TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN &

TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH & ĐIỆN TỬ**



**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**BẢO MẬT VÀ AN TOÀN HỆ THỐNG THÔNG TIN**

**ĐỀ TÀI:**

**TÌM KIẾM LỖ HỔNG BẢO MẬT BẰNG CÔNG CỤ GFI LANGUARD**

Sinh viên thực hiện: **HOÀNG THỊ HẢI VÂN**

**TRẦN NGỌC THIỆN**

**HÀ VIẾT HƯNG**

**LÊ NHẬT XUÂN**

Giảng viên hướng dẫn: TS.Hoàng Hữu Đức

Đà Nẵng, tháng 01 năm 2023

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN &

TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH & ĐIỆN TỬ**



**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**BẢO MẬT VÀ AN TOÀN HỆ THỐNG THÔNG TIN**

**ĐỀ TÀI:**

**TÌM KIẾM LỖ HỔNG BẢO MẬT BẰNG CÔNG CỤ GFI LANGUARD**

Sinh viên thực hiện: **HOÀNG THỊ HẢI VÂN** MSV: **20IT083**

**TRẦN NGỌC THIỆN** MSV: **20IT930**

**HÀ VIẾT HƯNG** MSV: **20IT051**

**LÊ NHẬT XUÂN** MSV: **20IT137**

Giảng viên hướng dẫn: TS.Hoàng Hữu Đức

Đà Nẵng, tháng 01 năm 2023

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

(TS.Hoàng Hữu Đức)

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

***Chữ ký của giảng viên***

LỜI CẢM ƠN

Trong thời gian nghiên cứu với sự giúp đỡ, tạo điều kiện của Trường đại học công nghệ thông tin và truyền thông Việt - Hàn, đặt biệt là sự hướng dẫn trực tiếp, chỉ bảo tận tình của giảng viên bộ môn TS.Hoàng Hữu Đức chúng em đã hoàn thành đề tài cùng với bản báo cáo này.

Với khả năng và thời gian có hạn nên không tránh khỏi những thiếu sót, chúng em rất mong nhận được sự quan tâm, giúp đỡ, tạo điều kiện của thầy cô giáo để chúng em hoàn thành hơn đề tài nghiên cứu trong thởi gian tới.

Để hoàn thành bài báo cáo này, cùng với sự cố gắng, nỗ lực tìm hiểu và nghiên cứu của cả nhóm. Chúng em xin gửi lời cảm ơn đến TS. Hoàng Hữu Đức đã tận tình hướng dẫn và giúp đỡ nhóm em trong thời gian làm bài báo cáo này.

Báo cáo đã hoàn thành nhưng còn nhiều hạn chế và thiếu sót. Chúng em rất mong được sự góp ý của thầy và các bạn!

***Sinh viên,***

MỤC LỤC

[DANH MỤC HÌNH ẢNH 7](#_Toc133528906)

[DANH MỤC CÁC TỪ VIẾT TẮT 9](#_Toc133528907)

[MỞ ĐẦU 10](#_Toc133528908)

[Chương 1 TỔNG QUAN VỀ BẢO MẬT MẠNG 11](#_Toc133528909)

[1.1. Bảo mật mạng 11](#_Toc133528910)

[1.2. Các loại lỗ hổng bảo mật 12](#_Toc133528911)

[1.2.1. Lỗ hổng theo khu vực phát sinh 12](#_Toc133528912)

[1.2.2. Lỗ hổng phát sinh do các khiếm khuyết của hệ thống thông tin 13](#_Toc133528913)

[1.2.3. Lỗ hổng theo vị trí phát hiện 13](#_Toc133528914)

[1.2.4. Lỗ hổng đã biết, lỗ hổng zero-day 14](#_Toc133528915)

[1.3. Một số phương thức tấn công mạng 15](#_Toc133528916)

[1.3.1. Tấn công vào trình duyệt (Browse Attacks) 15](#_Toc133528917)

[1.3.2. Tấn công bằng phần mềm độc hại 16](#_Toc133528918)

[1.3.3. Tấn công từ chối dịch vụ 16](#_Toc133528919)

[1.3.4. Kiểu tấn công sâu bọ (Worm Attacks) 17](#_Toc133528920)

[1.3.5. Tấn công cơ sở dữ liệu (SQL injection) 18](#_Toc133528921)

[1.3.6. Kiểu tấn công rà quét 18](#_Toc133528922)

[1.3.7. Kiểu tấn công mạng khác 18](#_Toc133528923)

[1.4. Các giải pháp và công cụ hỗ trợ bảo mật mạng 18](#_Toc133528924)

[1.4.1. Các giải pháp bảo mật mạng 19](#_Toc133528925)

[1.4.2. Các công cụ hỗ trợ bảo mật mạng 21](#_Toc133528926)

[Chương 2 TÌM KIẾM VÀ PHÂN TÍCH LỖ HỔNG BẢO MẬT VỚI GFI LANGUARD 26](#_Toc133528927)

[2.1. Giới thiệu phần mềm GFI Languard 26](#_Toc133528928)

[2.2. Cài đặt GFI Languard 27](#_Toc133528929)

[2.2.1. Một số lưu ý trước khi cài đặt 27](#_Toc133528930)

[2.2.2. Tiến hành tải xuống và cài đặt 27](#_Toc133528931)

[Chương 3 TRIỂN KHAI THỰC NGHIỆM 33](#_Toc133528932)

[3.1. Một số chức năng chính trong GFI LanGuard 33](#_Toc133528933)

[3.1.1. View Dashboard 33](#_Toc133528934)

[3.1.2. Remediate Security Issues 33](#_Toc133528935)

[3.1.3. Launch a Scan 34](#_Toc133528936)

[3.2. Tiến hành Scanning trên các máy 35](#_Toc133528937)

[KẾT LUẬN 38](#_Toc133528938)

[TÀI LIỆU THAM KHẢO 39](#_Toc133528939)

# **DANH MỤC HÌNH ẢNH**

[Hình 1-1 Bảo mật mạng 11](#_Toc133527511)

[Hình 1-2 Trình duyệt web bị tấn công 15](#_Toc133527512)

[Hình 1-3 Tấn công bằng phần mềm độc hại (malware) 15](#_Toc133527513)

[Hình 1-4 Tấn công từ chối dịch vụ DoS 16](#_Toc133527514)

[Hình 1-5 Tấn công cơ sở dữ liệu SQL injection 17](#_Toc133527515)

[Hình 1-6 Giải pháp tường lửa 18](#_Toc133527516)

[Hình 1-7 Mô hình tấn công từ chối dịch vụ DDoS 19](#_Toc133527517)

[Hình 1-8 Giải pháp mã hóa và bảo mật đường truyền 19](#_Toc133527518)

[Hình 1-9 Công cụ Nmap 21](#_Toc133527519)

[Hình 1-10 Giao diện công cụ wireshark 21](#_Toc133527520)

[Hình 1-11 Giao diện công cụ Nessus 22](#_Toc133527521)

[Hình 1-12 Giao diện công cụ OpenVAS 23](#_Toc133527522)

[Hình 1-13 Giao diện công cụ GFI LanGuard 23](#_Toc133527523)

[Hình 1-14 Giao diện công cụ Kerio Control 24](#_Toc133527524)

[Hình 2-1 Xem mạng và xem nơi các mối đe dọa xâm nhập 25](#_Toc133528003)

[Hình 2-2 Tìm những lỗ hổng mà các mối đe dọa có thể khai thác 26](#_Toc133528004)

[Hình 2-3 Khởi chạy trình cài đặt GFI LanGuard 27](#_Toc133528005)

[Hình 2-4 Cài đặt ngôn ngữ cho GFI LanGuard 27](#_Toc133528006)

[Hình 2-5 Chọn tải xuống và cài đặt thành phần 28](#_Toc133528007)

[Hình 2-6 Cửa sổ cài đặt Database 29](#_Toc133528008)

[Hình 2-7 Nhập tài khoản người dùng hoặc License key 29](#_Toc133528009)

[Hình 2-8 Cửa sổ chào mừng của GFI LanGuard 30](#_Toc133528010)

[Hình 2-9 Điền thông tin Administrator user account 30](#_Toc133528011)

[Hình 2-10 Chọn nơi cài đặt GFI LanGuard Central Management Server 31](#_Toc133528012)

[Hình 2-11 Hoàn tất quá trình cài đặt GFI LanGuard 31](#_Toc133528013)

[Hình 2-13 Tap View Dashboard trong công cụ GFI LanGuard 32](#_Toc133528014)

[Hình 3-1 Giao diện công cụ GFI LanGuard sau khi đã cài đặt thành công 32](#_Toc133528027)

[Hình 3-2 Tab Remediate Security Issues trong GFI LanGuard 33](#_Toc133528028)

[Hình 3-3 Launch a Scan trên GFI LanGuard 34](#_Toc133528029)

[Hình 3-4 Chọn scanning máy localhost 34](#_Toc133528030)

[Hình 3-5 Quá trình Scanning đang diễn ra 35](#_Toc133528031)

[Hình 3-6 Cửa sổ Results Overview 35](#_Toc133528032)

[Hình 3-7 Cửa sổ Scanner Activity Window 36](#_Toc133528033)

[Hình 3-8 Cửa sổ Scan Results Details hiển thị kết quả sau khi quét xong 36](#_Toc133528034)

# **DANH MỤC CÁC TỪ VIẾT TẮT**

# **MỞ ĐẦU**

# **TỔNG QUAN VỀ BẢO MẬT MẠNG**

* 1. **Bảo mật mạng**

Bảo mật mạng là sự bảo vệ hệ thống mạng nhằm tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính toàn vẹn, tính bảo mật của một thông tin tổ chức, doanh nghiệp. Theo như tiêu chuẩn của Liên minh Viện thông tin Quốc tế (ITU) thì là “Bảo mật mạng là tập hợp các công cụ, chính sách, khái niệm về bảo mật, hướng dẫn, phương pháp quản lý rủi ro, phản ứng, đào tạo, diễn tập, thiết bị và công nghệ có thể được dùng để bảo vệ hệ thống mạng và tài sản "



Hình 1-1 Bảo mật mạng

Vấn đề an toàn và bảo mật thông tin phải đảm bảo những yếu tố chủ yếu sau:

* Tính bảo mật: chỉ cho phép những người có quyền hạn được truy cập đến nó.
* Tính toàn vẹn dữ liệu: dữ liệu không bị sửa đổi, bị xóa một cách bất hợp pháp.
* Tính sẵn sàng: bất cứ khi nào chúng ta cần thì dữ liệu luôn sẵn sàng.
  1. **Các loại lỗ hổng bảo mật**

Lỗ hổng của hệ thống thông tin rất đa dạng và có thể do nhiều nguyên nhân khác nhau, có thể phát sinh từ những yếu tố về kỹ thuật, cũng có thể do các yếu tố về tổ chức và quản lý như: thiếu kinh nghiệm hoặc khiếm khuyết trong các biện pháp bảo vệ thông tin. Do vậy, có khá nhiều phương pháp phân loại lỗ hổng của hệ thống thông tin.

