BỘ GIÁO DỤC VÀ ĐÀO TẠO
**TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG**
-------o0o-------

# TÌM HIỂU CÔNG CỤ NESSUS TRONG PHÁT HIỆN VÀ PHÂN TÍCH LỖ HỔNG BẢO MẬT TRÊN HỆ THỐNG MẠNG

**ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY**

Ngành: Công nghệ Thông tin

**HẢI PHÒNG - 2020**

BỘ GIÁO DỤC VÀ ĐÀO TẠO
**TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG**
-------o0o-------

# TÌM HIỂU CÔNG CỤ NESSUS TRONG PHÁT HIỆN VÀ PHÂN TÍCH LỖ HỔNG BẢO MẬT TRÊN HỆ THỐNG MẠNG

**ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY**

Ngành: Công nghệ Thông tin

Sinh viên thực hiện : **Nguyễn Duy Quang**
Mã sinh viên : **1512101011**
Giáo viên hướng dẫn : **TS. Ngô Trường Giang**.

**HẢI PHÒNG - 2020**

BỘ GIÁO DỤC VÀ ĐÀO TẠO
**TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG**

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
**Độc lập - Tự do - Hạnh phúc**

-------o0o-------

# NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

Sinh viên: **Nguyễn Duy Quang** Mã sinh viên: **1512101011**

Lớp: **CT1901M** Ngành: **Công nghệ Thông tin**

Tên đề tài:

# "TÌM HIỂU CÔNG CỤ NESSUS TRONG PHÁT HIỆN VÀ PHÂN TÍCH LỖ HỔNG BẢO MẬT TRÊN HỆ THỐNG MẠNG"

# NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp a. Nội dung:

- Tổng quan về bảo mật mạng
- Tìm hiểu công cụ Nessus
- Sử dụng nessus để phát hiện và phân tích lỗ hổng bảo mật trên hệ thống mạng.

b. Các yêu cầu cần giải quyết

- Tìm hiểu các vấn đề cơ bản về bảo mật mạng.
- Tìm hiểu công cụ Nessus phân tích lỗ hổng mạng
- Cài đặt, cấu hình phần mềm nagios để phân tích lỗ hổng bảo mật trên hệ thống mạng.

2. Các số liệu cần thiết để thiết kế, tính toán

3. Địa điểm thực tập

## CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

**Người hướng dẫn thứ nhất:**

Họ và tên: **Ngô Trường Giang**

Học hàm, học vị: **Tiến sĩ.**

Cơ quan công tác: **Khoa Công nghệ Thông tin**

Nội dung hướng dẫn:

- Tổng quan về bảo mật mạng
- Tìm hiểu công cụ Nessus
- Sử dụng nessus để phát hiện và phân tích lỗ hổng bảo mật trên hệ thống mạng.

**Người hướng dẫn thứ hai:**

Họ và tên: …….....

Học hàm, học vị……

Cơ quan công tác: ……

Nội dung hướng dẫn: …….....

……..

……..

Đề tài tốt nghiệp được giao ngày 14 tháng 10 năm 2019

Yêu cầu hoàn thành trước ngày 10 tháng 01 năm 2020

| | |
|---|---|
| Đã nhận nhiệm vụ: Đ.T.T.N<br>Sinh viên | Đã nhận nhiệm vụ: Đ.T.T.N<br>Cán bộ hướng dẫn Đ.T.T.N |
| **Nguyễn Duy Quang** | **Ngô Trường Giang** |

*Hải Phòng, ngày .....tháng.....năm 2020*

HIỆU TRƯỞNG

**GS.TS.NGUT Trần Hữu Nghị**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**Độc lập – Tự do – Hạnh phúc**

# PHIẾU NHẬN XÉT CỦA CÁN BỘ HƯỚNG DẪN TỐT NGHIỆP

Họ và tên: **Ngô Trường Giang**

Cơ quan công tác: **Khoa Công nghệ Thông tin**

Họ tên sinh viên: **Nguyễn Duy Quang**

Ngành: **Công nghệ Thông tin**

Nội dung hướng dẫn:

- Tổng quan về bảo mật mạng
- Tìm hiểu công cụ Nessus
- Sử dụng nessus để phát hiện và phân tích lỗ hổng bảo mật trên hệ thống mạng.

**1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp:**

- Sinh viên chủ động tìm đọc các tài liệu liên quan tới đề tài.
- Chấp hành đúng kế hoạch, tiến độ đề ra.

**2. Đánh giá chất lượng của đồ án (so với nội dung yêu cầu đã đề ra trong nhiệm vụ đề tài tốt nghiệp trên các mặt lý luận, thực tiễn, tính toán số liệu..):**

- Đồ án đã trình bày tổng quan về bảo mật mạng, các chức năng cơ bản của công cụ Nessus và một số mô hình triển khai phát hiện và phân tích lỗ hổng mạng.
- Đồ án đã triển khai cài đặt, cấu hình công cụ Nessus, triển khai thử nghiệm phát hiện lỗ hổng trên website ở mức độ đơn giản.
- Về hình thức: Báo cáo trình bày sáng sủa, bố cục hợp lý.
- Đồ án đáp ứng được yêu cầu đề ra.

**3. Ý kiến của cán bộ hướng dẫn:**

Đạt [x] Không đạt [ ] Điểm:……...

Ngày 01 tháng 01 năm 2020

**Cán bộ hướng dẫn**

**TS. Ngô Trường Giang**

QC20-B18

# LỜI CẢM ƠN

Để hoàn thành tốt đề tài này em xin chân thành cảm ơn ban lãnh đạo Trường Đại Học Dân Lập Hải Phòng cùng tất cả các giảng viên đã tạo điều kiện thuận lợi và nhiệt tình giảng dạy cho em trong suốt thời gian học vừa qua để em có thể học tập tốt và đạt được kết quả như ngày hôm nay.

Em cũng xin chân thành gửi lời cảm ơn đến T.S Ngô Trường Giang đã tận tình hướng dẫn cho em về đề tài và đồng thời em cũng xin gửi lời cảm ơn đến các bạn thành viên ở một số webiste và diễn đàn đã cung cấp thêm một số thống tin hữu ích cho em thực hiện tốt đề tài này.

Do quy mô đề tài, thời gian và kiến thức còn hạn chế nên không tránh khỏi những sai sót. Kính mong quý thầy cô đóng góp ý kiến để em củng cố, bổ sung và hoàn thiện thêm kiến thức cho mình.

Hải Phòng, ngày 28 tháng 12 năm 2019

Sinh viên

Nguyễn Duy Quang

# MỤC LỤC

**LỜI CẢM ƠN ..... 1**

**DANH MỤC HÌNH VẼ ..... 4**

**MỞ ĐẦU ..... 5**

**CHƯƠNG 1: TỔNG QUAN VỀ BẢO MẬT MẠNG..... 6**

1.1 Bảo mật mạng ..... 6

1.2 Các loại lỗ hổng bảo mật ..... 6

1.2.1 Lỗ hổng theo khu vực phát sinh ..... 7

1.2.2 Lỗ hổng phát sinh do các khiếm khuyết của hệ thống thông tin .. 8

1.2.3 Lỗ hổng theo vị trí phát hiện ..... 8

1.2.4 Lỗ hổng đã biết, lỗ hổng zero-day ..... 9

1.3 Một số phương thức tấn công mạng ..... 11

1.3.1 Tấn công vào trình duyệt (Browse Attacks) ..... 11

1.3.2 Tấn công bằng phần mềm độc hại ..... 12

1.3.3 Tấn công từ chối dịch vụ ( Ddos Attacks ) ..... 13

1.3.4 Kiểu tấn công sâu bọ ( Worm Attacks ) ..... 14

1.3.5 Tấn công cơ sở dữ liệu ( SQL injection ) ..... 15

1.3.6 Kiểu tấn công rà quét ..... 16

1.3.7 Kiểu tấn công mạng khác ..... 16

1.4 Các giải pháp và công cụ hỗ trợ bảo mật mạng ..... 16

1.4.1 Các giải pháp bảo mật mạng ..... 16

1.4.2 Các công cụ hỗ trợ bảo mật mạng ..... 19

**CHƯƠNG 2: PHÁT HIỆN VÀ PHÂN TÍCH LỖ HỔNG BẢO MẬT VỚI NESSUS ..... 26**

2.1 Giới thiệu phần mềm Nessus ..... 26

2.2 Các mô hình triển khai Nessus ..... 27

2.2.1 Mô hình kiến trúc Nessus Client-Server ..... 27

2.2.2 Mô hình Nessus Knowledge Base. ..... 28

2.2.3 Mô hình Nessus Plugin. ..... 28

2.3 Cài đặt Nessus ..... 29

**CHƯƠNG 3: THỰC NGHIỆM ..... 35**

3.1 Mô hình triển khai thực nghiệm ..... 35

3.1.1 Phát biểu bài toán ..... 35

3.1.2 Mô hình ..... 35

3.2 Các bước triển khai ..... 35

**KẾT LUẬN ..... 42**

**TÀI LIỆU THAM KHẢO ..... 43**

# DANH MỤC HÌNH VẼ

Hình 1-1: Tấn công vào trình duyệt Web ..... 12
Hình 1-2**:** Tấn công bằng phần mềm độc hại ..... 12
Hình 1-3: Tấn công từ chối dịch vụ DoS ..... 14
Hình 1-4: Tấn công kiểu sâu bọ ..... 14
Hình 1-5: Tấn công cơ sở dữ liệu SQL injection ..... 15
Hình 1-6: Giải pháp tường lửa ..... 17
Hình 1-7: Sử dụng DDoS ..... 18
Hình 1-8: Giao diện công cụ Nmap ..... 21
Hình 1-9 Giao diện WireShark ..... 22
Hình 1-10: Giao diện công cụ Nessus ..... 23
Hình 1-11: Giao diện OpenVAS ..... 24
Hình 1-12: Công cụ Kerio Control ..... 25
Hình 2-1: Mô hình Client-Sever ..... 28
Hình 2-2: Mô hình Nessus Plugin ..... 29
Hình 2-3: Trang dowload Nessus ..... 30
Hình 2-4 Chạy cài đặt Nessus ..... 30
Hình 2-5 Câu lệnh cài đặt ..... 30
Hình 2-6 Lệnh khởi động Nessus ..... 31
Hình 2-7: Nessus tự động cập nhật các plugin ..... 31
Hình 2-8: Lấy mã kích hoạt Nessus ..... 32
Hình 2-9: Điền thông tin ..... 32
Hình 2-10: Vào Mail để lấy mã ..... 33
Hình 2-11: Nhập mã để kích hoạt Nessus ..... 33
Hình 2-12: Giao diện đăng nhập Nessus ..... 34
Hình 2-13: Giao diện sau khi đăng nhập vào công cụ Nessus ..... 34
Hình 3-1: Mô hình quét lỗ hổng Nessus ..... 35
Hình 3-2: Scan TemPlates ..... 36
Hình 3-3: Điền các thông tin trong Web application ..... 36
Hình 3-4: Thay đổi trường phạm vi quét cổng. ..... 37
Hình 3-5: Service Discovery. ..... 37
Hình 3-6: Tùy chỉnh ASSESSMENT. ..... 38
Hình 3-7: Plugin có trên Nessus. ..... 39
Hình 3-8: Quá trình quét ứng dụng web ..... 39
Hình 3-9: Kết quả dò quét tổng quan ..... 40
Hình 3-10: Các lỗi đã quét được ..... 41

# MỞ ĐẦU

Ngày nay, khi Internet đã phát triển phổ biến rộng rãi, các tổ chức, cá nhân đều có nhu cầu giới thiệu thông tin của mình trên xa lộ thông tin cũng như thực hiện các phiên giao dịch trực tuyến một cách tiện lợi nhất. Vấn đề nảy sinh là khi phạm vi ứng dụng của các ứng dụng trên internet ngày càng mở rộng thì khả năng xuất hiện lỗi càng cao. Từ đó nảy sinh ra các vấn đề về hệ thống mạng không đáng có xảy ra gây ảnh hưởng đến xã hội, kinh tế … Những lỗi này hầu như do người làm không kiểm duyệt kĩ lưỡng trước khi đưa cho người dùng cuối hay cũng có thể do có người cố tình phá hoại nhằm đánh cắp thông tin cá nhân như tài khoản ngân hàng, điện thoại, tin nhắn,…

Vì vậy cần có những công cụ phát hiện lỗ hổng bảo mật cho phép ta thực hiện kiểm tra lỗi trước khi đưa cho người sử dụng cuối hoặc kiểm tra và vá lại những lỗ hổng đó để có thể an toàn nhất khi ở trên mạng. Chính vì vậy em đã chọn đồ án tốt nghiệp : “Tìm hiểu công cụ Nessus trong phát hiện và phân tích lỗ hổng bảo mật trên hệ thống mạng”. Và mục tiêu của đồ án là nghiên cứu, tìm hiểu về những giải pháp phát hiện lỗ hổng bảo mật để giúp phát hiện lỗi sớm, và đưa ra những giải pháp tốt nhất cho hệ thống mạng.

