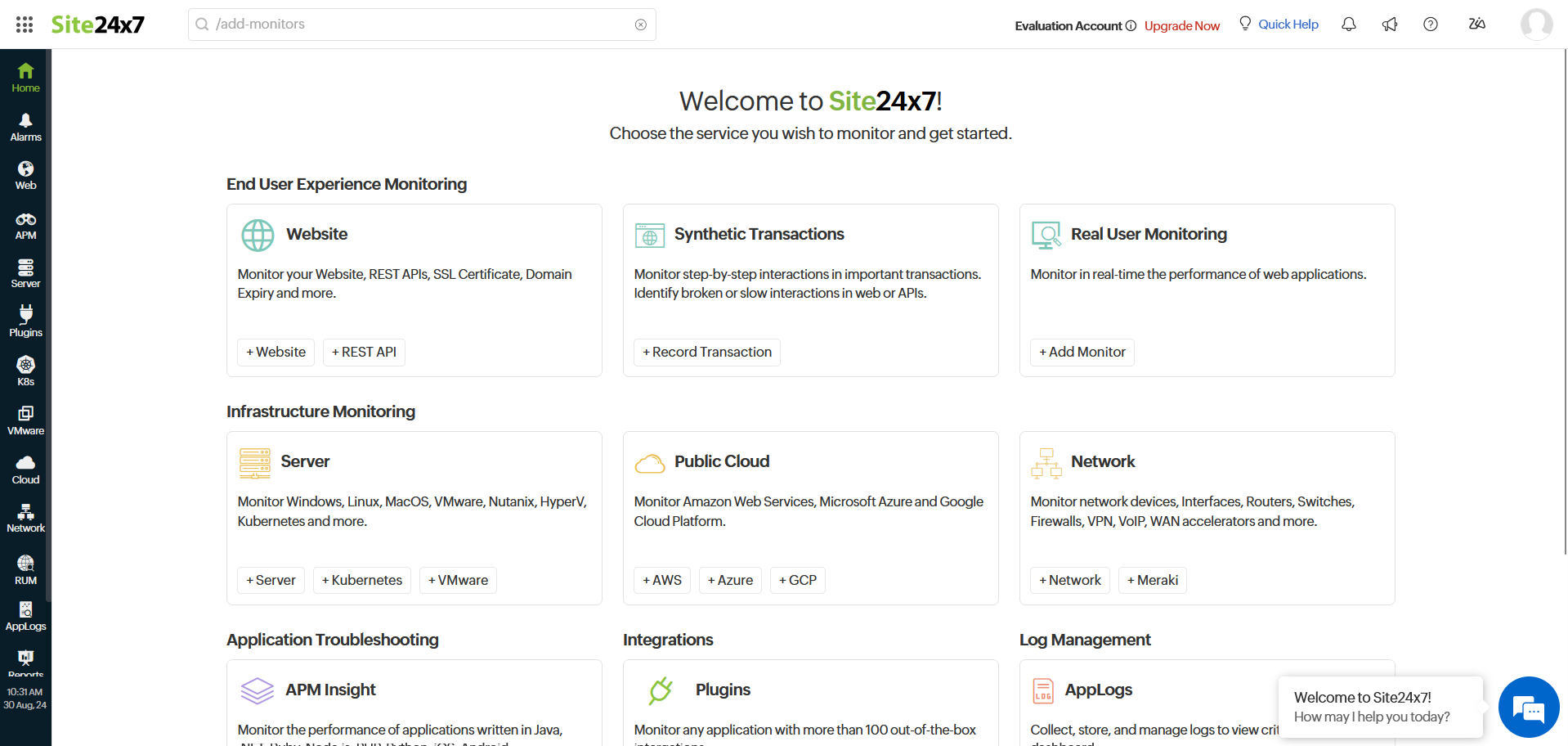
****

* Điền **Email**, **Password** và **Số điện thoại** để đăng ký tài khoản, hoặc có thể sử dụng tài khoản Gmail để đăng ký. Ở đây mình chọn đăng ký bằng tài khoàn Google



* Tiếp theo click chọn I agree to the Terms of service and Privacy policies of Zoho Corporation





* Click nút CREATE ACCOUNT



* Tại cửa sổ này, chọn Option 1: I am new to Site24x7



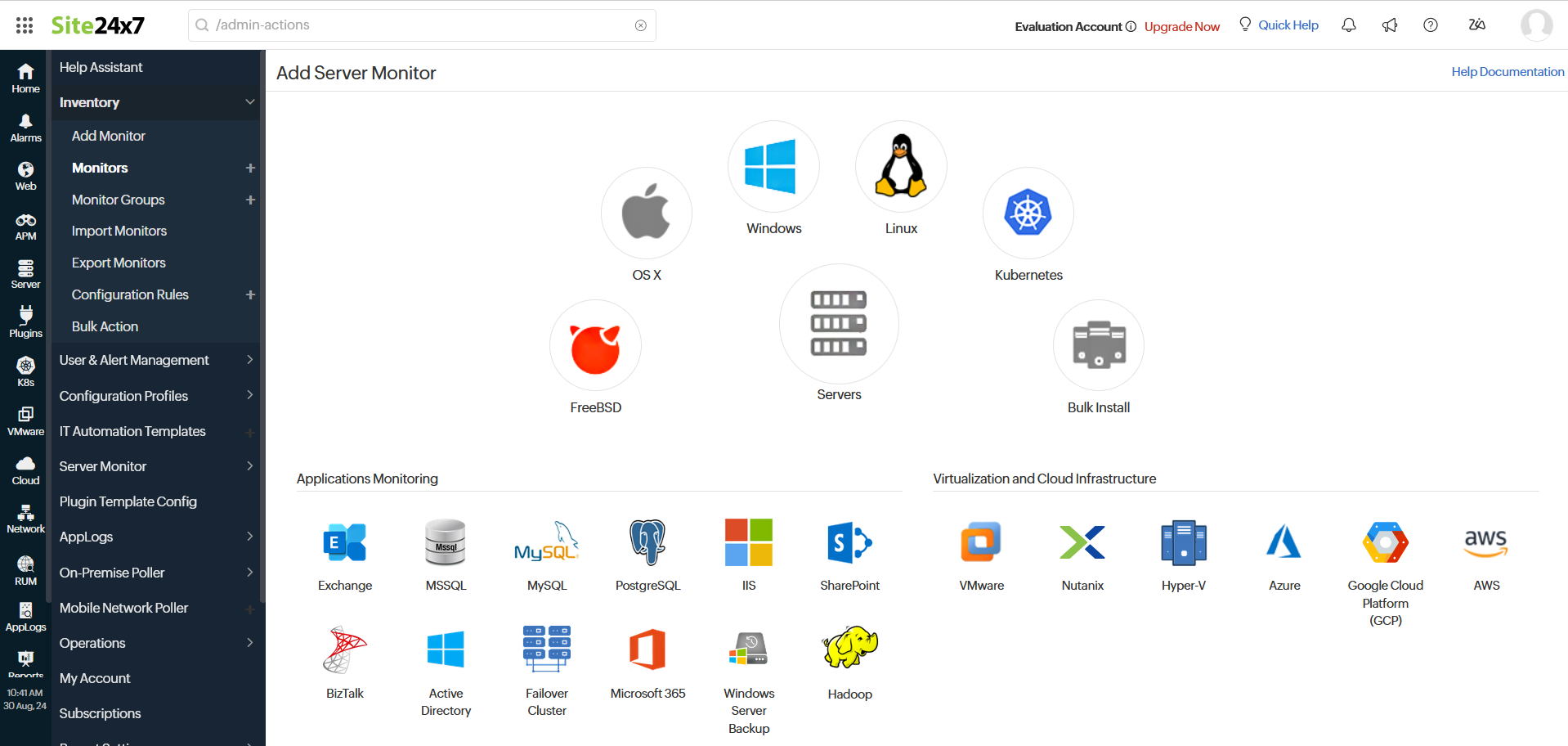
- Click nút **Create New Account**



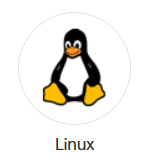
* B2: Thêm thiết bị Linux (Windows cũng làm tương tự)
* Để có thể thêm 1 Webserver CentOS vào Site24x7, ta chọn biểu tượng **Server** trên cột module



