

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

**PHÁT HIỆN LỖ HỔNG BẢO MẬT**  
**TRONG MẠNG LAN DỰA TRÊN PHẦN MỀM**  
**NGUỒN MỞ**

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

**Ngành: Công nghệ Thông tin**

Sinh viên thực hiện : **Nguyễn Bá Đức**

Mã sinh viên : **1512101010**

Giáo viên hướng dẫn: **TS. Ngô Trường Giang**

## 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 thông 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.

Sinh viên

## 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 kỹ 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 đề án tốt nghiệp : “ **Phát hiện lỗ hổng bảo mật trong mạng LAN dựa trên phần mềm nguồn mở**”. Và mục tiêu của em là nghiên cứu, tìm hiểu về những giải pháp phát hiện lỗ hổng bảo mật để giúp cho mọi người có thể phát hiện lỗi sớm, và đưa ra những giải pháp tốt nhất cho hệ thống mạng của mình.

Đề án gồm ba chương:

- Chương 1: Tổng quan về bảo mật mạng
- Chương 2: Giới thiệu công cụ dò quét lỗ hổng bảo mật
- Chương 3: Thực nghiệm

**MỤC LỤC**

<b>LỜI CẢM ƠN.....</b>	<b>1</b>
<b>MỞ ĐẦU.....</b>	<b>2</b>
<b>MỤC LỤC .....</b>	<b>3</b>
<b>DANH MỤC HÌNH VẼ.....</b>	<b>5</b>
<b>CHƯƠNG 1: TỔNG QUAN VỀ BẢO MẬT MẠNG.....</b>	<b>7</b>
1.1 Khái niệm về bảo mật mạng .....	7
1.2 Các loại lỗ hổng bảo mật .....	7
1.2.1 Lỗ hổng theo khu vực phát sinh .....	8
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.....	9
1.2.4 Lỗ hổng đã biết, lỗ hổng zero-day.....	10
1.3 Tấn công mạng .....	11
1.3.1 Các giai đoạn tấn công.....	12
1.3.2 Các phương thức tấn công mạng.....	14
<b>CHƯƠNG 2: CÔNG CỤ DÒ QUÉT LỖ HỔNG BẢO MẬT.....</b>	<b>18</b>
2.1 Giới thiệu và Kali Linux.....	18
2.2 Ưu điểm của Kali Linux .....	19
2.2.1 Tính tương thích kiến trúc.....	20
2.2.2 Hỗ trợ mạng không dây tốt hơn .....	20
2.2.3 Khả năng tùy biến cao .....	20
2.2.4 Dễ dàng nâng cấp các phiên bản Kali trong tương lai .....	20
2.2.5 Tài liệu hướng dẫn đa dạng.....	21
2.3 Một vài công cụ trên Kali Linux.....	21
2.3.1 Nmap (Network Mapper).....	22
2.3.2 John The Ripper (JTR).....	22
2.3.3 Wiresharks.....	23
2.3.4 Burp Suite.....	24
2.3.5 OWASP Zed.....	25
2.3.6 Aircrack-NG.....	25

---

2.3.7	Ettercap.....	26
2.3.8	Nikto.....	26
2.4	Cài đặt Kali Linux trên máy ảo VMware .....	27
2.4.1	Yêu cầu cài đặt Kali Linux .....	27
2.4.2	Điều kiện cài đặt tiên quyết.....	27
2.4.3	Quy trình cài đặt Kali Linux .....	27
<b>CHƯƠNG 3: THỰC NGHIỆM.....</b>		<b>39</b>
3.1	Triển khai công cụ Zenmap .....	39
3.1.1	Mô hình .....	39
3.1.2	Các bước thực hiện .....	40
3.1.3	Triển khai .....	41
3.2	Triển khai công cụ Nikto .....	45
3.2.1	Mô hình .....	45
3.2.2	Các bước thực hiện .....	46
3.2.3	Triển khai .....	46
<b>KẾT LUẬN.....</b>		<b>51</b>
<b>TÀI LIỆU THAM KHẢO.....</b>		<b>52</b>

**DANH MỤC HÌNH VẼ**

Hình 1-1: Mô hình quá trình thăm dò vào 1 hệ thống mạng.....	12
Hình 1-2: Quét trộm đối tượng với công hoạt động và không hoạt động .....	13
Hình 1-3: Trình duyệt Browse Attacks .....	14
Hình 2-1: Biểu tượng Nmap Project .....	22
Hình 2-2: Biểu tượng John the Ripper .....	22
Hình 2-3: Biểu tượng Wireshark .....	23
Hình 2-4: Biểu tượng Burp Suite .....	24
Hình 2-5: Biểu tượng ZAPROXY .....	25
Hình 2-6: Biểu tượng AirCrack-NG .....	25
Hình 2-7: Biểu tượng Ettercap.....	26
Hình 2-8: Biểu tượng Nikto.....	26
Hình 2-9: Giao diện tạo máy ảo.....	27
Hình 2-10: Giao diện chọn cấu hình .....	28
Hình 2-11: Giao diện chọn vị trí Kali Linux ISO.....	28
Hình 2-12: Giao diện chọn hệ điều hành và phiên bản.....	29
Hình 2-13: Giao diện đặt tên và vị trí cho máy ảo .....	29
Hình 2-14: Giao diện chọn dung lượng ổ đĩa.....	30
Hình 2-15: Giao diện hoàn thành cài đặt máy ảo .....	30
Hình 2-16: Giao diện mới khởi động Kali .....	31
Hình 2-17: Giao diện chọn ngôn ngữ.....	31
Hình 2-18: Giao diện chọn vị trí địa lí.....	32
Hình 2-19: Giao diện chọn bộ gõ.....	32
Hình 2-20: Giao diện đặt tên cho máy ảo .....	33
Hình 2-21: Giao diện cấu hình miền.....	33
Hình 2-22: Giao diện phân vùng ổ đĩa.....	34
Hình 2-23: Giao diện chọn ổ đĩa.....	34
Hình 2-24: Giao diện chọn kiểu lược đồ phân vùng.....	35
Hình 2-25: Giao diện chọn phân vùng xong và ghi thay đổi vào đĩa.....	35
Hình 2-26: Giao diện xác nhận ghi các thay đổi vào đĩa .....	36
Hình 2-27: Giao diện chọn mạng để dùng bất kì mạng nào .....	36
Hình 2-28: Giao diện thông tin ủy nhiệm HTTP.....	37
Hình 2-29: Giao diện cài đặt bộ nạp khởi động GRUB vào mục ghi .....	37
Hình 2-30: Giao diện thiết bị nơi cần cài đặt bộ nạp khởi động .....	38
Hình 2-31: Giao diện cài đặt xong.....	38
Hình 3-1: Mô hình Zenmap .....	40
Hình 3-2: Giao diện Username .....	41
Hình 3-3: Giao diện Password.....	42
Hình 3-4: Giao diện khởi động Zenmap trong Kali Linux .....	43
Hình 3-5: Giao diện các cổng tcp đang mở.....	43
Hình 3-6: Giao diện thông tin về máy nạn nhân .....	44
Hình 3-7: Mô hình Nikto .....	46

---

Hình 3-8: Giao diện Username .....	47
Hình 3-9: Giao diện Password .....	47
Hình 3-10: Giao diện khởi động Terminal.....	48
Hình 3-11: Giao diện quét với Nikto .....	49
Hình 3-12: Giao diện lỗi OSVDB.....	49

## CHƯƠNG 1: TỔNG QUAN VỀ BẢO MẬT MẠNG

### 1.1 Khái niệm về bảo mật mạng

Bảo mật mạng là bảo vệ dữ liệu an toàn trên môi trường trực tuyến không ai có thể truy cập lấy cắp hay điều khiển được những thông tin của mình. 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 tin

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 tặng 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 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 tổng tiền.

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 Các giai đoạn tấn công

#### 1.3.1.1 Quá trình thăm dò tấn công



Hình 1-1: Mô hình quá trình thăm dò vào 1 hệ thống mạng

#### 1.3.1.2 Thăm dò (Reconnaissance)

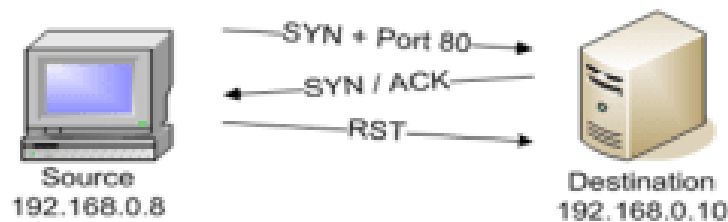
Thăm dò mục tiêu là một trong những bước quan trọng để biết những thông tin trên hệ thống mục tiêu. Hacker sử dụng kỹ thuật này để khám phá hệ thống mục tiêu đang chạy trên hệ điều hành nào, có bao nhiêu dịch vụ

đang chạy trên các dịch vụ đó, cổng dịch vụ nào đang đóng và cổng nào đang mở, gồm hai loại:

- Passive: Thu thập các thông tin chung như vị trí địa lý, điện thoại, email của các cá nhân, người điều hành trong tổ chức.
- Active: Thu thập các thông tin về địa chỉ IP, domain, DNS,... của hệ thống

### 1.3.1.3 Quét hệ thống (Scanning)

Quét thăm dò hệ thống là phương pháp quan trọng mà Attacker thường dùng để tìm hiểu hệ thống và thu thập các thông tin như địa chỉ IP cụ thể, hệ điều hành hay các kiến trúc hệ thống mạng. Một vài phương pháp quét thông dụng như: quét cổng, quét mạng và quét các điểm yếu trên hệ thống.



Hình 1.2 Quét trộm đối với cổng không hoạt động



Hình 1.3 Đối với cổng hoạt động

Hình 1-2: Quét trộm đối tượng với cổng hoạt động và không hoạt động

### 1.3.1.4 Chiếm quyền điều khiển (Gaining access)

- Mức hệ điều hành/ mức ứng dụng
- Mức mạng
- Từ chối dịch vụ

### 1.3.1.5 Duy trì điều khiển hệ thống (Maintaining access)

- Upload/download biến đổi thông tin

### 1.3.1.6 Xóa dấu vết(Clearing tracks)

Sau khi bị tấn công thì hệ thống sẽ lưu lại những vết do attacker để lại. Attacker cần xoá chúng đi nhằm tránh bị phát hiện.

## 1.3.2 Các phương thức tấn công mạng

### 1.3.2.1 Tấn công vào trình duyệt(Browse Attacks)



Hình 1-3: 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.

### 1.3.2.2 Tấn công vét cạn (Brute Force Attacks)

Hiểu một cách đơn giản, Brute Force Attacks là hình thức tấn công mạng sử dụng mật khẩu, tên người dùng... để tự động kết hợp chúng với nhau

cho tới khi chính xác. Kiểu tấn công Brute Attacks này có thể mất thời gian vì vậy tin tặc thường sử dụng phần mềm tự động hóa để nhập hàng trăm nghìn mật khẩu. Để phòng tránh kiểu tấn công này, người quản trị website cần cấu hình module giới hạn số lần đăng nhập sai cho mỗi tài khoản, hoặc giới hạn số lần đăng nhập từ các địa chỉ IP.