Đồ án gồm ba chương:

- Chương 1: Tổng quan về bảo mật mạng
- Chương 2: Phát hiện và phân tích lỗ hổng bảo mật mạng với Nessus
- Chương 3: Thực nghiệm

# CHƠƠNG 1: TỔNG QUAN VỀ BẢO MẬT MẠNG

## 1.1 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 "

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.

## 1.2 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.

### 1.2.1 Lỗ hổng theo khu vực phát sinh

Bao gồm:

Lỗ hổng code

- 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.
- 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.
- Lỗ hổng kiến trúc, phát sinh trong quá trình thiết kế hệ thống thông tin .
- Lỗ hổng tổ chức.
- 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.

### 1.2.2 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.

### 1.2.3 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.

### 1.2.4 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.

## 1.3 Một số phơơng 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.

### 1.3.1 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 1-1: Tấn công vào trình duyệt Web

### 1.3.2 Tấn công bằng phần mềm độc hại


Hình 1-2**:** Tấn công bằng phần mềm độc hại

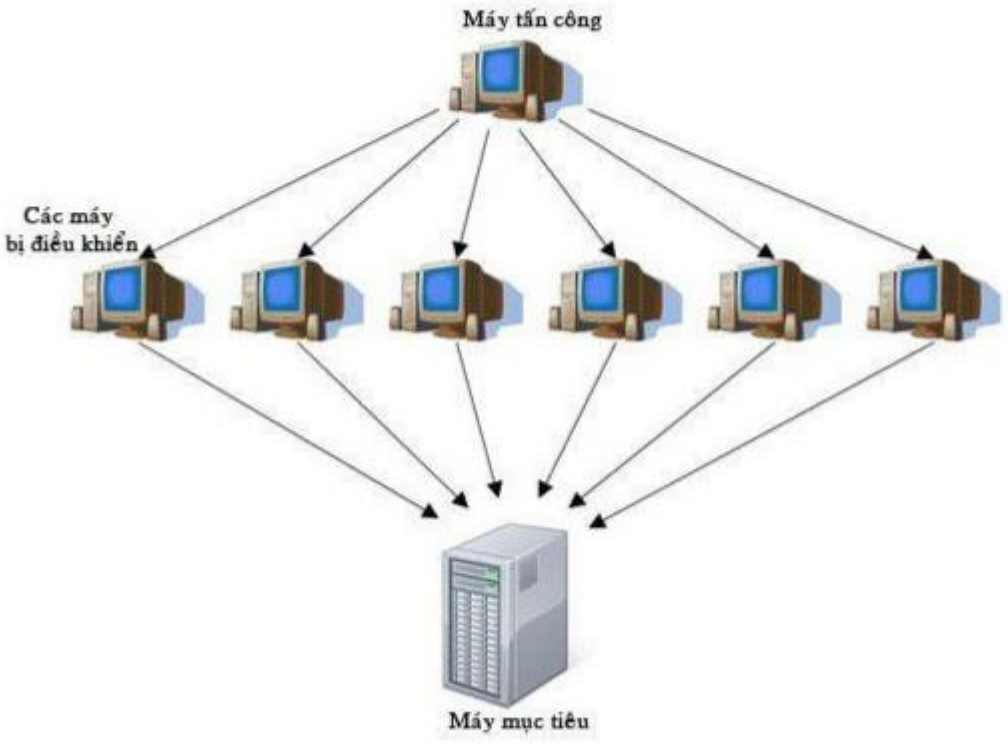
Tấn công Malware là hình thức phổ biến nhất. Malware bao gồm spyware ( phần mềm gián điệp ), ransomware ( mã độc tống tiền ), virus và worm (phần mềm độc hại có khả năng lây lan nhanh). Thông thường, tin tặc sẽ tấn công người dùng thông qua các lỗ hổng bảo mật, cũng có thể là dụ dỗ người dùng click vào 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.

### 1.3.3 Tấn công từ chối dịch vụ ( Ddos Attacks )

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.

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.




Hình 1-3: Tấn công từ chối dịch vụ DoS

### 1.3.4 Kiểu tấn công sâu bọ ( Worm Attacks )


Hình 1-4: Tấn công kiểu sâu bọ

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.

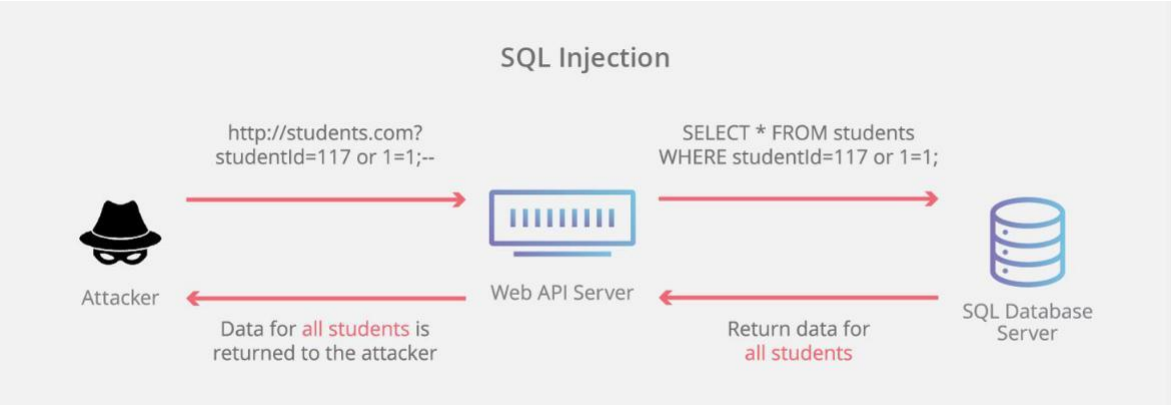
Một trong ví dụ tiêu biểu của phương thức tấn công này là mã độc WannaCry đã lây nhiễm hơn 300.000 máy tính chỉ sau một vài ngày. WannaCry nhắm vào mục tiêu lỗ hổng trên Windows, một khi máy bị nhiễm, phần mềm độc hại sẽ tự động quét hệ thống mạng kết nối với nhau, từ đó lây nhiễm sang các máy tính khác.

### 1.3.5 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<input>, chuỗi truy vấn (query strings), cookie và tệp tin.

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




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

### 1.3.6 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

### 1.3.7 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.

## 1.4 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

### 1.4.1 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, …

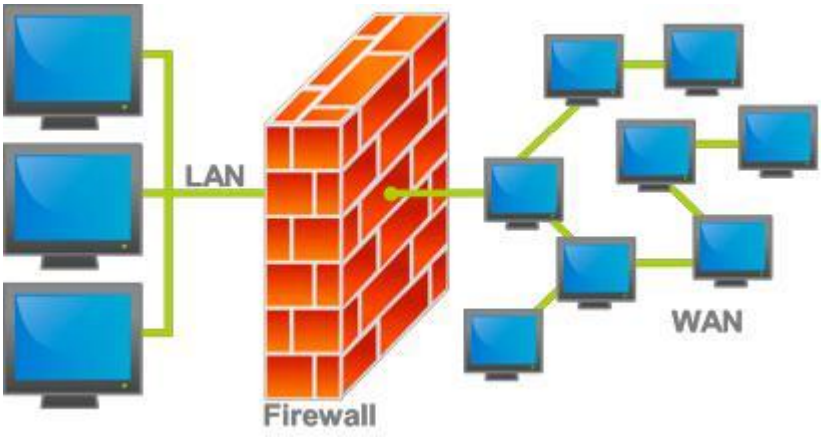
Dưới đây là nhưng giải pháp có chất lượng uy tín hàng đầu, được các chuyên gia trên toàn thế giới khuyên dùng

#### 1.4.1.1 Giải pháp tợờng 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



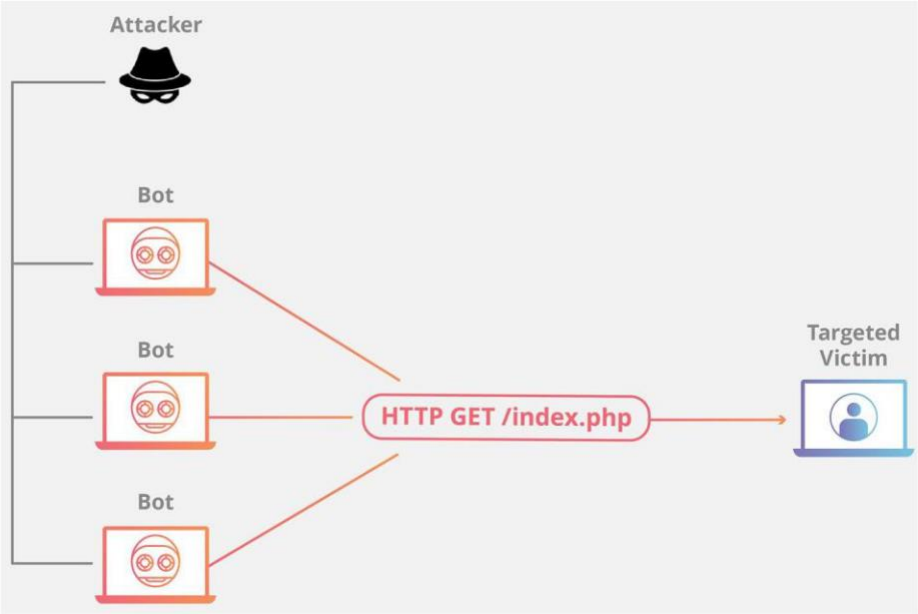

Hình 1-6: Giải pháp tường lửa

#### 1.4.1.2 Giải pháp chống xâm nhập và chống 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




Hình 1-7: Sử dụng DDoS

#### 1.4.1.3 Giải pháp mã hóa và bảo mật đoờng 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

#### 1.4.1.4 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

#### 1.4.1.5 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

### 1.4.2 Các công cụ hỗ trợ bảo mật mạng

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

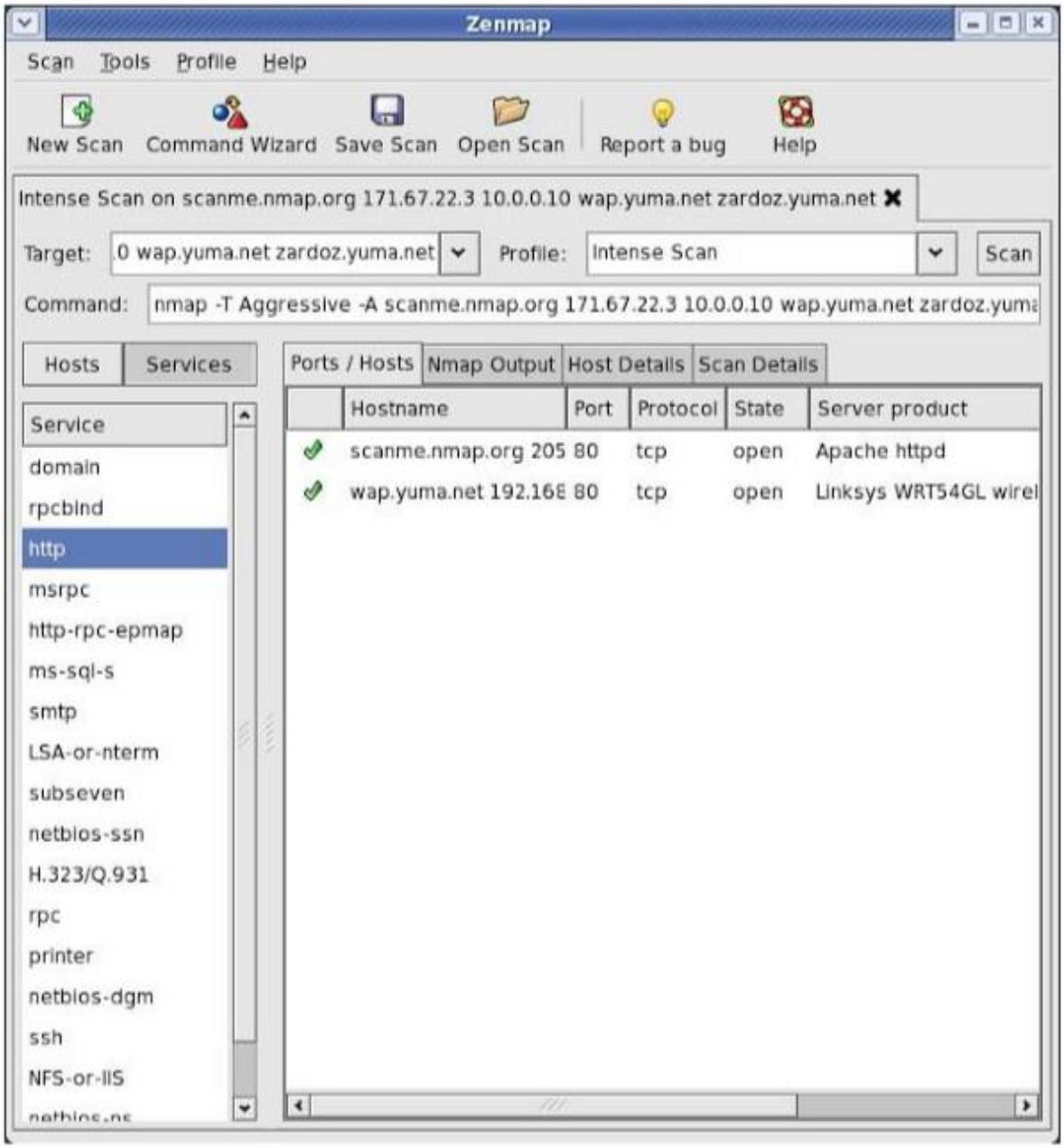
#### 1.4.2.1 Công cụ Nmap

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).