Lỗ hổng an toàn thông tin của hệ thống thông tin được chia thành ba loại:

* Lỗ hổng khách quan là lỗ hổng xuất phát từ các đặc tính kỹ thuật vốn có của thiết bị và phần mềm của hệ thống thông tin.
* Lỗ hổng chủ quan là lỗ hổng xuất phát từ hành vi của chủ thể, có thể là nhà thiết kế, các quản trị viên và người sử dụng.
* Lỗ hổng ngẫu nhiên là lỗ hổng xuất phát từ môi trường của hệ thống thông tin và những bối cảnh không dự đoán trước được.

Lỗ hổng an toàn thông tin được phân loại theo các giai đoạn trong vòng đời của hệ thống thông tin , bao gồm: lỗ hổng thiết kế, lỗ hổng chế tạo và lỗ hổng khai thác

* + 1. **Lỗ hổng theo khu vực phát sinh**

Lỗ hổng theo khu vực phát sinh bao gồm:

* ***Lỗ hổng code*** xuất hiện do lỗi trong quá trình xây dựng phần mềm, gồm các lỗi logic, cú pháp và ở các mức truy cập. Lỗ hổng code còn bao gồm cả những cài đặt cố ý của nhà thiết kế để tiếp cận trái phép vào hệ thống của người dùng phần mềm.
* ***Lỗ hổng cấu hình*** xuất hiện trong quá trình cài đặt, cấu hình và các phương tiện kỹ thuật của hệ thống thông tin , như các tham số cài đặt và thông số kỹ thuật của các thiết bị kỹ thuật.
* ***Lỗ hổng kiến trúc*** phát sinh trong quá trình thiết kế hệ thống thông tin
* ***Lỗ hổng tổ chức*** tồn tại do thiếu (hoặc do các khiếm khuyết) của các biện pháp tổ chức bảo vệ thông tin trong các hệ thống thông tin , hoặc do không tuân thủ các quy tắc khai thác hệ thống bảo vệ thông tin của hệ thống thông tin.
  + 1. **Lỗ hổng phát sinh do các khiếm khuyết của hệ thống thông tin**

Trong hệ thống thông tin tồn tại những khiếm khuyết sẽ làm xuất hiện nhiều lỗ hổng. Ví dụ: những khiếm khuyết dẫn đến rò rỉ, hoặc lộ thông thông tin tiếp cận hạn chế; khiếm khuyết liên quan đến tràn bộ nhớ (khi phần mềm thực hiện các bản ghi dữ liệu vượt ra ngoài giới hạn của bộ nhớ vùng đệm, kết quả là dữ liệu được ghi phía trước hoặc tiếp sau bộ đệm bị hư hại). Các khiếm khuyết của hệ thống thông tin làm phát sinh lỗ hổng an toàn thông tin thường liên quan đến các vấn đề như: cài đặt sai tham số trong đảm bảo chương trình, kiểm tra không đầy đủ dữ liệu đầu vào, khả năng giám sát đường tiếp cận các thư mục, phân quyền sử dụng các lệnh của hệ điều hành (ví dụ, lệnh xem cấu trúc thư mục, lệnh sao chép, lệnh loại bỏ tệp từ xa); áp dụng các toán tử tích hợp ngôn ngữ lập trình, sử dụng mã lệnh, rò rỉ thông tin tiếp cận hạn chế, sử dụng các biến đổi mật mã, quản lý tài nguyên, tràn bộ nhớ.

* + 1. **Lỗ hổng theo vị trí phát hiện**

Lỗ hổng trong đảm bảo chương trình toàn hệ thống: lỗ hổng hệ điều hành (lỗ hổng hệ thống tệp, lỗ hổng chế độ tải, lỗ hổng trong các cơ chế quản lý quy trình…), lỗ hổng hệ thống quản lý cơ sở dữ liệu.

Lỗ hổng trong phần mềm ứng dụng.

Lỗ hổng trong phần mềm chuyên dùng, tức là các lỗ hổng đảm bảo chương trình dùng để giải quyết các bài toán đặc thù của hệ thống thông tin, cụ thể là: lỗi lập trình, sự có mặt các chức năng không công bố có khả năng ảnh hưởng lên các phương tiện bảo vệ thông tin, khiếm khuyết trong các cơ chế hạn chế tiếp cận cho đến các đối tượng đảm bảo chương trình chuyên dùng.

Lỗ hổng tồn tại trong đảm bảo chương trình của các phương tiện kỹ thuật như: phần sụn các thiết bị nhớ, các mạch logic tích hợp, các hệ thống đầu vào/ra, chương trình trong các bộ điều khiển, giao diện….

Lỗ hổng trong các thiết bị cầm tay như: hệ điều hành các thiết bị di động, giao diện truy cập không dây....

Lỗ hổng trong các thiết bị mạng như: bộ định tuyến, tổng đài, các trang bị viễn thông khác như: giao thức dịch vụ mạng, giao thức điều khiển thiết bị viễn thông....

Lỗ hổng trong các thiết bị bảo vệ thông tin. Bao gồm lỗ hổng trong các phương tiện quản lý truy cập (kiểm soát tính toàn vẹn, phần mềm chống mã độc, hệ thống phát hiện xâm nhập, tường lửa…).

Bên cạnh đó, GOST P56546-2-15 còn phân loại lỗ hổng dựa trên các tiêu chí tìm kiếm như: tên của hệ điều hành, nền tảng phát triển, tên phần mềm và phiên bản, mức độ nguy hại của lỗ hổng, ngôn ngữ lập trình và dịch vụ sử dụng để vận hành phần mềm.

* + 1. **Lỗ hổng đã biết, lỗ hổng zero-day**

Với những kẻ tấn công, lỗ hổng là những kênh chính để xâm nhập trái phép vào hệ thống thông tin . Do đó, tìm kiếm lỗ hổng luôn là mối quan tâm hàng đầu. Khi phát hiện được lỗ hổng, kẻ tấn công lập tức tận dụng cơ hội để khai thác. Từ thời điểm phát hiện ra lỗ hổng đến lần vá đầu tiên sẽ mất một khoảng thời gian dài và đây chính là cơ hội để thực hiện lây nhiễm, phát tán mã độc. Còn với các chuyên gia bảo mật thông tin, phát hiện và khắc phục lỗ hổng là nhiệm vụ quan trọng hàng đầu. Việc phát hiện lỗ hổng đã khó khăn, nhưng khắc phục còn khó khăn hơn. Do vậy, để thuận tiện trong quá trình khắc phục, các chuyên gia đã chia lỗ hổng thành hai loại là lỗ hổng đã biết và lỗ hổng zero-day.

Lỗ hổng đã biết, là lỗ hổng đã được công bố, kèm theo các biện pháp thích hợp để bảo vệ hệ thống thông tin , các bản vá lỗi và bản cập nhật. Như vậy, mỗi khi lỗ hổng được phát hiện thuộc loại này, thì vấn đề cũng coi như đã được giải quyết.

Tuy nhiên, có những lỗ hổng mà chỉ đến thời điểm phát hành bản cập nhật, hoặc phiên bản mới của sản phẩm, nhà sản xuất mới biết về sự tồn tại của nó. Nhà sản xuất không đủ thời gian để nghiên cứu và khắc phục sản phẩm đã phát hành, nên các lỗ hổng loại này được đặt tên là lỗ hổng zero-day. Như vậy, trong suốt thời gian kể từ thời điểm tồn tại đến khi bị phát hiện, lỗ hổng này có thể đã được khai thác trong thực tế và gây ảnh hưởng tới tổ chức, doanh nghiệp, người dùng.

Lỗ hổng zero-day thường tồn tại trong thời gian dài, trung bình khoảng 300 ngày. Một số có “tuổi thọ” cao hơn rất nhiều. Hãng SAP đã công bố rằng, họ từng phát hiện và vá được các lỗ hổng có tuổi thọ 10 năm. Trong đó, nguy hiểm nhất là các lỗ hổng: CVE-2004-308 (làm tổn hại bộ nhớ), CVE-2005- 2974 (gây tấn công từ chối dịch vụ) và CVE-2005-3550 (cho phép thực hiện lệnh từ xa).

Ngoài các hãng bảo mật, “hacker” cũng có thể là những người đầu tiên phát hiện ra lỗ hổng. Với các “hacker mũ trắng” thì các lỗ hổng zero-day là đối tượng nghiên cứu hấp dẫn, nếu phát hiện và khắc phục được, họ cũng sẵn sàng thông báo cho nhà sản xuất. Nhưng với các “hacker mũ đen” thì đây là cơ hội tốt để trục lợi. Họ sẽ nghiên cứu phương án khai thác ngay lập tức, thậm chí đưa ra rao bán tại chợ đen với giá cao. Chẳng hạn, lỗ hổng zero-day cho phép chiếm quyền quản trị trên hệ điều hành Windows được rao bán với giá 90 nghìn USD. Tội phạm mạng hay các cơ quan đặc vụ sẵn sàng chi trả khoản tiền lớn để mua lại các lỗ hổng này, tạo nên thị trường chợ đen sôi động trên mạng Internet.

Vì thế, nhiều hãng bảo mật sẵn sàng chi những khoản tiền lớn để trả cho những ai phát hiện được lỗ hổng trong các sản phẩm của họ. Gần đây, Kaspersky Lab đã tăng tiền thưởng lên 100 nghìn USD cho người có thể phát hiện ra những lỗ hổng nghiêm trọng trong các sản phẩm của hãng này.

* 1. **Một số phương thức tấn công mạng**

Tấn công mạng hay còn gọi là chiến tranh trên không gian mạng. Có thể hiểu tấn công mạng là hình thức tấn công xâm nhập vào một hệ thống mạng máy tính, cơ sở dữ liệu, hạ tầng mạng, website, thiết bị của một cá nhân hoặc một tổ chức nào đó.

Cụm từ “Tấn công mạng” có 2 nghĩa hiểu:

* Hiểu theo cách tích cực (positive way): Tấn công mạng (penetration testing) là phương pháp Hacker mũ trắng xâm nhập vào một hệ thống mạng, thiết bị, website để tìm ra những lỗ hổng, các nguy cơ tấn công nhằm bảo vệ cá nhân hoặc tổ chức.
* Hiểu theo cách tiêu cực (negative way): Tấn công mạng (network attack) là hình thức, kỹ thuật Hacker mũ đen tấn công vào một hệ thống để thay đổi đối tượng hoặc tống tiền.