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

Ddos Attack hay còn gọi là tấn công từ chối dịch vụ – đứng thứ ba trong danh sách.

Phương thức tấn công Ddos chủ yếu nhằm vào các mục tiêu như: website, máy chủ trò chơi, máy chủ DNS... làm chậm, gián đoạn hoặc đánh sập hệ thống.

Theo khảo sát của Kaspersky, có tới 5.200 trường hợp bị tấn công từ chối dịch vụ Ddos tại 29 quốc gia khác nhau trong năm 2017 vừa qua. Dự đoán, tần suất và phương thức tấn công Ddos sẽ tăng lên trong năm 2018, người dùng hãy hết sức cẩn thận.

### 1.3.2.4 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.



### 1.3.2.5 Tấn công bằng phần mềm độc hại

Ba hình thức tấn công mạng thông qua phần mềm độc hại chủ yếu là:

- Email Phishings: Tin tặc thường lừa đảo người dùng bằng cách tạo ra những thông điệp để thu hút sự tò mò của nhân. Nhưng thực chất, những tệp này sẽ chứa các phần mềm độc hại và phát tán ngay sau khi người dùng tải về máy.
- Tấn công bằng website độc hại (Malicious Websites): Với cách thức này, kẻ tấn công thường tạo một trang web giả mạo có giao diện y hệt với giao diện của website gốc. Sau khi nạn nhân truy cập vào địa chỉ website đó, phần mềm độc hại sẽ từ từ thâm nhập vào hệ thống của họ. Điển hình cho ví dụ này là các vụ giả mạo website ngân hàng, website ngành hàng không vừa xảy ra trong năm 2016 – 2017.
- Tấn công bằng quảng cáo chứa mã độc (Malvertising): Đối với một số kẻ tấn công thông minh, chúng sẽ tận dụng mạng lưới các quảng cáo để gắn mã độc vào đó. Khi click vào quảng cáo độc hại này, người dùng sẽ bị điều hướng tới một website khác có chứa phần mềm độc hại. Nguy hiểm hơn, trong một số trường hợp người dùng không click vào quảng cáo cũng có thể bị tấn công.

### 1.3.2.6 Tấn công website(Website Attacks)

Các dịch vụ tấn công công cộng chẳng hạn như thông qua ứng dụng website, cơ sở dữ liệu thường là đối tượng mục tiêu tấn công nhằm vào website.

Các cuộc tấn công mạng thông qua lỗ hổng website chủ yếu là lỗ hổng SQL Injection, XSS, và path Traversal.

### 1.3.2.7 Kiểu tấn công rà quét(Scan Attacks)

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.

### 1.3.2.8 Kiểu tấn công mạng khác

Ngoài 7 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.

## CHƯƠNG 2: CÔNG CỤ DÒ QUÉT LỖ HỔNG BẢO MẬT

### 2.1 Giới thiệu và Kali Linux

Kali Linux là một bản phân phối Linux dựa trên nền tảng Debian nhằm vào kiểm tra thâm nhập và kiểm tra bảo mật nâng cao.

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.

Kali Linux được phát hành vào ngày 13 tháng 3 năm 2013 với tư cách là một bản dựng lại hoàn chỉnh từ đầu của BackTrack Linux, tôn trọng hoàn toàn các tiêu chuẩn phát triển Debian. Offensive Security đã công bố phiên bản tiến hóa của hệ điều hành BackTrack, tên của nó là Kali (được xem như phiên bản BackTrack 6), Kali là tên nữ thần của người Hindu, hàm ý sự biến đổi và khả năng hủy diệt hay có lẽ là tên một môn võ thuật của người Philippine ... Kali Linux về cơ bản là một bản phân phối của Debian Linux, nó tích hợp sẵn các công cụ bảo mật cực kì mạnh mẽ, cùng với các công cụ được sắp xếp theo từng chuyên mục giúp nâng cao khả năng hoạt động hiệu quả. Đi kèm là giao diện Gnome với hình ảnh đồ họa đẹp mắt và hiệu suất mượt mà, đem lại cho người dùng một cảm nhận và trải nghiệm tốt về độ chuyên nghiệp.

Phiên bản mới nhất là Kali Linux 2018 Phiên bản Kali Linux 1.x có tên là Kali Moto, bản 2.0 gọi là Kali Sana. Từ Sau năm 2016, Kali Linux đã không còn đặt tên như thế nữa, mà thay vào đó nó được đặt tên dựa vào năm phát hành và số cập nhật trong năm, gọi chung là Rolling Replease. Do là một bản phân phối của Debian Linux nên kali có thể cài đặt và sử dụng hầu hết các công cụ của các hệ điều hành khác thuộc bản phân phối Debian như

Ubuntu và cả những ứng dụng trên Windows bằng phần mềm Wine hoặc máy ảo VMWare.

Kali Linux có thể được sử dụng hoàn toàn độc lập như một hệ điều hành trên Desktop bình thường, nó còn có thể được cài đặt trên một LiveUSB hay thậm chí là một hệ điều hành cho thiết bị IOT như Raspberry PI. Các phiên bản cũ của Kali đều hoàn toàn có thể nâng cấp lên Kali phiên bản mới nhất chỉ cần vài dòng lệnh. Kali Linux với tiền thân là hệ điều hành Backtrack đây là một hệ điều hành mã nguồn mở được tự do phát triển, nó cơ bản dựa trên nền tảng của Debian, đây cũng là hệ điều hành được các chuyên gia về bảo mật sử dụng nhiều nhất và được đánh giá rất nhiều về bảo mật.

Kali bắt đầu xuất hiện vào năm 2006 và trong nhiều năm qua nó đã không ngừng cải tiến và phát triển để đạt được một vị trí nhất định trong cộng đồng hacker và những người làm bảo mật trên khắp thế giới. Kali linux chứa hơn 200 công cụ hack và kiểm tra bảo mật nổi tiếng tiến hóa từ BackTrack. Vì vậy, ngày nay thật khó để tìm thấy một người nào đó quan tâm đến an toàn thông tin mà chưa từng nghe về BackTrack.

Kali Linux là một hệ điều hành rất hữu ích đối với những chuyên gia đánh giá bảo mật, là một hệ điều hành tập hợp và phân loại gần như tất cả các công cụ thiết yếu nhất mà bất kỳ một chuyên gia bảo mật nào cũng cần dùng đến khi tác nghiệp. Đối với những người chưa biết BackTrack, thì nói một cách ngắn gọn nhất, BackTrack là một bản phân phối Linux dựa trên nền tảng hệ điều hành Ubuntu, với nhiều công cụ bảo mật được phân loại rõ ràng để sử dụng cho mục đích bảo mật và hacker.

## 2.2 Ưu điểm của Kali Linux

Kali phát triển trên nền tảng hệ điều hành Debian, do vậy nó cũng thừa hưởng các công cụ

- Đầu tiên là các Repository (Kho lưu trữ phần mềm) được đồng bộ hóa với các Repository của Debian nên nó có thể dễ dàng có được các bản

cập nhật vá lỗi bảo mật mới nhất và các cập nhật Repository. Duy trì cập nhật (up-to-date) đối với các công cụ Penetration Test là một yêu cầu vô cùng quan trọng giúp cải thiện tính năng và nâng cao hiệu suất hoạt động của các công cụ tích hợp.

- Một lợi thế khác đó là các công cụ trong hệ điều hành Kali đều tuân theo chính sách quản lý gói của Debian. Điều này có vẻ như không quan trọng lắm nhưng nó đảm bảo rõ ràng về mặt cấu trúc hệ thống bao quát tổng thể, nó cũng giúp cho chúng ta có thể dễ dàng hơn trong việc xem xét hoặc thay đổi mã nguồn của các công cụ.

### **2.2.1 Tính tương thích kiến trúc**

Một ưu điểm cực kỳ quan trọng trong Kali là nó đã cải tiến khả năng tương thích của nó với cấu trúc ARM(Advanced RISC Machine). Chúng ta có thể tự build Kali trên một Raspberry Pi hoặc build một bản để chạy được trên Samsung Galaxy Note.

### **2.2.2 Hỗ trợ mạng không dây tốt hơn**

Một trong những vấn đề được các nhà phát triển Kali chú trọng phát triển nhiều nhất, chính là việc hỗ trợ một số lượng lớn phần cứng bên trong các thiết bị mạng không dây. Điều này hỗ trợ và giúp ích rất nhiều cho các chuyên gia khi họ thực hiện đánh giá, kiểm tra và rà soát các mạng không dây trong công việc.

### **2.2.3 Khả năng tùy biến cao**

Kali rất linh hoạt trong việc tùy biến giao diện hoặc khả năng sửa đổi hệ thống. Đối với giao diện, giờ đây người dùng có thể lựa chọn cho mình nhiều loại Desktops như GNOME, KDE hoặc XFCE tùy theo sở thích, nhu cầu và thói quen sử dụng.

### **2.2.4 Dễ dàng nâng cấp các phiên bản Kali trong tương lai**

Đây là một tính năng quan trọng đối với bất kỳ ai sử dụng Kali. Với BackTrack trước kia, bất kỳ lúc nào có phiên bản mới được công bố thì người

dùng đều phải xóa bỏ và cài lại mới hoàn toàn. Tuy nhiên, với Kali, nhờ vào sự chuyển đổi sang nền tảng hệ điều hành Debian, Kalilinux đã rất dễ dàng hơn trong việc nâng cấp hệ thống khi có phiên bản mới hơn xuất hiện. Người dùng đơn giản chỉ cần vài dòng lệnh là hệ thống đã được cập nhật không phải cài lại mới hoàn toàn nữa.

### **2.2.5 Tài liệu hướng dẫn đa dạng**

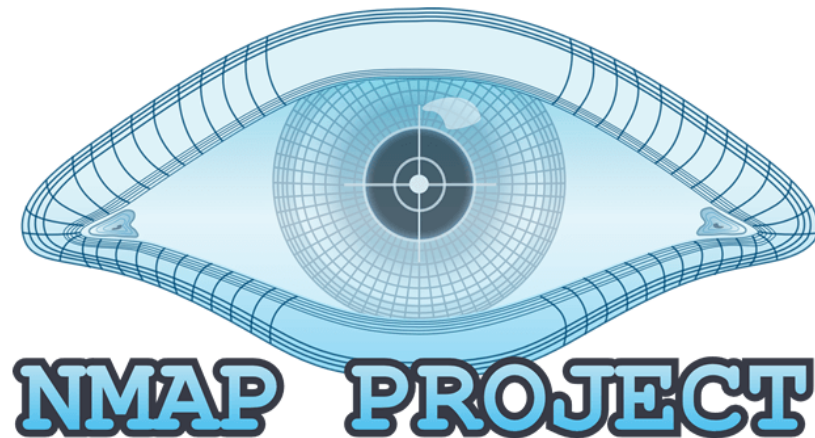
Một điều quan trọng khác, đó là Kali có hỗ trợ rất nhiều tài liệu hướng dẫn trên, điều này giúp cho người sử dụng có thể hiểu rõ về Kali, cũng như biết cách sử dụng những công cụ chuyên dụng khi thực hiện công việc tùy theo nhu cầu. Tóm lại, thì với Kali Linux thì đây không chỉ là một phiên bản mới của BackTrack, mà nó chính là một sự tiến hóa. Mục đích chính của các nhà phát triển Kali là duy trì và cung cấp các bản cập nhật mới nhất để hệ điều hành Kali trở thành sự lựa chọn tốt nhất cho bất cứ ai tìm kiếm một hệ điều hành Pentest. Và đây là một hệ điều hành dành cho công việc đánh giá bảo mật chuyên nghiệp.

