**TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT**

**VIỆN KỸ THUẬT – CÔNG NGHỆ**

**\*\*\*\*\*\*\*\*\*\*\***



**BÁO CÁO TIỂU LUẬN AN NINH MẠNG**

**Phân tích và triển khai giải pháp an ninh mạng trên Windows 10 cho Công ty GBF Groups**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | : ThS. Lê Từ Minh Trí |
| **Sinh viên:** Vương Võ Trung Quân | - 2024802010331 |
| Nguyễn Thành Trung | - 2024802010496 |
| Nguyễn Đức Trung | - 2024802010097 |
| Trần Văn Dinh | - 2024802010389 |

**TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT**

**VIỆN KỸ THUẬT – CÔNG NGHỆ**

**\*\*\*\*\*\*\*\*\*\*\***



**BÁO CÁO TIỂU LUẬN AN NINH MẠNG**

**Phân tích và triển khai giải pháp an ninh mạng trên Windows 10 cho Công ty GBF Groups**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | : ThS. Lê Từ Minh Trí |
| **Sinh viên:** Vương Võ Trung Quân | - 2024802010331 |
| Nguyễn Thành Trung | - 2024802010496 |
| Nguyễn Đức Trung | - 2024802010097 |
| Trần Văn Dinh | - 2024802010389 |

### MỞ ĐẦU

An toàn và bảo mật thông tin ngày nay là một vấn đề cực kỳ quan trọng và đặc biệt quan tâm trong môi trường kỹ thuật số hiện đại. Với sự phát triển nhanh chóng của công nghệ thông tin và viễn thông, việc bảo vệ thông tin quan trọng và đảm bảo an ninh mạng đã trở thành một nhiệm vụ không thể thiếu.

Trong thế giới kỹ thuật số ngày nay, một trong những công cụ quan trọng để kiểm tra và bảo vệ an ninh mạng là máy ảo Kali Linux. Kali Linux là một hệ điều hành dựa trên Linux được thiết kế đặc biệt cho việc thử nghiệm bảo mật và kiểm tra xâm nhập. Với các công cụ và tính năng chuyên biệt trong lĩnh vực này, Kali Linux cho phép chuyên gia an ninh mạng và những người quan tâm đến bảo mật thông tin thực hiện các phân tích và kiểm tra an toàn một cách hiệu quả.

Máy ảo Kali Linux cung cấp một môi trường cách li và an toàn để thực hiện các hoạt động thử nghiệm bảo mật, bao gồm phân tích mã độc, quét mạng, khai thác lỗ hổng và phục hồi dữ liệu. Với sự hỗ trợ của Kali Linux, người dùng có thể kiểm tra tích hợp mạng, hệ thống và ứng dụng, từ đó xác định các lỗ hổng tiềm năng và triển khai các biện pháp bảo mật phù hợp.

Tuy nhiên, việc sử dụng máy ảo Kali Linux cũng đòi hỏi sự hiểu biết và chuyên môn trong lĩnh vực bảo mật thông tin. Máy ảo Kali Linux không nên được sử dụng một cách trái phép hoặc xâm phạm quyền riêng tư của người khác. Thay vào đó, nó phải được sử dụng như một công cụ hỗ trợ để tăng cường khả năng phát hiện và bảo vệ an ninh mạng.

Do đó với mục tiêu là tìm hiểu chúng nên nhóm chúng em quyết định chọn đề tài

**“Phân tích và triển khai giải pháp an ninh mạng trên Windows 10 cho Công ty GBF Groups”** nhằm hiểu rõ hơn về khai thác lỗ hổng cũng như là nâng cao kiến thức về bảo mật thông tin.

### MỤC LỤC

[MỞ ĐẦU 1](#_Toc14196)

[MỤC LỤC 2](#_Toc16566)

[DANH MỤC HÌNH 3](#_Toc10460)

[DANH MỤC VIẾT TẮT 4](#_Toc2585)

[CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI 5](#_Toc26882)

[1.1. Tổng quan về đề tài nghiên cứu 5](#_Toc5464)

*[1.1.1.](#_Toc593)* [Ưu điểm: 5](#_Toc593)

*[1.1.2.](#_Toc15845)* [Nhược điểm: 5](#_Toc15845)

[1.2. Nhiệm vụ đồ án 5](#_Toc14944)

[CHƯƠNG 2. CƠ SỞ LÝ THUYẾT 7](#_Toc21307)

[2.1. Khái niệm về an ninh mạng 7](#_Toc18932)

[2.2. An ninh mạng của việt nam hiện nay 7](#_Toc7519)

*[2.2.1.](#_Toc18953)* [An toàn thông tin 8](#_Toc18953)

*[2.2.2.](#_Toc9792)* [Khái niệm khai thác lỗ hổng 10](#_Toc9792)

*[2.2.3.](#_Toc9772)* [Các loại lỗ hổng phổ biến, cụ thể gồm 3 loại như sau: 11](#_Toc9772)

*[2.2.4.](#_Toc30500)* [Các mối đe dọa an ninh mạng 11](#_Toc30500)

[2.3. Giới thiệu về hệ điều hành Linux 12](#_Toc9907)

*[2.3.1.](#_Toc12944)* [Hệ điều hành Linux 13](#_Toc12944)

*[2.3.2.](#_Toc31118)* [Các công cụ bảo mật trong Kali Linux 14](#_Toc31118)

[2.4. Giới thiệu về Windows 10 18](#_Toc30274)

*[2.4.1.](#_Toc5833)* [Hệ điều hành Windows 10 18](#_Toc5833)

*[2.4.2.](#_Toc3645)* [Các lỗ hổng trên Windows 10 20](#_Toc3645)

[CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM 21](#_Toc1526)

[3.1. Công cụ thực hiện VMware Workstation 21](#_Toc2296)

[3.2. Công cụ dò quét lỗ hổng OpenVAS 22](#_Toc29723)

[3.3. Giới thiệu Prometheus 24](#_Toc32295)

[3.4. Giới thiệu Grafana 25](#_Toc17879)

[3.5. Demo tiến hành quét lổ hỗng của máy windows 10 19H1 và thực hiện Detect 27](#_Toc9406)

[3.6. Các nguyên nhân gây mất thông tin 34](#_Toc28629)

[3.7. Hậu quả của việc mất an toàn thông tin 35](#_Toc31261)

[3.8. Một số giải pháp khác 36](#_Toc28623)

[CHƯƠNG 4. KẾT LUẬN VÀ KIẾN NGHỊ 38](#_Toc2949)

[4.1. Kết quả đạt được 38](#_Toc21165)

[4.2. Hướng phát triển trong tương lai 38](#_Toc15429)

[4.3. Kiến nghị 38](#_Toc22655)

[TÀI LIỆU THAM KHẢO 40](#_Toc30272)

### DANH MỤC HÌNH

[Hình 2.1 - Biểu đồ CIA (Nguồn:internet) 10](#_Toc29390)

[Hình 2.2 - Hình minh họa về an ninh mạng 11](#_Toc28424)

[Hình 2.4 - Giao diện Linux 14](#_Toc31888)

[Hình 2.5 - Giao diện John the ripper 15](#_Toc29633)

[Hình 2.6 - Ví dụ Nmap 16](#_Toc31612)

[Hình 2.7 - Giao diện Windows 10 19](#_Toc30292)

[Hình 3.1 - Logo VMware Workstation 21](#_Toc488)

[Hình 3.2 - OpenVAS  24](#_Toc5192)

[Hình 3.3 - Hệ thống giám sát Prometheus và Grafana 27](#_Toc385)

[Hình 3.4 - Quét lổ hỗng của máy windows 10 19h1 28](#_Toc16829)

[Hình 3.5 - Truy cập Window Exporter 28](#_Toc19077)

[Hình 3.6 - Xem Node\_Exporter 29](#_Toc28712)

[Hình 3.7 - Truy cập Prometheus 29](#_Toc10750)

[Hình 3.8 - prometheus.yml 30](#_Toc31788)

[Hình 3.9 - Khởi chạy Prometheus 30](#_Toc18108)

[Hình 3.10 - Giao diện web Prometheus 31](#_Toc9010)

[Hình 3.11 - Prometheus/Targets 31](#_Toc6930)

[Hình 3.12 - Chạy Grafana server 32](#_Toc1692)

[Hình 3.13 - Giao diện web Grafana 32](#_Toc6574)

[Hình 3.14 - Thêm data sources 33](#_Toc12755)

[Hình 3.15 - Thêm URL 33](#_Toc15877)

[Hình 3.16 - Vào giao diện Dashboards 34](#_Toc380)

[Hình 3.17 - Windows 10 19H1 Dashboard 34](#_Toc3357)

### DANH MỤC VIẾT TẮT

|  |  |
| --- | --- |
| Từ viết tắt | Giải thích |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| TCP | Transmission Control Protocol |
| HTML | Hypertext Markup Language |
| MP4 | Moving Pictures Expert Group 4 |
| IP | Internet Protocol |
| XML | eXtensible Markup Language |
| CSV | Comma Separated Values |

### CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI

##### Tổng quan về đề tài nghiên cứu

Đề tài **“Phân tích và triển khai giải pháp an ninh mạng trên Windows 10 cho**

**Công ty GBF Groups”**

* Mục tiêu là để tận dụng các điểm yếu hoặc lỗ hổng trong phần mềm này nhằm đạt được các mục tiêu xâm nhập hoặc gây hại.
* Nghiên cứu hệ điều hành kali
* Tìm hiểu về khai thác lỗ hổng và hoạt động hệ thống bảo mật thông tin.

##### Ưu điểm:

* Việc khai thác lỗ hổng có thể cho phép kẻ tấn công truy cập từ xa vào hệ thống mục tiêu, mang lại khả năng kiểm soát và thao túng hệ thống từ xa. Để ngăn chặn điều này, cần thường xuyên cập nhật phần mềm và hệ điều hành, cũng như sử dụng các công cụ giám sát mạng để phát hiện các hoạt động đáng ngờ.
* Kẻ tấn công có thể chèn mã độc, gây suy yếu dịch vụ hoặc truyền thông tin theo ý muốn. Sử dụng phần mềm diệt virus và phần mềm chống mã độc hiệu quả để ngăn chặn và loại bỏ mã độc khỏi hệ thống là rất quan trọng.

##### Nhược điểm:

* Việc triển khai các giải pháp an ninh mạng toàn diện đòi hỏi chi phí đáng kể cho phần mềm, phần cứng và các dịch vụ hỗ trợ. Ngoài ra, còn có chi phí duy trì và nâng cấp liên tục để đảm bảo hệ thống luôn an toàn trước các mối đe dọa mới. hạn chế trong môi trường ứng dụng.
* Với nhiều giải pháp bảo mật khác nhau (tường lửa, IDS/IPS, mã hóa dữ liệu), việc quản lý và phối hợp chúng một cách hiệu quả có thể trở nên phức tạp và tốn thời gian.

##### Nhiệm vụ đồ án

* + - Tiến hành nghiên cứu cơ bản về Windows 10, bao gồm cấu trúc và hoạt động của phần mềm, tính năng và giao diện người dùng.
    - Khảo sát các lỗ hỏng đã được phát hiện trong phiên bản Windows 10, bao gồm việc tìm hiểu về các lỗ hỏng bảo mật.
    - Hiểu rõ cấu trúc cơ bản của Windows 10, bao gồm nhân (kernel), các dịch vụ hệ điều hành, và các lớp ứng dụng. Nghiên cứu cách các thành phần này tương tác với nhau và với phần cứng để xác định các điểm yếu có thể bị khai thác.
* Tìm hiểu về các lỗ hổng bảo mật đã được phát hiện trong Windows 10. Điều này bao gồm việc nghiên cứu các báo cáo từ các tổ chức bảo mật, các bản vá lỗi từ Microsoft.
* Khám phá các tính năng bảo mật được tích hợp trong Windows 10
* Phân loại các lỗ hổng theo mức độ nghiêm trọng và tầm ảnh hưởng. Đánh giá các lỗ hổng dựa trên khả năng khai thác và ảnh hưởng đến hệ thống để xác định những điểm cần ưu tiên bảo vệ.
* Tổng kết và trình bày kết quả nghiên cứu trong báo cáo đồ án.

### CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

##### Khái niệm về an ninh mạng

An ninh mạng, hay còn gọi là bảo mật thông tin hoặc bảo mật mạng, là các biện pháp và quy trình được thực hiện để bảo vệ các hệ thống máy tính, mạng, chương trình và dữ liệu khỏi các cuộc tấn công kỹ thuật số, truy cập trái phép, thiệt hại hoặc trộm cắp. An ninh mạng bao gồm một loạt các chiến lược và công nghệ nhằm bảo vệ tính toàn vẹn, bảo mật và sẵn sàng của thông tin.

Các thành phần chính của an ninh mạng bao gồm:

* **Bảo mật thông tin (Information Security)**:
* Bảo vệ dữ liệu và thông tin khỏi bị truy cập, sử dụng, tiết lộ, gián đoạn, thay đổi hoặc phá hủy trái phép.
* **Bảo mật mạng (Network Security)**:
* Bảo vệ mạng máy tính khỏi các mối đe dọa bên trong và bên ngoài bằng cách sử dụng các công nghệ và biện pháp như tường lửa (firewall), hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), và mạng riêng ảo (VPN).
* **Bảo mật ứng dụng (Application Security)**:
* Bảo vệ các ứng dụng phần mềm và dịch vụ khỏi các lỗ hổng bảo mật thông qua việc kiểm tra, phát hiện và vá các lỗ hổng.

##### An ninh mạng của việt nam hiện nay

Tình hình an toàn an ninh mạng của Việt Nam hiện nay đang đối mặt với nhiều thách thức và mối đe dọa. Sự phát triển nhanh chóng của công nghệ thông tin và mạng internet đã mở ra cửa cho các cuộc tấn công mạng phức tạp và tinh vi.

Việt Nam đã ghi nhận nhiều vụ vi phạm an ninh mạng, bao gồm tấn công DDoS, lừa đảo trực tuyến, xâm nhập hệ thống và đánh cắp dữ liệu. Việc sử dụng phần mềm độc hại, mã độc và các kỹ thuật tấn công tiên tiến ngày càng gia tăng, đe dọa đến thông tin quan trọng của cả cá nhân và tổ chức.

Để tăng cường an toàn an ninh mạng, Việt Nam đã triển khai các chính sách và biện pháp bảo vệ mạng, bao gồm việc nâng cao nhận thức về an ninh mạng, tăng cường hợp tác quốc tế và đào tạo nhân lực chuyên gia về an ninh mạng. Tuy nhiên, vẫn còn nhiều thách thức cần vượt qua để đảm bảo an toàn an ninh mạng trong tương lai.

##### An toàn thông tin

An toàn thông tin là một khái niệm quan trọng trong lĩnh vực bảo mật thông tin, nhằm bảo vệ tính toàn vẹn, sẵn có, bảo mật và sử dụng hợp pháp của thông tin. Nó liên quan đến việc đảm bảo rằng thông tin được bảo vệ khỏi các mối đe dọa, tấn công hoặc việc truy cập trái phép.

An toàn thông tin bao gồm một loạt các biện pháp và quy trình nhằm đảm bảo rằng thông tin không bị rò rỉ, thay đổi trái phép, mất mát hoặc sử dụng sai mục đích. Các yếu tố quan trọng trong an toàn thông tin bao gồm:

*+ Tính bí mật:*

* Bí mật là thuật ngữ được sử dụng để tránh lộ thông tin đến những đối tượng người dùng không được xác nhận hoặc để lọt vào những mạng lưới hệ thống khác. Ví dụ : một thanh toán giao dịch tín dụng thanh toán qua Internet, số thẻ tín dụng thanh toán được gửi từ người mua hàng đến người bán, và từ người bán đến nhà sản xuất dịch vụ thẻ tín dụng. Hệ thống sẽ cố gắng nỗ lực thực thi tính bí hiểm bằng cách mã hóa số thẻ trong suốt quy trình truyền tin, số lượng giới hạn nơi nó hoàn toàn có thể Open ( cơ sở tài liệu, log file, sao lưu ( backup ), in hóa đơn … ) và bằng việc số lượng giới hạn truy vấn những nơi mà nó được lưu lại. Nếu một bên không được xác nhận ( ví dụ người dùng không có trong thanh toán giao dịch, hacker … ) lấy số thẻ này bằng bất kỳ cách nào, thì tính bí hiểm không còn nữa .Tính bí hiểm rất thiết yếu ( nhưng chưa đủ ) để trì sự riêng tư của người có thông tin được mạng lưới hệ thống lưu giữ .

*+ Tính toàn vẹn:*

* Trong an toàn thông tin, toàn vẹn có nghĩa rằng tài liệu không hề bị chỉnh sửa mà không bị phát hiện. Nó khác với tính toàn vẹn trong tham chiếu của cơ sở tài liệu, mặc dầu nó hoàn toàn có thể được xem như thể một trường hợp đặc biệt quan trọng của tính đồng nhất như được hiểu trong mô hình cổ xưa. Là một tập những thuộc tính bảo vệ rằng cơ sở tài liệu đáng an toàn và đáng tin cậy ) của giải quyết và xử lý thanh toán giao dịch. Tính toàn vẹn bị xâm phạm khi một thông điệp bị chỉnh sửa trong thanh toán giao dịch. Hệ thống thông tin an toàn luôn cung ứng những thông điệp toàn vẹn và bí hiểm .

*+Tính sẵn sàng:*

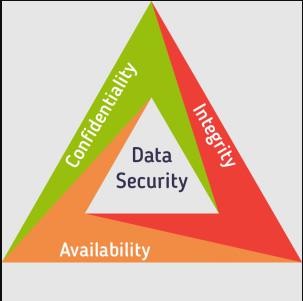
* Mọi mạng lưới hệ thống thông tin đều Giao hàng mục tiêu riêng của nó và thông tin phải luôn luôn sẵn sàng chuẩn bị khi thiết yếu. Điều đó có nghĩa rằng mạng lưới hệ thống đo lường và thống kê sử dụng để tàng trữ và giải quyết và xử lý thông tin, có một mạng lưới hệ thống tinh chỉnh và điều khiển bảo mật thông tin sử dụng để bảo vệ nó, và kênh liên kết sử dụng để truy vấn nó phải luôn hoạt động giải trí đúng chuẩn. Hệ thống có tính sẵn sàng chuẩn bị cao hướng đến sự sẵn sàng chuẩn bị ở mọi thời gian, tránh được những rủi ro đáng tiếc cả về phần cứng, ứng dụng như : sự cố mất điện, hỏng phần cứng, update, tăng cấp mạng lưới hệ thống … bảo vệ tính sẵn sàng chuẩn bị cũng có nghĩa là tránh được tiến công khước từ dịch vụ .

*+ Tính xác thực:*

* Trong hoạt động giải trí giám sát, kinh doanh thương mại qua mạng và an toàn thông tin, tính xác nhận là vô cùng thiết yếu để bảo vệ rằng tài liệu, thanh toán giao dịch, liên kết hoặc những tài liệu ( tài liệu điện tử hoặc tài liệu cứng ) đều là thật ( genuine ). Nó cũng quan trọng cho việc xác nhận rằng những bên tương quan biết họ là ai trong mạng lưới hệ thống .

*+ Tính không thể chối cãi:*

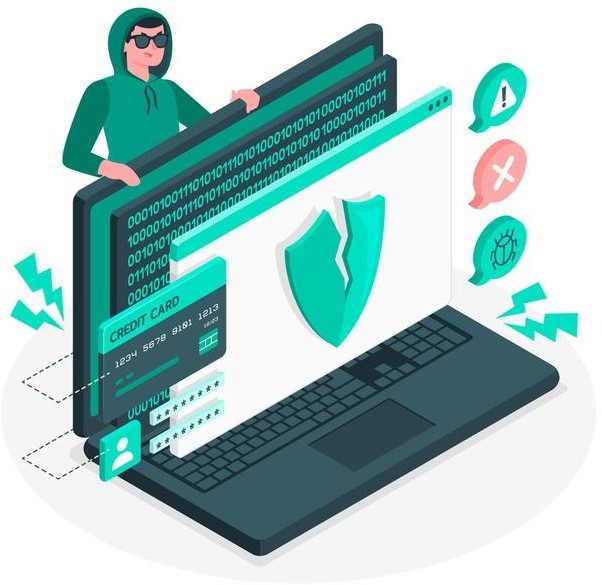
* Không thể chối cãi có nghĩa rằng một bên thanh toán giao dịch không hề phủ nhận việc họ đã thực thi thanh toán giao dịch với những bên khác. Ví dụ : trong khi thanh toán giao dịch mua hàng qua mạng, khi người mua đã gửi số thẻ tín dụng thanh toán cho bên bán, đã giao dịch thanh toán thành công xuất sắc, thì bên bán không hề phủ nhận việc họ đã nhận được tiền, ( trừ trường hợp mạng lưới hệ thống không bảo vệ tính an toàn thông tin trong thanh toán giao dịch ).



Hình 2.1 - Biểu đồ CIA (Nguồn:internet)

##### Khái niệm khai thác lỗ hổng

* + - * Lỗ hổng bảo mật là những điểm yếu tồn tại trên phần cứng, phần mềm hoặc trên một dịch vụ nào đó của hệ thống thông tin. Lỗ hổng bảo mật chính là mục tiêu mà tin tặc nhắm đến. Lý do là vi khi tìm ra lỗ hổng, chúng có thể xâm nhập được vào hệ thống mạng của doanh nghiệp để thực hiện các hành vi trái phép của mình.
      * Sau khi một lỗi được xác định là một lỗ hổng, lỗi đó sẽ được MITRE đăng ký dưới dạng CVE và được chấm điểm bởi hệ thống đánh giá lỗ hổng Common Vulnerability Scoring System (CVSS) để phản ánh nguy cơ mà nó có thể gây ra cho doanh nghiệp của bạn. Danh sách CVE này giữ vai trò tham chiếu cho các thiết bị rà quét lỗ hổng bảo mật.
      * Nguyên nhân: Có nhiều nguyên nhân gây ra lỗ hổng bảo mật: thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể còn tồn tại ngay chính tại hệ điều hành như trong Windows XP, Windows NT, UNIX, hệ điều hành các thiết bị router, modem hoặc trong các ứng dụng thường xuyên sử dụng như word processing, các hệ Databases.



Hình 2.2 - Hình minh họa về an ninh mạng

##### Các loại lỗ hổng phổ biến, cụ thể gồm 3 loại như sau:

* + - * *Lỗ hổng loại A*: cho phép người ngoài hệ thống có thể truy cập bất hợp pháp vào hệ thống, có thể phá hủy toàn bộ hệ thống.
      * *Lỗ hổng loại B:* lỗ hổng cho phép người sử dụng có thêm các quyền truy cập hệ thống mà không cần kiểm tra tính hợp lệ dẫn đến lộ, lọt thông tin.
      * *Lỗ hổng loại C:* cho phép thực hiện tấn công kiểu DoS (Denial of Services – từ chối dịch vụ) làm ảnh hướng tới chất lượng dịch vụ, ngưng trệ, gián đoạn hệ thống, nhưng không phá hỏng dữ liệu hoặc đạt được quyền truy cập hệ thống.

##### Các mối đe dọa an ninh mạng

* + - * Mối đe dọa an ninh mạng là những hành vi xâm hại đến an ninh quốc gia, gây tổn hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.
      * Một số mối đe dọa an ninh mạng phổ biến hiện nay gồm:
* ****Sử dụng mã độc****
* Gồm những phần mềm, tệp hoặc email chứa mã độc được thiết kế để gây hại cho máy tính thông qua mạng truy cập. Nhằm theo dõi, đánh cắp những dữ liệu nhạy cảm, mật khẩu, tài khoản, thông tin bảo mật của các cơ quan, tổ chức, cá nhân.
* Lừa đảo qua mạng
* Gồm những hành vi lừa đảo thông qua việc sử dụng email, tin nhắn, cuộc gọi để dụ dỗ, thuyết phục mọi người bấm vào liên kết có hại hoặc tự cung cấp những thông tin cá nhân.
* Hiện nay có rất nhiều đối tượng giả mạo các cơ quan uy tín như ngân hàng, công an, công ty nổi tiếng để nhắn tin, gọi điện cho người dân nhằm thực hiện hành vi lừa đảo qua mạng.
* Bên cạnh đó, còn có rất nhiều hình thức lừa đảo qua mạng khác rất tinh vi như giả mạo website, dùng đường link khảo sát, thông qua mã QR.
* Người dùng trong nội bộ

Gồm những người đã có quyền truy cập vào hệ thống máy tính, cơ sở dữ liệu nội bộ của cơ quan, tổ chức, cá nhân như nhân viên hoặc khách hàng. Những người này có thể vô tình hay cố ý thực hiện những hành động gây hại.