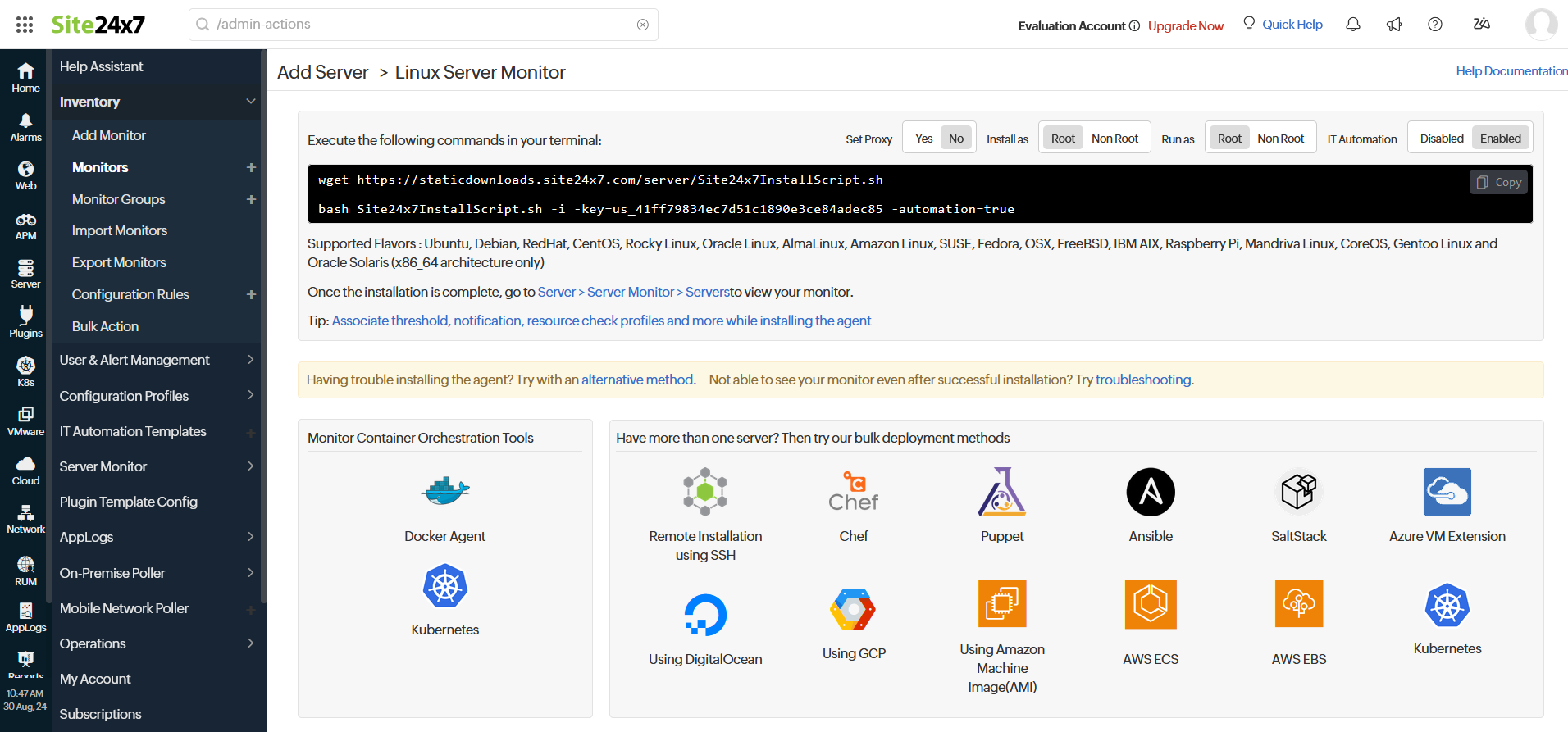
* Giao diện của module **Server** hiện ra



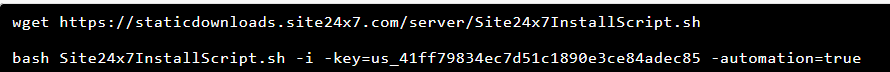
* Click chọn biểu tượng **Linux**



* Giao diện sau sẽ hiện ra

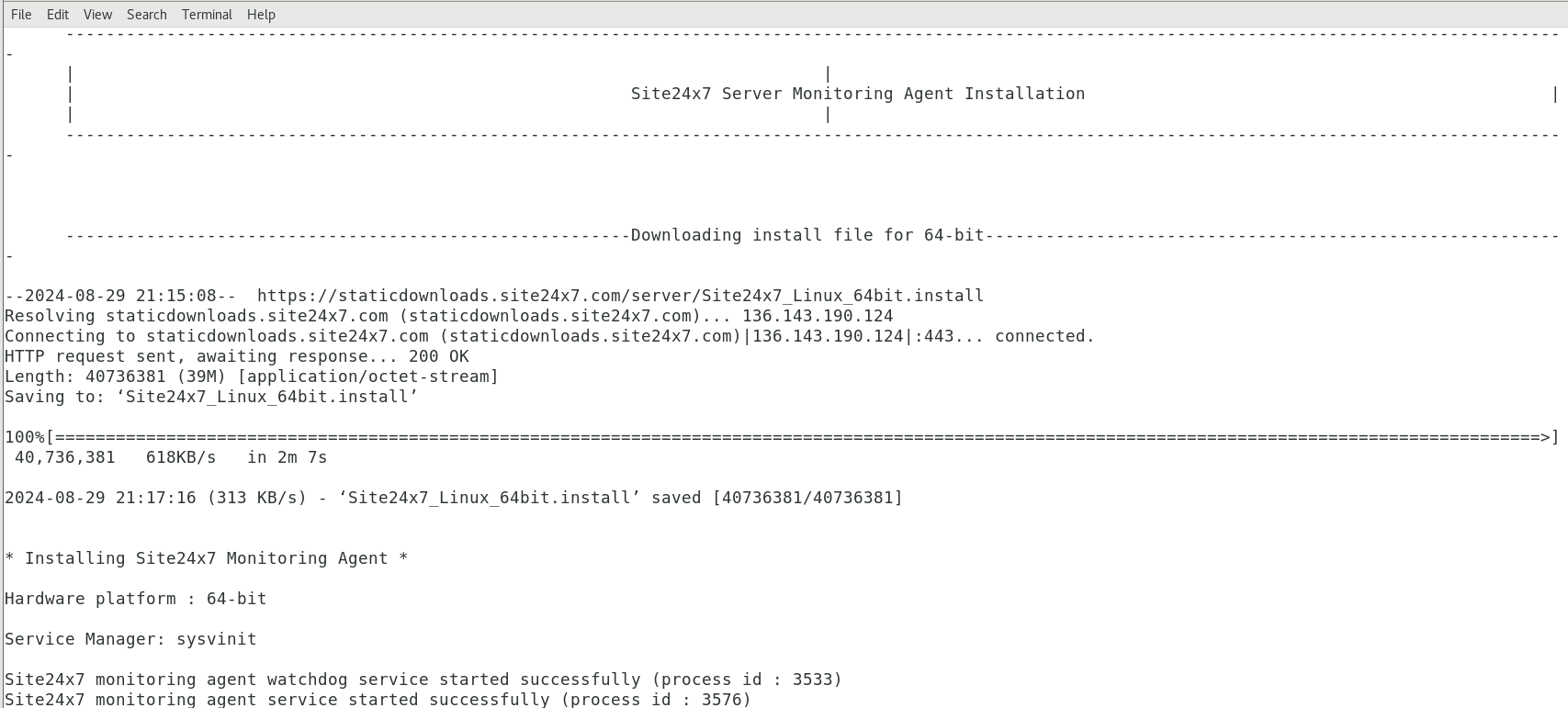


* Tại đây ta cần copy đoạn mã



* Rồi chạy nó trên **Terminal** của **Webserver CentOS.** Hãy đăng nhập với quyền **superuser** trước rồi chạy đoạn mã.



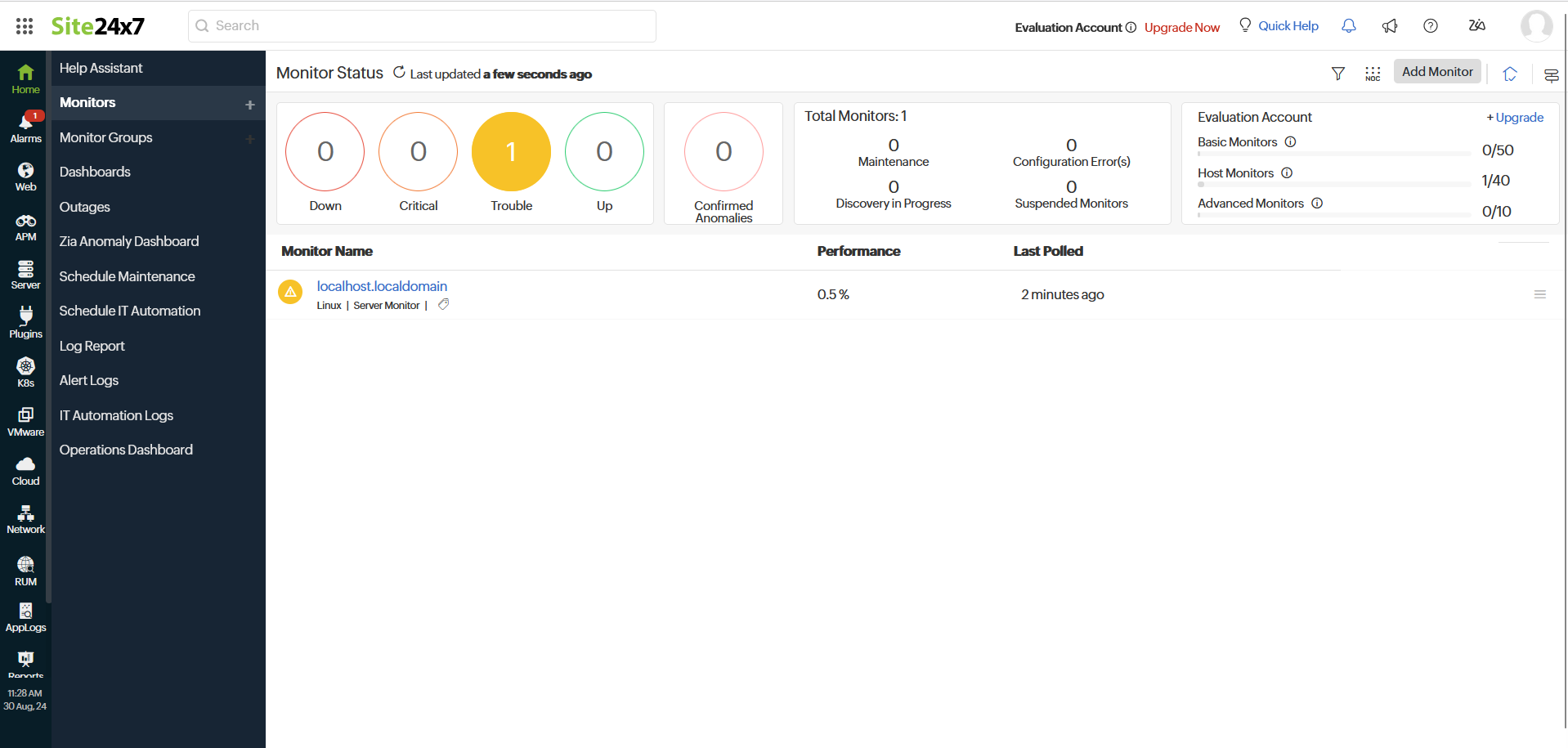


* Có thông báo việc cài Agent vào máy Linux đã thành công:

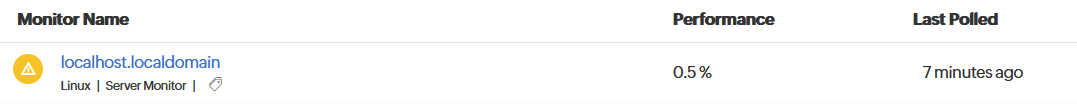
“ Site24x7 monitoring agent watchdog service started successfully

Site24x7 monitoring agent service started successfully ”

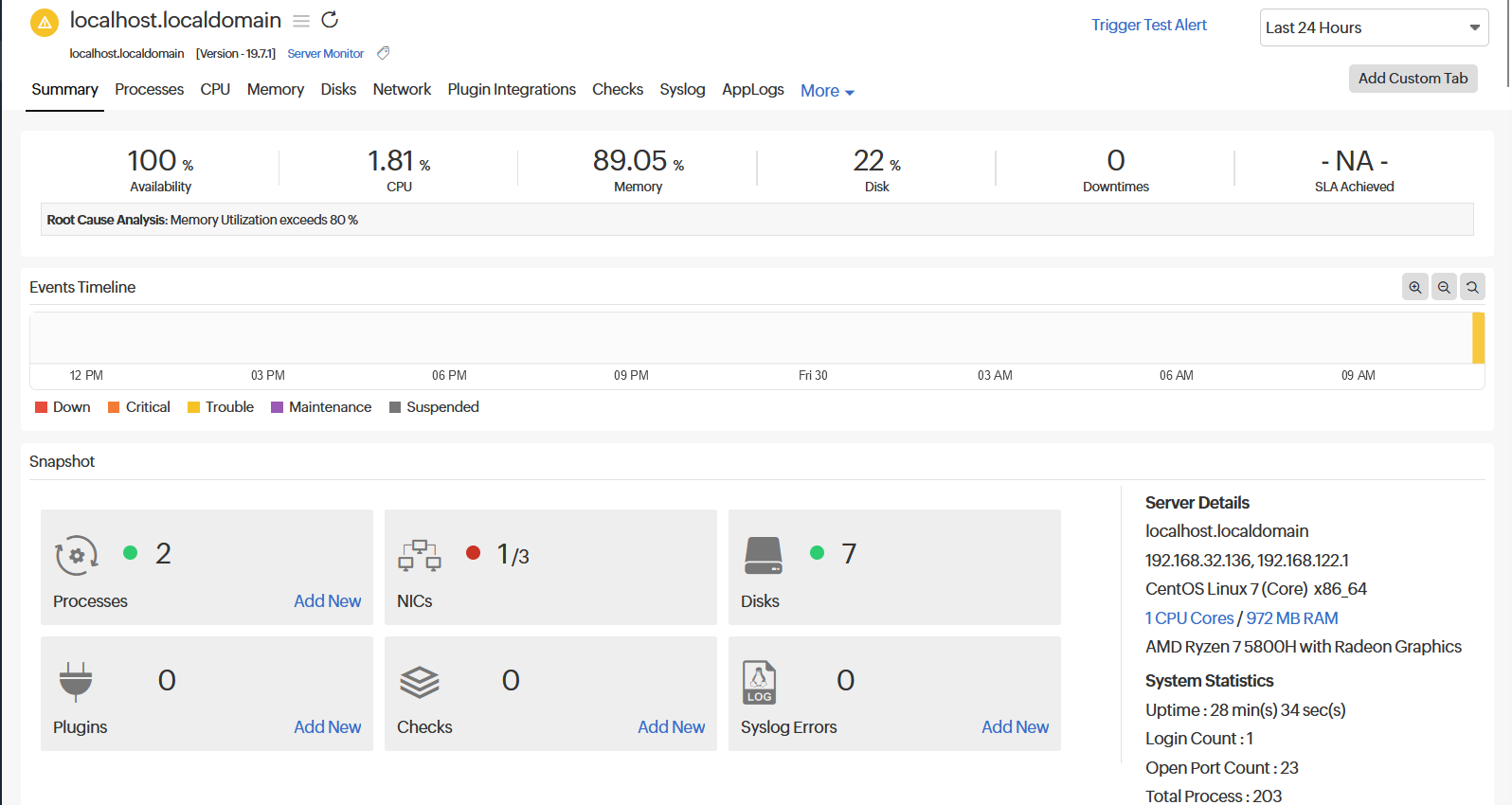
* Bây giờ quay lại trang Home của Site24x7



* Có 1 thiết bị mới bên dưới **Monitor Name** có tên là **localhost.localdomain** với hệ điều hành Linux, đấy chính là webserver CentOS của chúng ta vừa thêm.



* Click vào tên thiết bị để kiểm tra, giao diện sau sẽ hiện ra



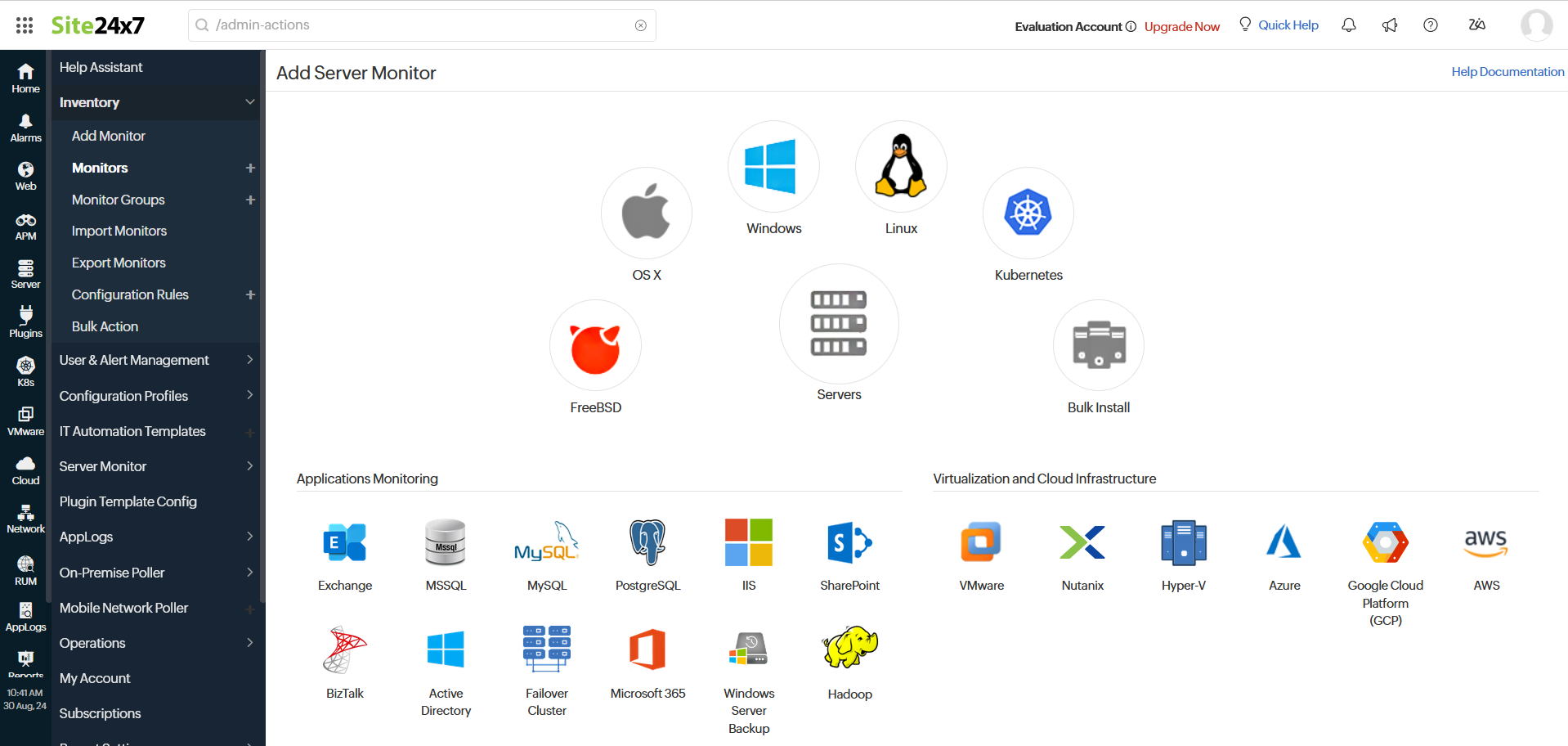
* Tại đây ta sẽ có được cái nhìn tổng quan về thiết bị như Tính khả dụng(Availability), %CPU đang sử dụng, Dung lượng bộ nhớ(Memory), % ổ đĩa đang được sử dụng(Disk),…
* Hoàn thành quá trình thêm thiết bị CentOS vào Site24x7 !