## **2.3 Một vài công cụ trên Kali Linux**

Những công cụ Hacking luôn là rất quan trọng đối với người làm bảo mật. Họ cần phải nắm rõ được nguyên lý hoạt động của các phần mềm này, từ đó lên được phương án bảo mật thích hợp nhất. Hầu hết những công cụ này cũng đã được đóng gói sẵn trong hệ điều hành Kali Linux. Về phần mềm hacking, hiện có hơn 300+ công cụ được thiết kế để phục vụ cho công việc này.

Trong đề tài này em xin giới thiệu một số công cụ giúp kiểm tra mức độ an toàn, cũng như những lỗ hổng tồn tại trong hệ thống mạng doanh nghiệp dựa trên những kiến thức đã học và những kiến thức tìm hiểu nâng cao. Em xin được đưa ra những công cụ đánh giá bảo mật chuyên dụng trên Kali Linux.

### 2.3.1 Nmap (Network Mapper)

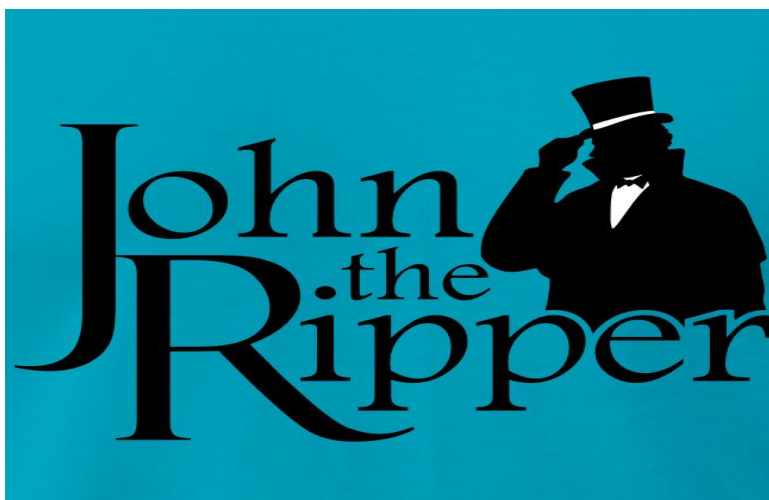


Hình 2-1: Biểu tượng Nmap Project

Nmap được dùng để quét cả hệ thống và tìm ra các cổng nào đang được mở. Với hacker mũ trắng, công cụ này được dùng để phát hiện máy tính nào đang online, và khảo sát bảo mật, các cổng đang mở cũng như service nào đang được chạy.

Công cụ có 2 giao diện GUI và Command Line. Zenmap là giao diện thường được khuyến khích sử dụng dành cho người mới, lần đầu tiên tiếp xúc với Command Line, và sau đó chuyển qua GUI nếu chúng ta thấy tự tin.

### 2.3.2 John The Ripper (JTR)



Hình 2-2: Biểu tượng John the Ripper



Jhon The Ripper là công cụ phổ biến để phá Password, được biết đến nhiều hơn với tên viết tắt JTR. Jhon The Ripper sử dụng những tệp văn bản, còn được gọi là “wordlist”, file này chứa những password thông dụng và những password đã từng bị phá, sau đó công cụ sẽ lần lượt thử từng password cũng như những tổ hợp các text để tìm ra password nạn nhân.

Về phương pháp, Jhon The Ripper khá tương tự với THC Hydra, tuy nhiên JTR được dùng để crack password offline thì THC Hydra lại được dùng để crack password các dịch vụ trực tuyến.

### 2.3.3 Wiresharks



Hình 2-3: Biểu tượng Wireshark

Wireshark là công cụ mã nguồn mở, được dùng để phân tích giao thông mạng của hệ thống, các gói tin... Với tên gọi cũ là Ethereal, Wireshark có thể chặn lưu lượng mạng, từ những thông tin kết nối đến từng bit của gói tin hiệu. Tất cả tác vụ này được thực hiện trong thời gian thực và hiển thị cho người dùng ở định dạng có thể đọc được.

Trong nhiều năm qua, Wireshark đã có nhiều sự thay đổi, nâng cấp đáng giá như là các bộ lọc, màu sắc các gói tin... việc này đã giúp ích nhiều cho nhà quản trị mạng quản lý và phân tích được những gì đang diễn ra trong hệ thống mạng của họ.



### 2.3.4 Burp Suite



Hình 2-4: Biểu tượng Burp Suite

Burp Suite là một ứng dụng nền web, giúp kiểm tra khả năng thâm nhập. Phần mềm là công cụ mạnh mẽ, có nhiều tính năng hacking mà có thể chúng ta đang tìm kiếm. Dưới đây là danh sách các thành phần tính năng của Burp Suite :

- **Intercepting Proxy** : tính năng này cho phép kiểm tra và chỉnh sửa tất cả các gói tin yêu cầu và phản hồi trả về của trình duyệt.
- **Spider** : công cụ tiện dụng dùng để liệt kê tất cả các thư mục và tập tin trên máy chủ.
- **Web Scanner** : phát hiện các lỗ hổng đang hiện diện trên Website.
- **Intruder** : tính năng cho phép tạo và tùy chỉnh các cuộc tấn công để tìm và khai thác các lỗi không mong muốn.
- **Repeater** : chỉnh sửa và gửi trả lại bất cứ gói tin request riêng lẻ nào.
- **Sequencer** : kiểm tra tính ngẫu nhiên của các token (csrf , authenticity\_token ).
- **Extensions** : cho phép người dùng viết và add plugin tự phát triển này vào gói công cụ, hoặc download các bản plugin có sẵn để add thêm, giúp đa dạng hơn trong các cuộc tấn công.

Bản Pro cũng cho phép người dùng Donate những plugin này.

### 2.3.5 OWASP Zed



Hình 2-5: Biểu tượng ZAPROXY

OWASP Zed Attack Proxy ( ZAP ) được biết đến như một công cụ Proxy, có thể dự phòng khá tốt cho công cụ Burp Suite, ưu điểm của ZAP là miễn phí và mã nguồn mở.

Công cụ được phát triển với mục đích tìm những lỗ hổng trong ứng dụng Web. Với cộng đồng người dùng rộng lớn có tên OWASP security Community, người mới làm quen có thể dễ dàng sử dụng cũng như nhận được sự hỗ trợ khá tốt. Chúng ta có thể dùng OWASP Zed Attack Proxy để scan đối tượng, thực hiện các chiến dịch Scan tự động, tìm ra các lỗ hổng, thực hiện test thủ công...

### 2.3.6 Aircrack-NG



Hình 2-6: Biểu tượng AirCrack-NG

Thêm một tool để crack password, tuy nhiên đặc biệt hơn, Aircrack-ng được thiết kế để crack password Wifi. Đối với những người mới lần đầu tiếp xúc với phần mềm này, Aircrack-ng có thể phá các loại pass wifi theo chuẩn 802.11 WEP và WPA-PSK. Cơ chế hoạt động của Tool sẽ chụp các gói tin có

chứa password, sau đó thực hiện giải mã chúng. Aircrack-ng được xem là một trong những Tool hàng đầu trong việc bẻ khóa Password Wifi.

### 2.3.7 Ettercap



Hình 2-7: Biểu tượng Ettercap

Phần mềm mã nguồn mở này được cung cấp miễn phí, và thường được dùng để thực hiện các cuộc tấn công trong mạng Lan. Ettercap được dùng để phân tích các Protocol mạng và theo dõi an ninh hệ thống. Hiện phần mềm có mặt ở hầu hết các hệ điều hành như Windows, Unix, Linux BSD, và các distro khác.

### 2.3.8 Nikto



Hình 2-8: Biểu tượng Nikto

Nikto là trình quét máy chủ web nguồn mở, thực hiện các thử nghiệm toàn diện đối với các máy chủ web cho nhiều mục, bao gồm hơn 6700 tệp / chương trình nguy hiểm tiềm tàng, kiểm tra các phiên bản lỗi thời của hơn 1250 máy chủ và các sự cố cụ thể về phiên bản trên hơn 270 máy chủ.

## 2.4 Cài đặt Kali Linux trên máy ảo VMware

### 2.4.1 Yêu cầu cài đặt Kali Linux

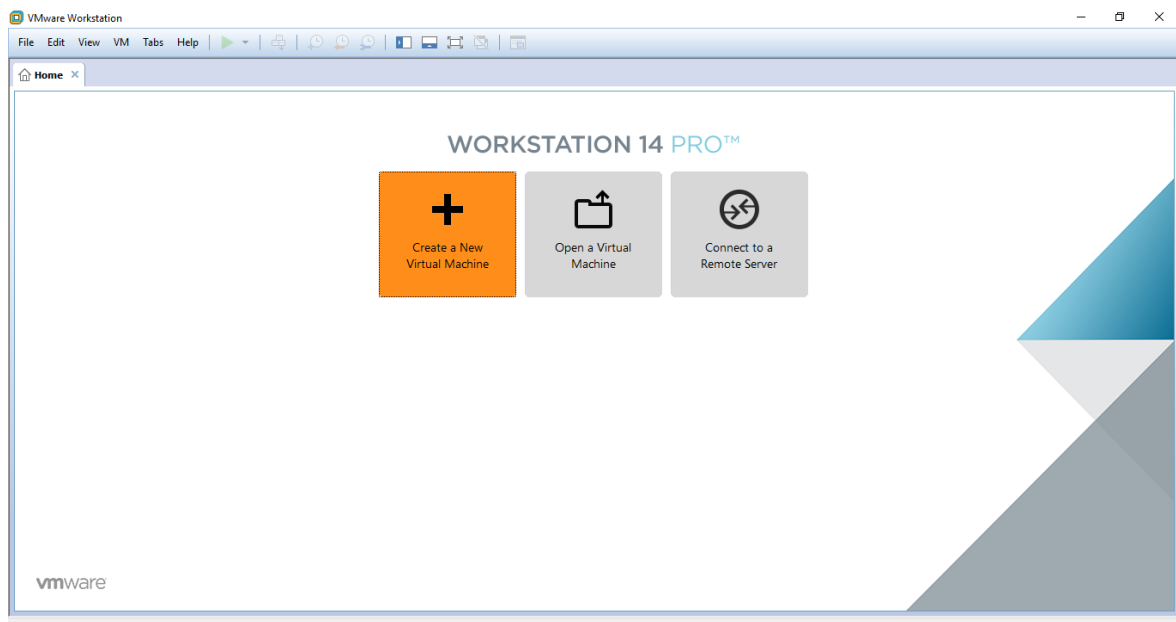
- Có sẵn máy ảo VMware
- Tải Kali Linux ISO từ trên mạng xuống

### 2.4.2 Điều kiện cài đặt tiên quyết

- Dung lượng ổ đĩa tối thiểu phải là 20 GB nếu muốn cài đặt Kali Linux.
- RAM cho cấu trúc i386 và amd64, tối thiểu phải là 1GB, nhưng chúng ta nên có từ 2GB trở lên sẽ tốt hơn.
- Hỗ trợ khởi động CD-DVD/USB.