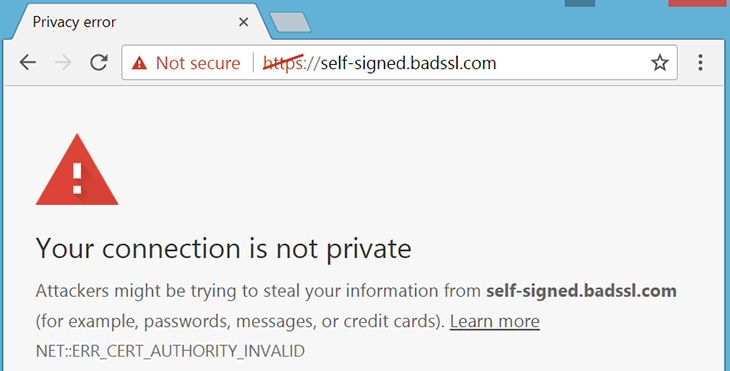
Đối tượng bị tấn công có thể là cá nhân, doanh nghiệp, tổ chức hoặc nhà nước. Hacker sẽ tiếp cận thông qua mạng nội bộ gồm máy tính, thiết bị, con người). Trong yếu tố con người, hacker có thể tiếp cận thông qua thiết bị mobile, mạng xã hội, ứng dụng phần mềm.

Tóm lại, một cuộc tấn công không gian mạng có thể nhằm vào cá nhân, doanh nghiệp, quốc gia, xâm nhập vào trong hệ thống, cơ sở hạ tầng mạng, thiết bị, con người dưới nhiều các khác nhau và mục tiêu khác nhau.

* + 1. **Tấn công vào trình duyệt (Browse Attacks)**

Một trong các kiểu tấn công mạng điển hình nhất năm 2017 phải kể đến là tấn công vào trình duyệt. Các cuộc tấn công của trình duyệt thường được bắt đầu bằng những trang web hợp pháp nhưng dễ bị tổn thương. Kẻ tấn công có thể xâm nhập vào website và gây hại cho đối tượng bằng phần mềm độc hại.

Cụ thể, khi có khách truy cập mới thông qua trình duyệt web, trang web đó sẽ lập tức bị nhiễm mã độc. Từ đó, mã độc sẽ xâm nhập vào hệ thống của nạn nhân qua lỗ hổng của trình duyệt.Các trình duyệt web bị tin tặc tấn công chủ yếu năm 2017 là Microsoft Internet Explorer Edge, Google Chrome, Mozilla, Firefox, Apple Safari, Opera.

****

Hình 1-2 Trình duyệt web bị tấn công

* + 1. **Tấn công bằng phần mềm độc hại**

Tấn công Malware là hình thức phổ biến nhất. Malware bao gồm spyware ( phần mềm gián điệp ), ransomware ( mã độc tống tiền ), virus và worm (phần mềm độc hại có khả năng lây lan nhanh). Thông thường, tin tặc sẽ tấn công người dùng thông qua các lỗ hổng bảo mật, cũng có thể là dụ dỗ người dùng click vào một đường link hoặc email để phần mềm độc hại tự động cài đặt vào máy tính. Một khi được cài đặt thành công, malware sẽ gây ra:

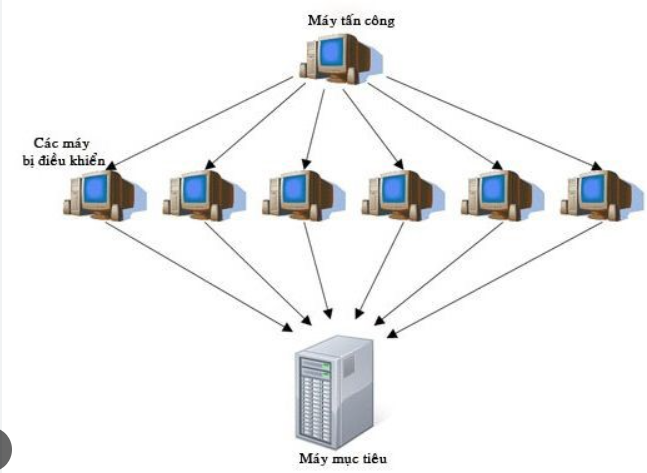
* Ngăn cản người dùng truy cập vào một file hoặc folder quan trọng (ransomware)
* Cài đặt thêm những phần mềm độc hại khác
* Lén lút theo dõi người dùng và đánh cắp dữ liệu (spyware)
* Làm hư hại phần mềm, phần cứng, làm gián đoạn hệ thống.

****

Hình 1-3 Tấn công bằng phần mềm độc hại (malware)

* + 1. **Tấn công từ chối dịch vụ**

DoS (Denial of Service) là hình thức tấn công mà tin tặc “đánh sập tạm thời” một hệ thống, máy chủ, hoặc mạng nội bộ. Để thực hiện được điều này, chúng thường tạo ra một lượng traffic/request khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải, từ đó người dùng không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.



Hình 1-4 Tấn công từ chối dịch vụ DoS

Một hình thức biến thể của DoS là DDoS (Distributed Denial of Service): tin tặc sử dụng một mạng lưới các máy tính (botnet) để tấn công nạn nhân. Điều nguy hiểm là chính các máy tính thuộc mạng lưới botnet cũng không biết bản thân đang bị lợi dụng để làm công cụ tấn công.

* + 1. **Kiểu tấn công sâu bọ (Worm Attacks)**

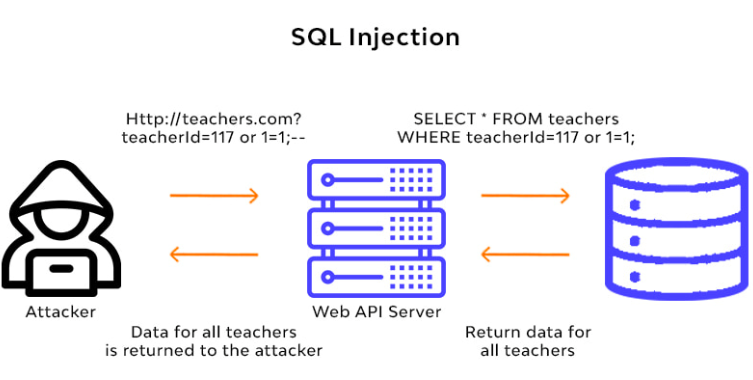
Worm là những chương trình có khả năng tự động khai thác, tấn công vào điểm đầu cuối hoặc những lỗ hổng đã có sẵn. Sau khi đã tận dụng các lỗ hổng thành công trong hệ thống, Worm sẽ tự động sao chép chương trình từ máy bị nhiễm rồi lây lan sang các máy khác.

Kiểu tấn công mạng Worm Attack thường yêu cầu người dùng tương tác trước để bắt đầu lây nhiễm. Worm Attacks thường được tấn công thông qua tệp tải xuống chứa email độc hại, usb, đầu lọc thẻ.

Một trong ví dụ tiêu biểu của phương thức tấn công này là mã độc WannaCry đã lây nhiễm hơn 300.000 máy tính chỉ sau một vài ngày. WannaCry nhắm vào mục tiêu lỗ hổng trên Windows, một khi máy bị nhiễm, phần mềm độc hại sẽ tự động quét hệ thống mạng kết nối với nhau, từ đó lây nhiễm sang các máy tính khác.

* + 1. **Tấn công cơ sở dữ liệu (SQL injection)**

Các cuộc tấn công SQL Injection được thực hiện bằng cách gửi lệnh SQL độc hại đến các máy chủ cơ sở dữ liệu thông qua các yêu cầu của người dùng mà website cho phép. Bất kỳ kênh input nào cũng có thể được sử dụng để gửi các lệnh độc hại, bao gồm các thẻ, chuỗi truy vấn (query strings), cookie và tệp tin.



Hình 1-5 Tấn công cơ sở dữ liệu SQL injection

Với SQL injection các hacker có thể truy cập một phần hoặc toàn bộ dữ liệu trong hệ thống, có thể gây ra những thiệt hại khổng lồ

Với việc SQL injection dễ tấn công, phổ biến, gây ra hậu quả nghiêm trọng. Đó là lý do mà SQL injection đứng đầu **trong 10 lỗ hổng bảo mật của OWASP**

* + 1. **Kiểu tấn công rà quét**

Thay vì sử dụng các hình thức tấn công toàn diện, Scan Attacks là kỹ thuật tấn công mạng rà quét lỗ hổng thông qua các dịch vụ, hệ thống máy tính, thiết bị, hạ tầng mạng của doanh nghiệp. Tin tặc sẽ sử dụng các công cụ để rà quét, nghe lén hệ thống mạng để tìm ra lỗ hổng sau đó thực thi tấn công.

* + 1. **Kiểu tấn công mạng khác**

Ngoài 6 kiểu tấn công mạng nổi bật nói trên, Hacker còn có thể xâm nhập vào bên trong hệ thống bằng cách:

* Tấn công vật lý (Physical Attacks). Tin tặc sẽ cố gắng phá hủy, ăn cắp dữ liệu kiến trúc trong cùng một hệ thống mạng.
* Tấn công nội bộ (Insider Attacks). Các cuộc tấn công nội bộ thường liên quan tới người trong cuộc. Chẳng hạn như trong một công ty, một nhân viên nào đó “căm ghét” người khác… các cuộc tấn công hệ thống mạng nội bộ có thể gây hại hoặc vô hại. Khi có tấn công mạng nội bộ xảy ra, thông tin dữ liệu của công ty có thể bị truy cập trái phép, thay đổi hoặc bán đổi.
  1. **Các giải pháp và công cụ hỗ trợ bảo mật mạng**

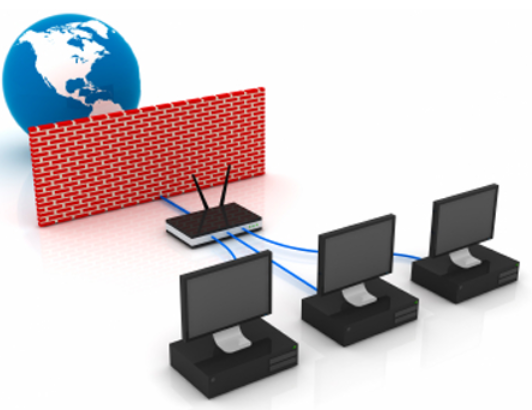
Với việc Internet và con người đang gần nhau, việc mà mỗi tổ chức, cá nhân cần làm là cần có những giải pháp và những công cụ để đảm bảo an toàn cho việc bảo mật thông tin. Sau đây sẽ là những giải pháp và một số công cụ hữu ích

* + 1. **Các giải pháp bảo mật mạng**

Trong thời đại ngày nay có rất nhiều phương pháp bảo mật an ninh mạng. Nhiều công ty lớn đã đưa ra nhưng giải pháp, công cụ, … để có thể bảo mật thông tin, chống đánh cắp dữ liệu, xâm nhập tài nguyên mạng, …