### Thêm thiết bị cần theo dõi

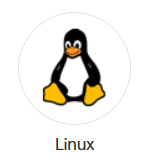
* Để có thể thêm 1 Webserver CentOS vào Site24x7, ta chọn biểu tượng **Server** trên cột module



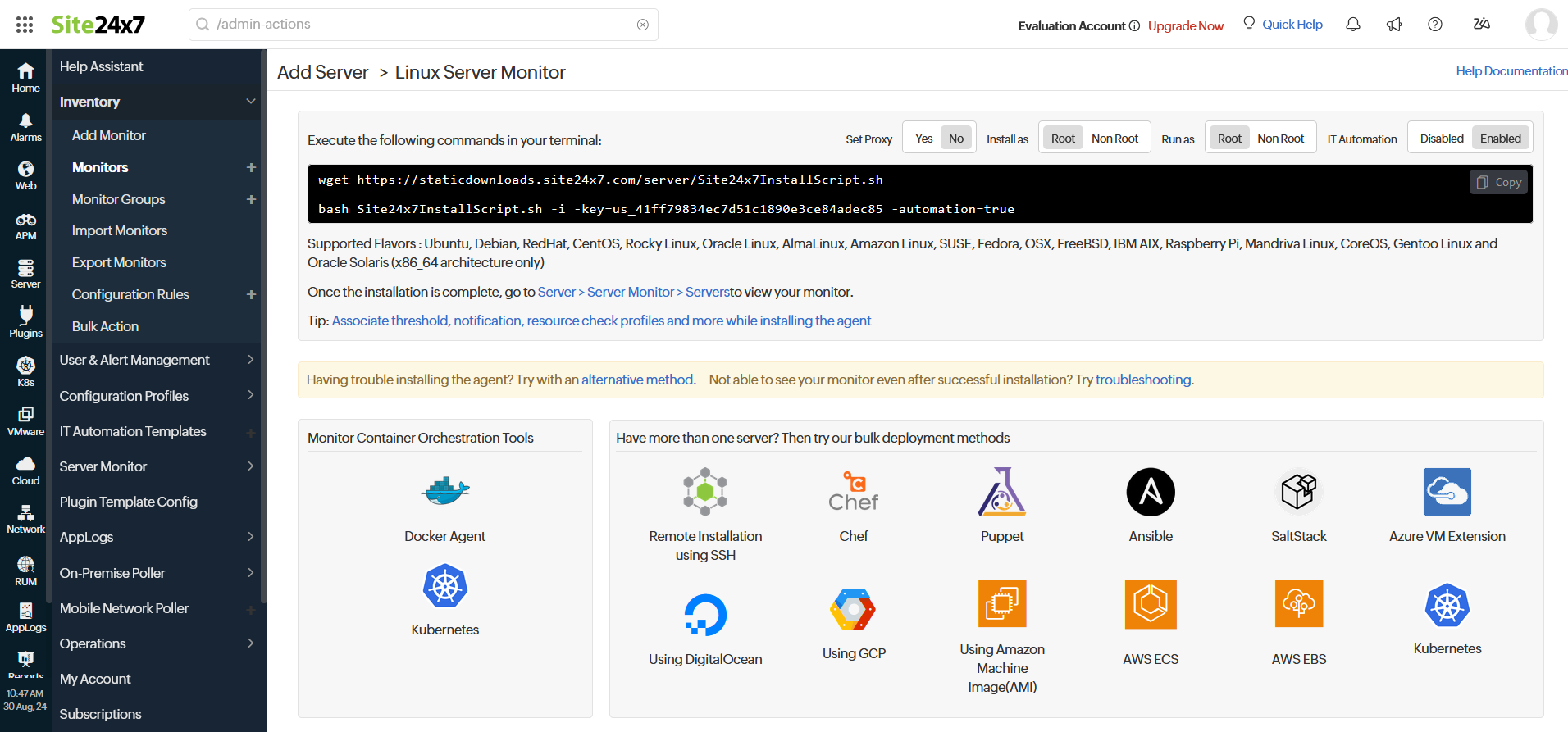
* Giao diện của module **Server** hiện ra



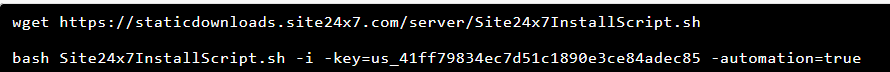
* Click chọn biểu tượng **Linux**



* Giao diện sau sẽ hiện ra

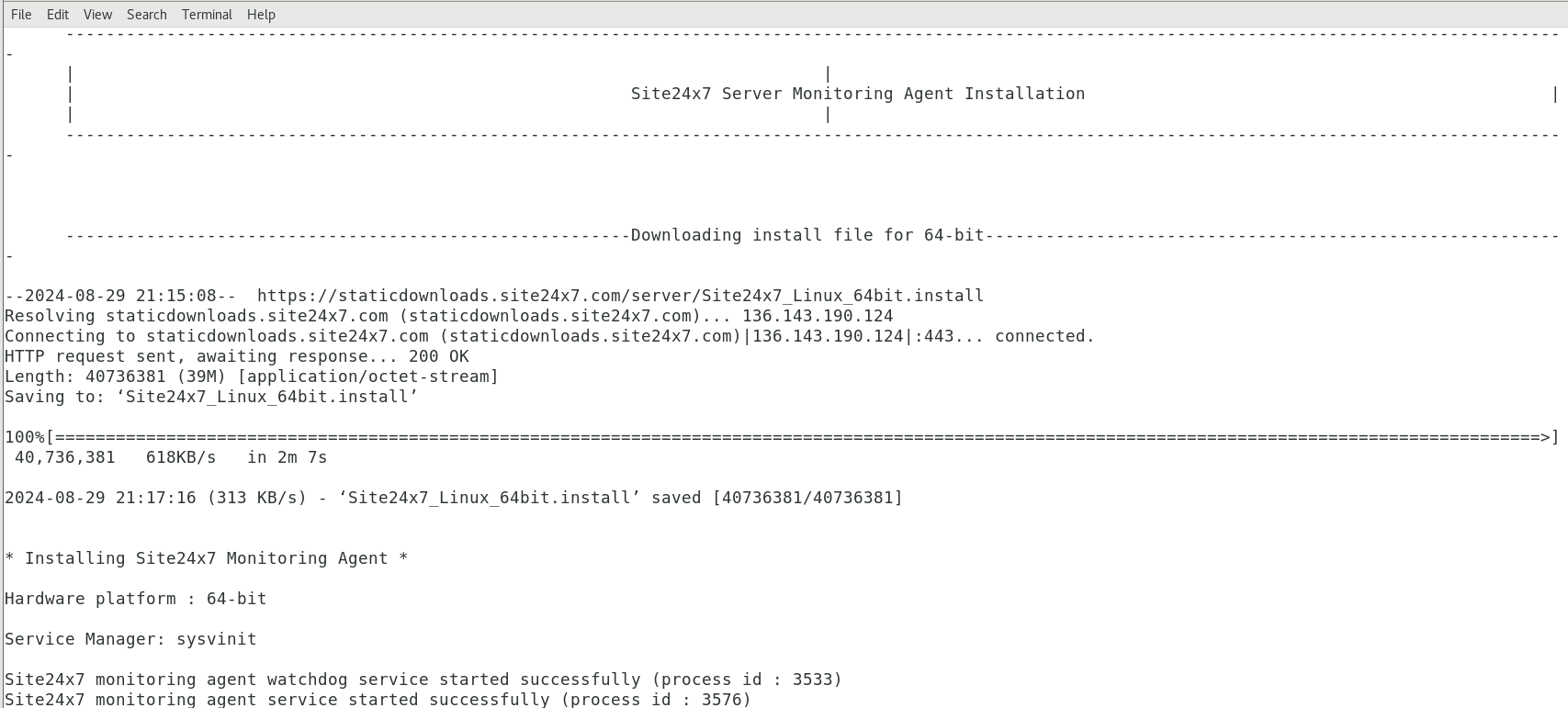


* Tại đây ta cần copy đoạn mã



* Rồi chạy nó trên **Terminal** của **Webserver CentOS.** Hãy đăng nhập với quyền **superuser** trước rồi chạy đoạn mã.