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




Hình 1-8: Giao diện công cụ Nmap

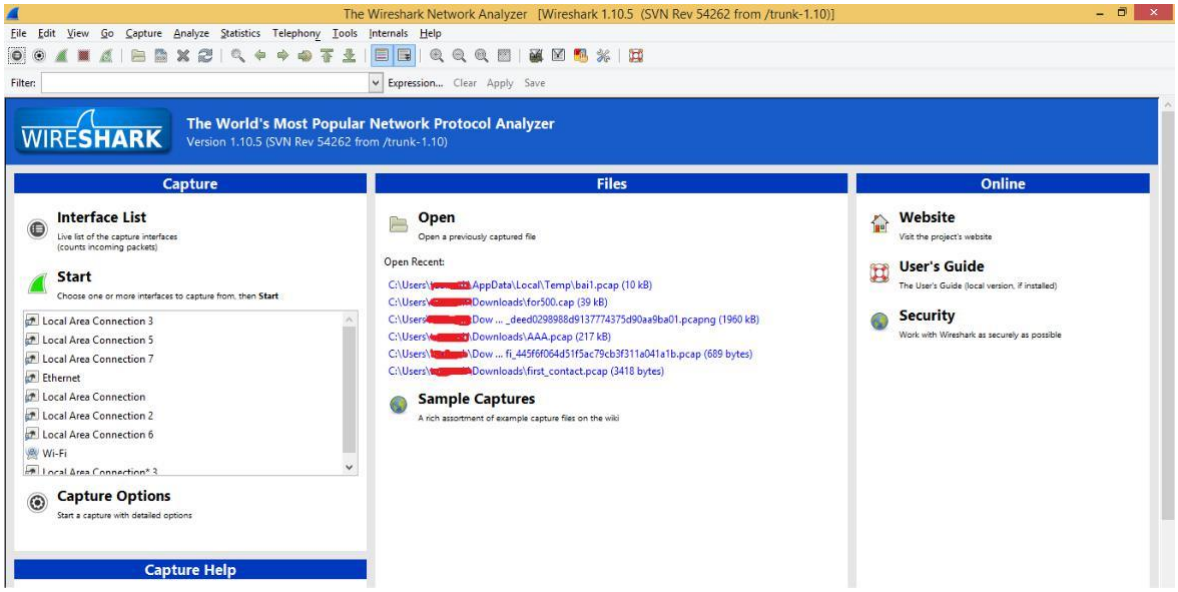
### 1.4.2.2 Công cụ Wireshark

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

- Các developers sử dụng để gỡ lỗi triển khai giao thức
- Đọc và xuất dữ liệu từ nhiều giao thức




Hình 1-9 Giao diện

WireShark **1.4.2.3 Công cụ Nessus**

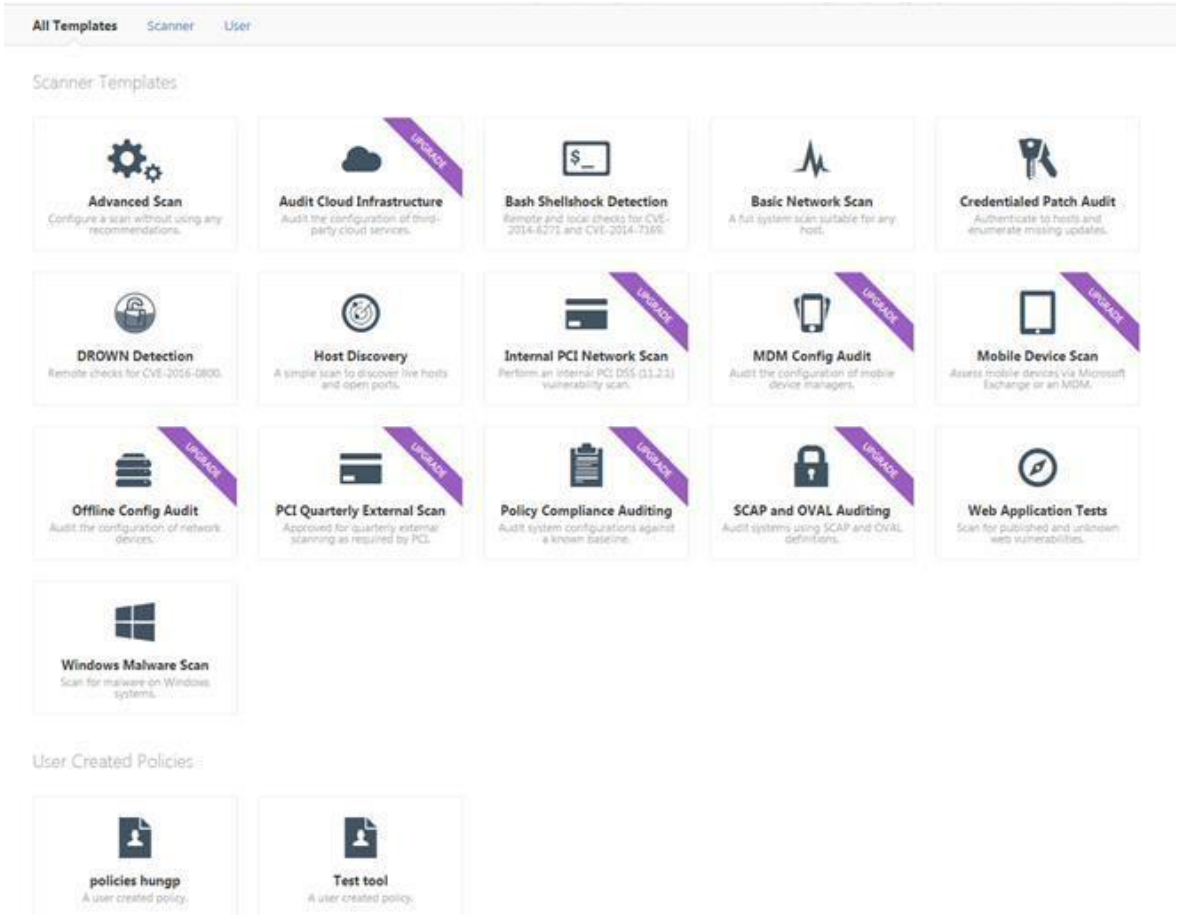
Quét các lỗ hổng bảo mật và đưa ra các biện pháp khắc phục trên hệ thống có nền tảng Windows, Linux, Mac.

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.

Hỗ trợ Cloud: Audit cấu hình của các cloud public như: Amazon Web Services, Microsoft Azure and Rackspace.

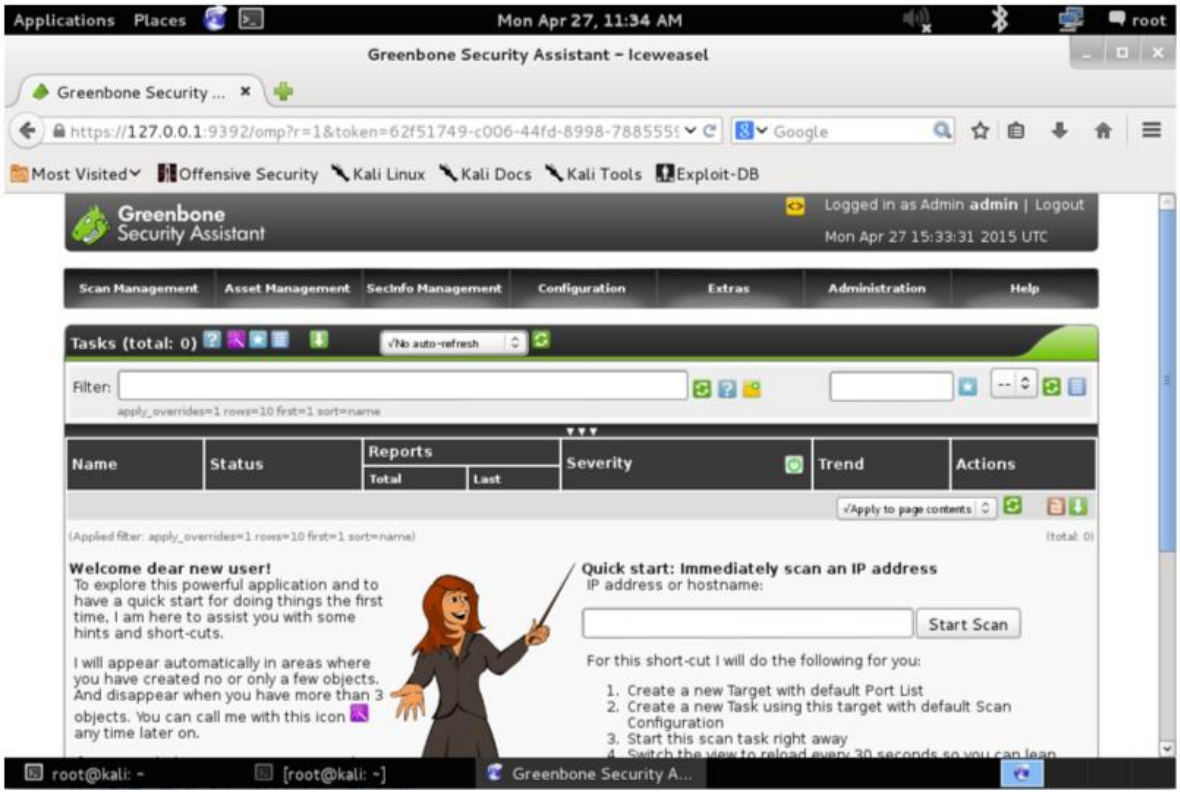



Hình 1-10: Giao diện công cụ Nessus

### 1.4.2.4 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




Hình 1-11: Giao diện OpenVAS

### 1.4.2.5 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 1-12: Công cụ Kerio Control

# CHƯƠNG 2: PHÁT HIỆN VÀ PHÂN TÍCH LỖ HỔNG BẢO MẬT VỚI NESSUS

## 2.1 Giới thiệu phần mềm Nessus

Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại.