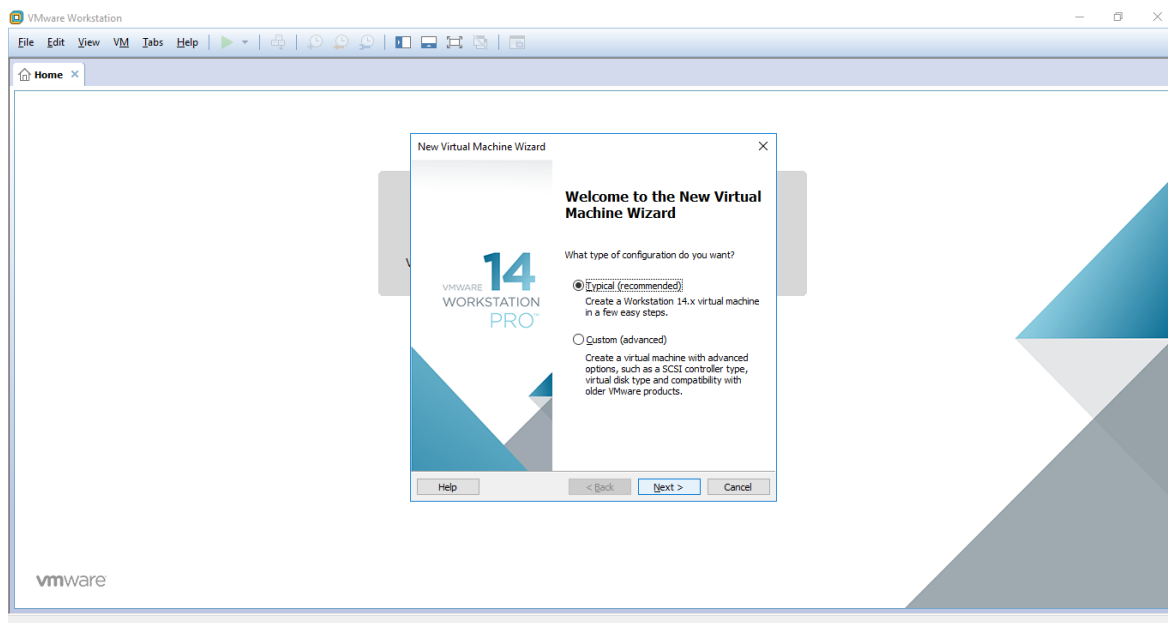
### 2.4.3 Quy trình cài đặt Kali Linux

Bước 1: Khởi động VMware và chọn Create a New Virtual Machine



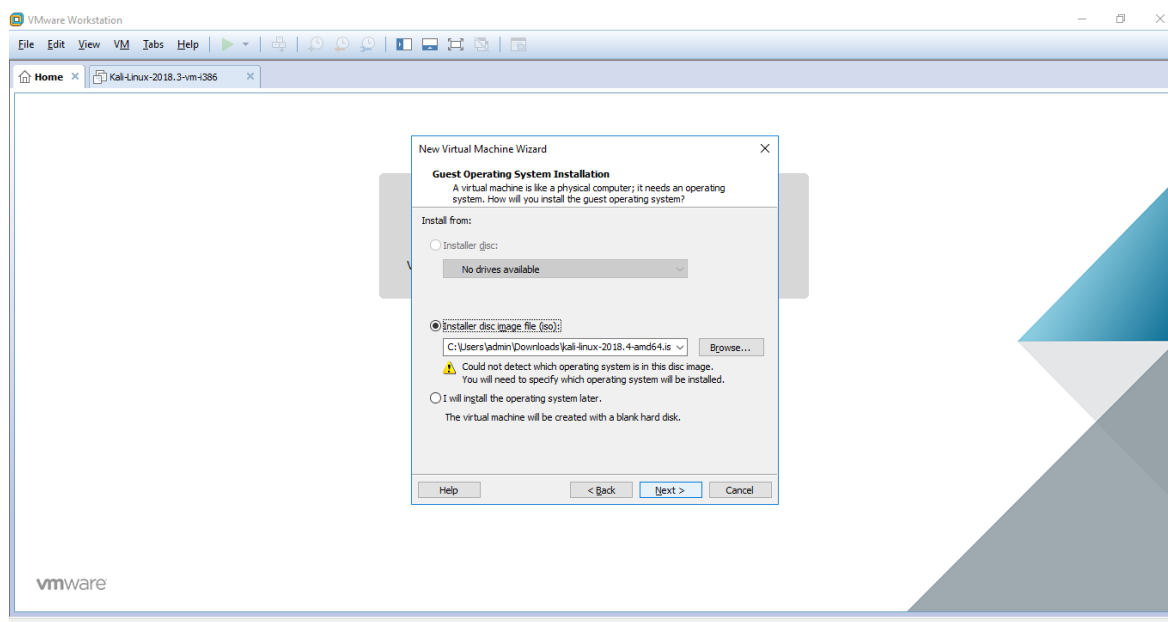
Hình 2-9: Giao diện tạo máy ảo

Bước 2: Chọn Typical



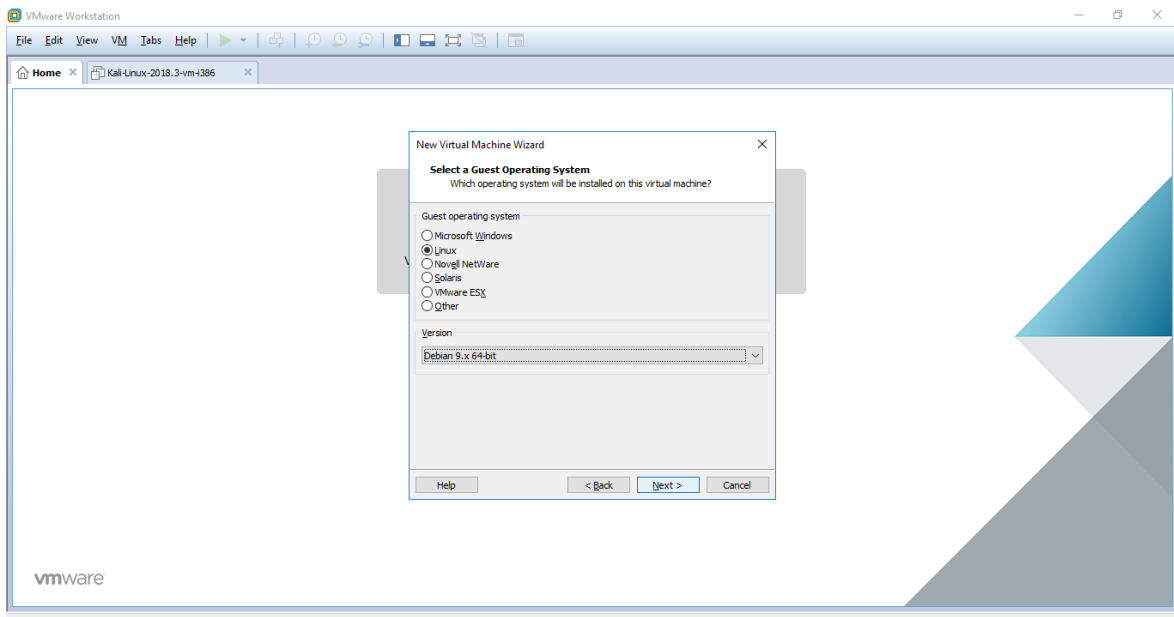
Hình 2-10: Giao diện chọn cấu hình

Bước 3: Chọn file Kali Linux ISO mà chúng ta đã tải

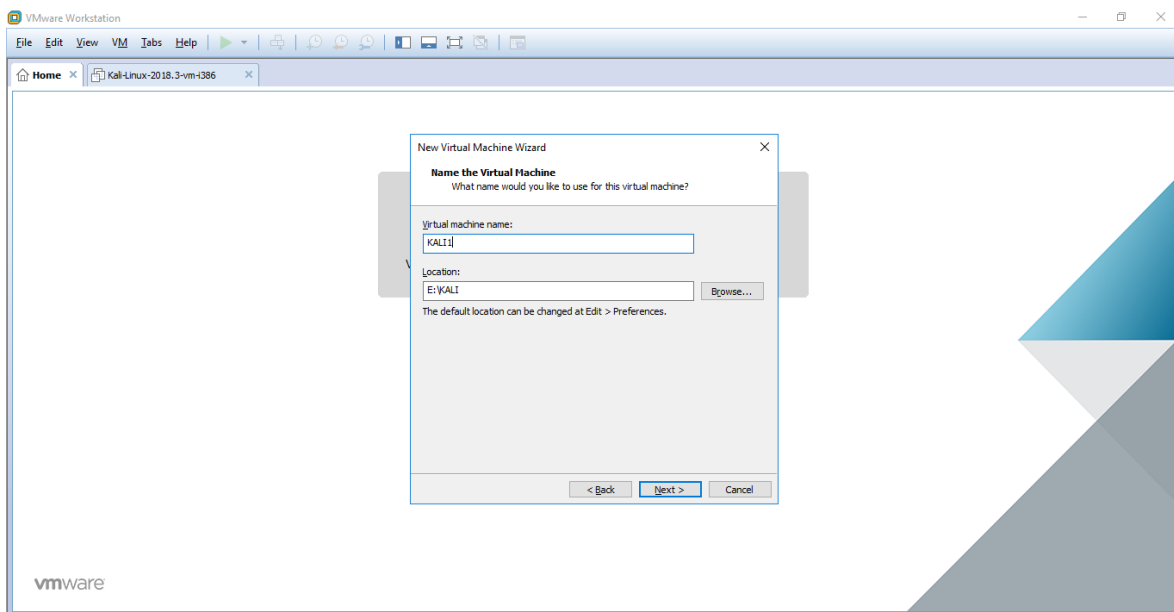


Hình 2-11: Giao diện chọn vị trí Kali Linux ISO

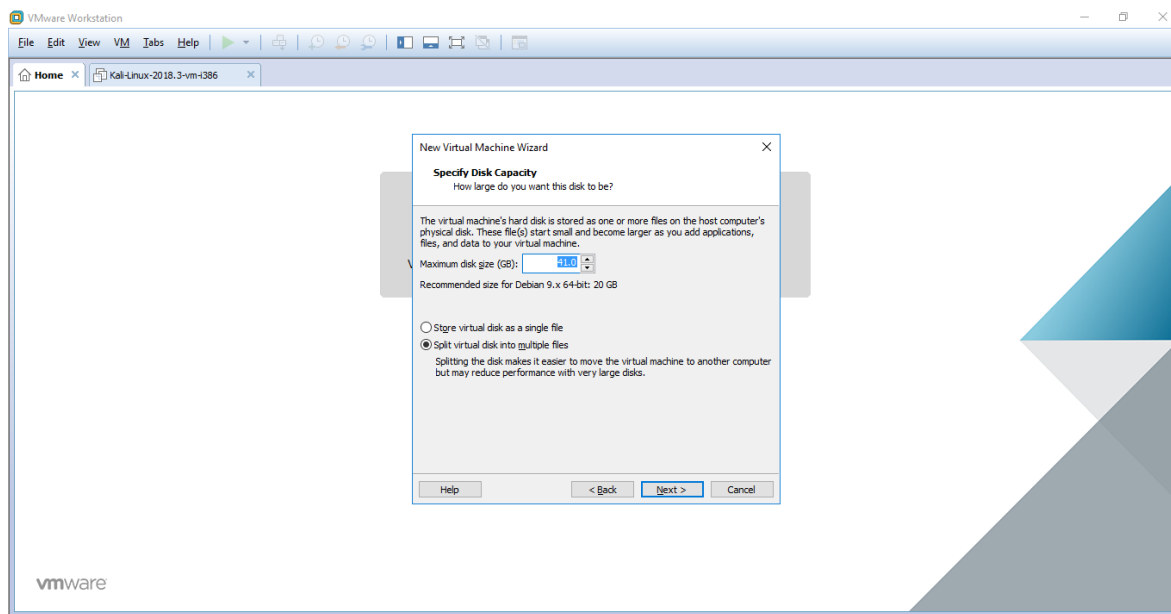
B4: Chọn Linux và Debian 9.x 64-bit



Hình 2-12: Giao diện chọn hệ điều hành và phiên bản  
Bước 5: Đặt tên cho máy ảo và vị trí