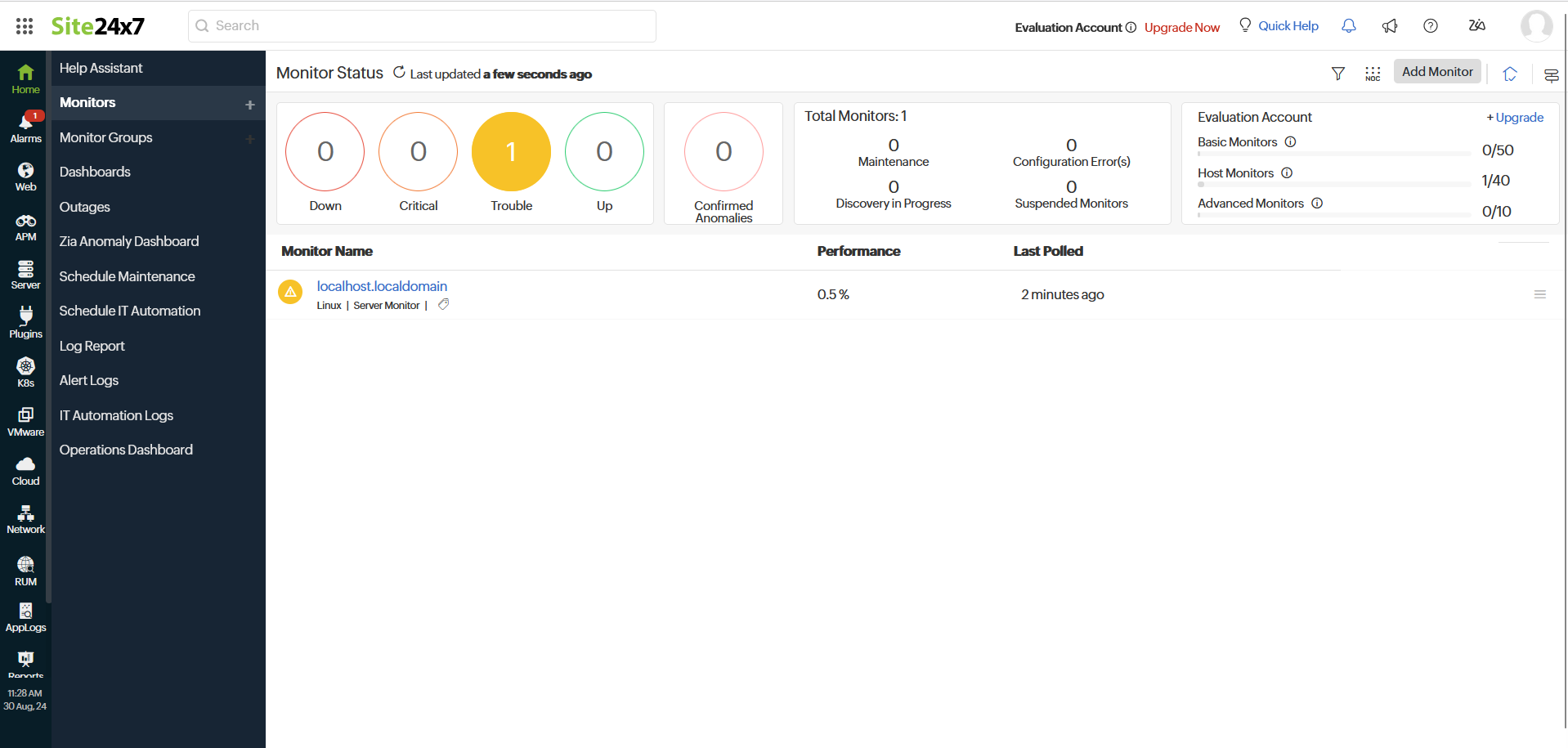


* Có thông báo việc cài Agent vào máy Linux đã thành công:

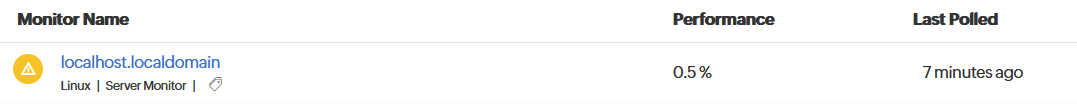
“ Site24x7 monitoring agent watchdog service started successfully

Site24x7 monitoring agent service started successfully ”

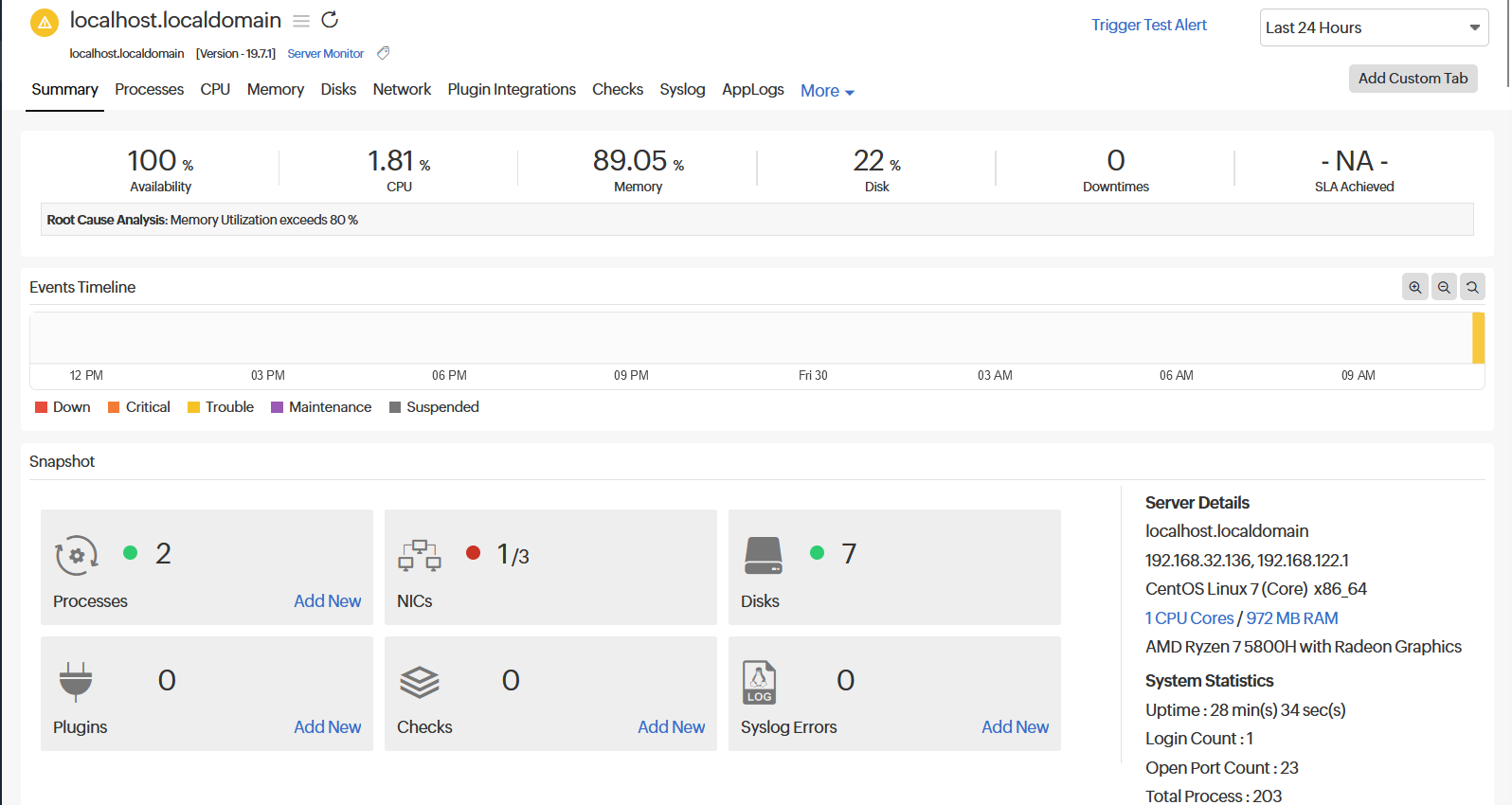
* Bây giờ quay lại trang Home của Site24x7



* Có 1 thiết bị mới bên dưới **Monitor Name** có tên là **localhost.localdomain** với hệ điều hành Linux, đấy chính là webserver CentOS của chúng ta vừa thêm.



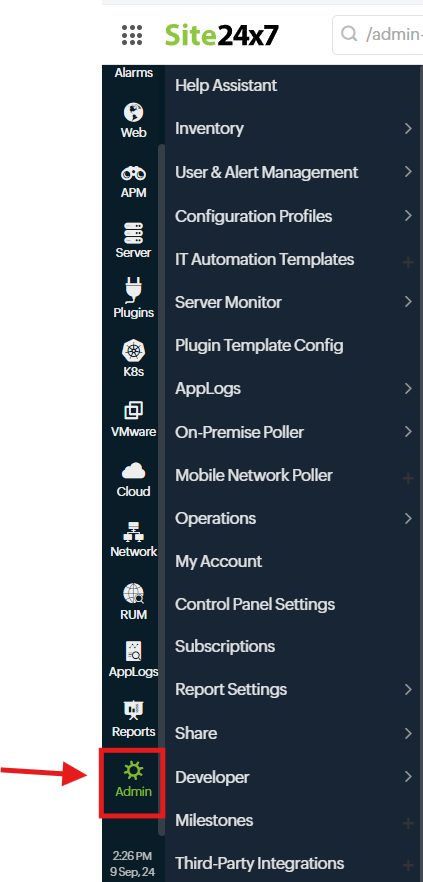
* Click vào tên thiết bị để kiểm tra, giao diện sau sẽ hiện ra



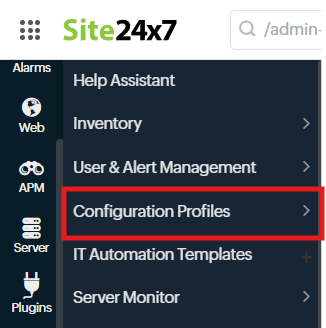
* Tại đây ta sẽ có được cái nhìn tổng quan về thiết bị như **Tính khả dụng(Availability)**, **%CPU đang sử dụng**, **Dung lượng bộ nhớ(Memory)**, **% ổ đĩa đang được sử dụng(Disk)**,…
* Hoàn thành quá trình thêm thiết bị CentOS vào Site24x7 !