* Tấn công có chủ đích

Tấn công có chủ đích là hành vi xâm nhập có mục tiêu cụ thể nhằm vào hệ thống mạng, máy chủ web hoặc máy tính riêng lẻ của cơ quan, tổ chức, cá nhân bất kể chúng đang ở mức độ bảo vệ nào.

Tấn công có chủ đích do một nhóm tội phạm an ninh mạng, các tổ chức khủng bố hay các cơ quan đặc vụ quốc gia thực hiện. Đây là loại tấn công phức tạp, tinh vi với trình độ cao với mục đích chiếm quyền kiểm soát hệ thống trong thời gian lâu dài nhất.

##### Giới thiệu về hệ điều hành Linux

##### Hệ điều hành Linux

**Kali Linux** là một bản phân phối Linux đặc biệt được thiết kế để sử dụng trong lĩnh vực thử nghiệm và kiểm tra bảo mật mạng. Nó cung cấp các công cụ và tính năng mạnh mẽ để phát hiện và khai thác lỗ hổng bảo mật trong một môi trường kiểm thử.

Kali chứa hàng trăm công cụ được hướng tới các nhiệm vụ bảo mật thông tin khác nhau, chẳng hạn như Penetration Testing, Security research, Computer Forensics và Reverse Engineering. Kali Linux được phát triển, tài trợ và duy trì bởi Offensive Security, một công ty đào tạo an ninh thông tin hàng đầu.

* + - * *Ưu điểm của Kali Linux bao gồm:*

Các công cụ bảo mật mạnh mẽ: Kali Linux đi kèm với hơn 600 công cụ bảo mật phục vụ cho việc kiểm thử và thử nghiệm bảo mật mạng. Các công cụ này cung cấp khả năng phát hiện lỗ hổng bảo mật, tiến hành kiểm tra xâm nhập và phân tích bảo mật mạng.

Tích hợp đa dạng: Kali Linux tích hợp nhiều công cụ và phần mềm khác nhau, từ trình duyệt web, máy chủ, đến các công cụ mã hóa và phân tích dữ liệu. Điều này mang lại sự tiện ích và linh hoạt cho các chuyên gia bảo mật trong quá trình kiểm thử.

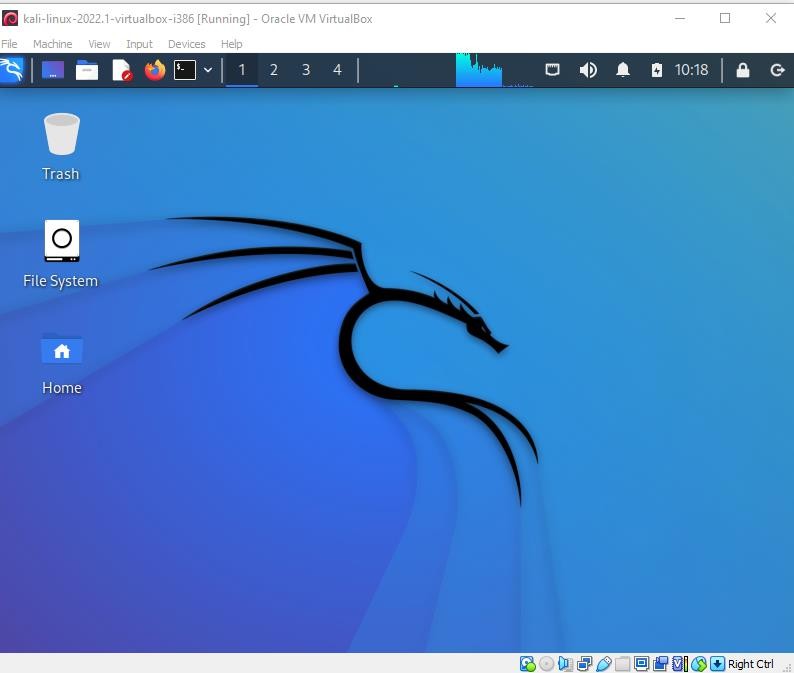
Cộng đồng hỗ trợ mạnh mẽ: Kali Linux được hỗ trợ bởi một cộng đồng rộng lớn gồm các chuyên gia bảo mật và nhà phát triển. Người dùng có thể tìm thấy hướng dẫn, tài liệu và sự giúp đỡ từ cộng đồng này.

* + - * *Một số nhược điểm Kali Linux:*

Phức tạp cho người dùng mới: Kali Linux được thiết kế dành cho những người có kiến thức chuyên sâu về bảo mật mạng. Điều này có nghĩa là người dùng mới sẽ gặp khó khăn khi sử dụng và làm quen với giao diện và công cụ phức tạp của nó.

Khả năng gây lạm dụng: Vì tính chất của Kali Linux là kiểm thử và khai thác bảo mật, việc sử dụng nó một cách sai mục đích hoặc không đúng pháp luật có thể gây ra hậu quả nghiêm trọng. Việc sử dụng Kali Linux cần có sự ý thức và tuân thủ đúng các quy định và luật pháp liên quan.

Hỗ trợ phần cứng hạn chế: Do mục tiêu chuyên sâu vào lĩnh vực bảo mật, Kali Linux có thể gặp khó khăn trong việc hỗ trợ một số phần cứng cụ thể, đặc biệt là các phần cứng mới nhất trên thị trường.



Hình 2.4 - Giao diện Linux

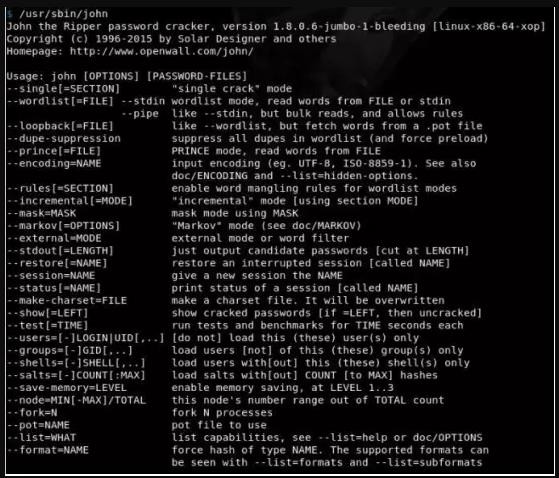
*(Nguồn: internet)*

##### Các công cụ bảo mật trong Kali Linux

* **Password Attacks – John the ripper:**

Được phát hành lần đầu vào năm 1996, John the Ripper (JtR) là một công cụ bẻ khóa mật khẩu ban đầu được sản xuất cho các hệ thống dựa trên UNIX. Nó được thiết kế để kiểm tra độ mạnh của mật khẩu, mật khẩu được mã hóa (băm) brute-force và bẻ khóa mật khẩu thông qua các cuộc tấn công từ điển. John the Ripper hỗ trợ một danh sách khổng lồ các loại mật mã và băm khác nhau như:

* + - * + Mật khẩu người dùng Unix, macOS và Windows
        + Ứng dụng web
        + Máy chủ cơ sở dữ liệu
        + Lưu lượng truy cập mạng ghi lại
        + Khóa riêng tư được mã hóa
        + Các tài liệu



Hình 2.5 - Giao diện John the ripper

*(Nguồn: internet)*

* **Information Gathering – Nmap:**

Đầu tiên là Nmap - một công cụ không thể thiếu trong quá trình phân tích và tìm kiếm thông tin về mục tiêu. Các tính năng mà Nmap có thể mang lại như:

* Kiểm tra và lập sơ đồ mạng: bao gồm máy chủ, bộ định tuyến và cách chúng kết nối như thế nào
* Tạo lưu lượng (traffic) đến host trên mạng, phân tích phản hồi và đo thời gian phản hồi
* Dò tìm dịch vụ (Service discovery)
* Kiểm tra bảo mật và khai thác lỗ hổng trên hệ thống mạng.
* Thực hiện ping kiểm tra kết nối và sử dụng Nmap để quét cổng TCP và UDP

Hình 2.6 - Ví dụ Nmap

*(Nguồn: internet)*

Một số tính năng thường hay được sử dụng trong nmap:

* Kiểm tra xem máy chủ có đang được mở (online) hay không?
* Phát hiện những cổng nào đang được mở trên máy chủ.
* Xác định được máy chủ sử dụng những dịch vụ nào, được chạy trên cổng tương ứng nào và phiên bản là gì?.
* Kiểm tra xem máy chủ chạy trên hệ điều hành nào và phiên bản của hệ điều hành đó.
* Phát hiện ra lỗ hổng bảo mật.

Ban đầu nmap chỉ có trên Linux, nhưng theo thời gian vì tính hữu dụng nên nó đã được port sang nhiều hệ điều hành khác như Windows, MacOS, …. Chương trình được sử dụng chủ yếu bằng dòng lệnh, nmap cũng hỗ trợ những chức năng khác như tính toán thời gian trễ, thời gian chờ gói tin, quét port song song, phát hiện máy chủ “down” thông qua ping song song.

* **Vulnerability Analysis – Nikto:**

Nikto là một công cụ rà quét lỗ hổng bảo mật nhằm tìm ra các điểm yếu đối với các máy chủ web và bạn có thể sử dụng nó với bất kỳ máy chủ web nào (Apache, Nginx, IHS, OHS, Litespeed, v.v.).. Nó có khả năng quét hơn 6700 mục để phát hiện cấu hình sai, các tệp có nguy cơ, v.v. và một số tính năng bao gồm:

* Quét nhiều cổng trên máy chủ
* Tìm miền phụ
* Liệt kê người dùng Apache
* Kiểm tra các phiên bản lỗi thời
* Hỗ trợ SSL
* Lưu báo cáo dưới dạng HTML, XML, CSV

Ngoài các công cụ trên thì còn rất nhiều công cụ khai thác khác như: HashCat, Aircrack-ng,Cisco-torch, Commix, Crackle, Eploitdb...

##### Giới thiệu về Windows 10

##### Hệ điều hành Windows 10

* + - * Windows 10 là hệ điều hành của Microsoft được phát hành vào ngày 29 tháng 7 năm 2015. Nó là phiên bản tiếp theo sau Windows 8 và 8.1, mang lại nhiều cải tiến và tính năng mới.
      * Quá trình hình thành: Windows 10 được phát triển như một nền tảng kết hợp giữa giao diện Windows 7 truyền thống và các yếu tố hiện đại của Windows 8. Microsoft nhằm tạo ra một trải nghiệm đồng nhất trên nhiều thiết bị, từ máy tính để bàn, máy tính xách tay, máy tính bảng cho đến điện thoại thông minh.
      * Phiên bản: Windows 10 có nhiều phiên bản phù hợp với các nhu cầu và yêu cầu khác nhau. Bao gồm Windows 10 Home dành cho người dùng cá nhân, Windows 10 Pro với tính năng mở rộng cho doanh nghiệp, Windows 10 Enterprise dành cho các tổ chức lớn và Windows 10 Education dành cho giáo dục.
      * Giao diện và tính năng: Windows 10 mang đến giao diện Start Menu đã quen thuộc từ Windows 7, kết hợp với khung ứng dụng Metro từ Windows 8. Nó cũng có tính năng cửa sổ multi-tasking, Virtual Desktops, và trình duyệt web Microsoft Edge. Ngoài ra, Windows 10 cung cấp tính năng bảo mật tăng cao với Windows Hello (nhận diện khuôn mặt hoặc vân tay) và Windows Defender (chương trình chống vi-rút tích hợp sẵn).