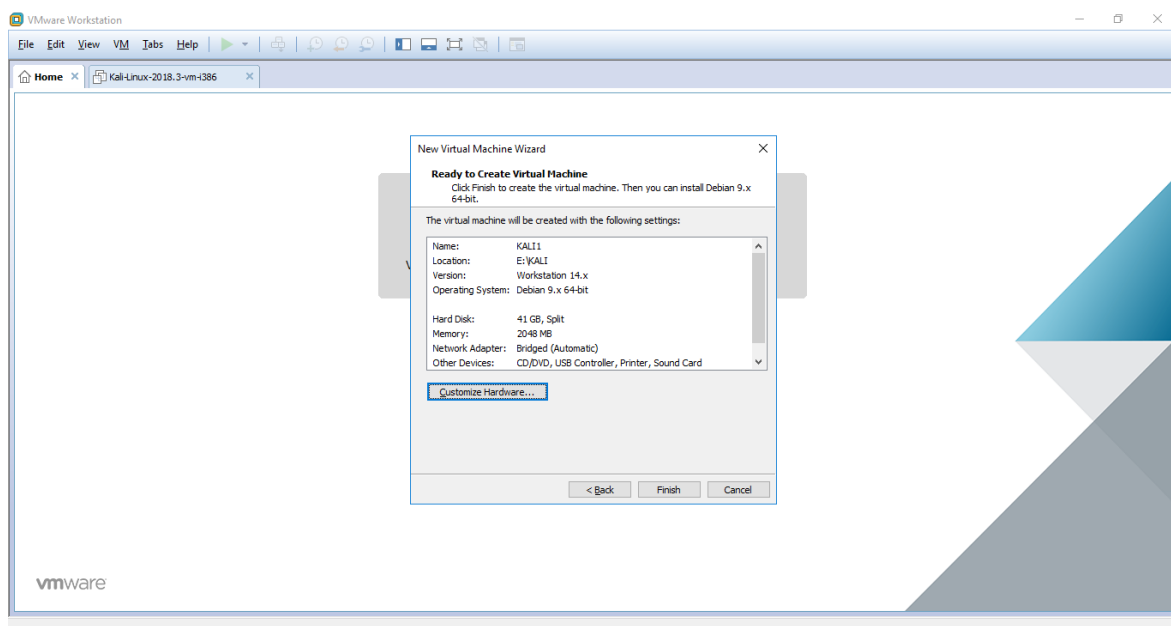


Hình 2-13: Giao diện đặt tên và vị trí cho máy ảo  
Bước 6: Chọn dung lượng ổ đĩa, chúng ta lên để >40GB để máy ảo hoạt động tốt.



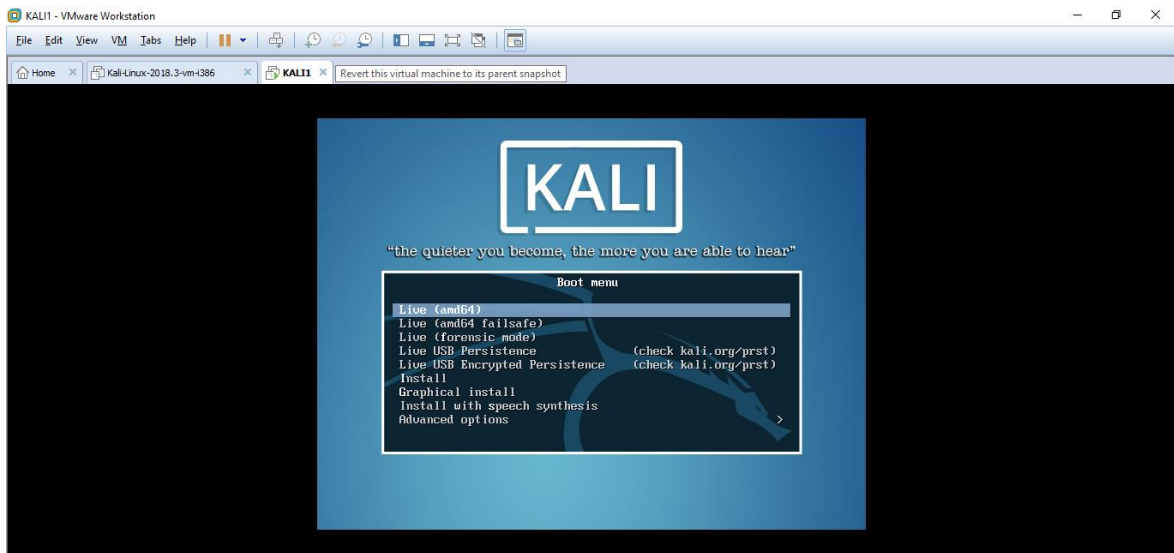
Hình 2-14: Giao diện chọn dung lượng ổ đĩa

Bước 7: Tùy chỉnh Ram và Network sau đó nhấn finish để VMware bắt đầu chạy quá trình cài đặt



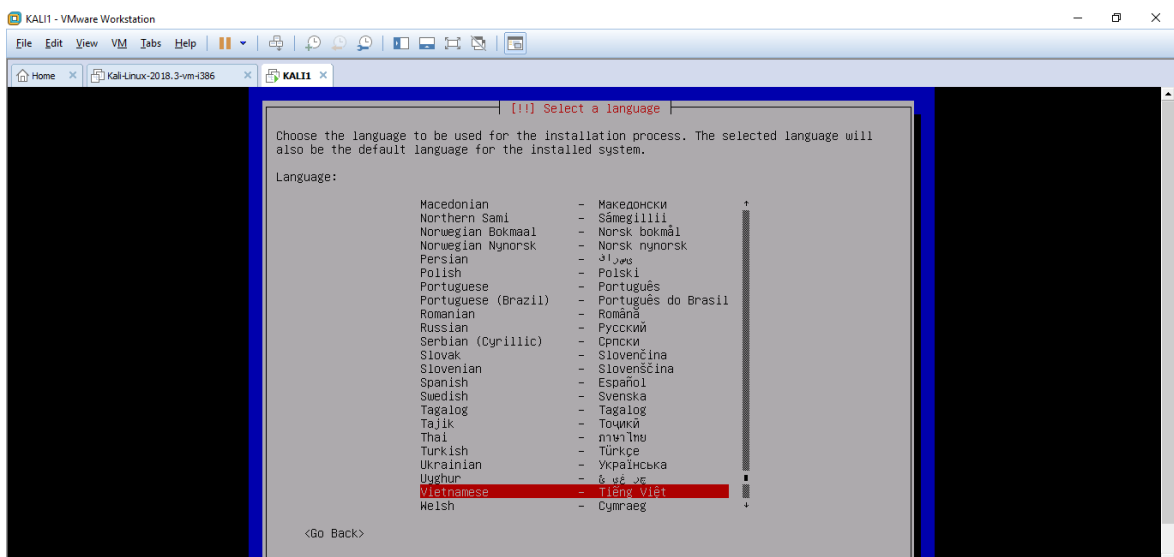
Hình 2-15: Giao diện hoàn thành cài đặt máy ảo

Bước 8: Ở đây chúng ta chọn Install



Hình 2-16: Giao diện mới khởi động Kali

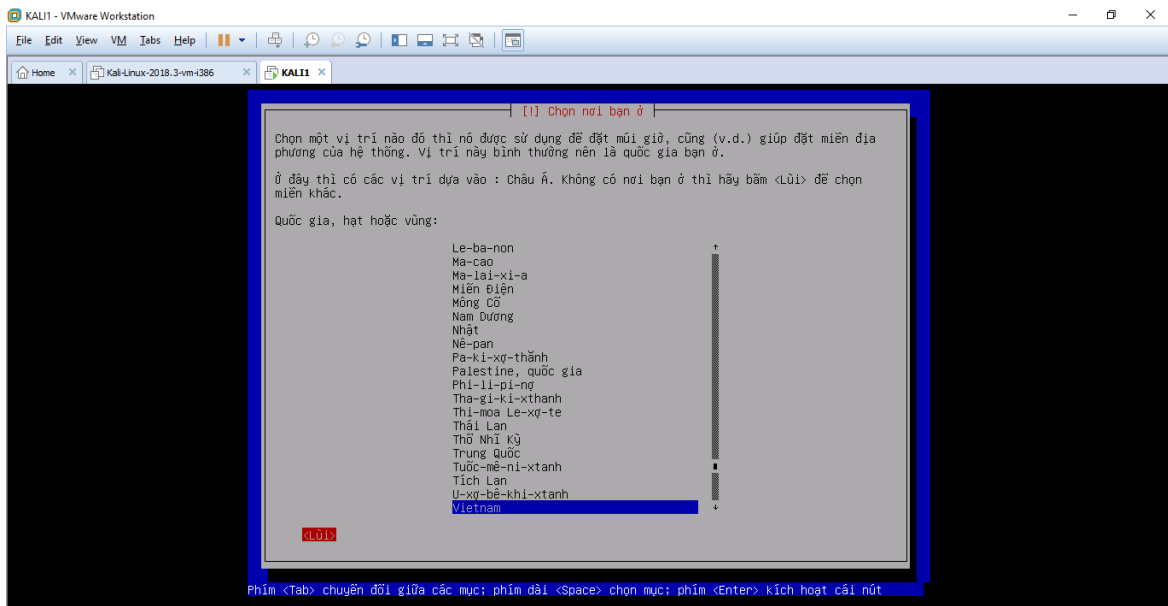
Bước 9: Chọn ngôn ngữ tùy theo ý chúng ta