### Đặt ngưỡng cảnh báo

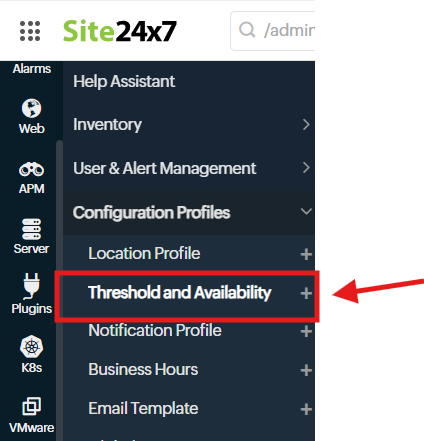
* Tại trang chủ Site24x7, ở cột module bên tay trái, kéo xuống và chọn **Admin**



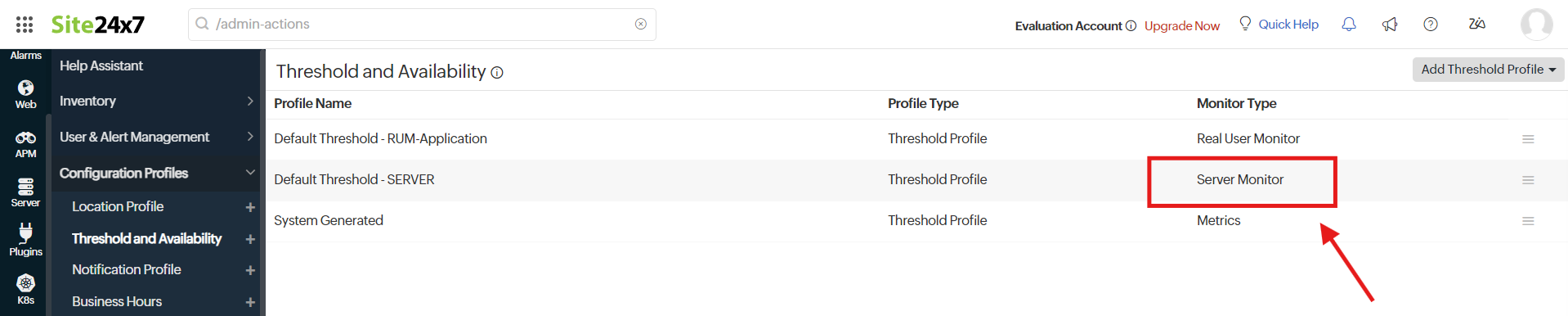
* Bên cạnh cột module là Inventory, tại đó chọn **Configuration Profiles**



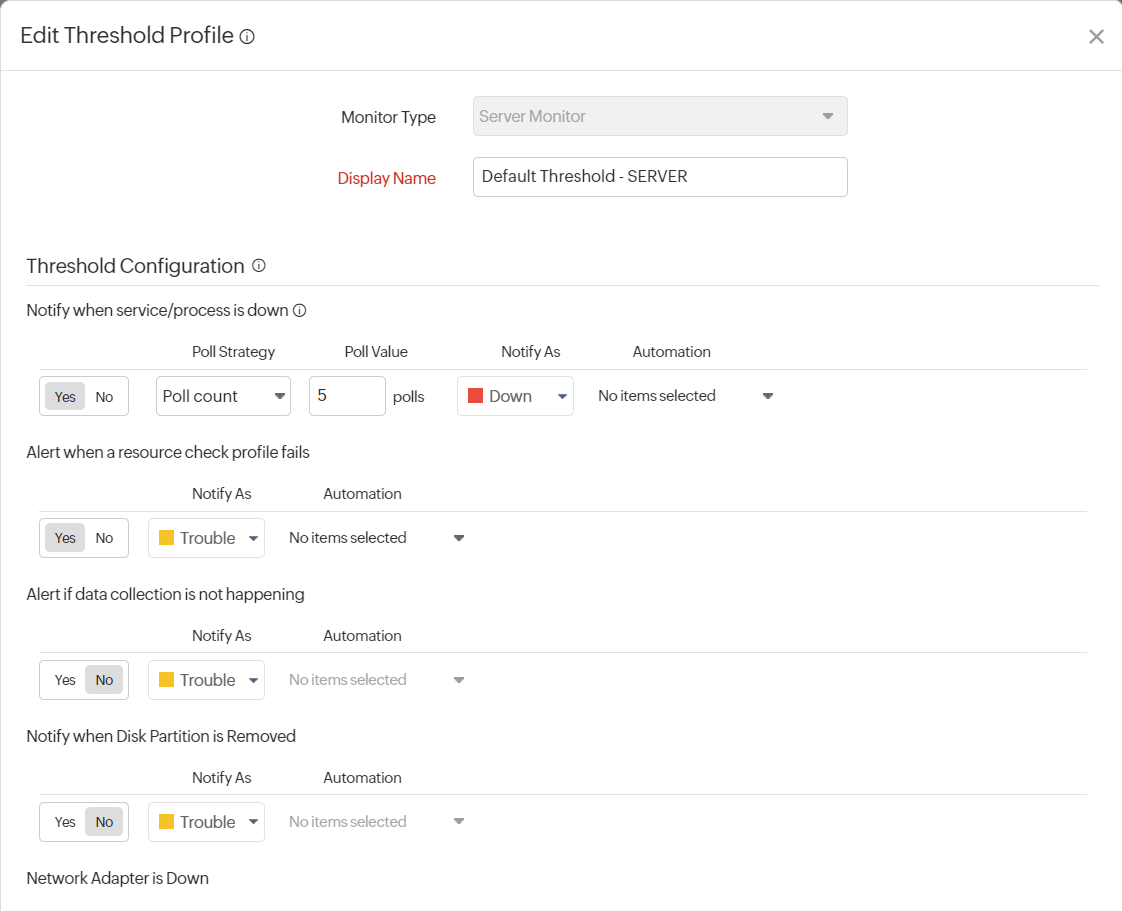
* Chọn tiếp **Threshold and Availability**



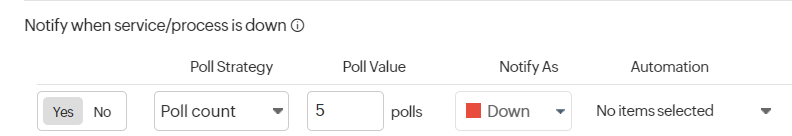
* Lúc này 1 giao diện hiện ra, ở góc trên bên phải click vào **Server Monitor** để đặt ngưỡng cảnh báo cho Server



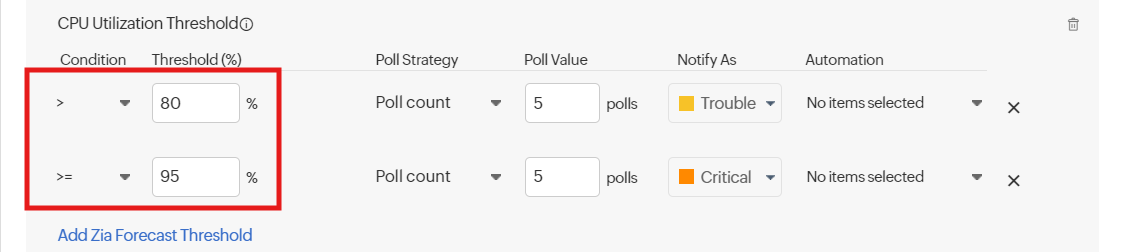
- Giao diện cấu hình sau hiện ra



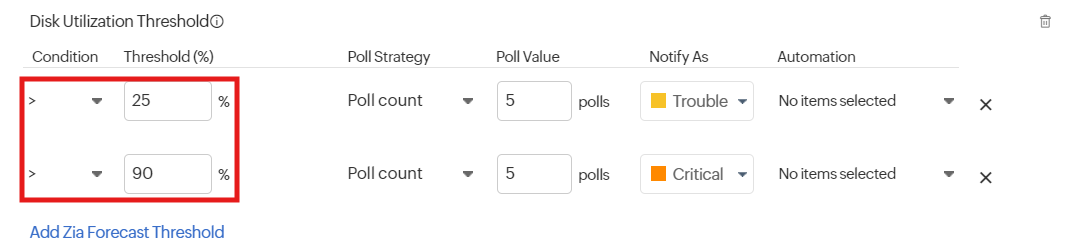
* Giờ ta sẽ cấu hình cho một số phần:
* **Notify when service/process is down**(Thông báo khi thiết bị sập). Chọn **Yes**, ở trường **Notify As** chọn **Down.**