Ban đầu Nessus là một dự án nguồn mở "Nessus Project" được đề xuất bởi Renaud Derasion vào năm 1998, mã nguồn của các thành phần được công bố công khai

Nessus còn là một trong những sản phẩm được đánh giá cao trên toàn thế giới, với tính năng đa dạng, thống kê toàn diện về hệ thống đầy đủ,phát hiện những dữ liệu nhạy cảm và phân tích lỗ hổng, đáp ứng cao về nhu cầu bảo mật

Nessus có thể chạy trên nhiều nền tảng khác nhau như: UNIX, LINUX, Mac OS, Windows

Nessus cho phép:

- Lỗ hổng cho phép một hacker từ xa kiểm soát hoặc truy cập dữ liệu nhạy cảm trên hệ thống.
- Cấu hình sai (ví dụ như chuyển tiếp thư mở, các bản vá lỗi bị thiếu,...).
- Mật khẩu mặc định, một vài mật khẩu thường được sử dụng, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển
- Tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại
- Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS).
- Các thành phần của Nessus:

- Nessus Engine: nhận, thực thi và trả lời lại các câu yêu cầu quét của người dùng. Việc quét các lỗ hổng được thực hiện theo các chỉ dẫn của các plugin
- Nessus Plugin: hệ thống file của ngôn ngữ kịch bản NASL, gồm các file định nghĩa .inc và file kịch bản .nasl.
- Nessus Server: thực hiện các yêu cầu quét của người dùng, sau đó phân tích, tổng hợp, trả lại kết quả cho Nessus client
- Nessus Client: hiện thị kết quả quét cho người dùng thông qua trình duyệt web
- Nessus Knowledge Base: "Cơ sở dữ liệu đã biết" của Nessus cho phép các plugin sau tận dụng dữ liệu của plugin trước đó. Điều này giúp Nessus dễ dàng mở rộng và tăng tốc độ thực thi

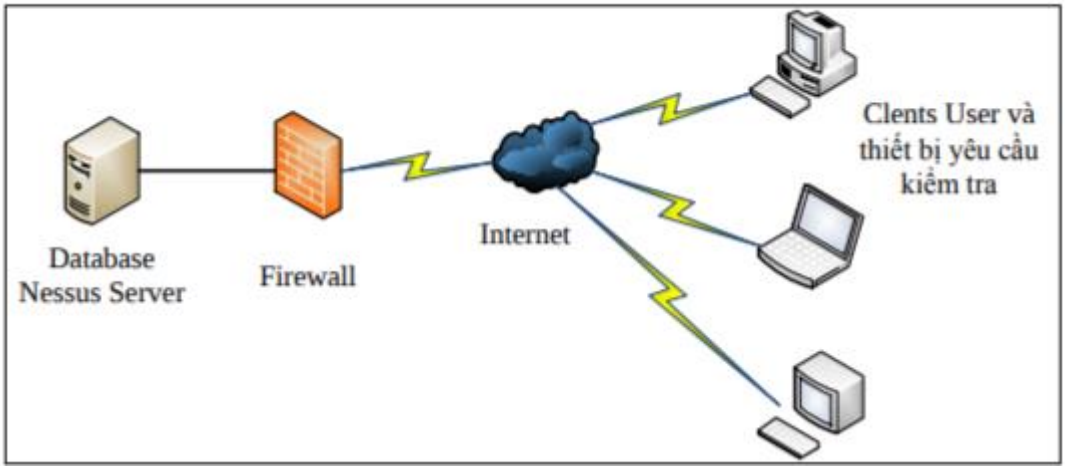
## 2.2 Các mô hình triển khai Nessus

### 2.2.1 Mô hình kiến trúc Nessus Client-Server

Ban đầu, Server sẽ tổng hợp tất cả các lỗi bảo mật hiện nay. Khi một máy tính

Client yều cầu được kiểm tra các lỗi có tồn tại trên máy tính của mình hay không, đầu tiên chúng phải được kiểm tra xem có kết nối tới server hay không, sau khi đã kiểm tra kết nối chúng sẽ được quét tùy thuộc vào các mức độ yêu cầu khi quét.

Mô hình này sẽ dựa vào kết quả sau khi máy Client yêu cầu kiểm tra, và dựavào những lỗi đã được xác định có thể đưa ra những những hướng giải quyết một cách nhanh nhất.




Hình 2-1: Mô hình Client-Sever

### 2.2.2 Mô hình Nessus Knowledge Base.

Mô hình Nessus Knowledge Base là gì?

Mô hình này khá đơn giản nó thu thập danh sách các lỗi bảo mật khác đang được thử nghiệm. Nó cho phép bổ sung, hoặc chia sẻ những thông tin về hệ thống đang được kiểm tra.

Phương thức hoạt động của Nessus Knowledge Base

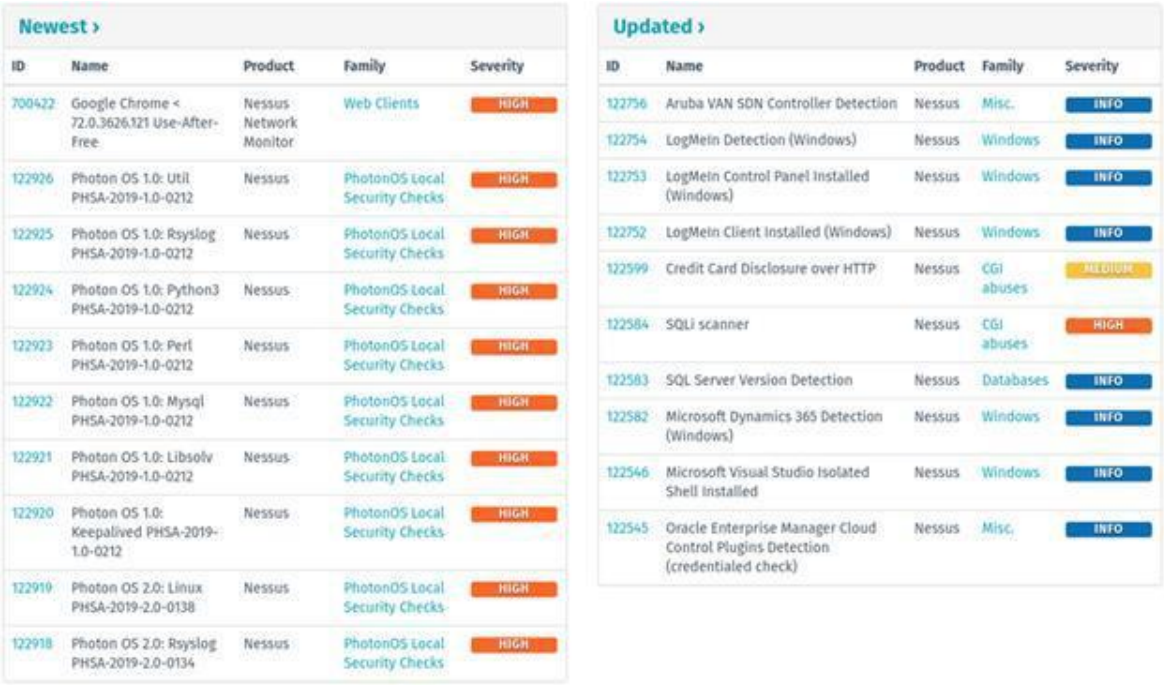
Giả sử chúng ta thực hiện quét kiểm tra lỗi bảo mật trên trang Server at5akma.com, quá trình kiểm tra hoàn tất và không thấy một lỗi bảo mật nào có trên đó. Lúc này Nessus Knowledge Base được tạo ra cho máy chủ này (/usr/local/var/Nessus/users/mh/ kbs/at5a.com) cho thấy khoảng 1800 lỗi, Người ta phải nhớ rằng Nessus Knowledge Base cũng chỉ có khoảng 1725 lỗi đã được trusted. Và những thông số đó được sử dụng cho những nghiên cứu sau này để đảm bảo rằng liên tục cập nhật những lỗi bảo mật mới nhất.

### 2.2.3 Mô hình Nessus Plugin.

Là một chương trình dùng để kiểm tra tính bảo mật của một trang web từ xa, máy tính cục bộ hay những thiết bị bảo vệ thông tin

Mô hình hoạt động của Nessus Plugin khá đơn giản, ta có thể dùng gia diện hoặc dùng command line để quét. Bằng việc sử dụng Plugin đã có sẵn sau khi cài để kiểm tra tính bảo mật.

Khi thông tin về các lỗ hổng mới được phát hiện và phát hành vào phạm vi công cộng chung, Tenable Research thiết kế các chương trình để phát hiện chúng. Các chương trình này được đặt tên plugin và được viết bằng Ngôn ngữ kịch bản tấn công Nessus (NASL). Các plugin chứa thông tin về lỗ hổng, một tập hợp các hành động khắc phục đơn giản và thuật toán để kiểm tra sự hiện diện của vấn đề bảo mật. Tenable Research đã xuất bản



Newest ›

| ID | Name | Product | Family | Severity |
|---|---|---|---|---|
| 700422 | Google Chrome < 72.0.3626.121 Use-After-Free | Nessus Network Monitor | Web Clients | HIGH |
| 122926 | Photon OS 1.0: Util PHSA-2019-1.0-0212 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122925 | Photon OS 1.0: Rsyslog PHSA-2019-1.0-0212 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122924 | Photon OS 1.0: Python3 PHSA-2019-1.0-0212 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122923 | Photon OS 1.0: Perl PHSA-2019-1.0-0212 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122922 | Photon OS 1.0: Mysql PHSA-2019-1.0-0212 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122921 | Photon OS 1.0: Libsolv PHSA-2019-1.0-0212 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122920 | Photon OS 1.0: Keepalived PHSA-2019-1.0-0212 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122919 | Photon OS 2.0: Linux PHSA-2019-2.0-0138 | Nessus | PhotonOS Local Security Checks | HIGH |
| 122918 | Photon OS 2.0: Rsyslog PHSA-2019-2.0-0134 | Nessus | PhotonOS Local Security Checks | HIGH |

Updated ›

| ID | Name | Product | Family | Severity |
|---|---|---|---|---|
| 122756 | Aruba VAN SDN Controller Detection | Nessus | Misc. | INFO |
| 122754 | LogMein Detection (Windows) | Nessus | Windows | INFO |
| 122753 | LogMein Control Panel Installed (Windows) | Nessus | Windows | INFO |
| 122752 | LogMein Client Installed (Windows) | Nessus | Windows | INFO |
| 122599 | Credit Card Disclosure over HTTP | Nessus | CGI abuses | MEDIUM |
| 122584 | SQLi scanner | Nessus | CGI abuses | HIGH |
| 122583 | SQL Server Version Detection | Nessus | Databases | INFO |
| 122582 | Microsoft Dynamics 365 Detection (Windows) | Nessus | Windows | INFO |
| 122546 | Microsoft Visual Studio Isolated Shell Installed | Nessus | Windows | INFO |
| 122545 | Oracle Enterprise Manager Cloud Control Plugins Detection (credentialed check) | Nessus | Misc. | INFO |

Hình 2-2: Mô hình Nessus Plugin

## 2.3 Cài đặt Nessus

Như đã nói ở phần trên Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại

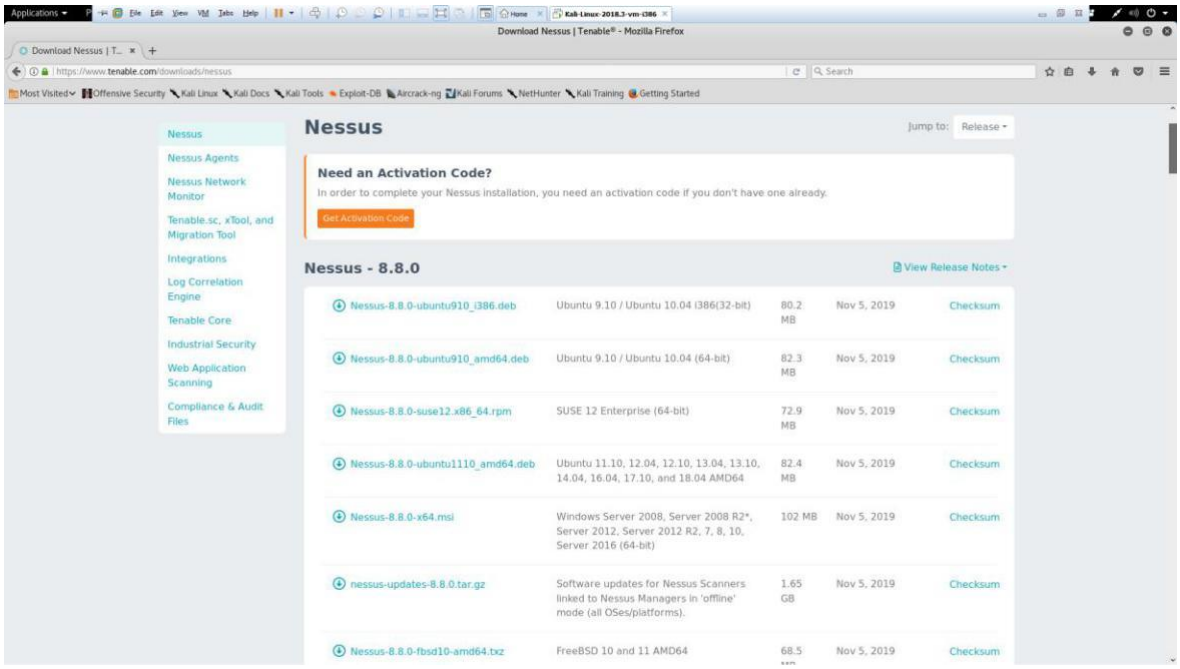
Tuy nhiên miễn phí bản Nessus Home và tính phí Nessus Professional, thật ra 2 bản này khác nhau là giới hạn IP, bản Home có thể scan một lúc 16 IP và bản Pro là không giới hạn

Sau đây là bản cài đặt Nessus trên nền tảng Kali Linux

Bước 1: Tải gói cài đặt từ trang trủ Tenable:

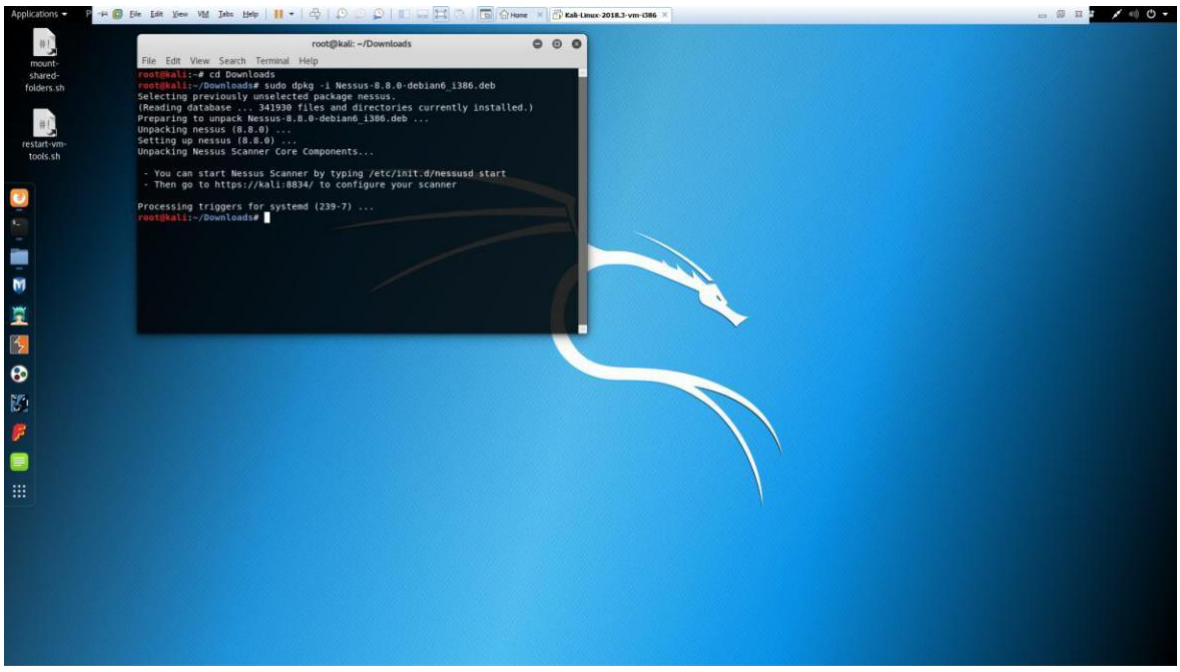
http://www.tenable.com/downloads/Nessus

Gói tin: Nessus-8.8.0-debian6_i386.deb




Hình 2-3: Trang dowload Nessus

Bước 2: Dùng terminal chạy lệnh cài đặt




Hình 2-4 Chạy cài đặt Nessus

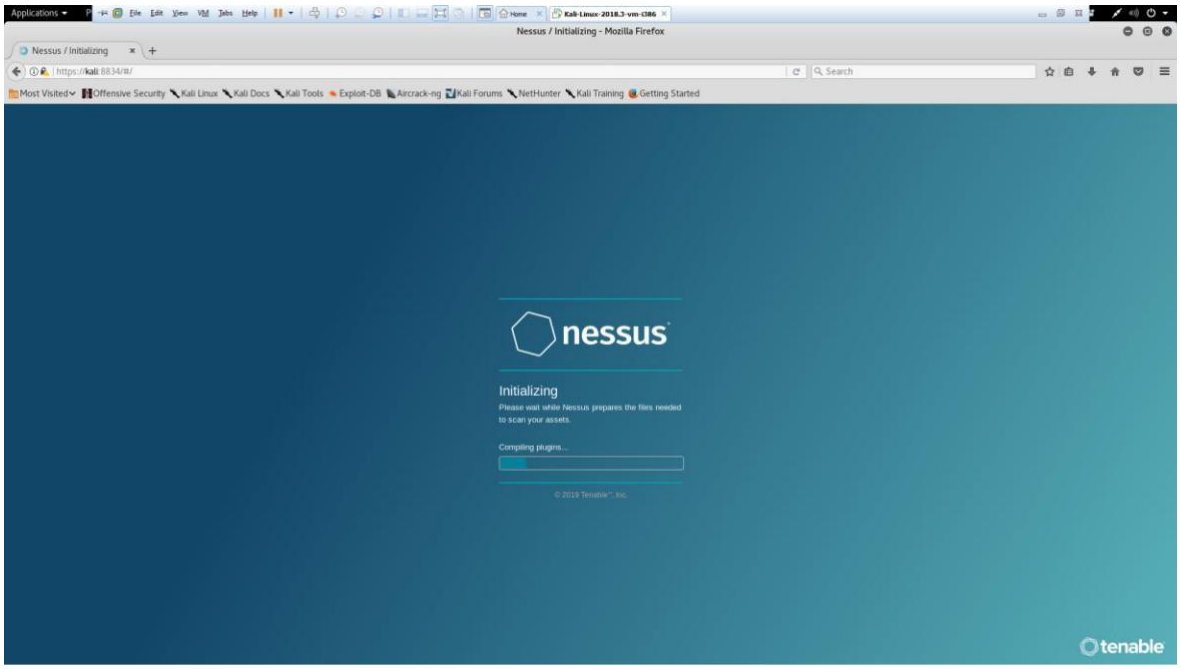
```
root@kali:~# cd Downloads
root@kali:~/Downloads# sudo dpkg -i Nessus-8.8.0-debian6_i386.deb
```

Hình 2-5 Câu lệnh cài đặt

Sau khi hoàn thành bước cài đặt ta dùng câu lệnh sau để truy cập vào địa chỉ Nessus :


Hình 2-6 Lệnh khởi động Nessus

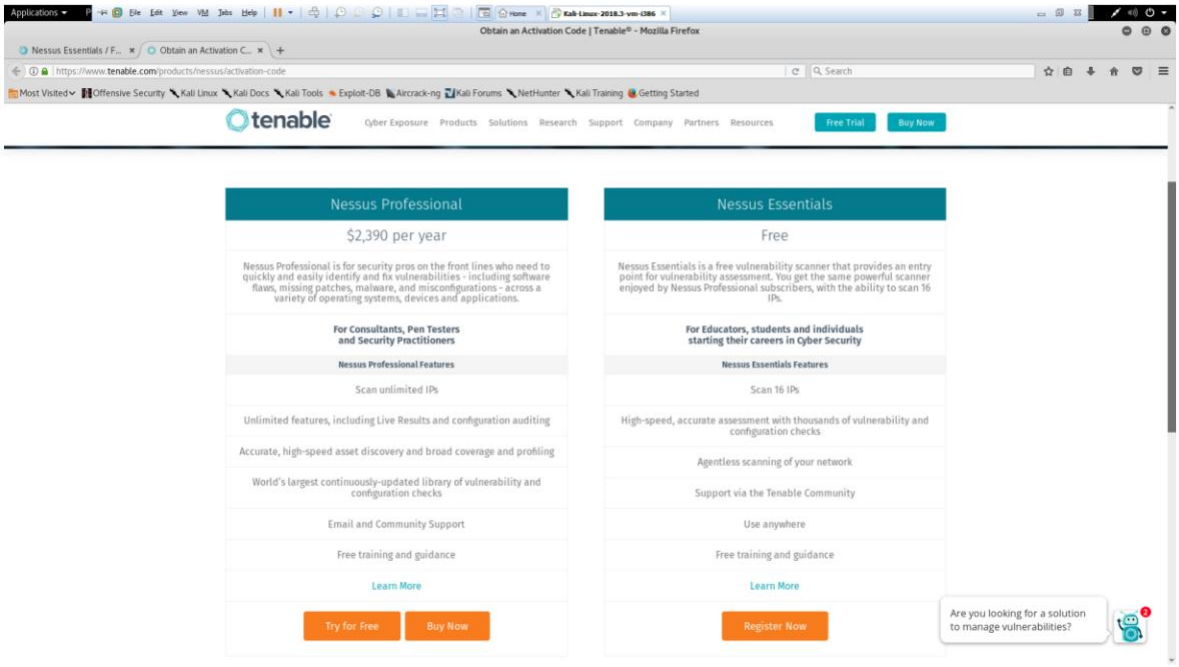
Mở đường dẫn “https://[ IP máy chủ]:8834/” ( Đường dẫn sẽ được hiển thị trong bước cài đặt phía ) trong trình duyệt.




Hình 2-7: Nessus tự động cập nhật các plugin

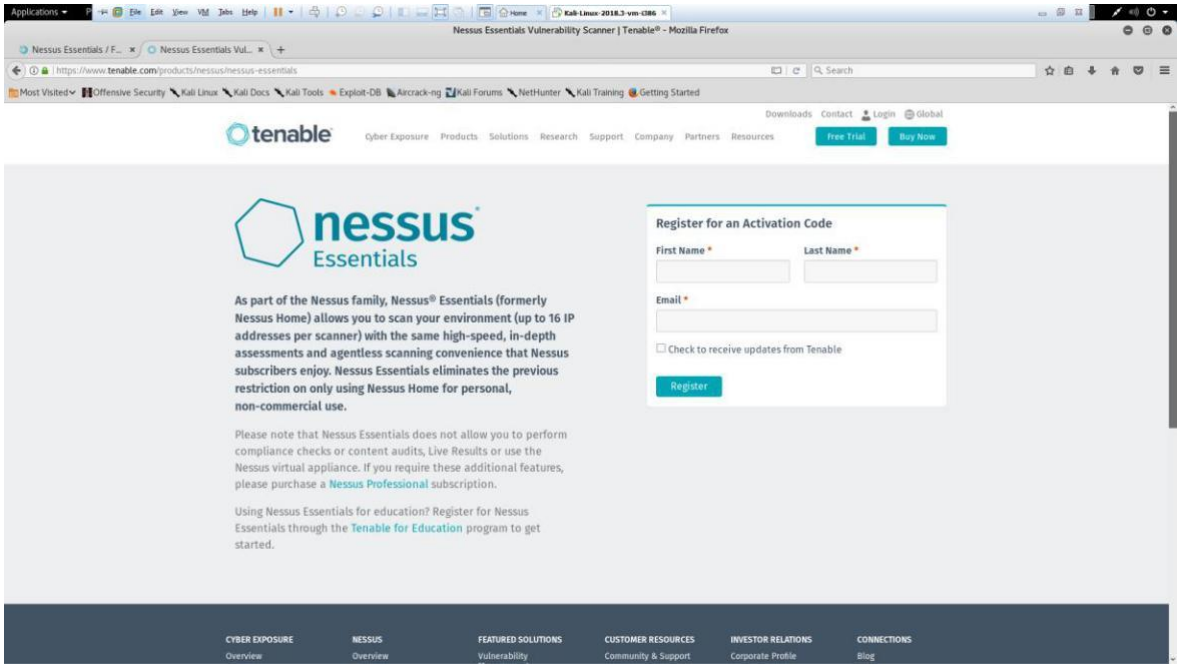
Sau khi cập nhật xong, cần phải đăng nhập vào đường dẫn để có thể kích hoạt Nessus

Truy cập vào đường dẫn: https://www.tenable.com/products/Nessus/active-code để lấy mã kích hoạt