Hình 2.7 - Giao diện Windows 10

*(Nguồn: internet)*

* + - * Microsoft chưa cho biết kế hoạch nâng cấp Windows 10, cũng như các phiên bản cụ thể và giá bán. Hệ điều hành Windows kế tiếp dự kiến sẽ xuất hiện trên thị trường vào cuối năm sau, 2015. Nhưng bắt đầu từ 1/10, Microsoft cũng tung ra phiên bản Technical Preview cho phép dùng thử và gửi các phản hồi về lại hãng.
      * Một trong những thay đổi đáng chú ý nhất trên Windows 10 là Start Menu quen thuộc của Windows, vốn đã bị Microsoft loại bỏ trên bản 8 hiện tại. Start Menu mới có giao diện kết hợp giữa phong cách truyền thống vốn có từ các bản Windows 7 và trước đó, cùng với giao diện Modern UI với các biểu tượng Live Tiles trên Windows 8 hiện nay.
      * Windows 10 cung cấp nhiều phiên bản để phù hợp với các nhu cầu và yêu cầu khác nhau của người dùng. Phiên bản phổ biến bao gồm:

*+ Windows 10 Home*: Đây là phiên bản dành cho người dùng cá nhân. Nó cung cấp các tính năng cơ bản như giao diện Start Menu, trình duyệt Microsoft Edge, Cortana (trợ lý ảo), Windows Store và khả năng sử dụng các ứng dụng trên cửa sổ múlti-tasking.

*+ Windows 10 Pro*: Phiên bản này cung cấp các tính năng nâng cao hơn cho doanh nghiệp và người dùng chuyên nghiệp. Nó bao gồm tất cả các tính năng của Windows 10 Home và bổ sung thêm như quản lý máy tính từ xa, BitLocker (mã hóa ổ đĩa), Windows Update for Business và khả năng tham gia vào mạng domain.

+ *Windows 10 Enterprise:* Được thiết kế cho các tổ chức lớn, phiên bản này bao gồm các tính năng bảo mật và quản lý mạnh mẽ hơn. Nó cung cấp các tính năng của Windows 10 Pro và bổ sung thêm như AppLocker (quản lý ứng dụng), DirectAccess (truy cập từ xa an toàn), Credential Guard (bảo vệ thông tin xác thực) và Windows To Go (khả năng chạy Windows từ ổ đĩa di động).

+ *Windows 10 Education:* Đây là phiên bản dành cho ngành giáo dục, cung cấp các tính năng của Windows 10 Enterprise và tập trung vào các giải pháp và công cụ hỗ trợ giảng dạy và học tập trong môi trường giáo dục.

##### Các lỗ hổng trên Windows 10

* + - * Windows 10 - Hệ điều hành phổ biến của Microsoft - không tránh khỏi những lỗ hổng bảo mật, đòi hỏi người dùng phải luôn tỉnh táo và áp dụng biện pháp bảo mật để bảo vệ thông tin quan trọng và đảm bảo an toàn cho hệ thống.
      * Dưới đây là một số lỗ hổng thường gặp:

+ *Lỗ hổng Zero-day*: Đây là các lỗ hổng bảo mật chưa được biết đến trước đó, cho phép tin tặc tấn công và khai thác các điểm yếu mà người dùng chưa kịp bảo vệ. Các lỗ hổng Zero-day có thể được sử dụng để truy cập trái phép vào hệ thống hoặc đánh cắp thông tin quan trọng.

+ *Lỗ hổng trong phần mềm ứng dụng*: Các ứng dụng bên thứ ba trên Windows 10 có thể chứa các lỗ hổng bảo mật, cho phép tin tặc tấn công và kiểm soát hệ thống. Điều này có thể xảy ra trong các trình duyệt web, trình phát nhạc, trình đọc PDF và các ứng dụng khác.

+ *Lỗ hổng trình duyệt web*: Trình duyệt web như Microsoft Edge và Internet Explorer có thể gặp các lỗ hổng bảo mật, như lỗ hổng xâm nhập mã độc (code injection) hoặc lỗ hổng đè lên bộ nhớ đệm (buffer overflow), cho phép tin tặc thực hiện các cuộc tấn công từ xa hoặc đánh cắp thông tin.

* + - * Để giảm thiểu nguy cơ lỗ hổng bảo mật trên Windows 10, người dùng cần thực hiện các biện pháp bảo mật như cài đặt các bản vá bảo mật, sử dụng phần mềm chống vi-rút và malware, giữ mật khẩu mạnh và cập nhật hệ điều hành và ứng dụng thường xuyên.

### CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM

##### Công cụ thực hiện VMware Workstation

* + - * VMware Workstation Pro (được gọi là VMware Workstation cho đến khi phát hành VMware Workstation 12 vào năm 2015) là một trình quản lý ảo được lưu trữ (Loại 2) chạy trên các phiên bản x64 của hệ điều hành Windows và Linux. Trước đây đã từng có phiên bản IA-32 cho các phiên bản trước đó của phần mềm. Nó cho phép người dùng thiết lập các máy ảo (VM) trên một máy vật lý duy nhất và sử dụng chúng đồng thời cùng với máy chủ. Mỗi máy ảo có thể chạy hệ điều hành riêng của mình , bao gồm các phiên bản Microsoft Windows , Linux , BSD và MS-DOS . VMware Workstation được phát triển và bán bởi VMware, Inc. Cho đến phiên bản 17.5.2, có một phiên bản miễn phí có tên là VMware Workstation Player (được gọi là VMware Player cho đến khi phát hành VMware Workstation 12 vào năm 2015), dành cho mục đích sử dụng phi thương mại. Các VM Linux làm sẵn được thiết lập cho các mục đích khác nhau có sẵn từ một số nguồn.
      * VMware Workstation bao gồm khả năng nhóm nhiều máy ảo trong một thư mục hàng tồn kho. Các máy trong thư mục như vậy sau đó có thể được bật và tắt như một đối tượng duy nhất, hữu ích cho việc thử nghiệm các môi trường máy khách-máy chủ phức tạp.



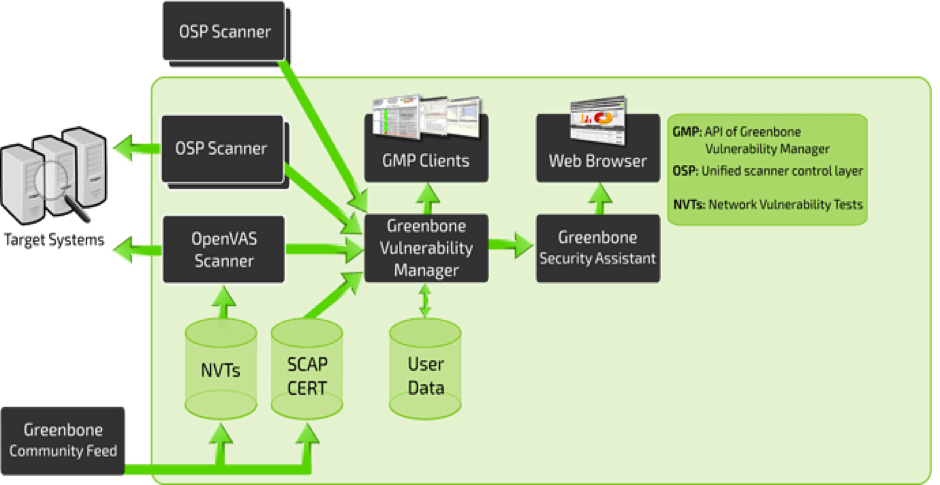
Hình 3.1 - Logo VMware Workstation

*(Nguồn: intermet)*

* + - * Chức năng: VMware Workstation cung cấp nhiều tính năng, bao gồm:
* Tạo và quản lý máy ảo: Người dùng có thể tạo ra các máy ảo mới và tùy chỉnh các cấu hình của chúng như bộ nhớ, ổ cứng ảo, card mạng và các tùy chọn khác.
* Chia sẻ tệp tin và tài nguyên: WMware cho phép chia sẻ tệp tin và tài nguyên giữa máy tính vật lý và máy ảo. Điều này giúp dễ dàng chuyển tệp tin và truy cập vào các tài nguyên từ cả hai môi trường.
* Mạng ảo: WMware cung cấp các chế độ mạng ảo để kết nối máy ảo với mạng bên ngoài hoặc với các máy ảo khác trên cùng một máy chủ.
* Hỗ trợ nhiều hệ điều hành: Chạy nhiều hệ điều hành khác nhau trên cùng một máy tính, bao gồm Windows, Linux, macOS, BSD và Solaris.
* Snapshots: Chụp ảnh nhanh trạng thái của máy ảo để dễ dàng quay lại điểm trước đó nếu cần.
* Clone máy ảo: Tạo bản sao nhanh chóng của máy ảo hiện có để tiết kiệm thời gian và công sức.
* Tích hợp với các công cụ khác: VMware Workstation tích hợp với các công cụ DevOps và CI/CD phổ biến để tự động hóa việc triển khai và quản lý máy ảo.
  + - Cách hoạt động: VMware Workstation sử dụng công nghệ ảo hóa Hypervisor để chia sẻ tài nguyên phần cứng của máy tính vật lý cho nhiều máy ảo. Hypervisor hoạt động như một lớp trung gian giữa hệ điều hành vật lý và hệ điều hành của máy ảo, cho phép mỗi máy ảo hoạt động độc lập và hiệu quả.
    - Ngoài ra, VMware Workstation còn có thể kết hợp với các công cụ và phần mềm khác để tăng cường chức năng:
* VMware Tools: Cung cấp các tính năng nâng cao như đồng bộ hóa clipboard, kéo thả tệp và chia sẻ thư mục giữa máy ảo và máy tính vật lý.
* VMware vSphere: Quản lý tập trung nhiều máy ảo được triển khai trên nhiều máy chủ vật lý.
* VMware Workstation Player: Phiên bản miễn phí của VMware Workstation để chạy máy ảo đã được tạo sẵn.

##### Công cụ dò quét lỗ hổng OpenVAS

* + - OpenVAS là thành phần máy quét của Greenbone Vulnerability Management, một khung phần mềm gồm một số dịch vụ và công cụ cung cấp tính năng quét lỗ hổng và quản lý lỗ hổng. Tất cả các sản phẩm Quản lý lỗ hổng Greenbone đều là phần mềm miễn phí và hầu hết các thành phần đều được cấp phép theo Giấy phép Công cộng GNU.
    - OpenVAS có 3 thành phần chính: Greenbone Vulnerability Manager (GVMd), Greenbone Security Assistant (GSA), OpenVAS Scanner.
* *GVMd*: là trung tâm dịch vụ, hợp nhất các công cụ quét lỗ hổng đơn giản thành một giải pháp quản lý lỗ hổng đầy đủ. GVMd điều khiển OpenVAS Scanner qua một giao thức nội bộ và cung cấp thêm một giao thức chung Open Scanner Protocol (OSP) để có thể tích hợp các máy quét khác. Bản thân GVMd cũng cung cấp một giao thức dựa trên XML khác, Greenbone Management Protocol (GMP) để các thành phần khác có thể gửi những yêu cầu xử lý như tạo người dùng, tạo lịch quét, tạo một mục tiêu quét, tạo một nhiệm vụ để quét mục tiêu, bắt đầu nhiệm vụ quét một mục tiêu,… .GVMd cũng kiểm soát cơ sở dữ liệu SQL ( Postgres ở phiên bản GVM 10 và SQLite 3 cho các phiên bản trước) nơi tất cả dữ liệu kết quả và cấu hình quét được lưu trữ tập trung.
* *GSA*: là giao diện web của GVM. Nó kết nối với GVMd để cung cấp giao diện cho người dùng với đầy đủ những tính năng của công cụ quản lý lỗ hổng. GSA bao gồm các thành phần: • GSA - ứng dụng web được viết bằng React. • GSAD – Là HTTP server giao tiếp với GVMd thông qua giao thức GMP.
* *OpenVAS Scanner*: là một công cụ quét đầy đủ tính năng để thực thi một mẫu thử NVT nhằm mục đích kiểm tra một mục tiêu quét có vi phạm các lỗ hổng bảo mật, chưa cập nhật các bản vá cho hệ thống và các mục đích khác của một công cụ dò quét lỗ hổng. Và hầu hết Openvas Scanner sẽ thực hiện các nhiệm vụ và trả lại kết quả mà GVMd gọi đến.