Hình 2-17: Giao diện chọn ngôn ngữ

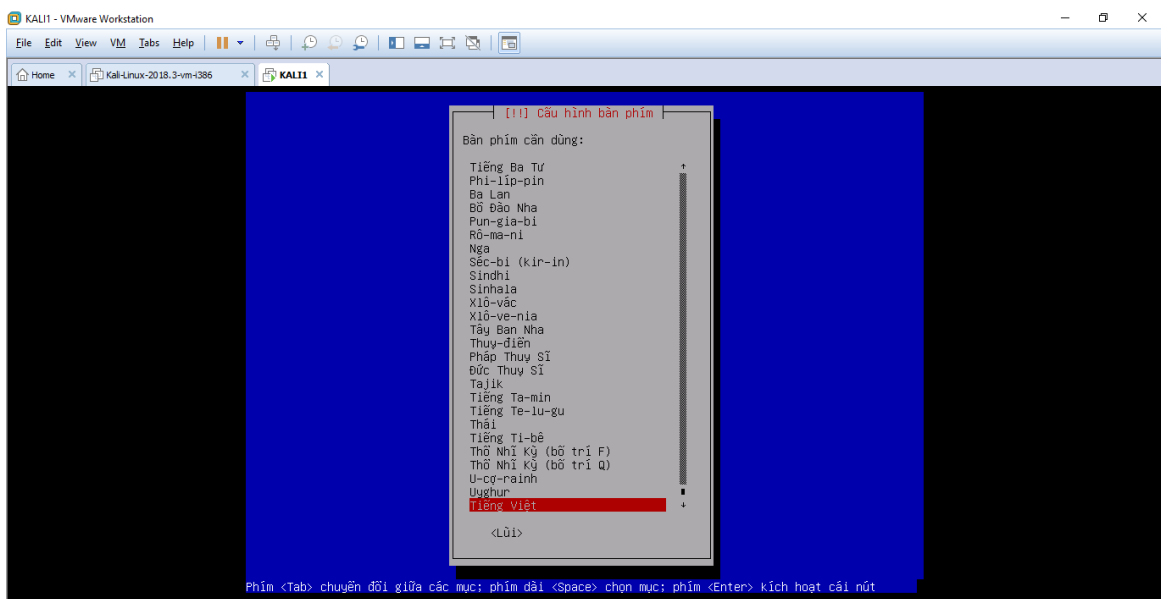
Bước 10: Chọn vị trí địa lí là Việt Nam





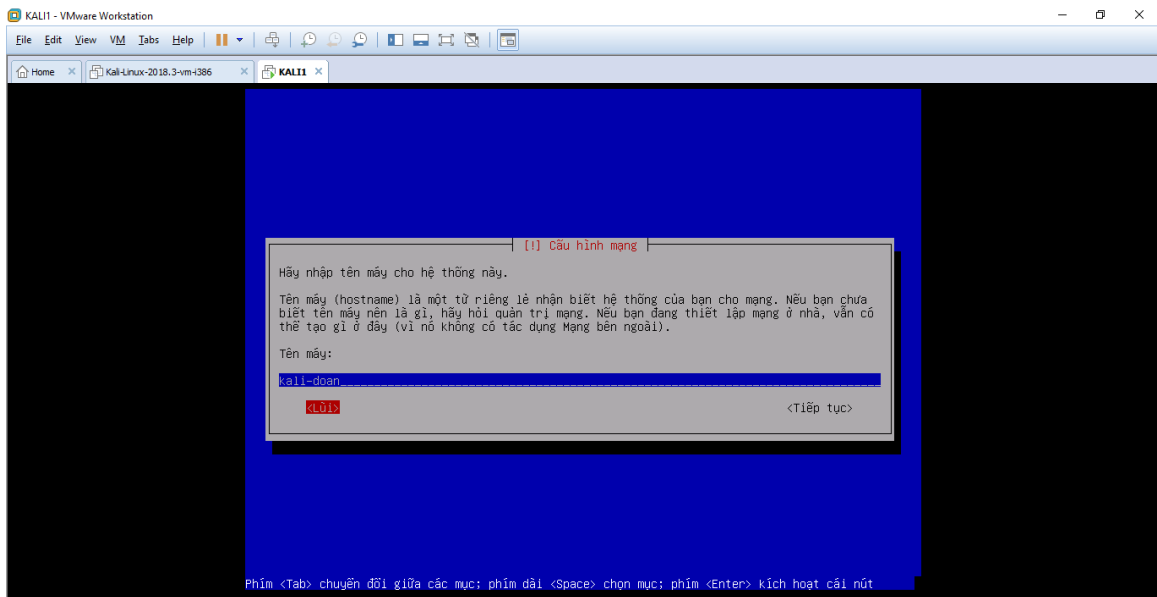
Hình 2-18: Giao diện chọn vị trí địa lí

Bước 11: Chọn bộ gõ cho bàn phím, chúng ta chọn Tiếng Việt



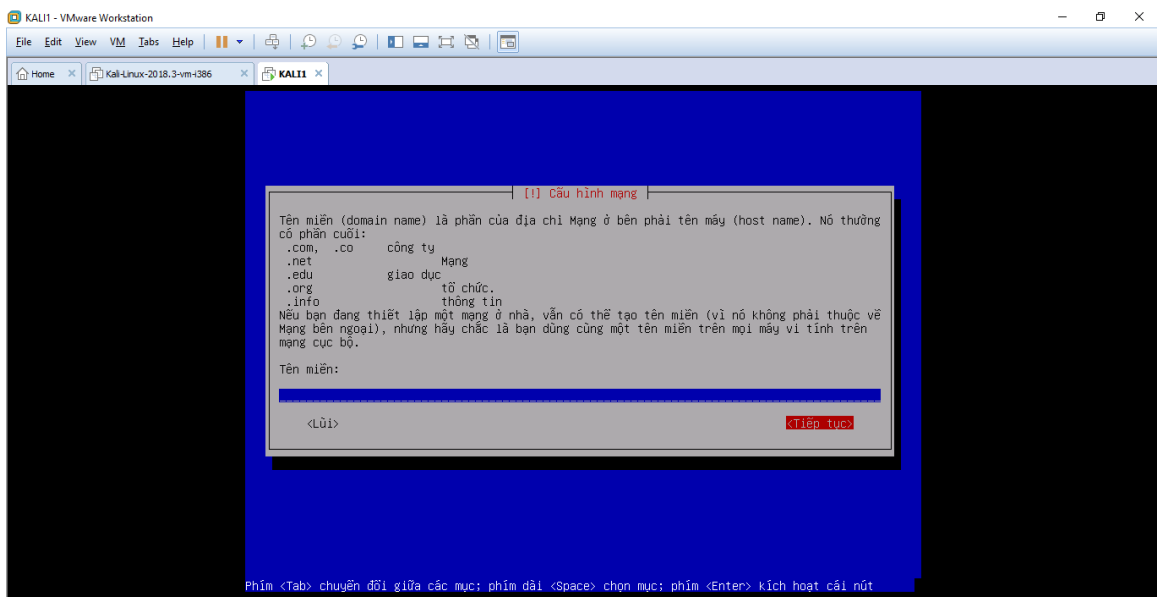
Hình 2-19: Giao diện chọn bộ gõ

Bước 12: Chúng ta đặt tên cho máy ảo



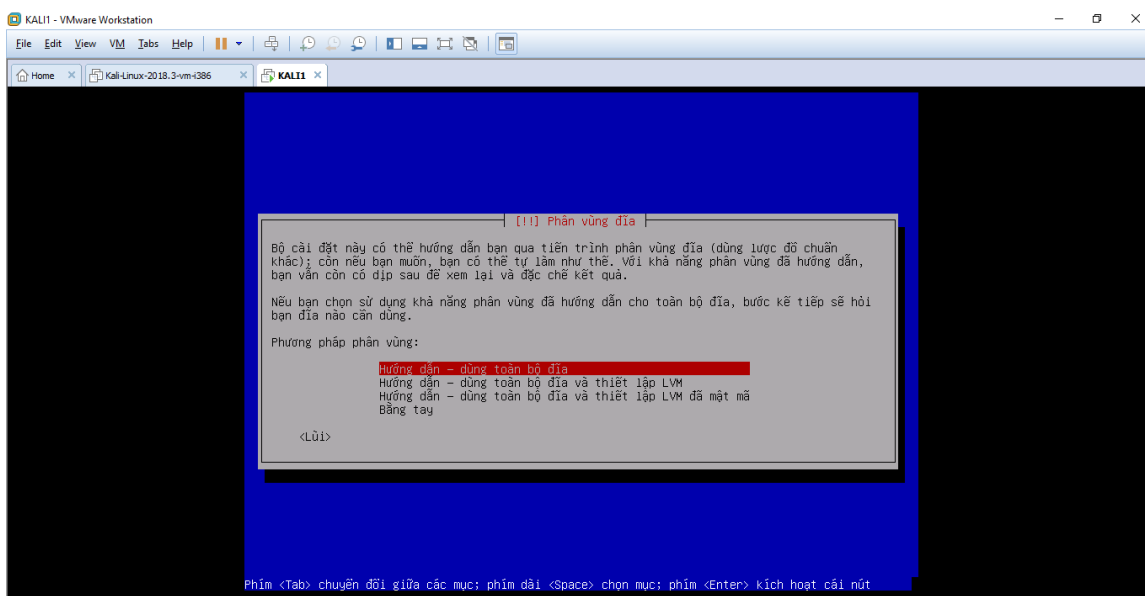
Hình 2-20: Giao diện đặt tên cho máy ảo

Bước 13: Chúng ta bỏ qua bước này chọn Tiếp tục, hệ thống sẽ tự tạo một domain với tên gọi localhost