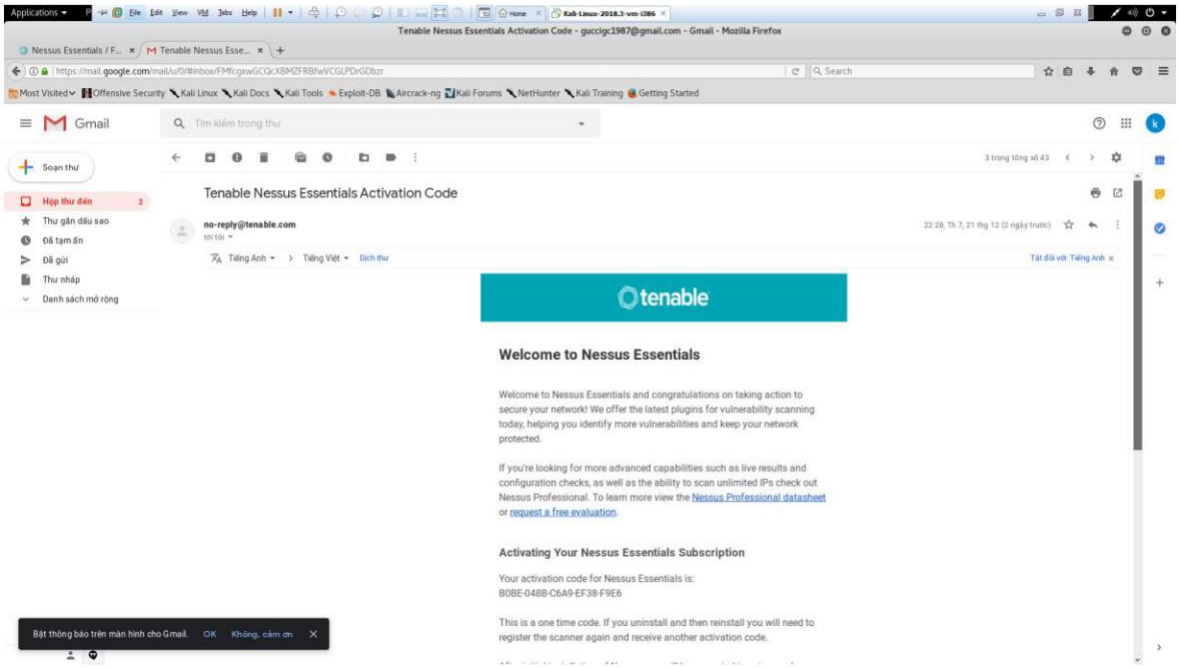

Hình 2-8: Lấy mã kích hoạt Nessus

Sau đó điền thông tin cá nhân và email

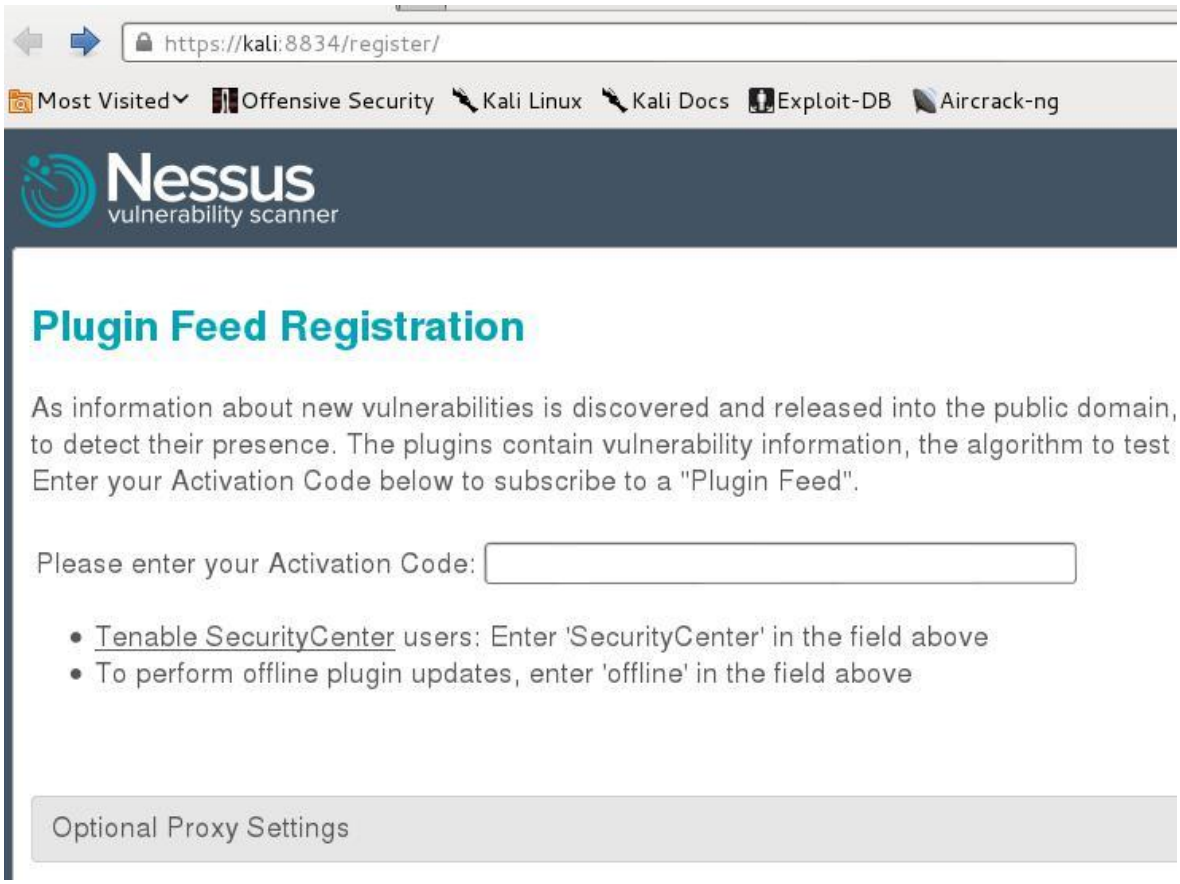



Hình 2-9: Điền thông tin

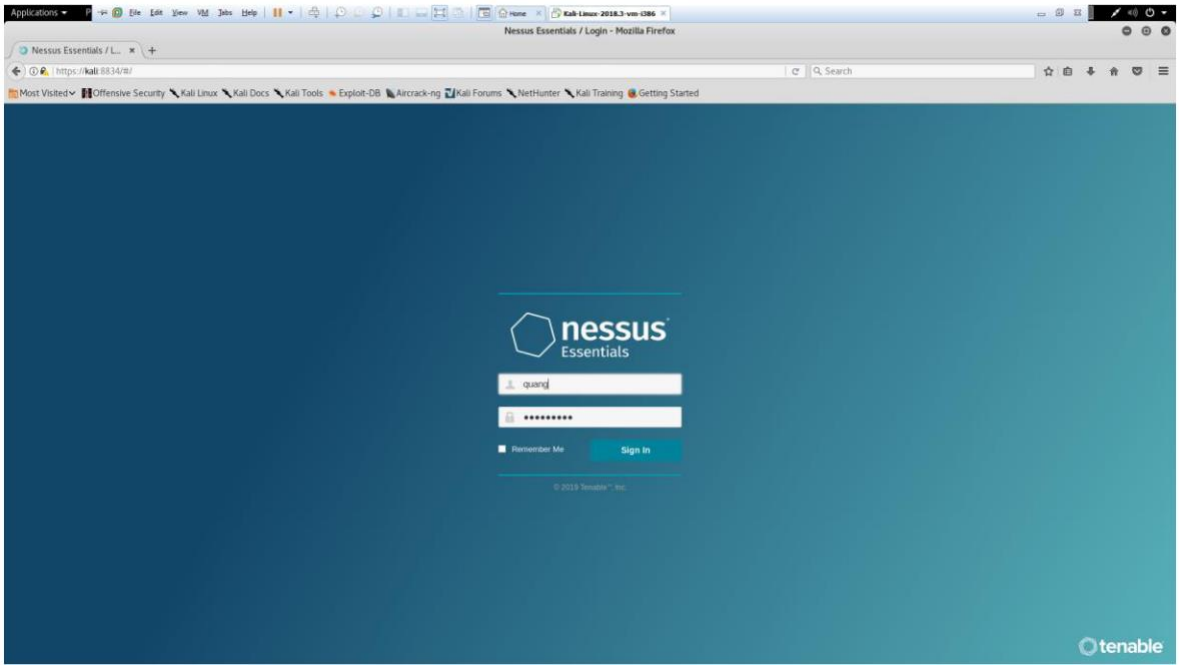
Tiếp theo ta đăng nhập vào mail để lấy mã kích hoạt Nessus và bắt đầu đăng nhập vào công cụ Nessus




Hình 2-10: Vào Mail để lấy mã

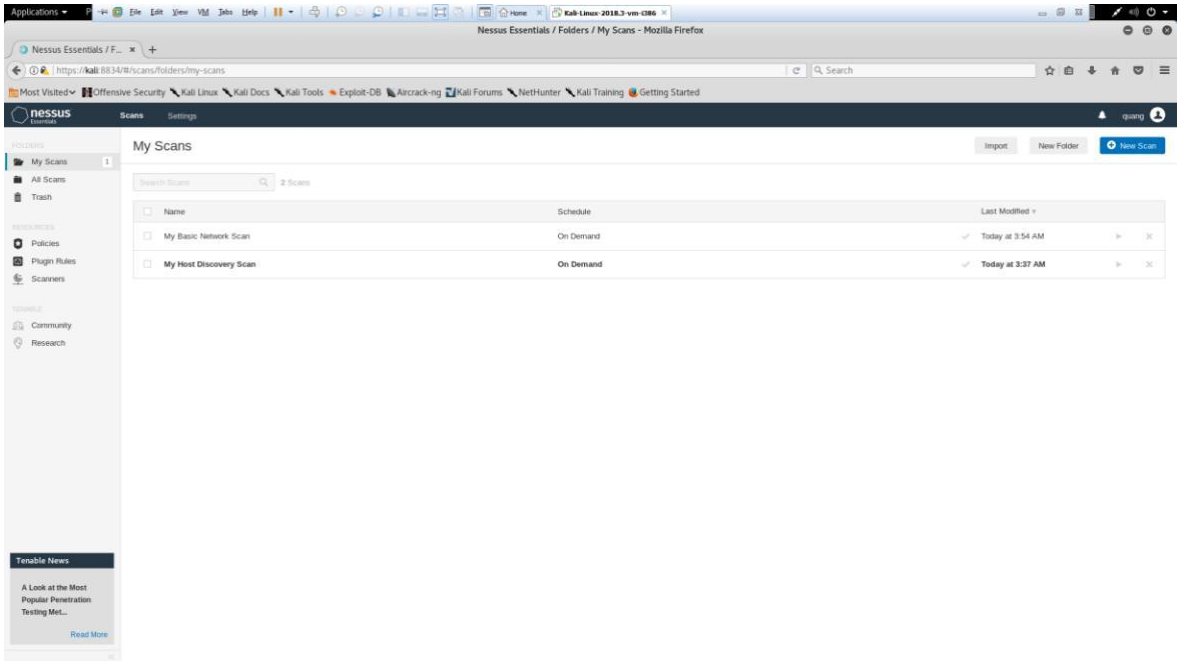



Hình 2-11: Nhập mã để kích hoạt Nessus




Hình 2-12: Giao diện đăng nhập Nessus

Sau khi hoàn thành cài đặt và đăng nhập vào hệ thống thì giao diện ban đầu sẽ như hình đây cũng là Tab My Scans nơi mà lưu trữ, liệt kê kết quả quét bạn đã tiến hành, hiện đang chạy hoặc đã được import.




Hình 2-13: Giao diện sau khi đăng nhập vào công cụ Nessus

# CHƯƠNG 3: THỰC NGHIỆM

## 3.1 Mô hình triển khai thực nghiệm

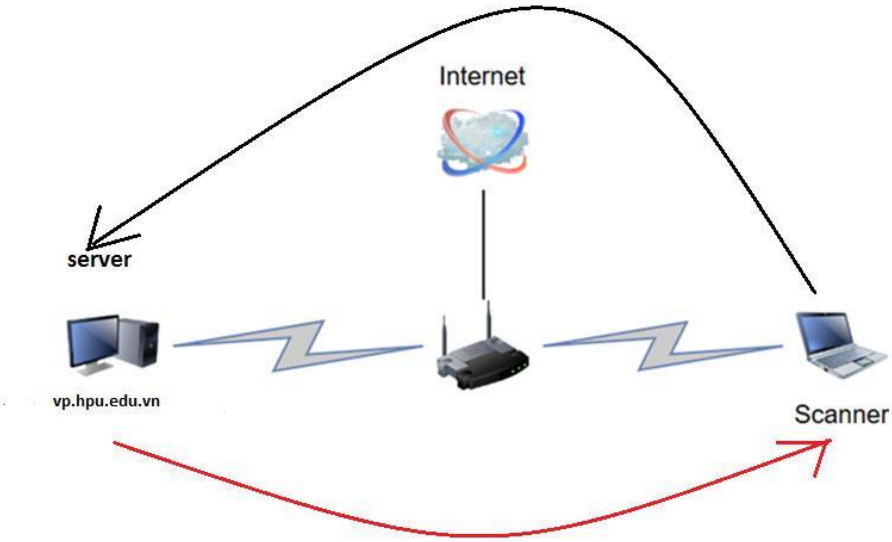
### 3.1.1 Phát biểu bài toán

Sử dụng công cụ Nessus đã cài đặt để tiến hành kiểm tra lỗ hổng trên một số website