Dưới đây là nhưng giải pháp có chất lượng uy tín hàng đầu, được các chuyên gia trên toàn thế giới khuyên dùng

* + - 1. **Giải pháp tường lửa**

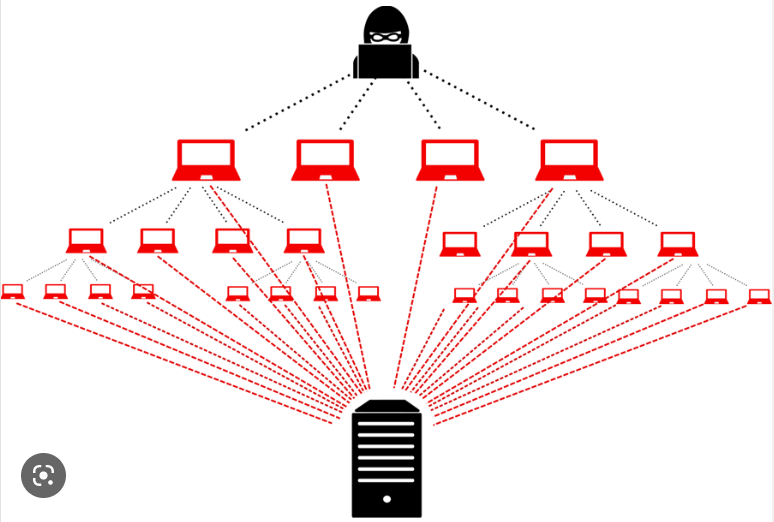


Hình 1-6 Giải pháp tường lửa

Lợi ích: bảo vệ cổng hệ thống (gateway), ngăn chặn các rủi ro từ môi trường internet

Tính năng:

* Lọc web
* Chống xâm nhập (IPS)
* Chống DDoS
* Chống virus, spam
* Lọc các cổng dịch vụ
* Giám sát ứng dụng và người dùng
  + - 1. **Giải pháp chống xâm nhập và chống tấn công từ chối dịch vụ**

****

Hình 1-7 Mô hình tấn công từ chối dịch vụ DDoS

Lợi ích: thiết bị chuyên dụng ngăn chặn hình thức tấn công DDoS.

Tính năng:

* Ngăn chặn các hình thức xâm nhập
* SSL offload
* Chống tấn công DDoS
  + - 1. **Giải pháp mã hóa và bảo mật đường truyền**

****

Hình 1-8 Giải pháp mã hóa và bảo mật đường truyền

Lợi ích: giải pháp chuyên dụng bảo vệ kết nối giữa các site trong cùng một hệ thống, đặc biệt phù hợp với các doanh nghiệp có nhiều chi nhánh và yêu cầu bảo mật cao trên đường truyền.

Tính năng:

* Mã hóa từ mức layer 2 (theo mô hình OSI), hỗ trợ các giao thức Ethernet, Fibre Channel/FICON và SDH/SONET từ 20Mbps đến 10Gbps
* Mã hóa cuộc gọi/ voice
* Mã hóa đường truyền fax
  + - 1. **Giải pháp giám sát và phân tích mã độc**

Lợi ích: xác định các loại mã độc đang hiện hữu trên hệ thống, tích hợp các giải pháp mức gateway ngăn chặn mã độc xâm hại trên hệ thống

Tính năng:

* Phát hiện và chống lại APTs và các tấn công có mục tiêu Zero-day malware và các khai thác lỗ hổng trên document
* Các hành vi tấn công mạng
* Email threats (phishing, spear-phishing): Bots, Trojans, Worms, Key Loggers and Crime ware
* Giám sát thời gian thực, phân tích sâu dựa trên giao diện điều khiển trực quan
* Giám sát tập trung vào các nguy cơ có mức độ nghiêm trọng cao và các đối tượng có giá trị
* Cung cấp các thông tin về an ninh hệ thống, và đưa ra các biện pháp khắc phục
  + - 1. **Giải pháp phòng chống spam/virus mức gateway**

Lợi ích: giải pháp chuyên dụng ngăn chặn các hình thức spam email, ngăn chặn virus.

Tính năng:

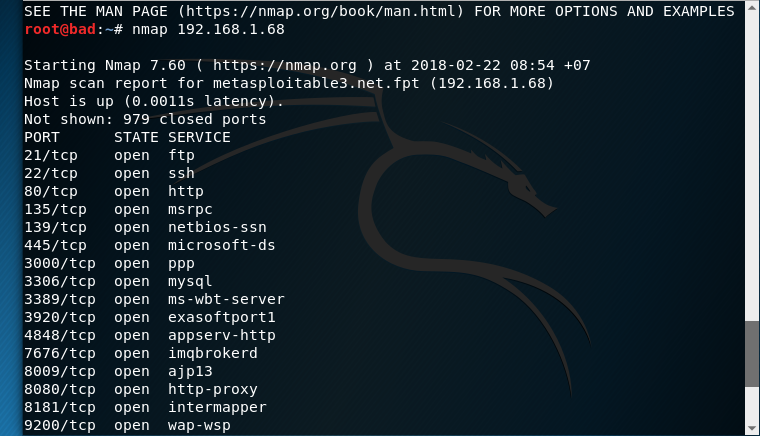
* SSL offload
* Lọc email spam
* Lọc email đính kèm virus
* Cô lập các kết nối đến liên kết có mã độc
  + 1. **Các công cụ hỗ trợ bảo mật mạng**

Ngoài những giải pháp trên chúng ta vẫn cần đến những công cụ sau:

* + - 1. **Công cụ Nmap**

Nmap là công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap có mã nguồn mở, miễn phí, dùng để quét lỗ cổng và các lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

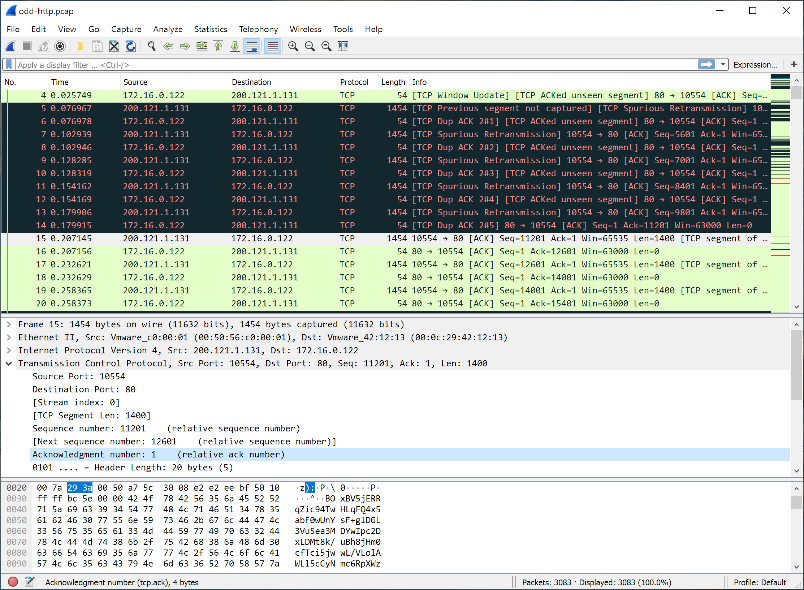
Nmap có thể được sử dụng để giám sát các máy chủ đơn lẻ cũng như các cụm mạng lớn bao gồm hàng trăm nghìn thiết bị và nhiều mạng con hợp thành. Mặc dù Nmap đã không ngừng được phát triển, cải tiến qua nhiều năm và cực kỳ linh hoạt, nhưng nền tảng của nó vẫn là một công cụ quét cổng, thu thập thông tin bằng cách gửi các gói dữ liệu thô đến các cổng hệ thống. Sau đó nó lắng nghe và phân tích các phản hồi và xác định xem các cổng đó được mở, đóng hoặc lọc theo một cách nào đó, ví dụ như tường lửa. Các thuật ngữ khác được sử dụng để chỉ hoạt động quét cổng (port scanning) bao gồm dò tìm cổng (discovery) hoặc liệt kê cổng (enumeration).



Hình 1-9 Công cụ Nmap

Một trong những lý do dẫn đến sự phổ biến rộng rãi của Nmap là nó có thể được sử dụng được trên rất nhiều hệ điều hành khác nhau Nó chạy được trên Windows và macOS cũng như được hỗ trợ trên các bản phân phối của Linux bao gồm Red Hat, Mandrake, SUSE và Fedora

* + - 1. **Công cụ Wireshark**

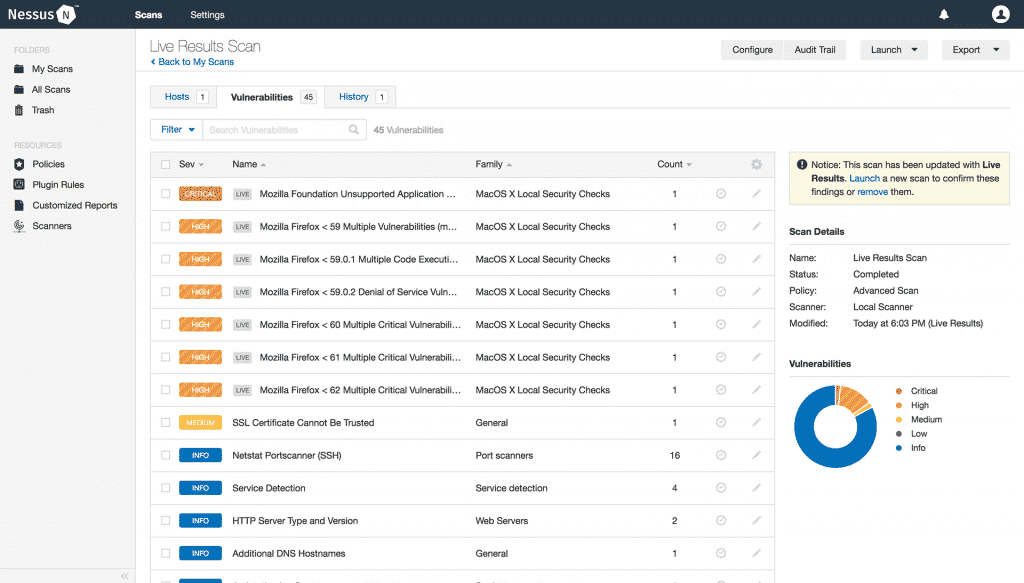
****

Hình 1-10 Giao diện công cụ wireshark

Wireshark là một ứng dụng dể phân tích dữ liệu hệ thống mạng, theo dõi và giám sát gói tin theo thời gian thực hiện, hiển thị chính xác và báo qua người dùng qua một giao diện đơn giản

Chức năng của Wireshark là:

* Phân tích chuyên sâu các giao thức mạng và đang được bổ sung hằng ngày Dùng để khắc phục sự cố mạng
* Dùng để khắc phục sự cố mạng
* Các developers sử dụng để gỡ lỗi triển khai giao thức Đọc và xuất dữ liệu từ nhiều giao thức
  + - 1. **Công cụ Nessus**

****

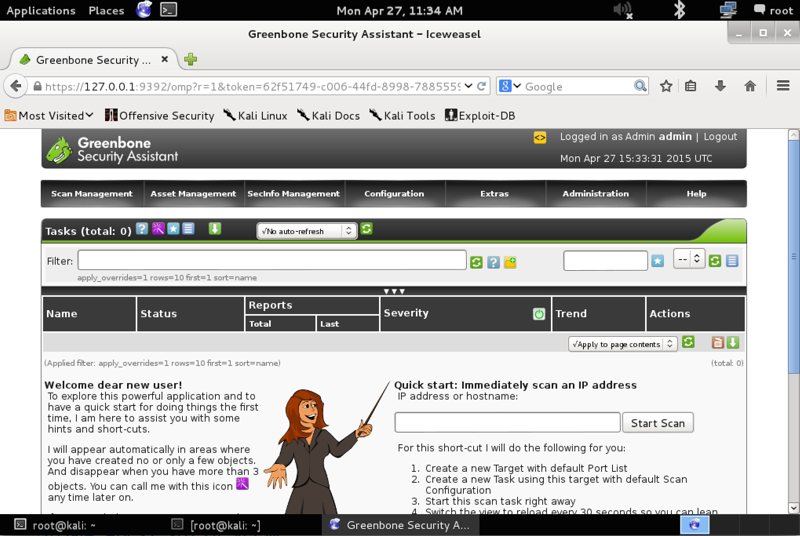
Hình 1-11 Giao diện công cụ Nessus

Quét các lỗ hổng bảo mật và đưa ra các biện pháp khắc phục trên hệ thống có nền tảng Windows, Linux, Mac.

Kiểm tra các bản vá hệ điều hành Windows, Linux và các ứng dụng như trình duyệt web, phần mềm, …

Đánh giá các lỗ hổng trên các loại thiết bị:

* Điện thoại chạy nền tảng Android, IOS, Windows Phone.
* Các thiết bị mạng khác: switch, router, access points, máy in,…
* Hỗ trợ phân tích cả trên các thiết bị ảo hóa.
* Cho phép cấu hình tự động quét theo một lịch trình nhất định.
* Phát hiện các phần mềm độc hại chạy trên hệ thống.
* Quét các lỗ hổng ứng dụng web dựa trên OWASP.
* Audit file cấu hình thiết bị.
  + - 1. **Công cụ OpenVAS**

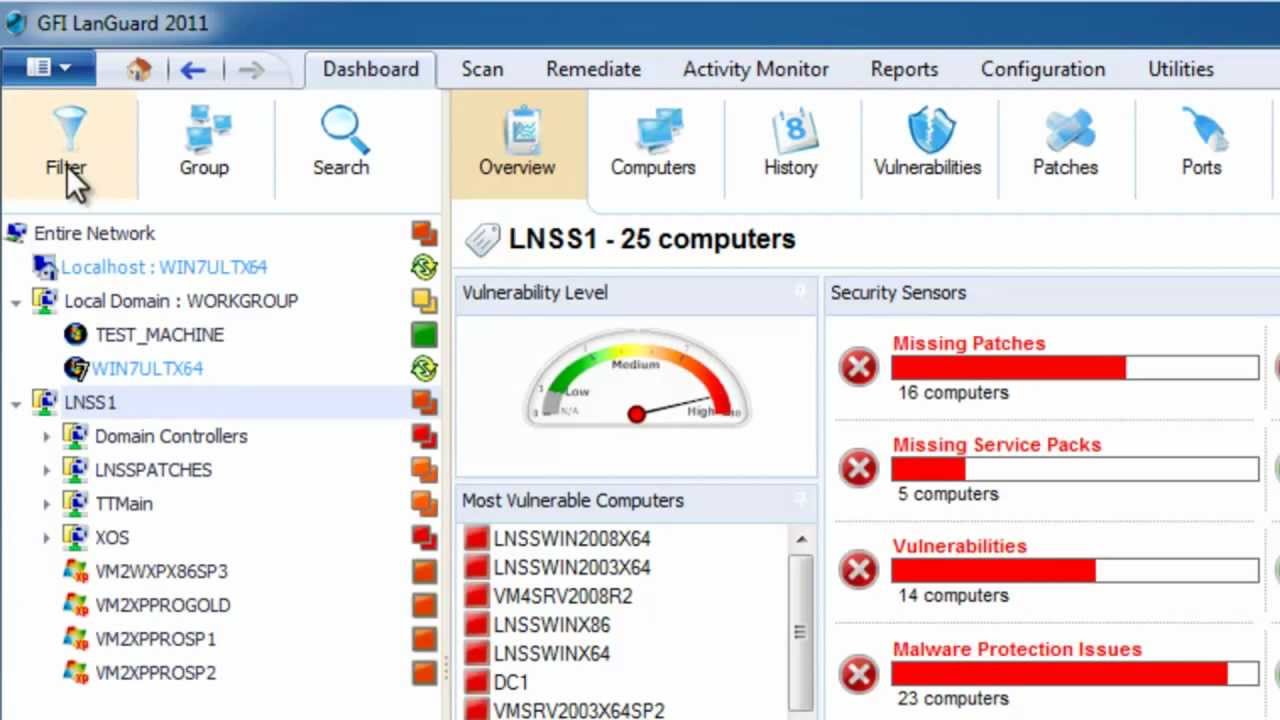
****

Hình 1-12 Giao diện công cụ OpenVAS

OpenVAS là một khung phần mềm của một số dịch vụ và cung cấp chức năng quét lỗ hổng và quản lý lỗ hổng.

Công cụ cũng có nhiều tính năng phong phú,OpenVAS có thể quét hàng trăm ngàn lỗ hổng khác nhau. Hơn thế nữa, công cụ này có thể tự động lên lịch rà quét và hỗ trợ nhiều nhiệm vụ thực thi cùng lúc

* + - 1. **Công cụ GFI Languard**

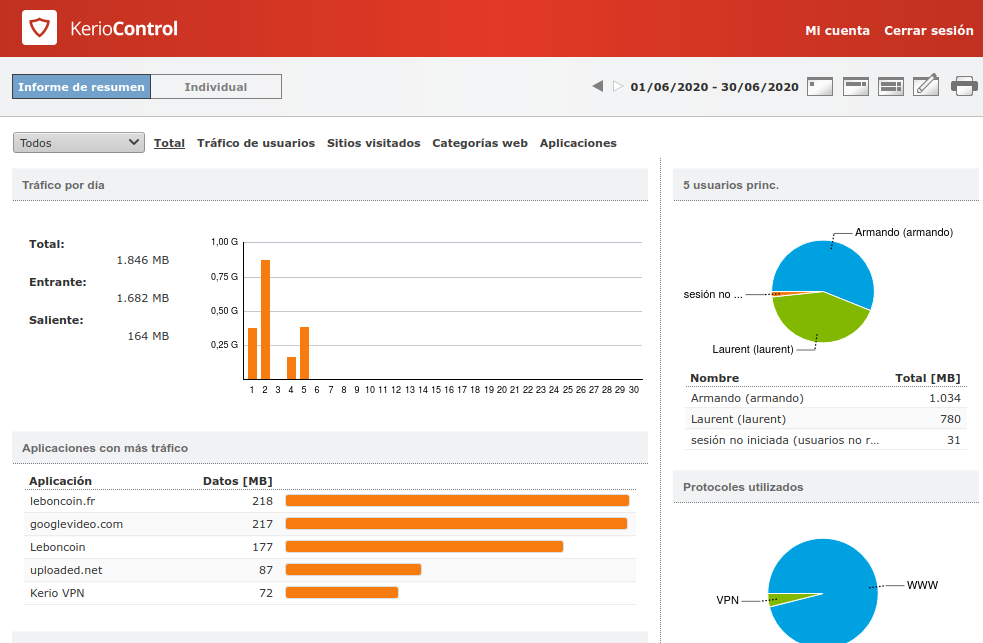
****

Hình 1-13 Giao diện công cụ GFI LanGuard

GFI LanGuard là một phần mềm vá lỗ hổng (patch management) và an ninh mạng, làm nhiệm vụ cố vấn an ninh thế giới ảo.

* Phần mềm này cung cấp:
* Patch Management dành cho Windows, Mac OS and Linux
* Patch Management dành cho những ứng dụng bên thứ ba
* Web reporting console
* Tìm kiếm ra những lỗ hổng mới nhất và missing updates
* Quét lỗ hổng bảo mật cho máy tính và thiết bị di động
* Kiểm kê thông minh hệ thống mạng và phần mềm
  + - 1. **Công cụ Kerio Control**

Kerio Control là một phần mềm hiện đại có khả năng bảo mật cho tường lửa, ngăn chặn sự thâm nhập của virus, phần mềm chứa mã độc, phát hiện và chống IPS. Đây thực sự là một phần mềm bảo mật hệ thống doanh nghiệp hiệu quả mà chúng ta nên sử dụng.



Hình 1-14 Giao diện công cụ Kerio Control

1. **TÌM KIẾM VÀ PHÂN TÍCH LỖ HỔNG BẢO MẬT VỚI GFI LANGUARD**
   1. **Giới thiệu phần mềm GFI Languard**

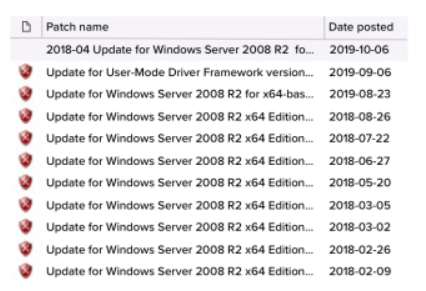
GFI LANguard là một giải pháp an ninh mạng, quét lỗ hổng phần mềm và đã từng đạt giải thưởng về công nghệ. Được sử dụng một cách rộng rãi bởi các doanh nghiệp vừa và nhỏ (SMB) trên toàn thế giới. GFI LANguard giúp quản trị viên có được cái nhìn tổng quan về an ninh mạng một cách hoàn chỉnh, mà không cần nhiều nỗ lực trong công tác quản trị, đồng thời việc khắc phục hậu quả cũng được thực hiện thông qua tính năng quản lý bản vá. Dễ dàng cài đặt và sử dụng, GFI Languard hoạt động như một nhà tư vấn ảo, cung cấp phân tích rủi ro và giúp bạn duy trì một trạng thái mạng an toàn, phù hợp nhanh hơn và hiệu quả hơn. GFI Languard giúp bạn trong việc quản lý bản vá, đánh giá tổn thương trong hệ thống mạng và kiểm soát phần mềm, kiểm kê tài sản, quản lý thay đổi, phân tích rủi ro và phân tích việc tuân thủ.