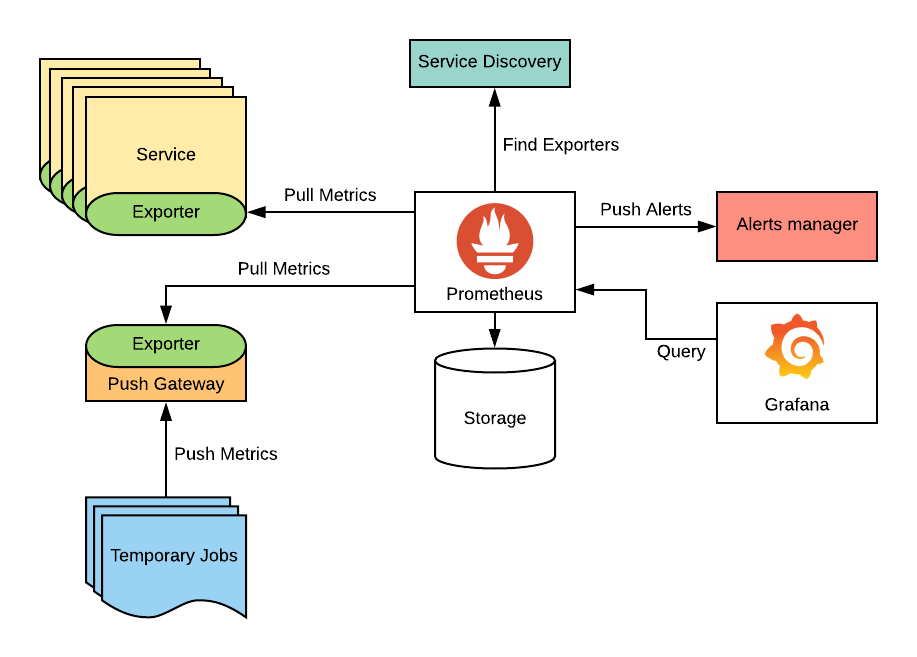
Hình 3.2 - OpenVAS

##### Giới thiệu Prometheus

* + - Prometheus là một dịch vụ theo dõi và cảnh báo về hệ thống. Đây là một dịch vụ mã nguồn mở (Open source) hoàn toàn miễn phí. SoundCloud đã khởi đầu xây dựng Prometheus từ năm 2012. Prometheus đã được rất nhiều hệ thống tin tưởng áp dụng. Dự án có một cộng đồng người đóng góp, phát triển rất tích cực.
    - Tính năng quan trọng nhất của Prometheus là thu thập thông số, dữ liệu từ các mục tiêu (dịch vụ) được nhắm đến theo khoảng thời gian nhất định đã được cài đặt trước. Ngoài ra còn các API khác thể hiện được kết quả, đánh giá bằng biểu thức quy tắc và đưa ra cảnh báo. Prometheus còn cung cấp một ngôn ngữ truy vấn rất mạnh PromQL, cực kì hữu ích khi giao tiếp với các dịch vụ monitor khác.
    - Một số tính năng của Prometheus:
* *Mô hình dữ liệu Time series đặc biệt phù hợp để theo dõi số liệu theo thời gian.*
* *Có ngôn ngữ truy vấn riêng PromQL rất mạnh mẽ.*
* *Tích hợp tốt với rất nhiềunền tảng ứng dụng.*
* *Yêu cầu hạ tầng để triển khai đơn giản.*
* *Hỗ trợ Push Gateway (khi làm việc với các dịch vụ tồn tại trong thời gian ngắn và hủy sau khi hoàn thành).*
* *Có hỗ trợ Service discovery hoặc cấu hình tĩnh để tìm, nhắm mục tiêu cần theo dõi.*
  + - Các thành phần chính trong hệ thống Prometheus
* *Máy chủ Prometheus.*
* *Thư viện kết nối đến máy chủ Prometheus cho các ứng dụng. (Có thể sử dụng dạng JSON nếu không có thư viện hỗ trợ)*
* *Push Gateway Prometheus: sử dụng để hỗ trợ các job có thời gian thực hiện ngắn (tạm thời). Đơn giản là các tác vụ công việc này không tồn tại lâu đủ để Prometheus chủ động lấy dữ liệu. Vì vậy là mà các dữ liệu chỉ số (metric) sẽ được đẩy về Push Gateway rồi đẩy về Prometheus Server.*
* *Exporter hỗ trợ giám sát các dịch vụ hệ thống và gửi về Prometheus theo chuẩn Prometheus mong muốn.*
* *AlertManager: dịch vụ quản lý, xử lý các cảnh báo (alert).*
  + - Prometheus rất thích hợp với những hệ thống Microservices và có các dịch vụ Listening. Một hệ thống theo dõi chủ động sẽ giúp người quản trị phát hiện sớm những dấu hiệu cảnh báo xấu.

##### Giới thiệu Grafana

* + - Grafana là một công cụ mã nguồn mở giúp cho việc trực quan hóa và giám sát dữ liệu, được tích hợp với các nguồn dữ liệu phức tạp như Prometheus, InfluxDB, Graphite, và ElasticSearch. Cho phép bạn tạo cảnh báo, thông báo và bộ lọc tạm thời cho dữ liệu của bạn, đồng thời giúp việc cộng tác với thành viên nhóm dễ dàng hơn thông qua các tính năng chia sẻ tích hợp sẵn.
    - Là một nền tảng để xây dựng các analytics và monitoring. Nói nôm na cho mọi người dễ hình dung là sau khi lấy được metric từ các thiết bị, grafana sẽ sử dụng metric đó để phân tích và tạo ra dashboard mô tả trực quan các metric cần thiết cho việc monitoring ví dụ như cpu, ram, dish, network, iops, session.
    - Grafana mang đến nhiều tính năng phổ biến và hữu ích hỗ trợ đắc lực cho người dùng khi làm việc với số liệu. Cụ thể, các tính năng của Grafana bao gồm:
* *Trực quan hóa: Grafana cung cấp nhiều tùy chọn một cách trực quan, cho phép người dùng hiểu rõ hơn về dữ liệu của họ thông qua hình ảnh.*
* *Cảnh báo: Grafana đơn giản hóa việc quản lý cảnh báo bằng cách cho phép người dùng xác định các ngưỡng trực quan. Bạn có thể nhận thông báo thông qua các nền tảng như Slack và PagerDuty, đảm bảo phản hồi kịp thời cho các vấn đề quan trọng.*
* *Hợp nhất dữ liệu: Grafana trao quyền cho người dùng tập hợp dữ liệu từ nhiều nguồn khác nhau, cung cấp môi trường để bạn phân tích dữ liệu được tập hợp đó, đảm bảo tích hợp liền mạch với hàng chục cơ sở dữ liệu.*
* *Mã nguồn mở: Grafana là giải pháp nguồn mở mang lại sự linh hoạt khi triển khai trên các nền tảng.*
* *Phân tích Nhật ký: Bằng cách sử dụng bộ lọc, người dùng có thể lọc nhật ký mở rộng hiệu quả, giúp bạn truy xuất và phân tích dữ liệu nhanh chóng.*
* *Hiển thị bảng điều khiển: Grafana cho phép người dùng trình bày dữ liệu thông qua các báo cáo mẫu hoặc tùy chỉnh, giúp dễ dàng thể hiện và truyền đạt tới các thành viên trong nhóm của bạn.*
* *Tạo và chia sẻ báo cáo: Bạn có thể tạo và chia sẻ các báo cáo đầy đủ thông tin cho các bên liên quan. Tính năng này được mở khi bạn nâng cấp nền tảng.*
  + - Grafana được ứng dụng phổ biến nhất là công cụ giám sát cơ sở hạ tầng. Nó cho phép bạn theo dõi hiệu suất ứng dụng và tỷ lệ lỗi. Grafana cung cấp cho bạn một nền tảng được xây dựng theo mục đích duy nhất đi từ bảng thông tin tổng quan đến nguồn nâng cao.
    - Ngoài ra, bạn có thể sử dụng Grafana khi bạn có nhiều nguồn dữ liệu và cần tổng hợp phân tích dữ liệu từ nhiều nguồn đó. Công cụ này cho phép bạn xác định vị trí các dự kiện chuỗi thời gian, mục nhập nhật ký và truy vấn tùy chỉnh, bạn có thể sử dụng ngay lập tức. Bạn có thể xây dựng một bảng điều khiển tổng quan hiển thị việc sử dụng tài nguyên phần cứng, các dòng nhật ký quan trọng và biểu đồ đăng ký người dùng mới trong cơ sở dữ liệu của bạn trên một màn hình. Điều này sẽ cung cấp cho bạn một điểm đến để hướng tới khi bạn cần một bản tóm tắt về mọi thứ đang diễn ra trong tổ chức của mình.
    - Prometheus và Grafana thường được coi là một cặp đôi hoàn hảo trong việc giám sát và trực quan hóa hệ thống. Hai công cụ này hoạt động cùng nhau để cung cấp một giải pháp đáng tin cậy và mạnh mẽ cho việc giám sát và hiển thị dữ liệu.



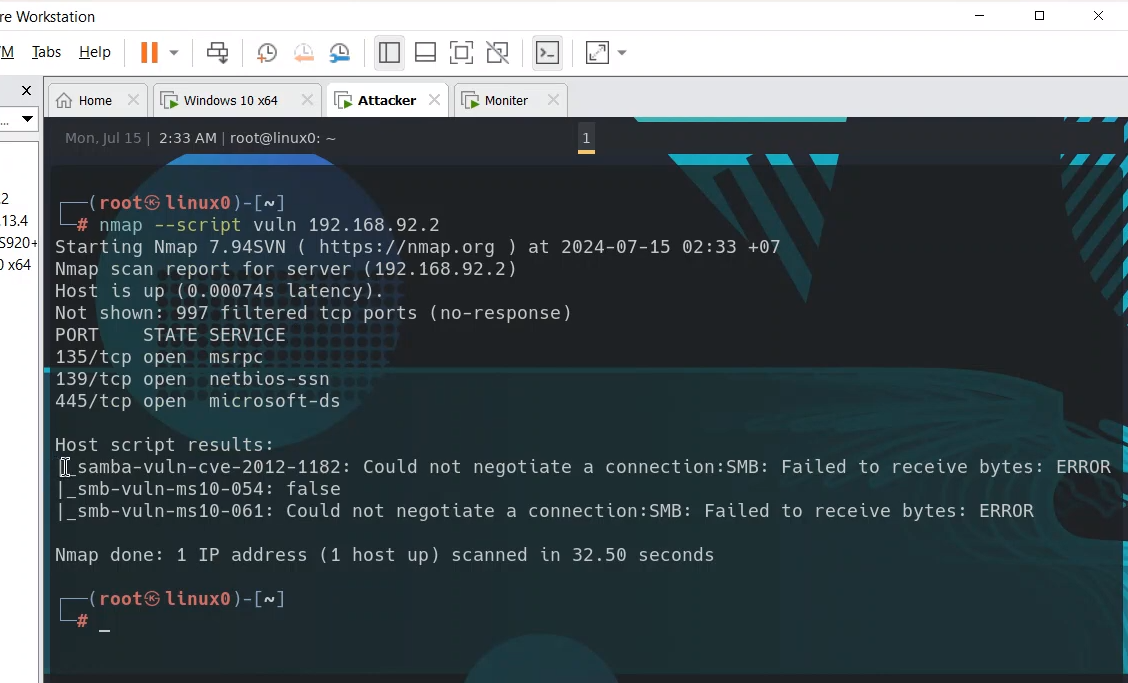
Hình 3.3 - Hệ thống giám sát Prometheus và Grafana

*(Nguồn: intermet)*

##### Demo tiến hành quét lổ hỗng của máy windows 10 19H1 và thực hiện Detect

* Chuẩn bị ba máy:
  + - Máy hệ điều hành windows 10 (sử dụng để Node\_exporter trên windows 10 19H1 để thu thập thông tin về hệ thống và tài nguyên tại máy chủ hoặc các thành phần trong mạng)
    - Một máy hệ điều hành kali linux (Attacker)
    - Một máy hệ điều hành kali linux (Monitor)
* Dùng máy kali để tiến hành quét lổ hỗng của máy windows 10 19h1