### 3.1.2 Mô hình

Xây dựng mô hình quét Nessus gồm có

- Một máy ảo có hệ điều hành Kali Linux
- Công cụ Nessus
- Mạng Internet

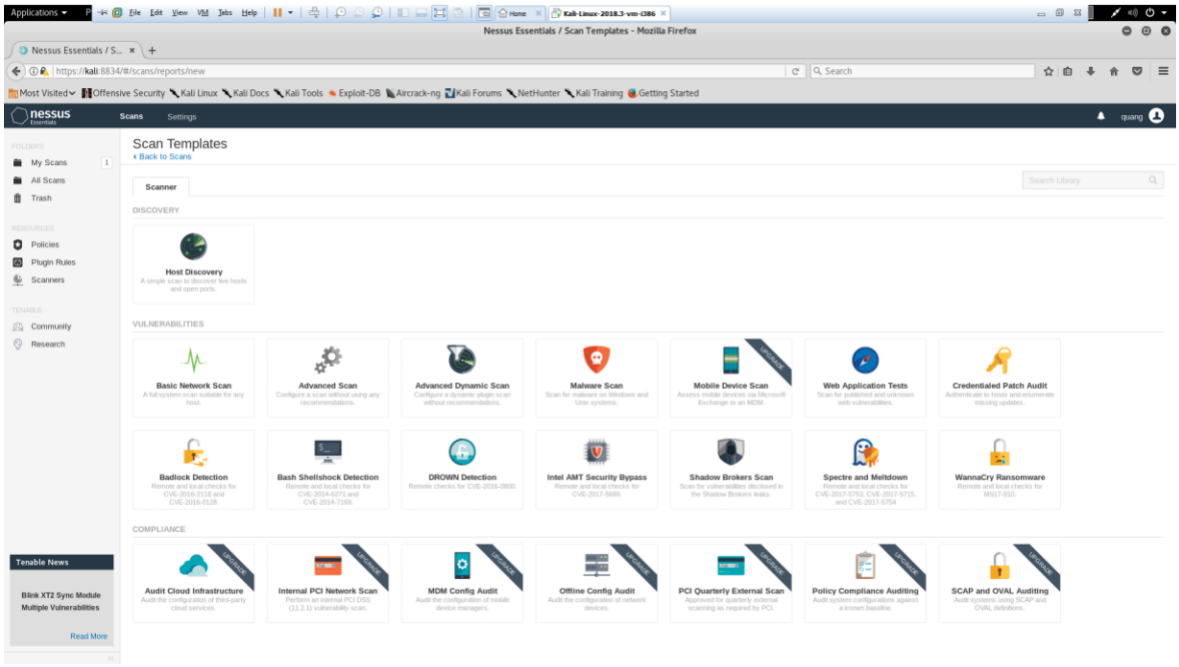



Hình 3-1: Mô hình quét lỗ hổng Nessus

Với mô hình này ta sử dụng công cụ Nessus đã cài sẵn ở máy ảo có hệ điều hành Kaili Linux có internet. Sau khi quét công cụ Nessus sẽ thông báo cho chúng ta trang web đã có những lỗ hổng gì cần được khắc phục

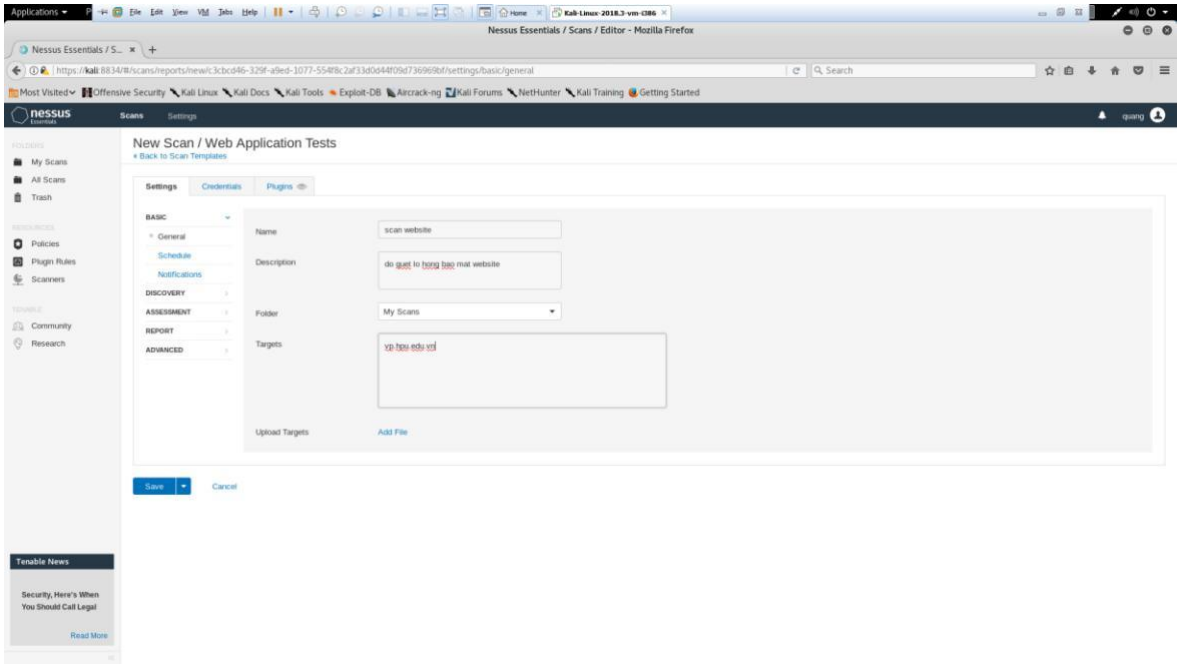
## 3.2 Các bước triển khai

Bước 1: Trên trang Scan chọn New Scans và sau đó chọn Web Application Test trên trang Scan Templates.



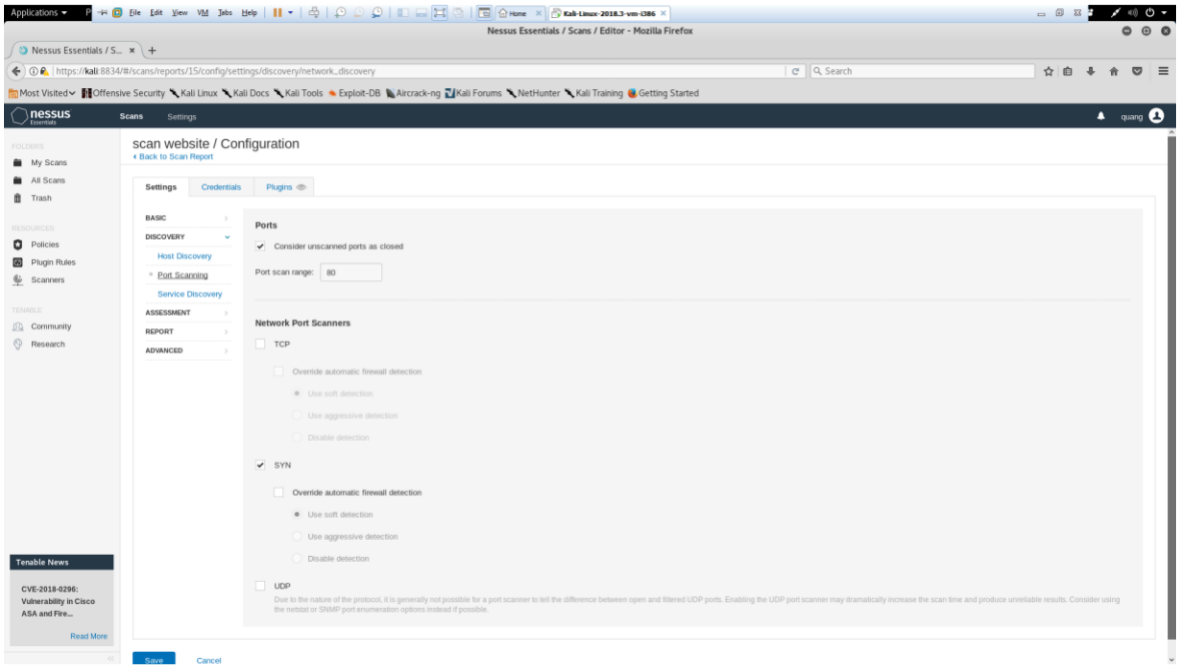

Hình 3-2: Scan TemPlates

Bước 2: Sau khi chọn Web Application ta điền các thông tin cần thiết



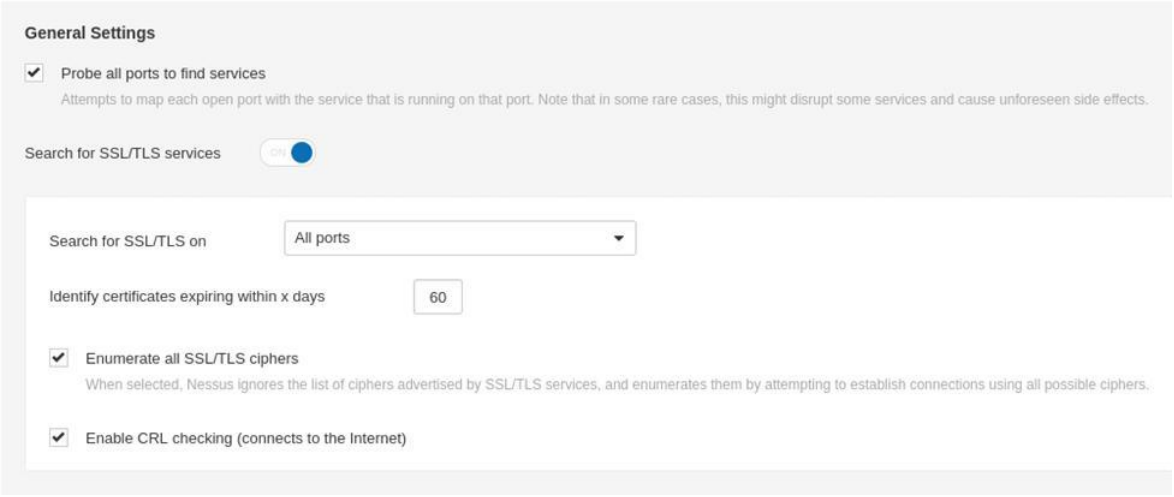

Hình 3-3: Điền các thông tin trong Web application

Bước 3: Đặt Phạm vi Quét Cổng Cổng thành chỉ các cổng mà ứng dụng Web đích đang sử dụng. Trong ví dụ này, chúng ta đang chạy trên cổng 80.



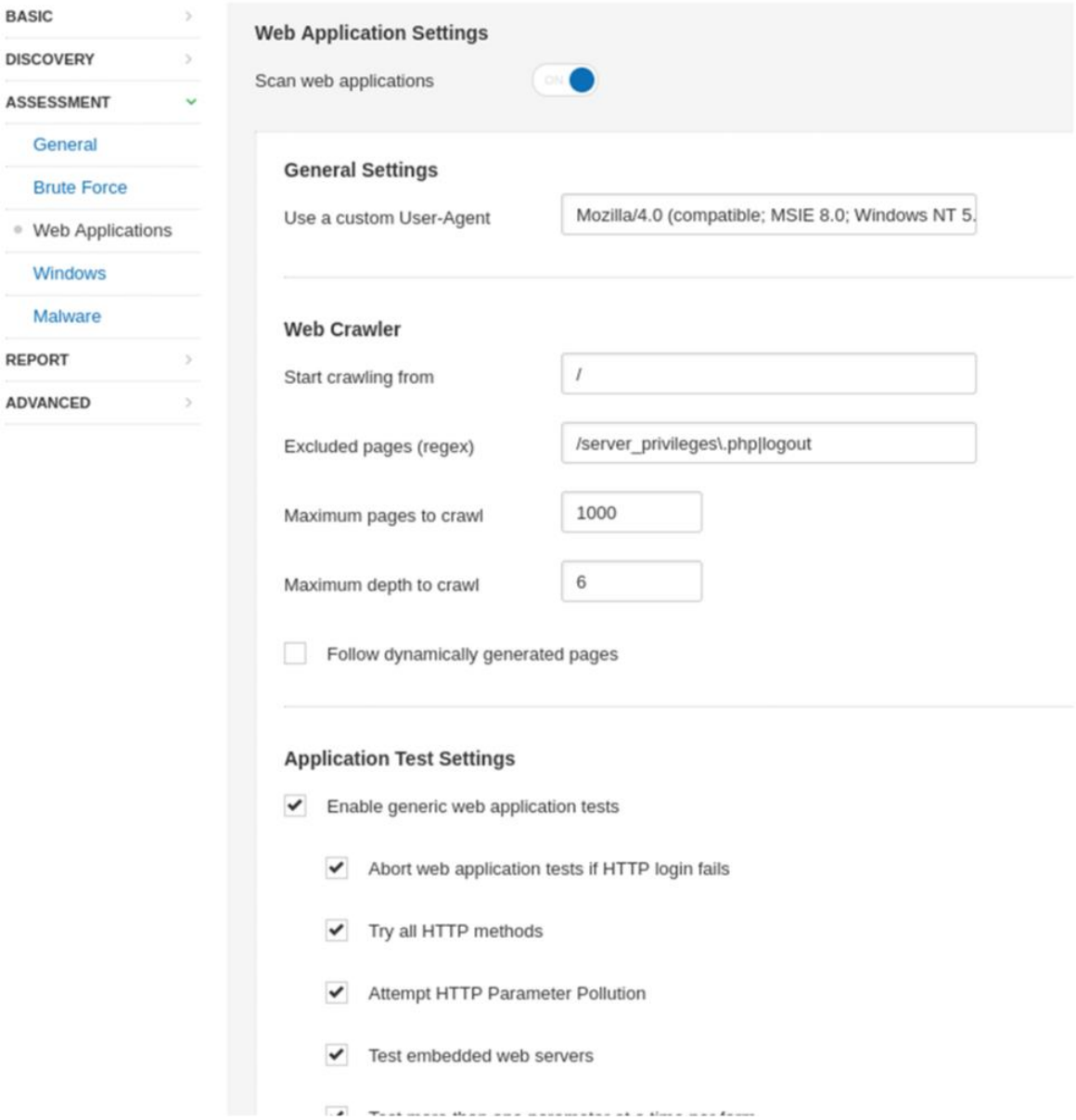

Hình 3-4: Thay đổi trường phạm vi quét cổng.