* Tự động khám phá tất cả các thành phần trong mạng của bạn, bao gồm máy tính, máy tính xách tay, điện thoại di động, máy tính bảng, máy in, máy chủ, máy ảo, bộ định tuyến và bộ chuyển mạch.
* Nhóm các thiết bị của bạn để quản lý tốt hơn. Phân phối quản lý cho các nhóm khác nhau và xem mọi thứ từ bảng điều khiển quản lý trung tâm.



Hình 2-1 Xem mạng và xem nơi các mối đe dọa xâm nhập

* Quét mạng của bạn để tìm các bản vá bị thiếu.
* Tìm lỗ hổng trong các hệ điều hành phổ biến. Xác định các bản vá còn thiếu trong trình duyệt web và phần mềm của bên thứ ba.
* Xác định các lỗ hổng chưa vá bằng cách sử dụng danh sách cập nhật gồm hơn 60.000 sự cố đã biết cũng như các mục như cổng mở và thông tin hệ thống về người dùng, thư mục dùng chung và dịch vụ.



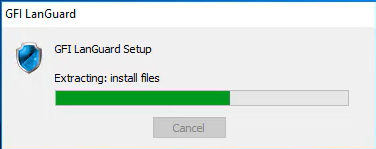
Hình 2-2 Tìm những lỗ hổng mà các mối đe dọa có thể khai thác

* Tự động triển khai các bản vá tập trung hoặc triển khai các tác nhân trên các máy riêng lẻ. Đừng dựa vào các cá nhân để giữ cho vành đai của bạn được vá.
* Kiểm soát các bản vá bạn cài đặt và khôi phục mọi bản vá nếu bạn thấy có vấn đề.
* Cài đặt các bản vá bảo mật không chỉ để sửa lỗi mà còn giúp các ứng dụng chạy tốt hơn
  1. **Cài đặt GFI Languard**
     1. **Một số lưu ý trước khi cài đặt**

Trước khi chạy trình hướng dẫn cài đặt:

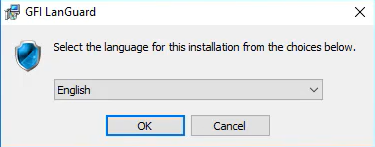
* Nếu bạn hiện đang sử dụng phiên bản trước của GFI LanGuard, bạn có thể nâng cấp cài đặt hiện tại của mình đồng thời giữ lại tất cả các cài đặt cấu hình hiện có của mình. Nâng cấp là không thể đảo ngược; bạn không thể hạ cấp xuống phiên bản trước mà bạn đã cài đặt.
* Bạn phải có Tài khoản GFI hoặc khóa cấp phép để cài đặt GFI LanGuard.
* Đảm bảo rằng máy sắp cài đặt GFI LanGuard đáp ứng các yêu cầu hệ thống.
* Định cấu hình tường lửa của bạn để cho phép GFI LanGuard kết nối với máy chủ GFI và với các máy từ xa sẽ được giám sát.
* Vô hiệu hóa phần mềm chống vi-rút của bên thứ ba trong quá trình cài đặt.
* Lưu mọi công việc đang chờ xử lý và đóng tất cả các ứng dụng đang mở trên máy.
  + 1. **Tiến hành tải xuống và cài đặt**

**Bước 1:** Khởi chạy trình cài đặt GFI Languard



Hình 2-3 Khởi chạy trình cài đặt GFI LanGuard

**Bước 2:** Chọn ngôn ngữ cho cài đặt của bạn và nhấp vào OK.



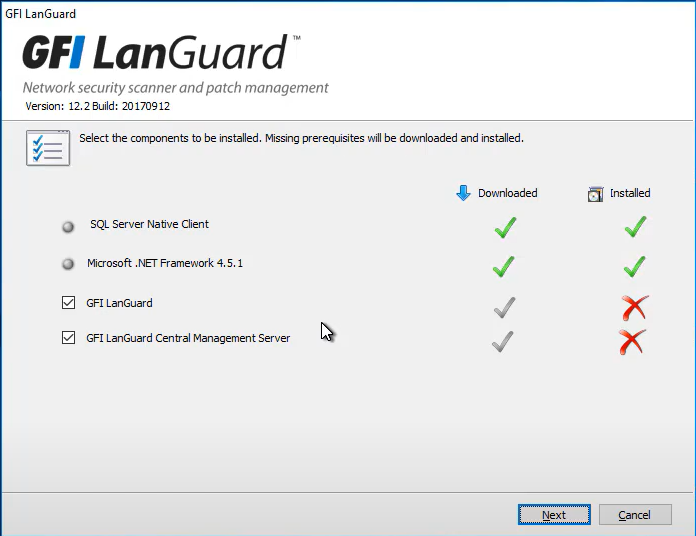
Hình 2-4 Cài đặt ngôn ngữ cho GFI LanGuard

***Lưu ý:***

* *Máy chủ quản lý trung tâm GFI LanGuard và tất cả các phiên bản GFI LanGuard được kết hợp với nó cần phải được cài đặt bằng cùng một ngôn ngữ.*
* *Giao diện người dùng đồ họa của Máy chủ quản lý trung tâm GFI LanGuard chỉ có sẵn bằng tiếng Anh, kể cả trong các trường hợp khi GFI LanGuard được cài đặt bằng ngôn ngữ khác.*

**Bước 3:** Từ danh sách các thành phần, chọn GFI LanGuard và nhấp vào Tiếp theo. Trình hướng dẫn cài đặt sẽ tự động tải xuống và cài đặt mọi thành phần bị thiếu.

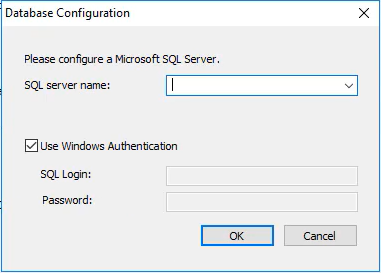
***Lưu ý:*** *cần có internet để tải các thành phần còn thiếu*

**

Hình 2-5 Chọn tải xuống và cài đặt thành phần

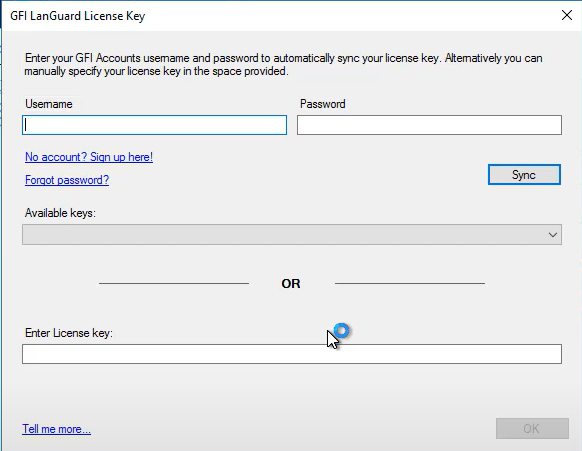
**Bước 4:** Điền thông tin vào cửa sổ cấu hình máy chủ cơ sở dữ liệu

* **Database server name:** Tên của máy chủ Microsoft SQL nơi lưu trữ cơ sở dữ liệu GFI LanGuard.
* **SQL database name:** Hiển thị tên cơ sở dữ liệu. GFI LanGuard giữ tên mặc định của cơ sở dữ liệu. Trong quá trình nâng cấp, bạn có thể quyết định chỉ địnhmột tên cơ sở dữ liệu khác để bạn có thể sử dụng cơ sở dữ liệu sạch trong khi duy trì cơ sở dữ liệu cũ từ phiên bản trước.
* ***Use Windows Authentication:*** Chọn tùy chọn này nếu bạn muốn GFI LanGuard sử dụng thông tin đăng nhập Microsoft Windows của người dùng hiện đang đăng nhập khi kết nối với cơ sở dữ liệu Microsoft SQL.
* ***Username / Password:*** Nếu GFI LanGuard không sử dụng Xác thực Windows khi kết nối với cơ sở dữ liệu Microsoft SQL, hãy cung cấp tên người dùng và mật khẩu để có thể kết nối với cơ sở dữ liệu.

**

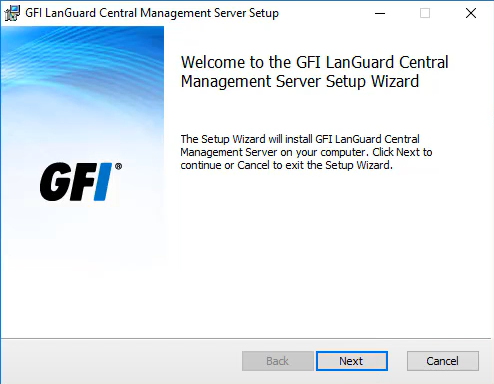
Hình 2-6 Cửa sổ cài đặt Database

**Bước 5:**Trong các trường Tên người dùng và Mật khẩu, hãy nhập thông tin đăng nhập khu vực Tài khoản GFI của bạn hoặc tài khoản được sử dụng khi đăng ký để tải xuống GFI LanGuard. Nhấp vào Đồng bộ hóa để truy xuất khóa cấp phép đã đăng ký vào tài khoản của bạn. Chọn một khóa từ trình đơn thả xuống Các phím khả dụng. Nếu bạn không có tài khoản GFI hoặc nếu bạn không có khóa cấp phép, hãy nhấp vào Đăng ký tại đây và điền vào mẫu đăng ký.