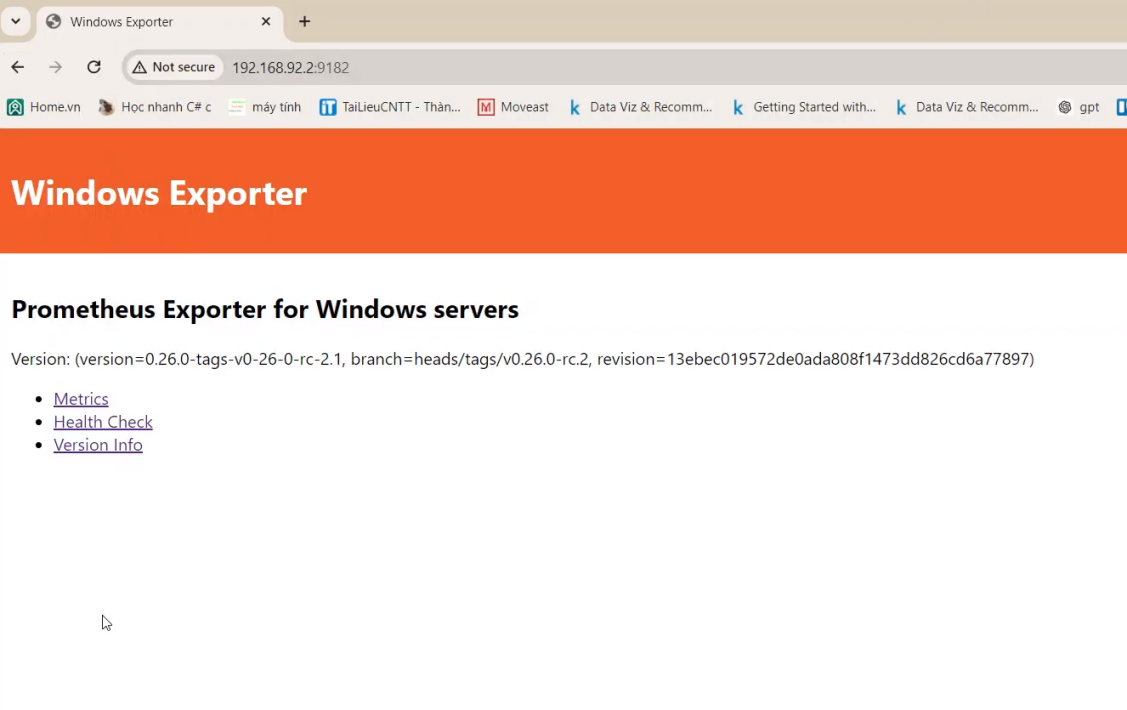
dùng lệnh: **sudo nmap --script vuln 192.168.92.2**



Hình 3.4 - Quét lổ hỗng của máy windows 10 19h1

* Detect: dùng Prometheus + Grafana
  + - Node\_exporter trên windows 10 19H1:

chạy **192.168.92.2:9182**

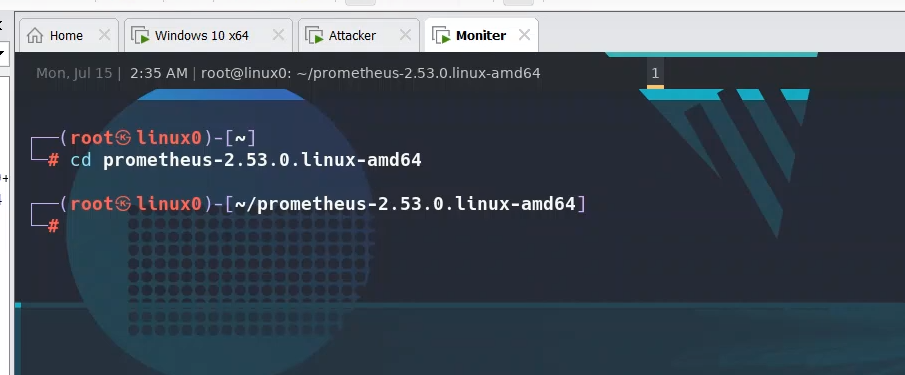


Hình 3.5 - Truy cập Window Exporter



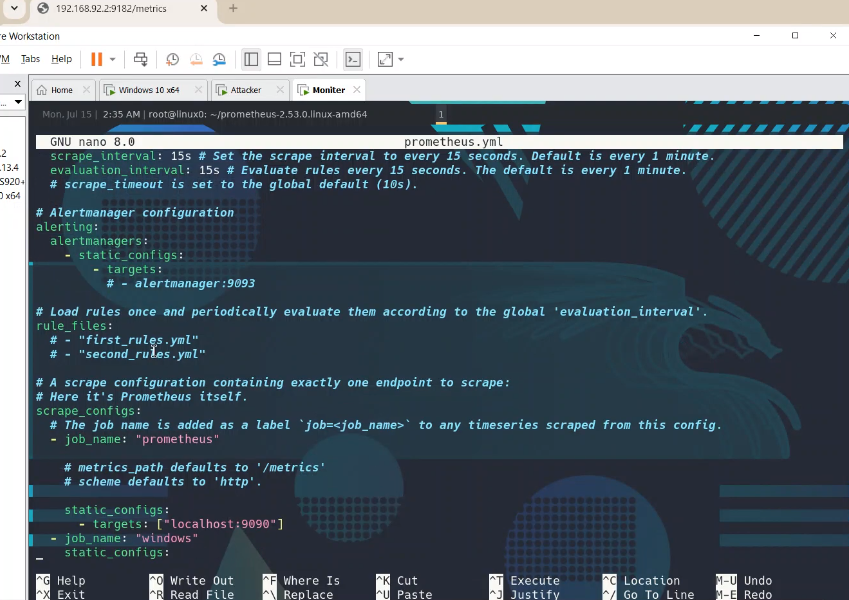
Hình 3.6 - Xem Node\_Exporter

* + - Máy Kali (moniter):
* *Truy cập Prometheus:*



Hình 3.7 - Truy cập Prometheus

* *Cấu hình file prometheus.yml*

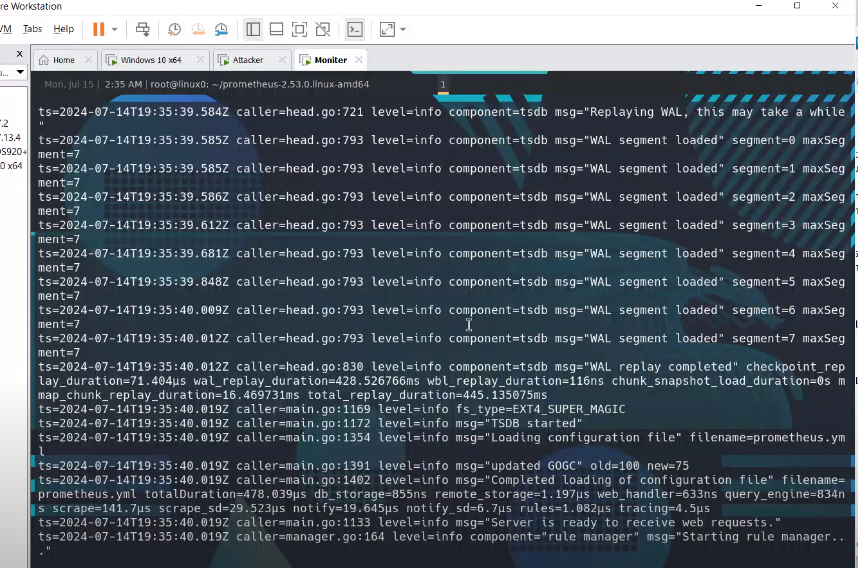


Hình 3.8 - prometheus.yml

* *Chạy prometheus:*

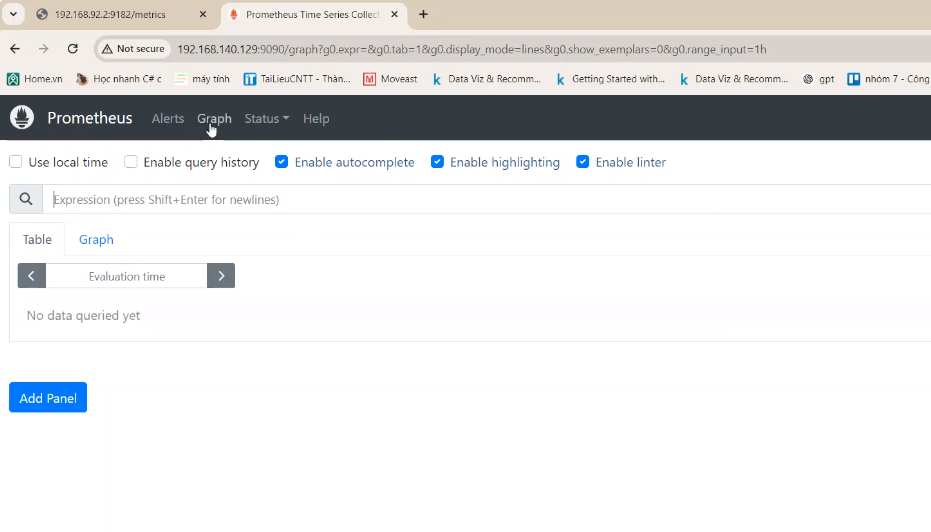
Sau khi đã **cd prometheus-2.53.0.linux-amd64**