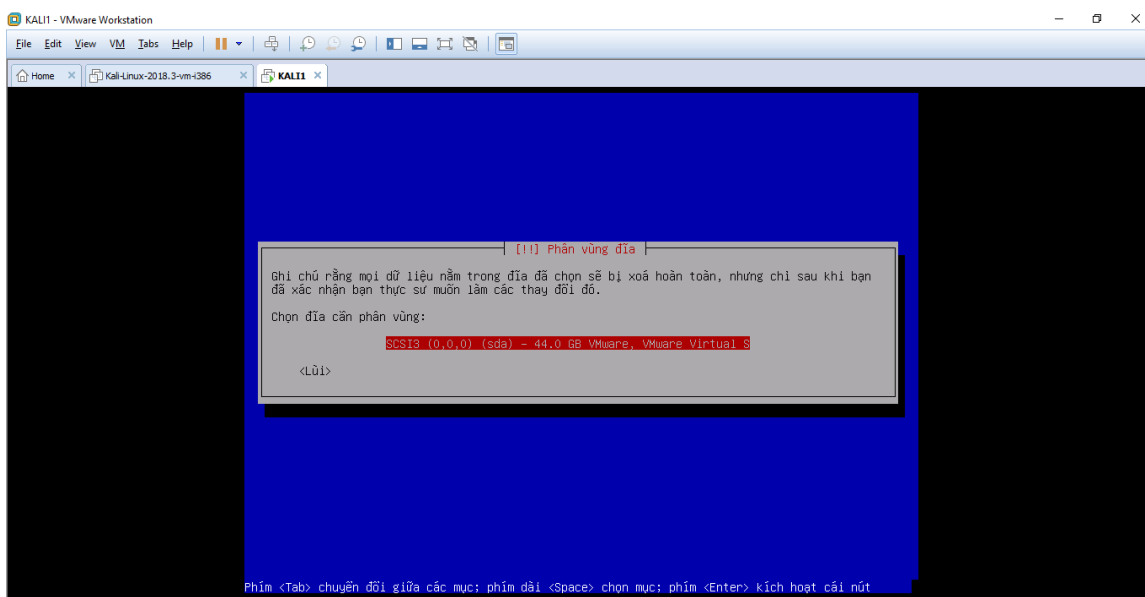
Hình 2-21: Giao diện cấu hình miền

Bước 14: Chọn mật khẩu và phân vùng ổ đĩa, chúng ta chọn dùng toàn bộ ổ đĩa



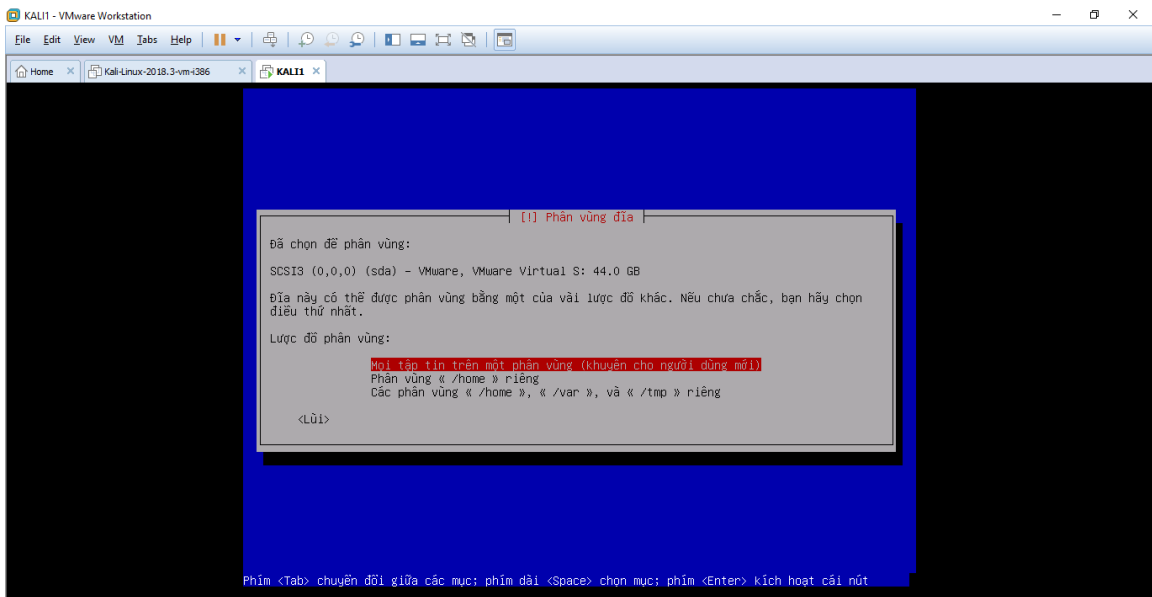
Hình 2-22: Giao diện phân vùng ổ đĩa

## Bước 15: Chọn ổ đĩa mà chúng ta đã thiết lập

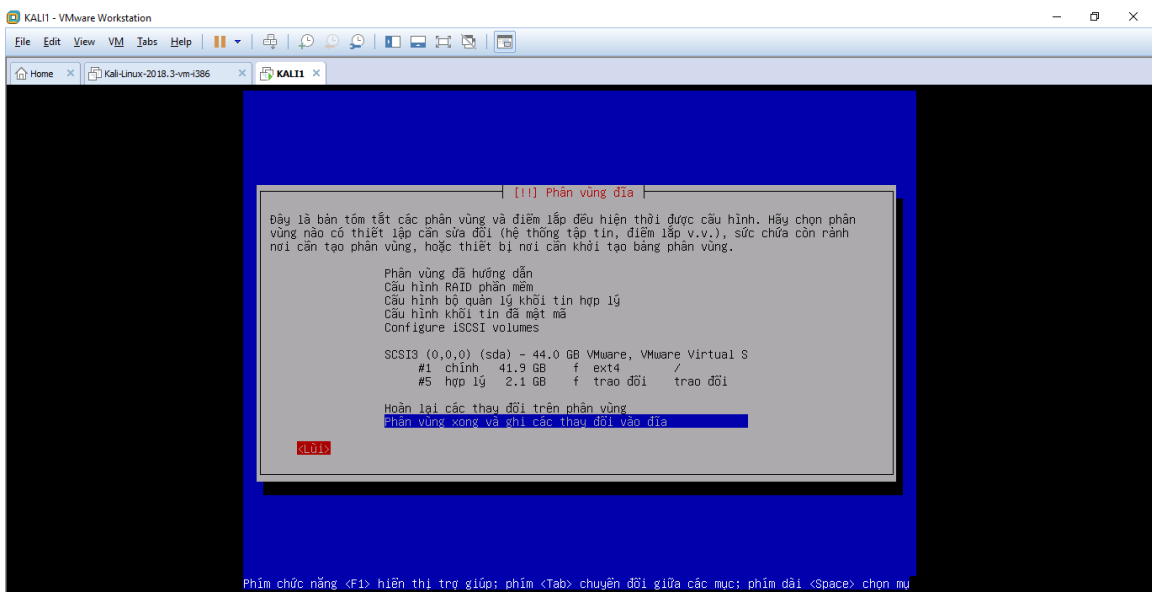


Hình 2-23: Giao diện chọn ổ đĩa

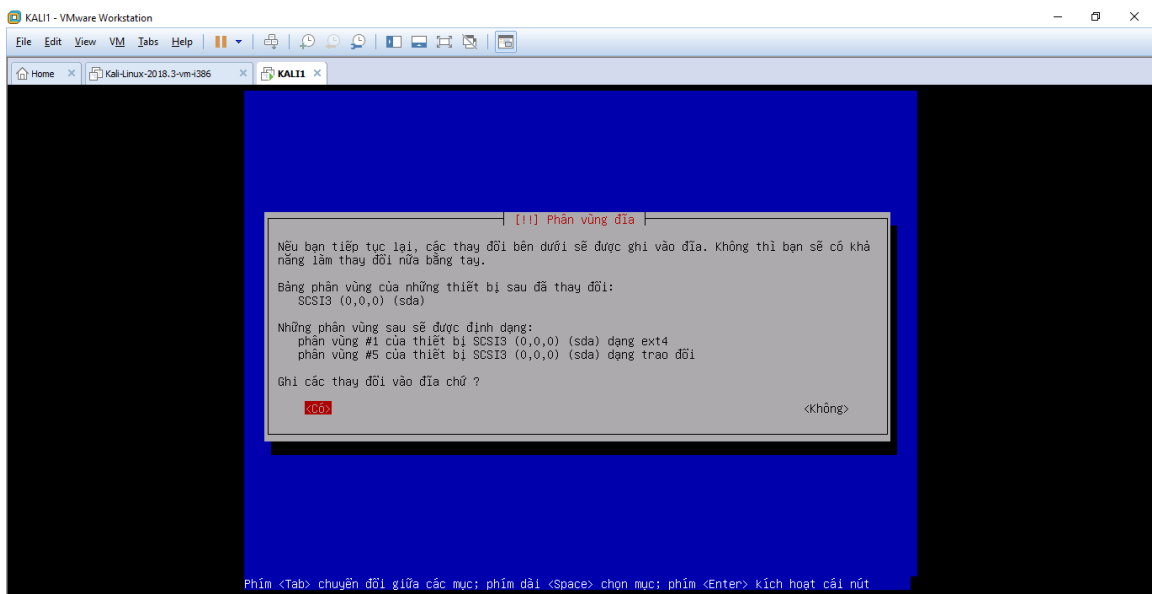
Bước 16: Chúng ta chọn một tập tin trên một phân vùng để đặt tất cả các file vào một chỗ



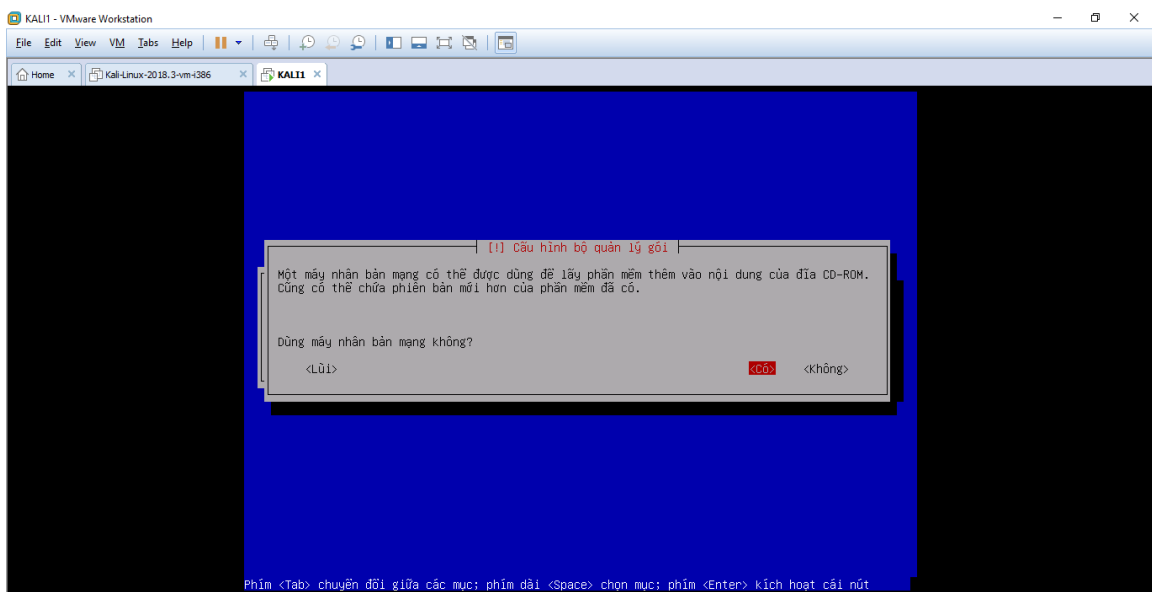
Hình 2-24: Giao diện chọn kiểu lược đồ phân vùng  
Bước 17: Chọn phân vùng và ghi các thay đổi vào đĩa