**

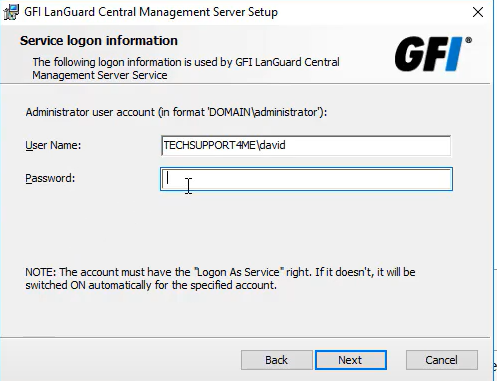
Hình 2-7 Nhập tài khoản người dùng hoặc License key

**Bước 6:** Trong màn hình chào mừng của GFI LanGuard, click vào Next.

**

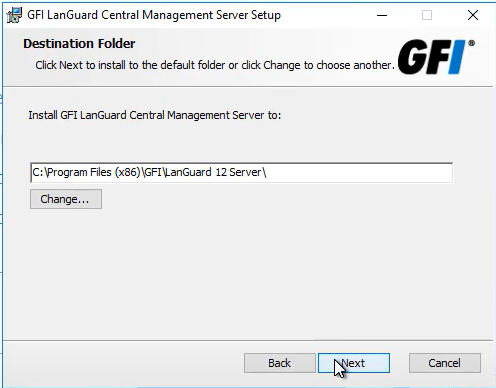
Hình 2-8 Cửa sổ chào mừng của GFI LanGuard

**Bước 7:** Điền thông tin Administrator user account trong cửa sổ Service logon infomation

**

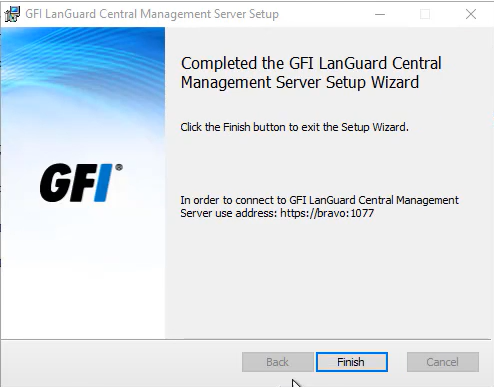
Hình 2-9 Điền thông tin Administrator user account

**Bước 8**: Chọn nơi cài đặt GFI LanGuard Central Management Server:

**

Hình 2-10 Chọn nơi cài đặt GFI LanGuard Central Management Server

**Bước 9:** *Để hoàn tất quá trình cài đặt GFI LanGuard, chọn Finish.*

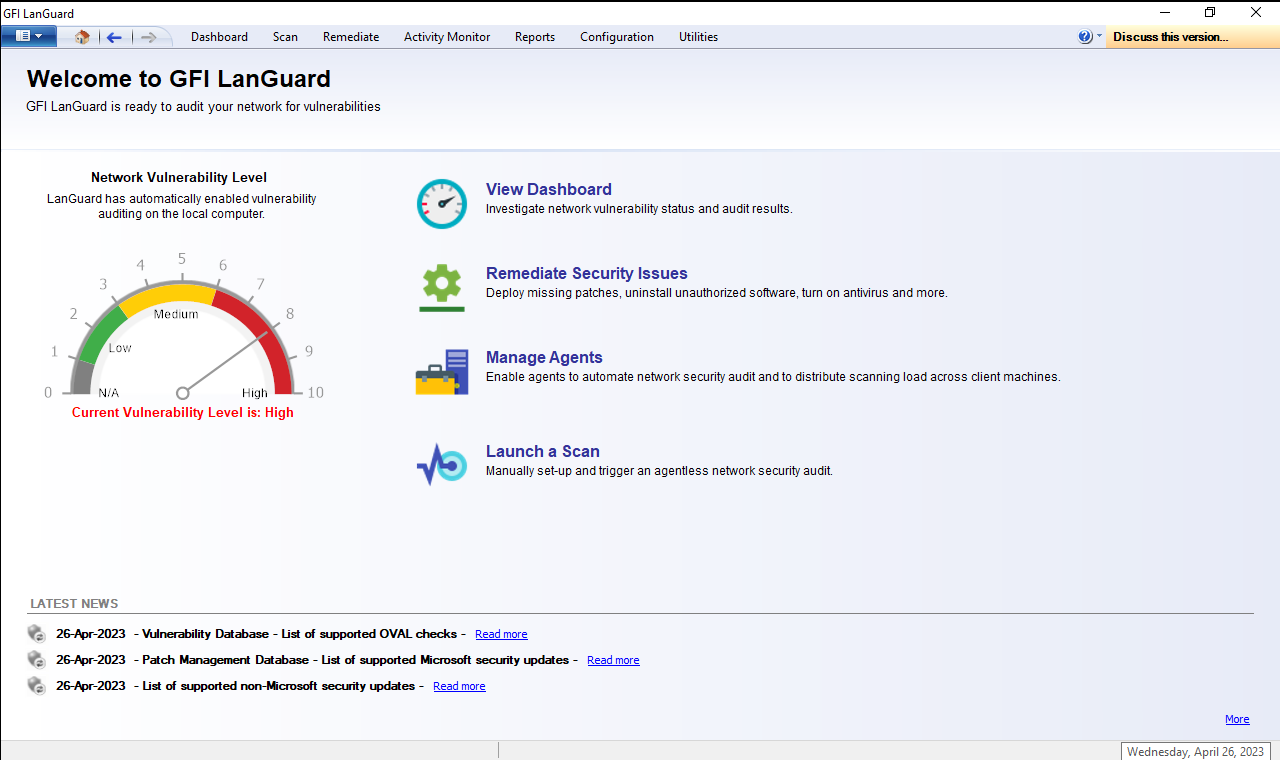
**

Hình 2-11 Hoàn tất quá trình cài đặt GFI LanGuard

**Bước 10:** Khởi động GFI LanGuard tiến hành thử nghiệm

Khi được khởi động lần đầu tiên, GFI LanGuard sẽ tự động kích hoạt kiểm tra trên bộ máy tính cục bộ và quét bộ máy tính cục bộ để tìm lỗi. Sau khi hoàn tất, Trang chủ GFI LanGuard hiển thị kết quả về lỗi truy cập.

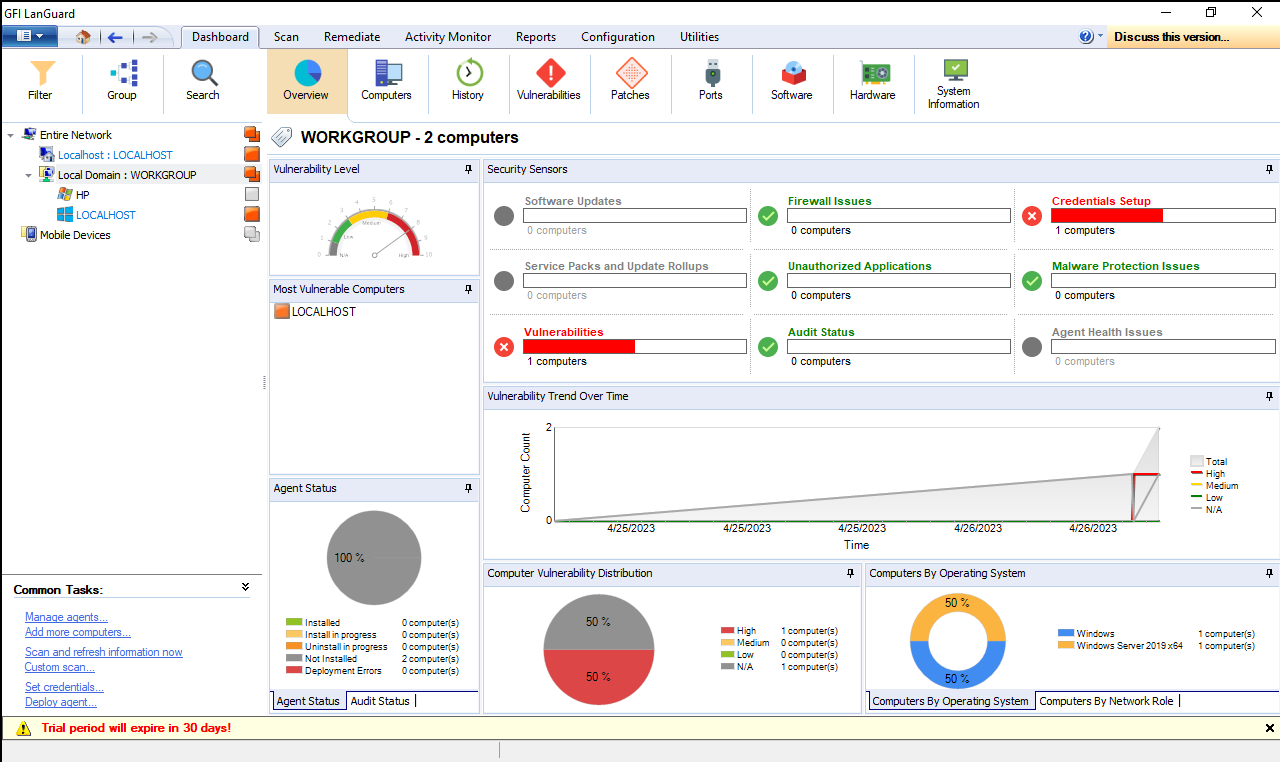
1. **TRIỂN KHAI THỰC NGHIỆM**
   1. **Một số chức năng chính trong GFI LanGuard**

**

Hình 3-1 Giao diện công cụ GFI LanGuard sau khi đã cài đặt thành công

* + 1. **View Dashboard**

Tab Dashboard hiển thị chi tiết các thông tin bảo vệ mà dữ liệu thu được trong quá trình scan, các máy tính trong mạng lan đã được scan và lỗi của các máy đó, đánh giá mức độ và khả năng tấn công có thể xảy ra

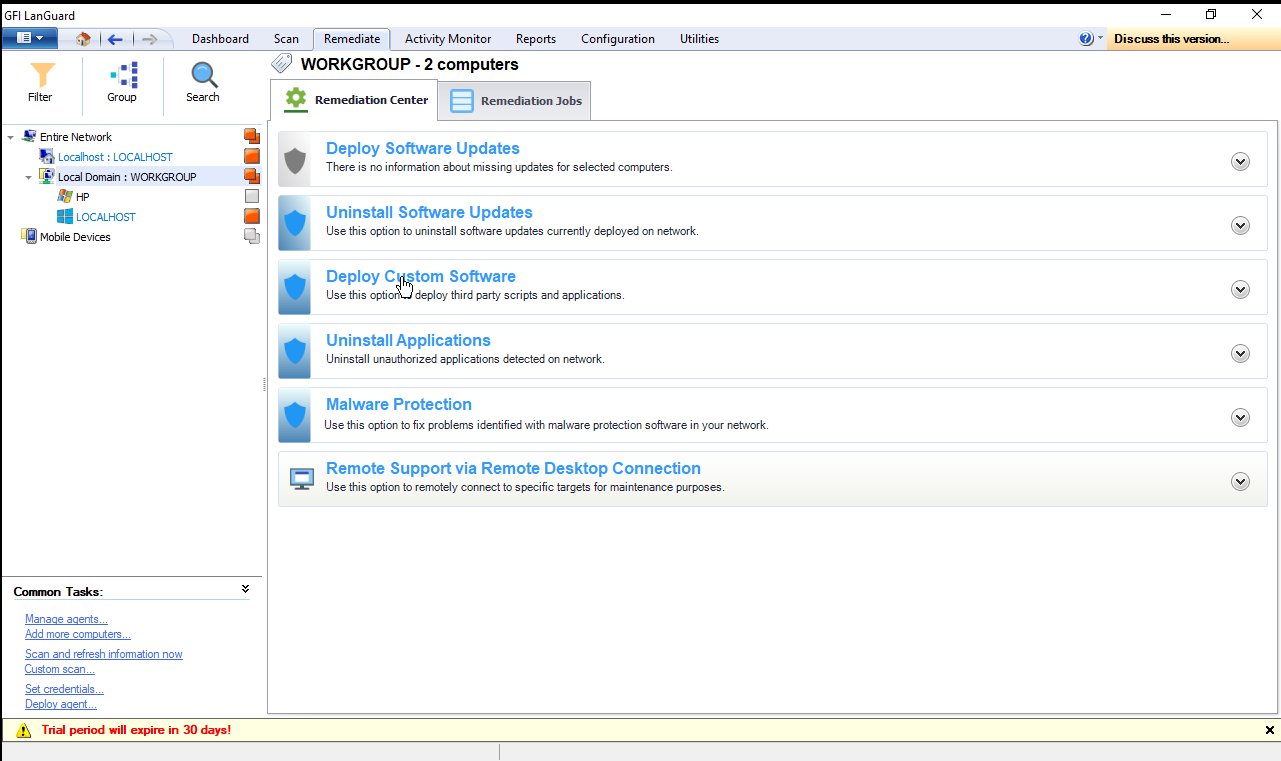
****

Hình 2-13 Tap View Dashboard trong công cụ GFI LanGuard

Ngoài ra, trang dashboard còn hiển thị chi tiết về lịch sử và thời gian scan trên các máy, số Ports, thông tin hệ thống, phần mềm, phần cứng,…