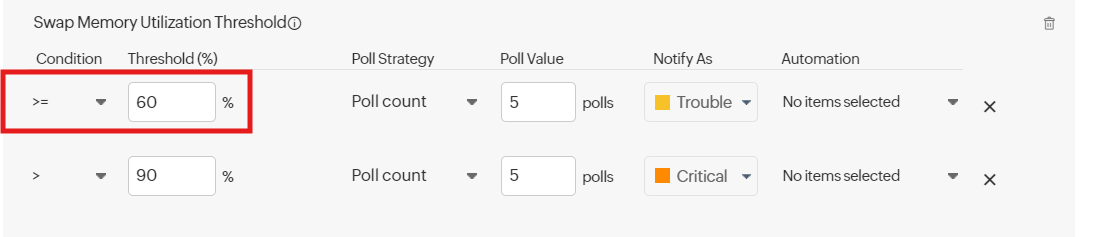
* Kéo xuống phần **CPU Uttillization**(Mức sử dụng CPU). Đặt mức thông báo **Trouble** là **> 80%**. **Critical** là **>= 95%**



* Phần **Disk Utilization Threshold** (Cảnh báo ngưỡng sử dụng ổ đĩa). Để **Trouble** là **>25%**



Phần Swap Memory Untillization Threshold (Ngưỡng cho phép hoán đổi ổ đĩa). Đặt Trouble là >=60%



### So sánh Site24x7 với các công cụ Zabbix, Snort

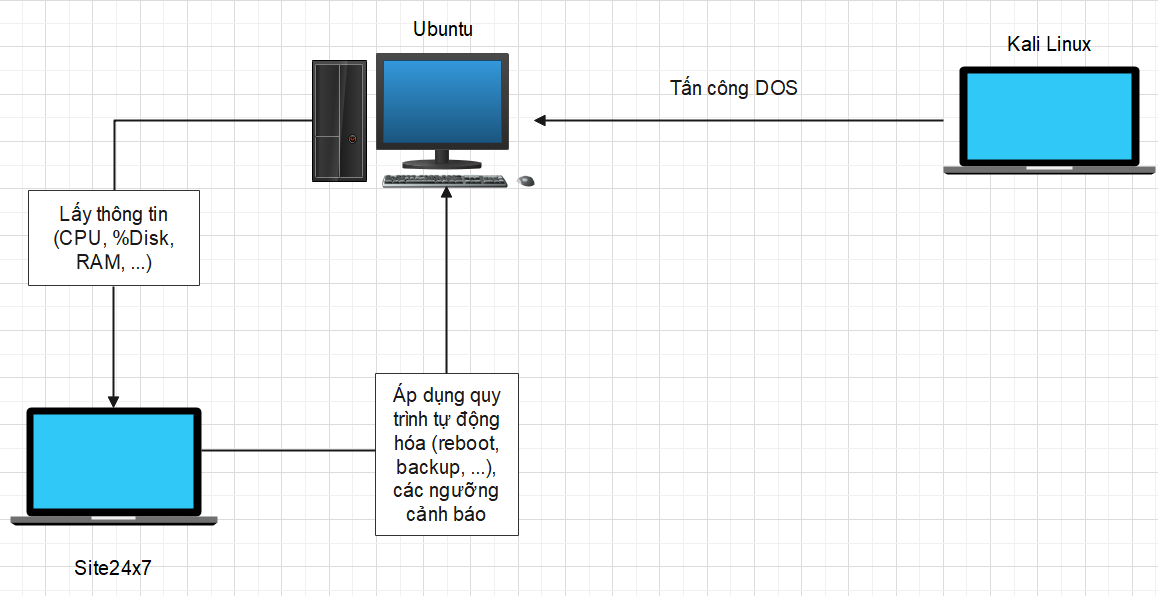
|  |  |  |  |
| --- | --- | --- | --- |
| TIÊU CHÍ | SITE24x7 | SNORT | ZABBIX |
| Loại hình giám sát | Giám sát toàn diện (Website, ứng dụng, máy chủ) | Chuyên phát hiện xâm nhập mạng (IDS/IPS) | Giám sát toàn diện |
| Phân tích trải nghiệm người dùng | Có (Synthetic Monitoring và Real User Monitoring) | Không | Không |
| Triển khai và sử dụng | Cloud-based, dễ triển khai và không cần bảo trì nhiều | Phải triển khai tại chỗ, phức tạp hơn | Self-host, cần cài đặt, quản lý thủ công |
| Khả năng cảnh báo tự động | Có. Cảnh báo đa dạng qua mail, SMS, Slack | Có. Nhưng chủ yếu cho các vấn đề bảo mật | Có, nhưng cần cấu hình thủ công cho từng cảnh báo |
| Tính năng giám sát bảo mật | Giám sát cơ bản, không chuyên sâu về bảo mật | Chuyên phát hiện và ngăn chặn các cuộc tấn công | Giám sát bảo mật cơ bản qua logs và dữ liệu |
| Tích hợp AI | Có tích hợp AI cho dự đoán lỗi và tối ưu hóa | Không | Không |
| Khả năng mở rộng | Rất linh hoạt và mở rộng theo quy mô cloud | Mở rộng dựa trên cấu trúc phần cứng tại chỗ | Khả năng mở rộng tốt nhưng cần nhiều tài nguyên |

**KẾT LUẬN**: Qua một số giải pháp về giám sát mạng mà nhóm em tìm hiểu, chúng em quyết định chọn Site24x7 làm giải pháp chính với lý do: đây là giải pháp hiện đại, đầy đủ và thuận tiện nhất cho việc giám sát và phát hiện tấn công sớm ở hệ thống mạng.

# TIẾN HÀNH TRIỂN KHAI VÀ THỬ NGHIỆM

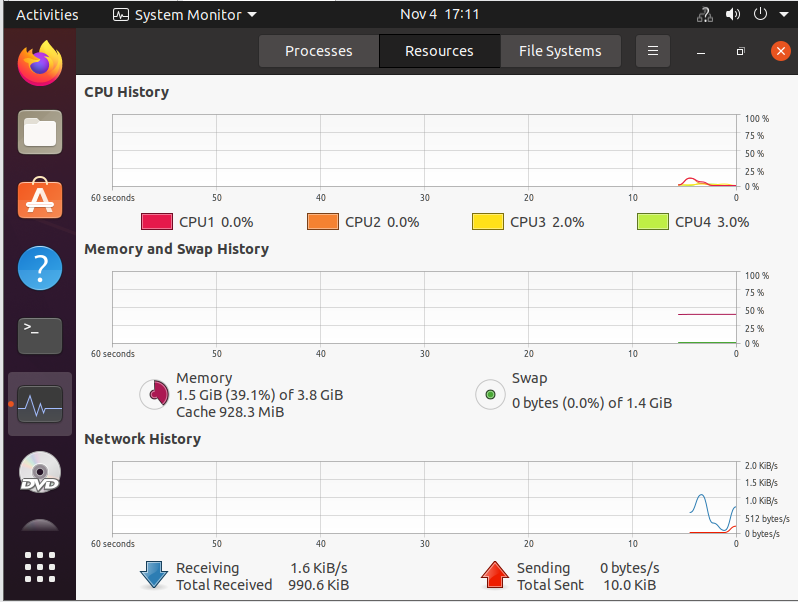
## Kịch bản

* Máy Kali Linux là máy tấn công
* Máy Ubuntu Webserver là máy bị tấn công
* Máy quản trị viên dùng công cụ Site24x7 để giám sát và phòng chống
* Thực hiện tấn công 2 lần:
* Lần 1: Tin tặc tấn công vào webserver làm suy giảm hiệu năng, Site24x7 đưa ra các thông số RAM, %Disk, …
* Lần 2: Tin tặc tấn công vào webserver đã được Site24x7 áp dụng các ngưỡng phòng chống, đưa ra các thông số