**./prometheus**

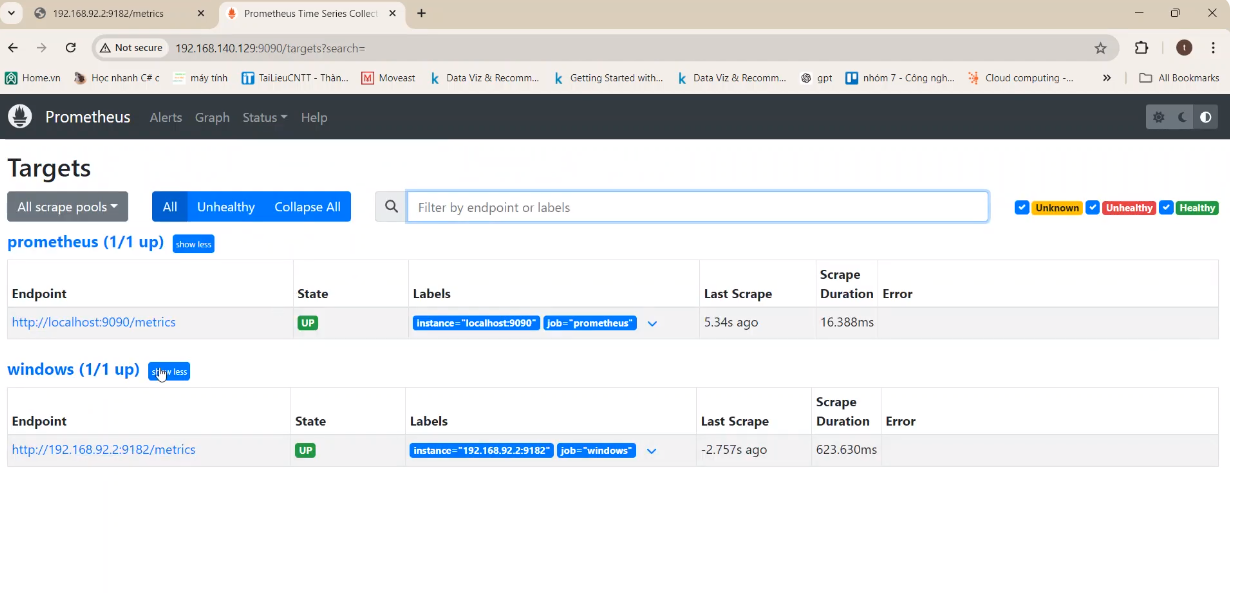


Hình 3.9 - Khởi chạy Prometheus

Truy cập **http://localhost:9090 (192.168.140.129:9090):**



Hình 3.10 - Giao diện web Prometheus

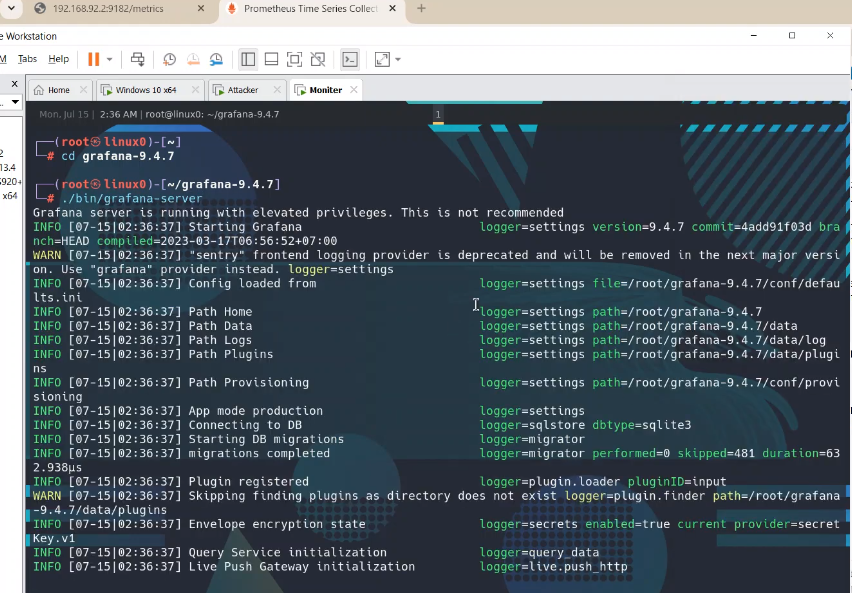


Hình 3.11 - Prometheus/Targets

* *Từ máy monitor, chạy Grafana:*

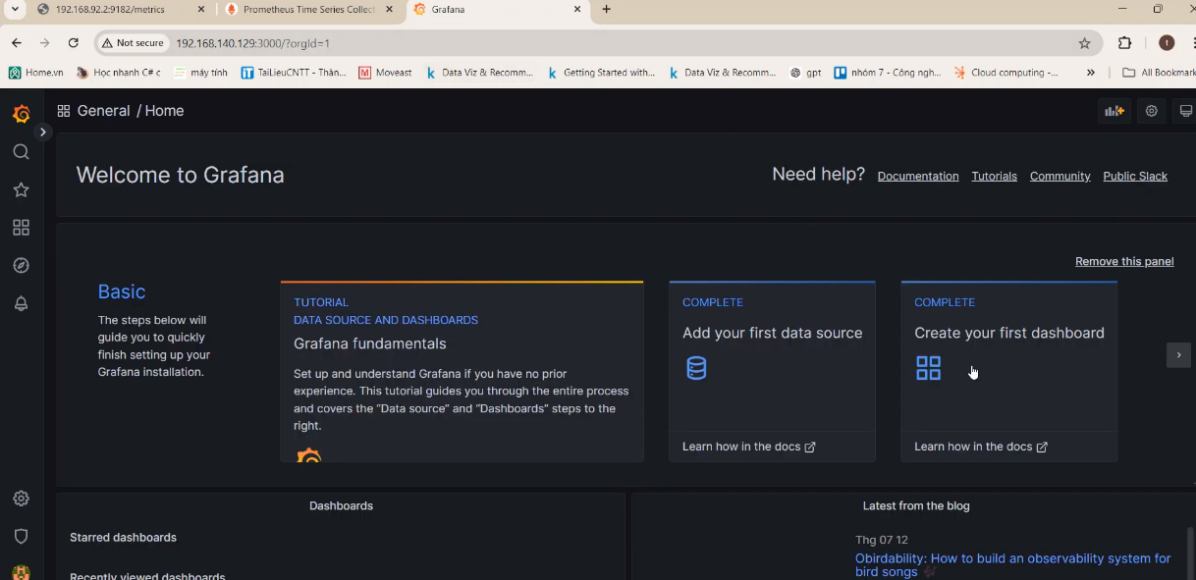
Sau khi đã **cd grafana-9.4.7**

**./bin/grafana-server**



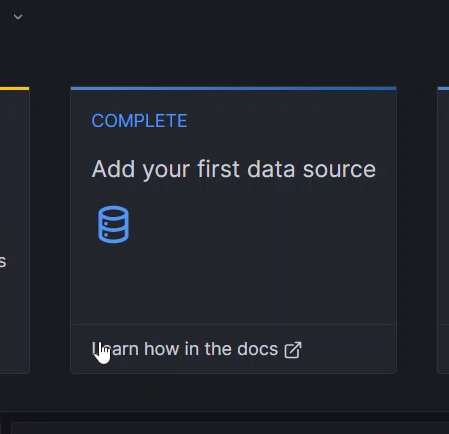
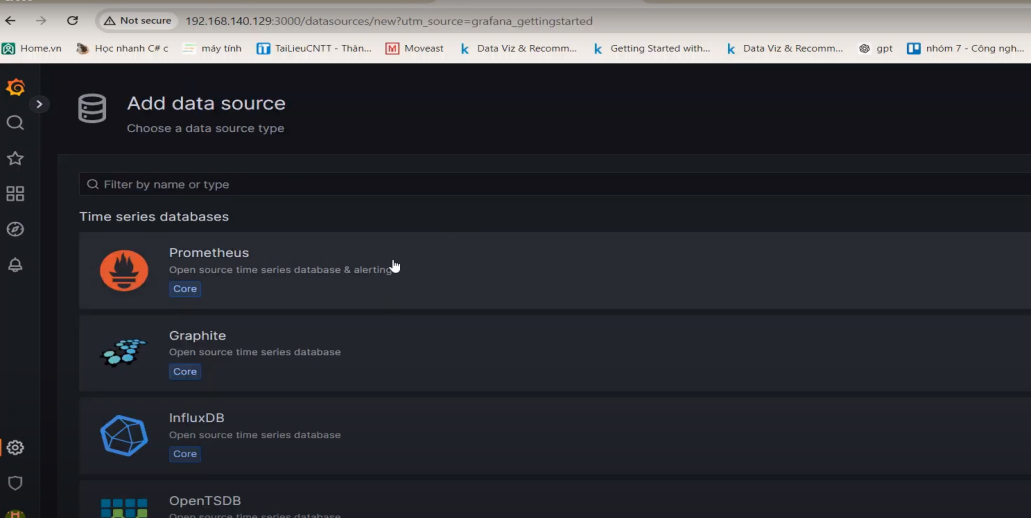
Hình 3.12 - Chạy Grafana server