* + 1. **Remediate Security Issues**

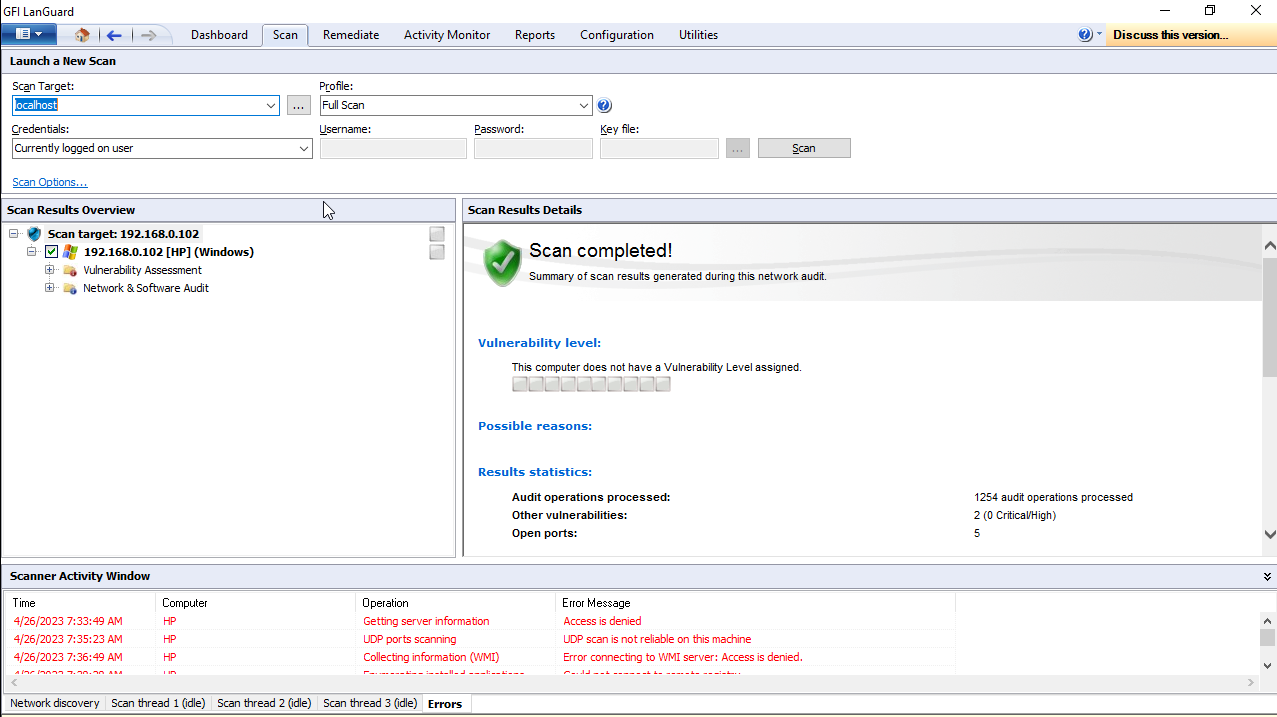
Chọn trang Remediate Security Issues để tiến hành khắc phục các sự cố bảo mật.

****

Hình 3-2 Tab Remediate Security Issues trong GFI LanGuard

* Để triển khai cập nhật phần mềm chọn Deploy Software Updates
* Gỡ cài đặt các bản cập nhật phần mềm chọn Uninstall Software Updates, Sử dụng tùy chọn này để gỡ cài đặt các bản cập nhật phần mềm hiện được triển khai trên mạng.
* Triển khai phần mềm tùy chỉnh chọn Deploy Custom Software, sử dụng tùy chọn này để triển khai các tập lệnh và ứng dụng của bên thứ ba
* Để gỡ cài đặt các ứng dụng trái phép chọn Uninstall Applications
* Bảo vệ phần mềm độc hại chọn Malware Protection, sử dụng tùy chọn này để khắc phục sự cố được xác định bằng phần mềm bảo vệ phần mềm độc hại trong mạng của chúng ta.
* Sử dụng tùy chọn Remote Support via Remote Desktop Connection để kết nối từ xa với các mục tiêu cụ thể cho mục đích bảo trì.
  + 1. **Launch a Scan**

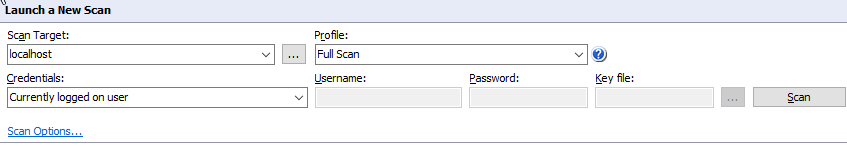
Tiến hành scanning máy localhost hoặc các máy tính trong mạng Lan bằng cách tùy chọn vào Scan.

****

Hình 3-3 Launch a Scan trên GFI LanGuard

* 1. **Tiến hành Scanning trên các máy**

Đầu tiên, chúng ta sẽ tiến hành scanning trên máy localhost bằng cách chọn các thông tin như hình sau đó click vào Scan. Quá trình Scan khoảng 10 – 15 phút.

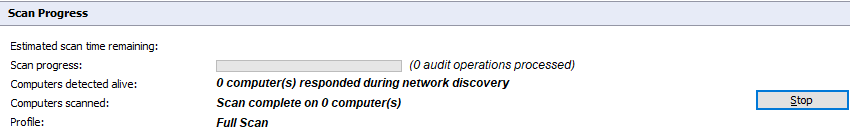
****

Hình 3-4 Chọn scanning máy localhost

Trong quá trình Scan, ở phần Scan Progress hiển thị các thông tin sau:

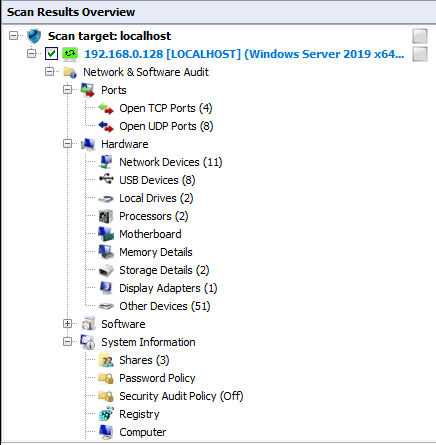
* Estimated scan time remaining: thời gian scan
* Scan progress: quá trình scan đang diễn ra
* Computers detected alive: số máy đang đc scan
* Computers scanned: quá trình hoàn thành trên các máy
* Profile: quét toàn bộ

Có thể click vào Stop nếu muốn dừng quá trình scan.

****

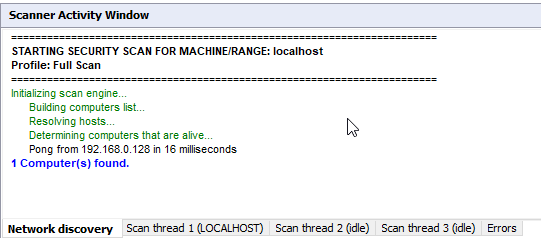
Hình 3-5 Quá trình Scanning đang diễn ra

Ở phần Scan Results Overview hiển thị máy đang được scan và các thành phần. Máy localhost đang được scan ở đây là Windows Server 2019 có địa chỉ IP là 192.168.0.128.

****

Hình 3-6 Cửa sổ Results Overview

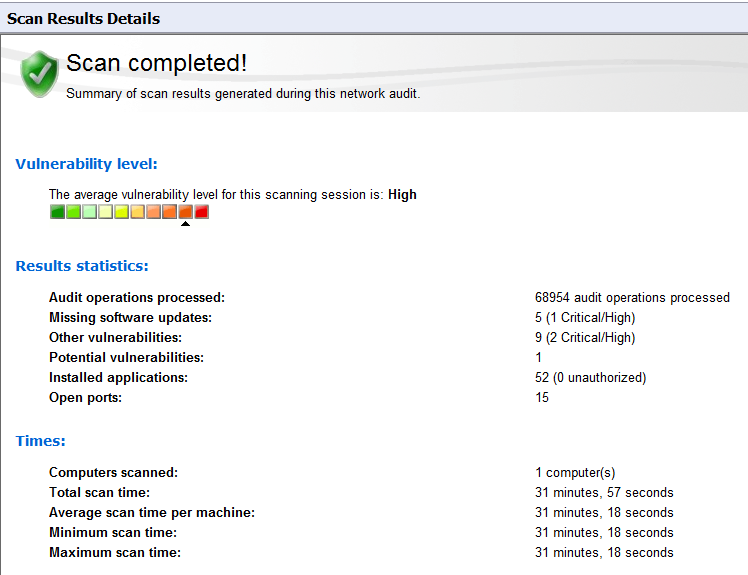
Có thể thấy các tiến trình scan đang diễn ra trong mục Scanner Activity Window.

****

Hình 3-7 Cửa sổ Scanner Activity Window

Sau khi đã hoàn tất quá trình scan, phần Scan Result Details cho chúng ta thấy kết quả của quá trình scan vừa rồi.

* Vulnerability exploits: Các mức độ, khả năng tấn công xảy ra
* Results statistics: Thống kê kết quả
* Missing software updates: Thiếu cập nhật phần mềm
* Other vulnerabilities: 9 nguy cơ tấn công trực tiếp
* Potential vulnerabilities: 1 nguy cơ tấn công trực tiếp
* Installed applications: 52 ứng dụng đã đc cài đặt
* Open ports: cổng đang mở là cổng 21



Hình 3-8 Cửa sổ Scan Results Details hiển thị kết quả sau khi quét xong

**KẾT LUẬN**

1. **Hướng phát triển**
2. **Kết luận**

# **TÀI LIỆU THAM KHẢO**