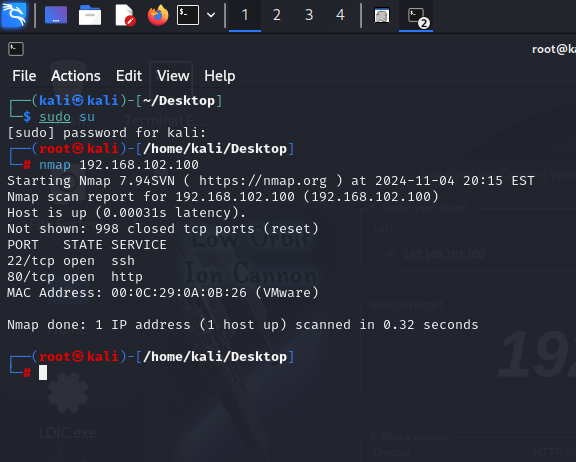


## Triển khai tấn công lần 1

Trước khi tấn công

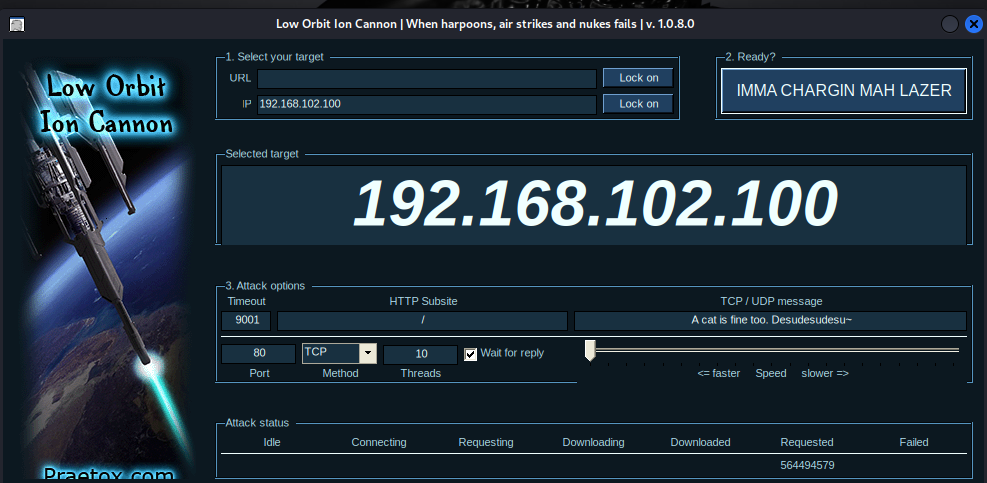


* CPU vẫn hoạt động ổn định ở ngưỡng 0 - 20%
* Phương pháp tấn công: Tấn công HTTP Flood
* Kịch bản: Sử dụng máy Kali tấn công HTTP Flood vào máy Ubuntu, sau đó sẽ đưa ra kết quả của cuộc tấn công và giải pháp ngăn chặn.
* B1: Quét cổng trên máy Kali



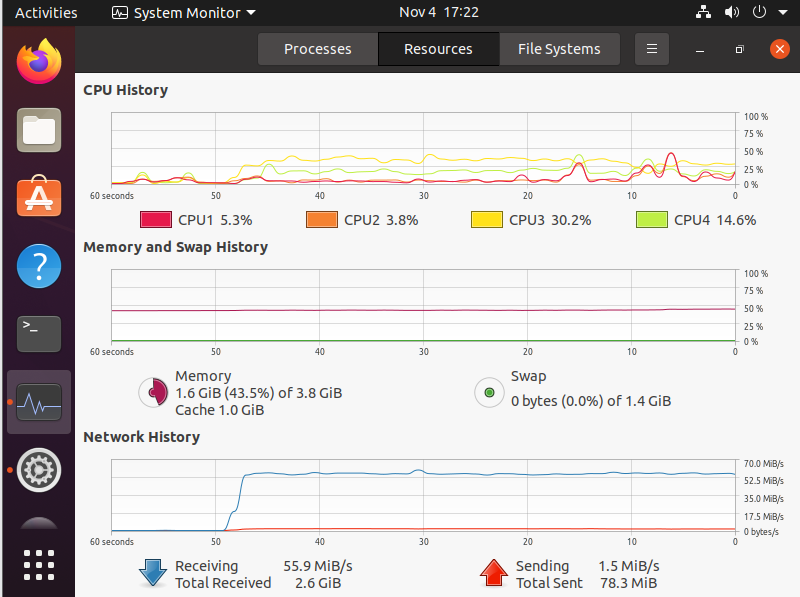
Ta thấy có 2 cổng đang mở là 22 và 80

* B2: Sử dụng công cụ LLOIC

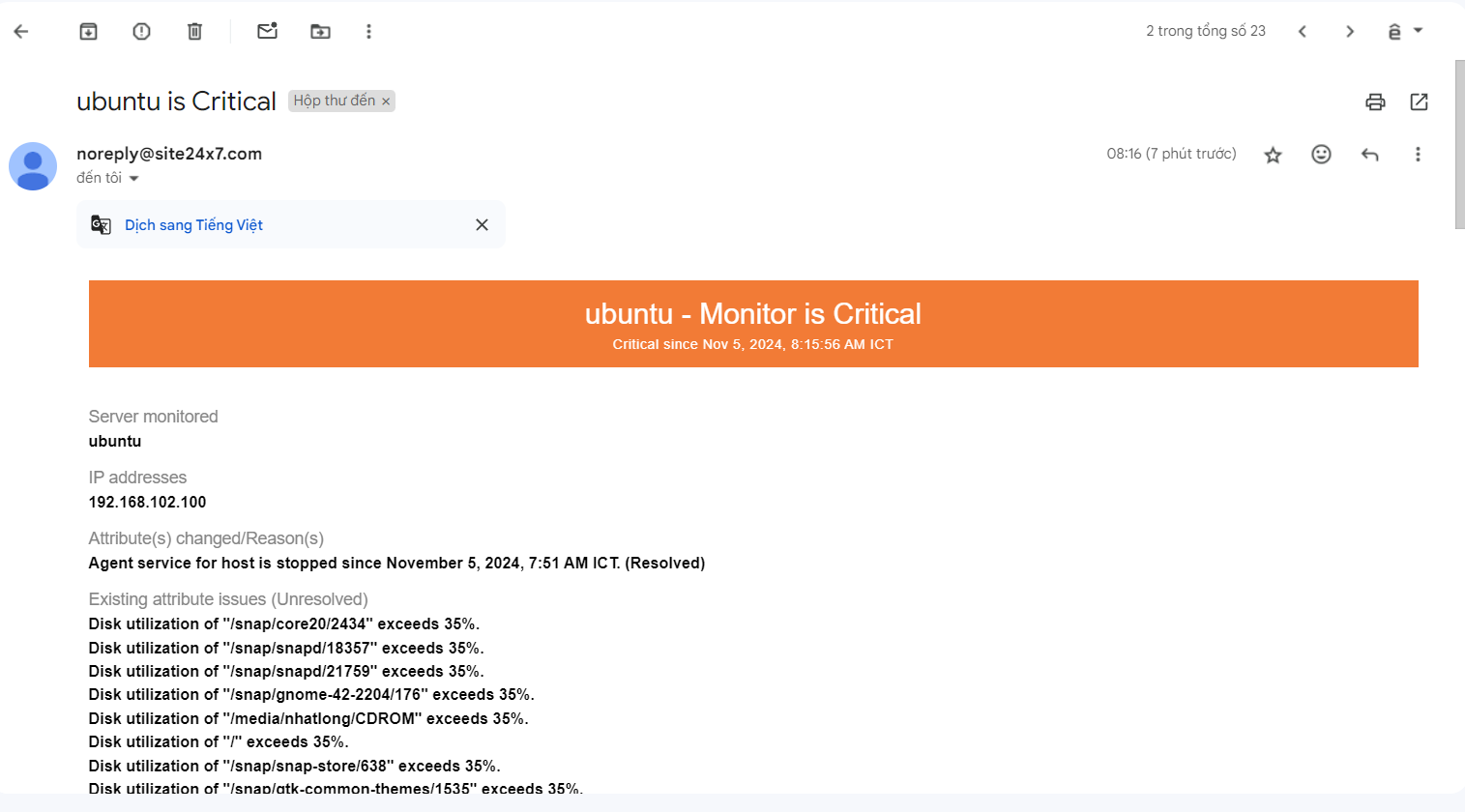


* B3: Kết quả thu được

CPU tăng cao bất thường, số Request nhận được cũng cao vượt trội

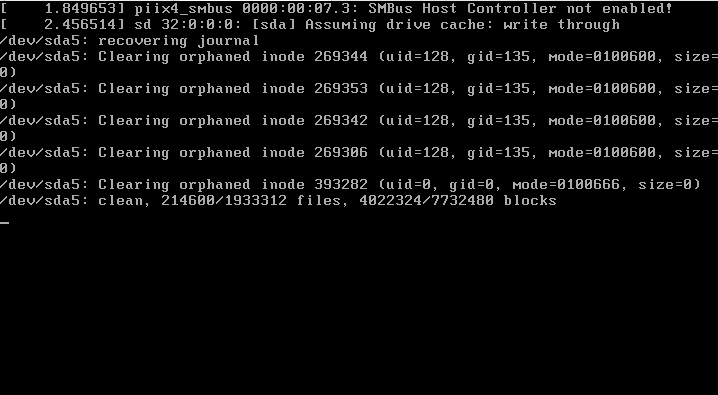


Site24x7 đưa ra cảnh báo:

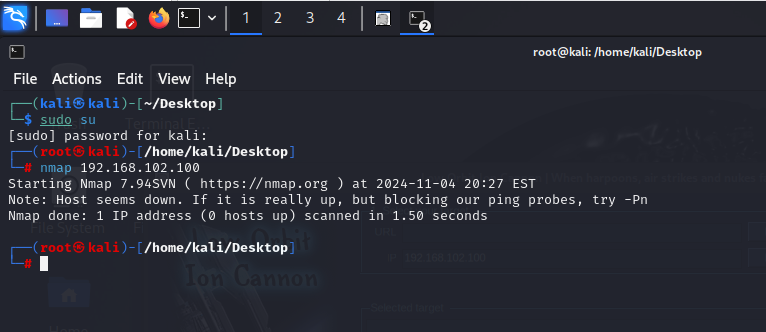


## Triển khai tấn công lần 2

Sau khi áp đặt quy trình tự động hóa reboot máy chủ, ubuntu sẽ tự động reboot lại



Ip và DNS cũng được reset lại, khiến cho máy tấn công không thể có được IP chính xác của ubuntu nữa



Thông báo reboot thành công cũng Site24x7 được gửi qua mail