Truy cập **http://localhost:3000 (192.168.140.129:3000)**

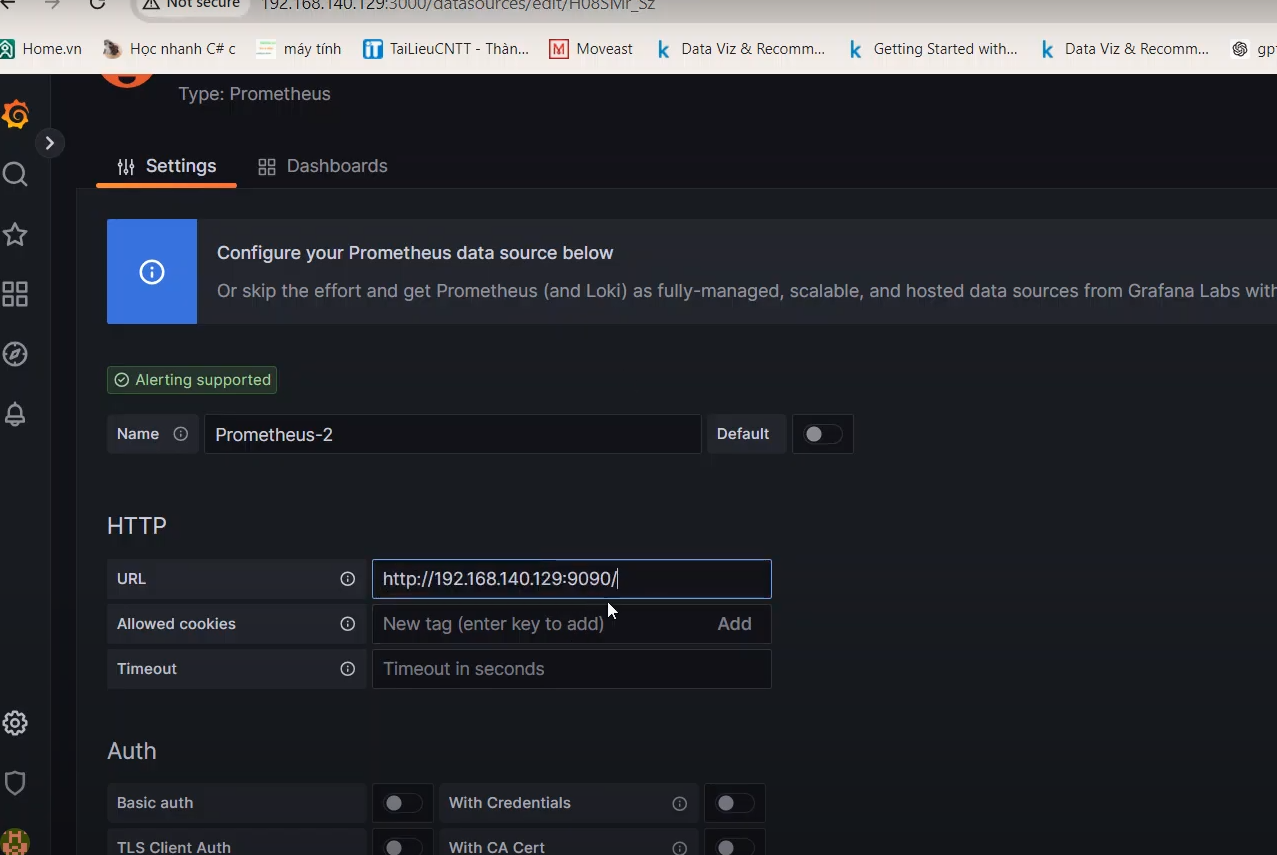


Hình 3.13 - Giao diện web Grafana

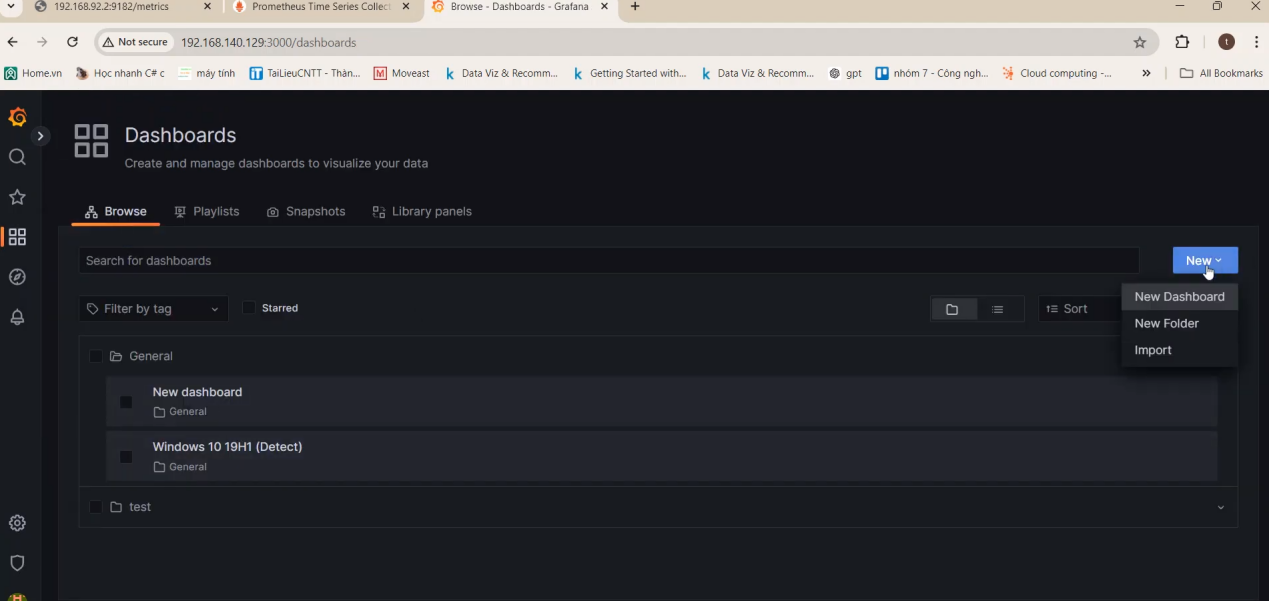
* *Tạo data Sources -> Tạo Dashboards:*



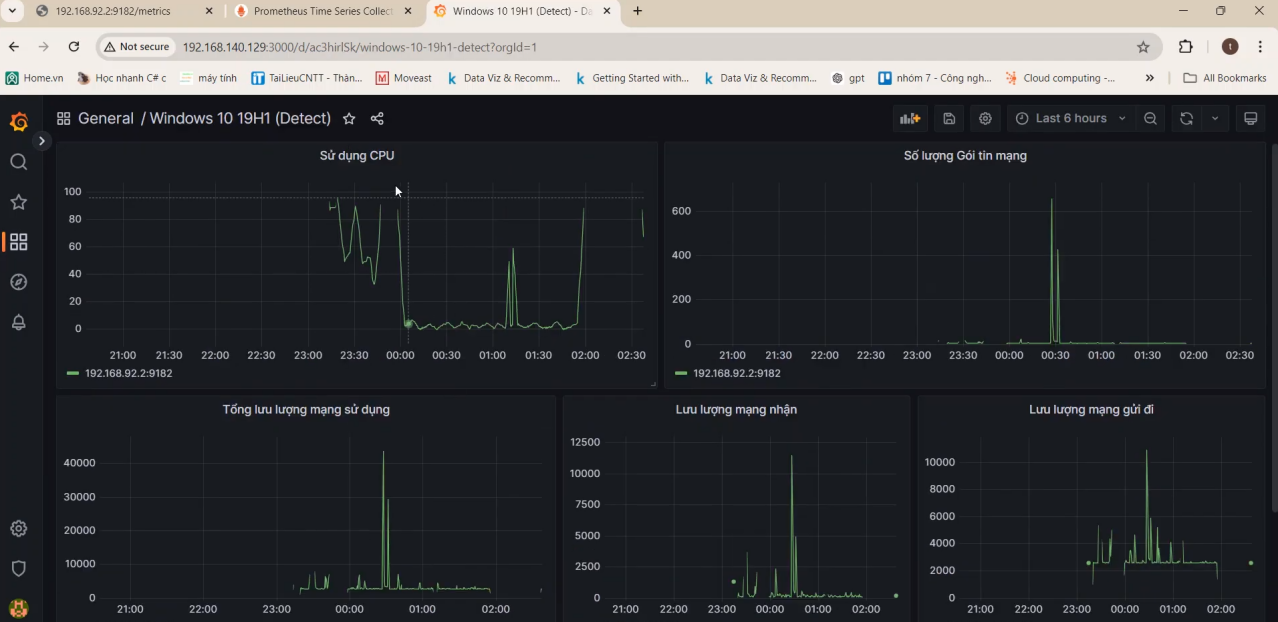
Hình 3.14 - Thêm data sources



Hình 3.15 - Thêm URL



Hình 3.16 - Vào giao diện Dashboards



Hình 3.17 - Windows 10 19H1 Dashboard

##### Các nguyên nhân gây mất thông tin

Nguyên nhân đầu tiên và có lẽ là nguyên nhân cơ bản nhất dẫn tới các sự cố ATTT tăng cao. Thậm chí trong một số trường hợp, Hacker không cần dùng tới công cụ hay phần mềm tấn công nhưng nạn nhân vẫn bị lừa đảo.

Không phân quyền rõ ràng: Một trong những nguyên nhân làm mất thông tin dữ liệu chính là người quản trị không phân quyền rõ ràng cho thành viên. Lợi dụng điều này, nhân viên nội bộ có thể đánh cắp, tráo đổi, thay đổi thông tin của công ty.

Lỗ hổng tồn tại trên thiết bị: Thực tế rằng, nhiều người dùng tải và cài đặt phần mềm mới, ứng dụng mới cho điện thoại, laptop, PC… mà không tự hỏi rằng “Liệu phần mềm này có chứa lỗ hổng hay không”. Trong khi đó, các phần mềm ứng dụng luôn tồn tại những lổ hổng bảo mật và nguy cơ tấn công.

Lỗ hổng trong hệ thống: Hệ thống có thể là hệ thống website, hệ thống mạng, hệ thống các ứng dụng, thiết bị, phần mềm. Nguyên nhân làm mất an toàn thông tin trong trường hợp này là do các đơn vị không thường xuyên rà quét lỗ hổng, đánh giá bảo mật cho hệ thống dẫn tới những nguy cơ thiệt hại về tài chính to lớn.

##### Hậu quả của việc mất an toàn thông tin

Mất an toàn thông tin có thể gây ra những hậu quả nghiêm trọng cho cá nhân, tổ chức và xã hội. Khi thông tin cá nhân, thông tin nhạy cảm hoặc thông tin tài chính bị tiếp cận trái phép, người dùng sẽ mất quyền riêng tư và có nguy cơ trở thành nạn nhân của việc lừa đảo, gian lận tài chính hoặc mất tiền.

Không bảo mật tốt thông tin cũng gây tổn hại đến danh tiếng và uy tín của cá nhân, tổ chức hoặc doanh nghiệp. Mất danh tiếng có thể dẫn đến mất khách hàng, đối tác và cơ hội kinh doanh. Hơn nữa, việc mất sự tin tưởng và lòng tin từ phía khách hàng, đối tác và cộng đồng cũng là một hậu quả đáng lo ngại.

Đồng thời gây ra các vấn đề pháp lý, như vi phạm quy định về bảo mật thông tin và quyền riêng tư, đồng thời đối mặt với các biện pháp trừng phạt và mất tiền bồi thường.

Ngoài ra, mất an toàn thông tin còn ảnh hưởng đến năng suất và hoạt động của cá nhân, tổ chức hoặc doanh nghiệp, gây gián đoạn và gây thiệt hại kinh tế. Do đó, bảo vệ an toàn thông tin là một yếu tố quan trọng để đảm bảo sự bền vững và thành công trong môi trường kỹ thuật số ngày nay.

##### Một số giải pháp khác

* Đặt mật khẩu mạnh: Đảm bảo rằng các tài khoản trên mạng xã hội, website, ứng dụng của bạn cần đặt mật khẩu mạnh. Mật khẩu nên chứa dấu gạch dưới hoặc @, số, ký tự chữ. Cá nhân nên tránh đặt những mật khẩu dễ như 123456, 123456789, tên + ngày sinh,…
* Mã hóa dữ liệu :Đối với những thông tin quan trọng, mật thiết, chúng ta nên mã hóa trước khi gửi đi.Mục đích của việc mã hóa thông tin là tránh khỏi sự nhòm ngó, tấn công của Hacker.
* Cập nhật phần mềm : Một trong những giải pháp tránh mất thông tin hiệu quả là cài đặt phần mềm. Bạn có thể cài phần mềm diệt virus, phần mềm cảnh báo tấn công, phần mềm giám sát hệ thống..
* Sử dụng mã hóa dữ liệu: Mã hóa dữ liệu giúp bảo vệ thông tin quan trọng khỏi việc truy cập trái phép. Sử dụng các công nghệ mã hóa mạnh mẽ để bảo vệ dữ liệu khi nó được lưu trữ, truyền và xử lý.
* Xây dựng chính sách và quy trình bảo mật: Thiết lập chính sách bảo mật rõ ràng và các quy trình để đảm bảo tuân thủ và thực thi bảo mật thông tin trong tổ chức. Điều này bao gồm việc quản lý quyền truy cập, xử lý thông tin nhạy cảm và phản ứng với các sự cố bảo mật.
* Tắt các kết nối Wifi, Bluetooth, NFC khi không sử dụng: Hãy nhớ sau khi vào mạng, bạn phải tắt các kết nối Wifi, bluetooth, NFC để tránh nguy cơ bị rò rỉ mật khẩu, tài liệu và thông tin cá nhân.
* Cài đặt phần mềm diệt virus : Cài đặt phần mềm chống virus xâm nhập cũng là một giải pháp được các chuyên gia khuyến cáo. Lưu ý, người dùng nên quét virus trước khi tải phần mềm về máy. Một số công cụ online giúp kiểm tra mã độc online như: virus total, 6scan security, sitecheck.
* Kiểm tra và đánh giá định kỳ: Thực hiện kiểm tra bảo mật định kỳ để xác định và khắc phục các lỗ hổng trong hệ thống. Đánh giá môi trường bảo mật và áp dụng các biện pháp cần thiết để nâng cao an toàn thông tin.

### CHƯƠNG 4. KẾT LUẬN VÀ KIẾN NGHỊ

##### Kết quả đạt được

* + - Phân tích và triển khai giải pháp bảo mật thành công trên Window 10 19H1.
    - Nắm bắt được các khái niệm liên quan đế đề tài.
    - Tăng khả năng giao tiếp,làm việc nhóm.

##### Hướng phát triển trong tương lai

Đề tài “Phân tích và triển khai giải pháp an ninh mạng trên Windows 10 cho Công ty GBF Groups” có thể được phát triển theo các hướng sau:

Phân tích chuyên sâu, chi tiết các tính năng bảo mật tích hợp sẵn của Windows 10 19H1, đánh giá hiệu quả và so sánh với các giải pháp bên thứ ba. Nghiên cứu các giải pháp bảo mật mới nổi như AI và ML để ứng dụng vào bảo vệ hệ thống mạng.

Triển khai thực tế: Đầu tiên, lập kế hoạch triển khai chi tiết, bao gồm cài đặt, cấu hình, thử nghiệm và vận hành. Sau đó, triển khai giải pháp trên môi trường thử nghiệm trước khi áp dụng cho hệ thống chính. Theo dõi, giám sát hiệu quả hoạt động và cập nhật, điều chỉnh giải pháp phù hợp với các mối đe dọa mới. Đồng thời, đảm bảo phối hợp chặt chẽ giữa các bộ phận liên quan trong quá trình triển khai và vận hành.

Ngoài ra, đề tài có thể được phát triển theo hướng nghiên cứu giải pháp bảo mật cho các ứng dụng và dịch vụ cụ thể trên Windows 10 19H1.

Với các hướng phát triển này, chúng ta có thể cung cấp giải pháp an ninh mạng toàn diện và hiệu quả cho Windows 10 19H1, giúp bảo vệ hệ thống mạng khỏi các mối đe dọa ngày càng tinh vi.

##### Kiến nghị

* + - Nghiên cứu và phân tích các lỗ hổng bảo mật tiềm ẩn trong Windows 10 19H1: Việc này giúp xác định những điểm yếu trong hệ điều hành và đưa ra các biện pháp khắc phục phù hợp.
    - Đề xuất các giải pháp bảo mật cho các nhóm người dùng cụ thể: Ví dụ như: người dùng doanh nghiệp, người dùng cá nhân, học sinh, sinh viên, v.v.
    - Phát triển các công cụ và phần mềm hỗ trợ việc triển khai và quản lý giải pháp an ninh mạng: Các công cụ này giúp tự động hóa các quy trình, nâng cao hiệu quả và giảm thiểu chi phí vận hành.
    - Nghiên cứu và ứng dụng các tiêu chuẩn an ninh mạng quốc tế: Ví dụ như: ISO 27001, NIST Cybersecurity Framework, v.v.
    - Nâng cao nhận thức và đào tạo người dùng về an ninh mạng: Đây là yếu tố quan trọng để đảm bảo hiệu quả hoạt động của hệ thống an ninh mạng.
    - Chia sẻ kinh nghiệm và giải pháp hay về an ninh mạng cho cộng đồng: Việc này góp phần nâng cao kiến thức và kỹ năng cho mọi người trong việc bảo vệ hệ thống mạng của họ.
    - Đề xuất biện pháp bảo mật và nâng cao an toàn: Dựa trên các kết quả nghiên cứu và phân tích, đề xuất các biện pháp bảo mật và giải pháp tăng cường an toàn cho VLC media player. Điều này có thể bao gồm việc xây dựng các công cụ phát hiện và ngăn chặn tấn công, cải thiện quy trình phản ứng sự cố và đào tạo người dùng

Tài liệu tham khảo

### TÀI LIỆU THAM KHẢO

**Tiếng Việt**

1. Thái Thanh Tùng, Giáo trình Mật mã học và Hệ thống Thông tin an toàn. NXB Thông tin và Truyền thông, 2011.
2. Nguyễn, V. D. (2021). Nghiên cứu phát triển giải pháp dò quét lỗ hổng trong các hệ thống thông tin (Doctoral dissertation).
3. Prometheus - Hệ thống giám sát hệ thống mã nguồn mở https://viblo.asia/p/gioi-thieu-ve-prometheus-cong-cu-monitoring-hieu-qua-Ljy5VYzblra

**Tiếng Anh**

1. Alan G. Konheim, Computer Security and Cryptography. Wiley, 2007
2. W. Stallings and L. Brown, Computer Security: Principles & Practice. Pearson, 20
3. Joseph Migga Kizza, Guide To Computer Network Security, 2020.