Bước 4: Tùy chỉnh Service Discovery tùy theo mục đích quét .



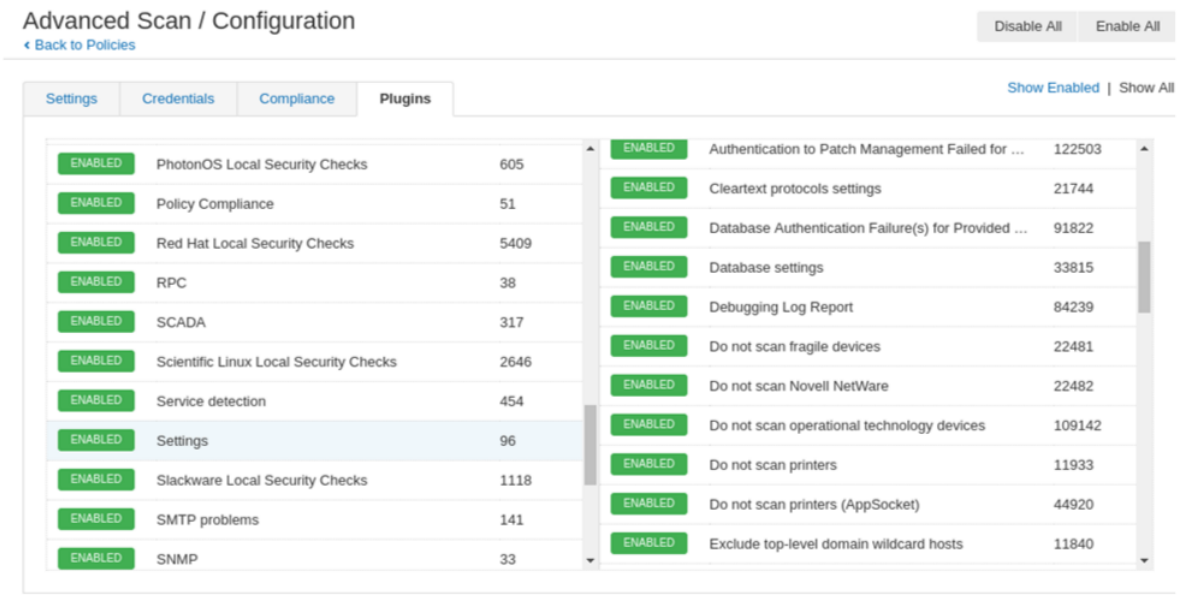

Hình 3-5: Service Discovery.

Bước 5: Tùy chỉnh ASSESSMENT ¸ trong ASSESSMENT nên tập trung vào Web Application khi thiết lập policies cho quét ứng dụng web application.




Hình 3-6: Tùy chỉnh ASSESSMENT.

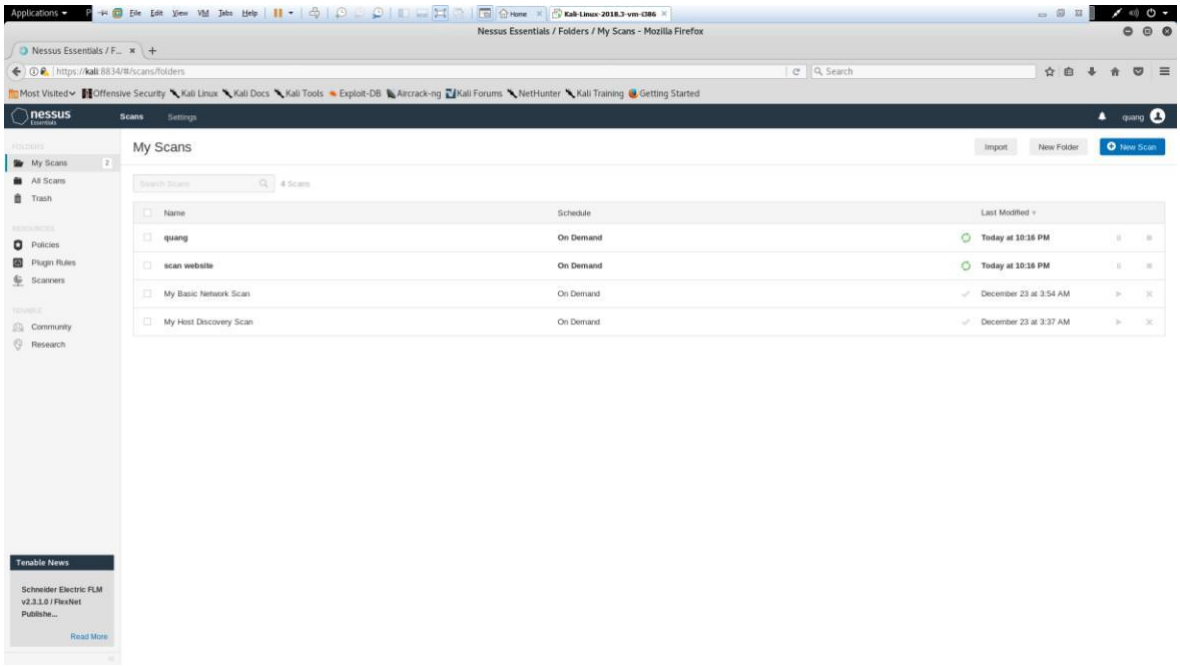
Bước 6: Chọn plugin cần thiết.




Hình 3-7: Plugin có trên Nessus.

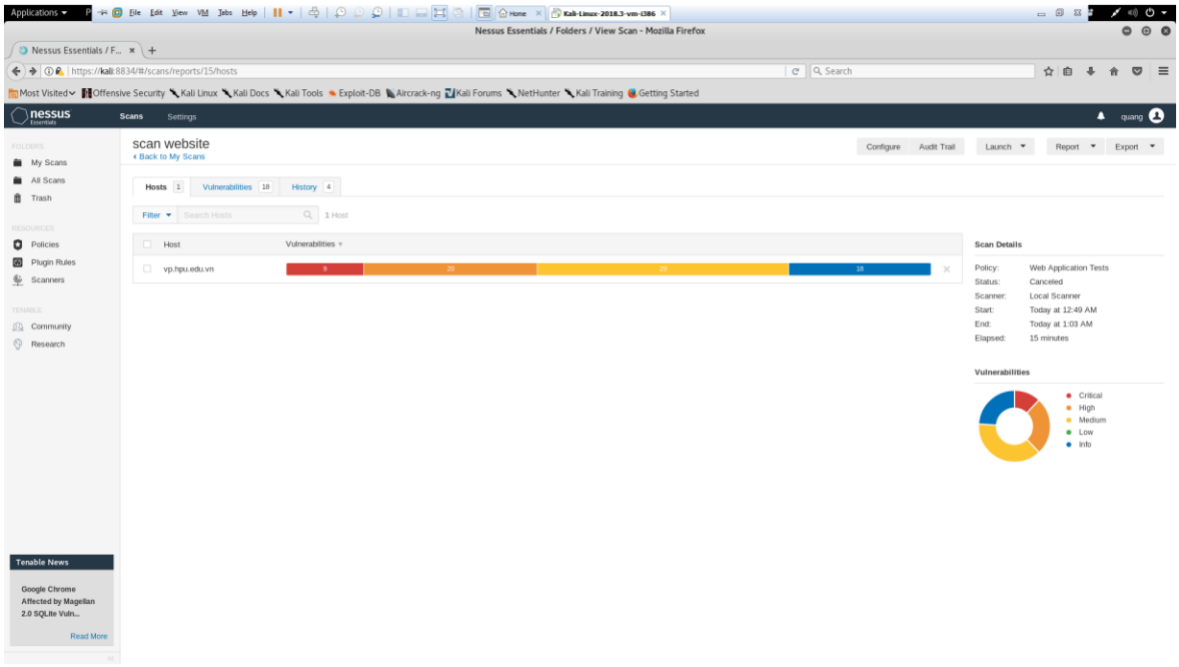
Sau khi chọn các Plugin chúng ta chọn Save để lưu thông tin

Bước 7: Tại ngoài My scans ta chọn Launch để Nessus tự động quét ứng dụng web mà website ta đã chọn




Hình 3-8: Quá trình quét ứng dụng web

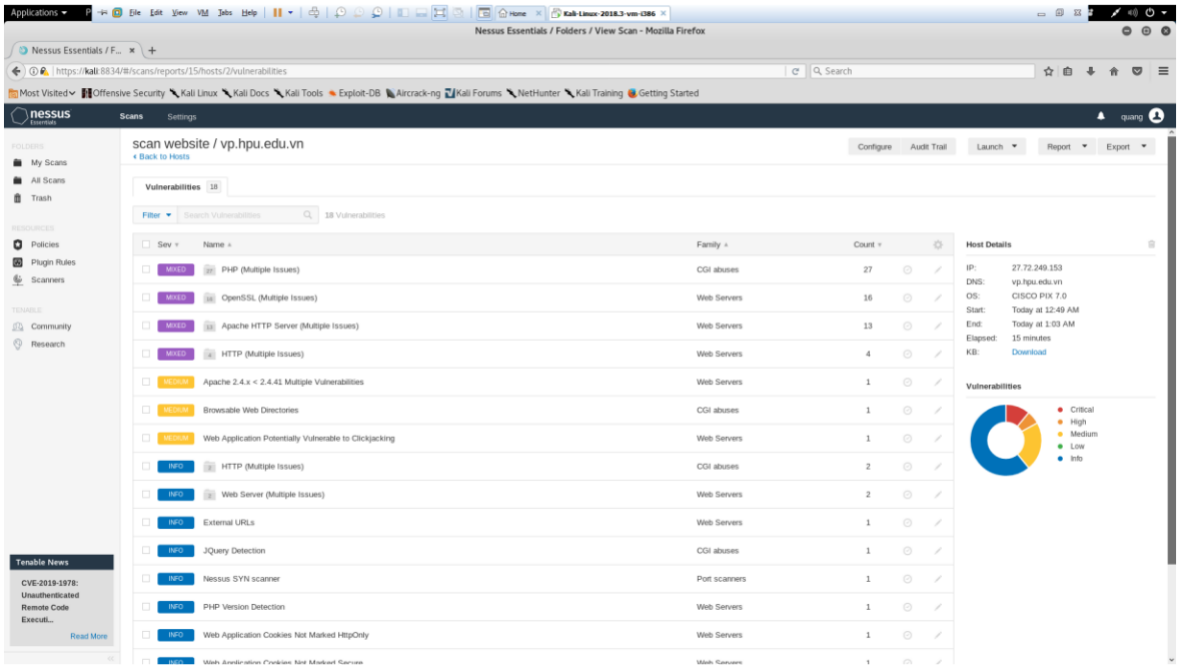
Sau khi hoàn thành các bước như trên thì chúng ta thu được kết quả của quá trình quét ứng dụng




Hình 3-9: Kết quả dò quét tổng quan

Nessus đưa ra kết quả quét rất trực quan giúp người dùng hoặc quản trị viên có thể dễ dàng nhận thấy được số lượng lỗ hổng cũng như mức độ nguy hiểm của các lỗ hổng này.

Để có được thông tin chi tiết hơn về các lỗ hổng tồn tại trên website ta chỉ cần chuyển qua Tab Vulnerabilities, ở tab này Nessus cung cấp khá đầy đủ thông tin về một lỗ hổng bảo mật như: Tên, mức độ nguy hiểm, mô tả, cách khắc phục .v.v




Hình 3-10: Các lỗi đã quét được

# KẾT LUẬN

Trong đồ án em đã nghiên cứu về công cụ hỗ trợ bảo mật Nessus, sử dụng công cụ Nessus để tìm lỗ hổng website

Em đã cố gắng nghiên cứu sử dụng tài liệu kết hợp với kiến thức đã được học. Em đã hiểu về an toàn bảo mật mạng, công cụ Nessus và sử dụng công cụ trong việc tìm lỗ hổng web. Tuy nhiên do thời gian và khả năng còn hạn chế, nên em vẫn chưa tìm hiểu kĩ về công cụ này cũng như những tính năng khác của công cụ

Trong thời gian tới em sẽ tiếp tục và nghiên cứu sâu hơn về công cụ Nessus này để có thể sử dụng công cụ trong việc bảo mật

Em xin chân thành cảm ơn

# TÀI LIỆU THAM KHẢO

[1]. https://whitehat.vn/threads/huong-cai-dat-Nessus-tren-kali-linux.7603/

[2]. https://vnpro.vn/thu-vien/tong-quan-lo-hong-bao-mat-va-mot-so-ky-thuat-tan-cong-vao-mang-2443.html

[3]. https://123doc.org//document/3908482-huong-dan-ra-soat-va-khai-thac-lo-hong-bang-Nessus.htm

[4]. https://whitehat.vn/threads/Nessus-%E2%80%93-cong-cu-tro-giup-pentest-he-thong.6871/