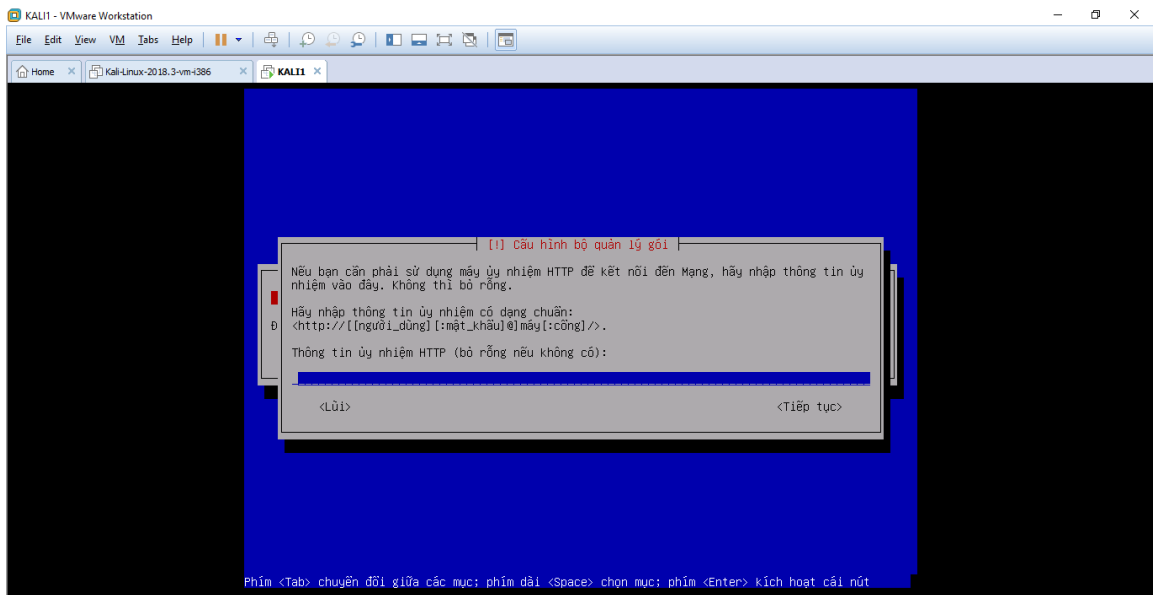
Hình 2-25: Giao diện chọn phân vùng xong và ghi thay đổi vào đĩa  
Bước 18: Chọn Có để lưu thay đổi



Hình 2-26: Giao diện xác nhận ghi các thay đổi vào đĩa  
Bước 19: Chọn Có để dùng bất kì mạng nào để update sau này

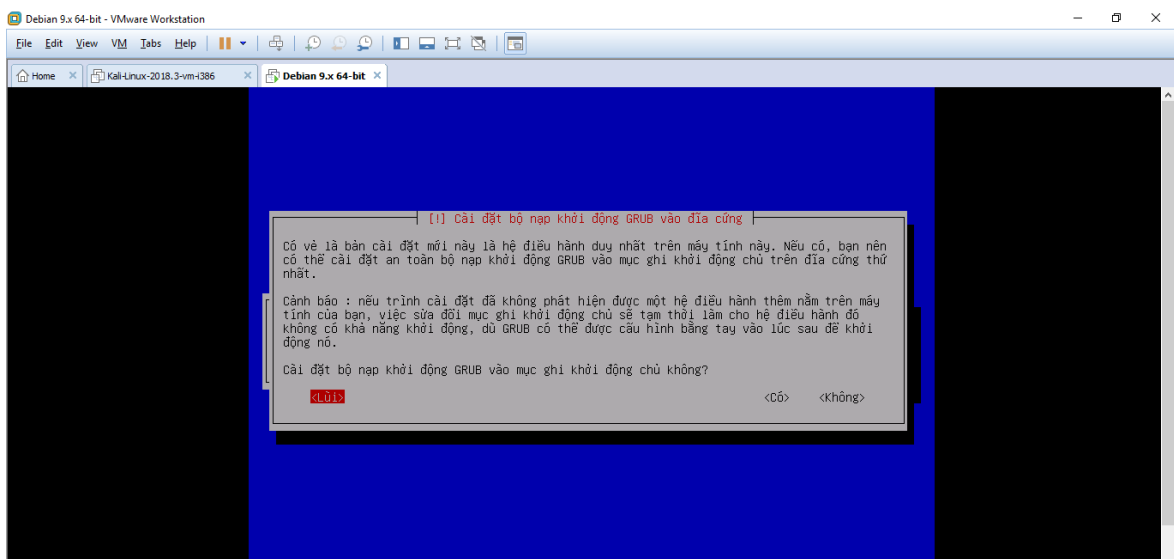


Hình 2-27: Giao diện chọn mạng để dùng bất kì mạng nào  
Bước 20: Chúng ta bỏ qua phần này và chọn Tiếp tục



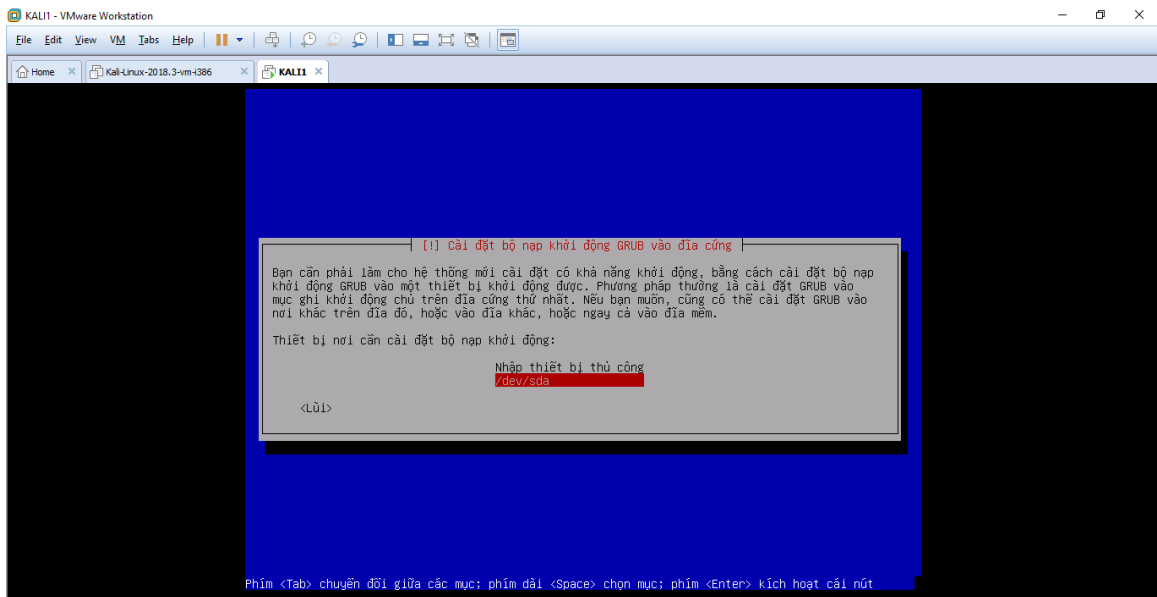
Hình 2-28: Giao diện thông tin ủy nhiệm HTTP

Bước 21: Chúng ta chọn Có để cài đặt bộ nạp khởi động GRUB



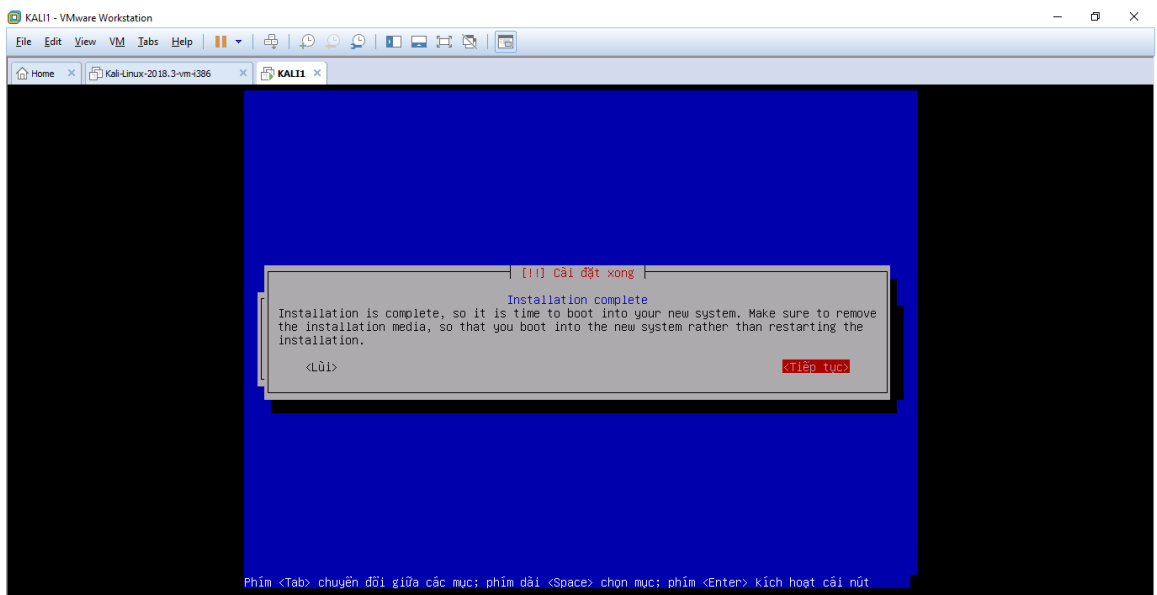
Hình 2-29: Giao diện cài đặt bộ nạp khởi động GRUB vào mục ghi

Bước 22: Chọn /dev/sda để hệ thống cài đặt GRUB



Hình 2-30: Giao diện thiết bị nơi cần cài đặt bộ nạp khởi động

Bước 23: Sau đó sẽ xuất hiện thông báo như này nghĩa là đã thành công, ấn Tiếp tục để khởi động lại là chúng ta đã cài đặt xong.



Hình 2-31: Giao diện cài đặt xong

## CHƯƠNG 3: THỰC NGHIỆM

### 3.1 Triển khai công cụ Zenmap

Nmap là một công cụ khá hữu ích dành cho người làm chuyên về ngành security. Nmap có khả năng quét các hệ thống và tìm ra lỗi, những cổng chưa đóng trên hệ thống giúp cho người quản trị tiết kiệm được thời gian và công sức khi bảo trì. Nmap còn có thể cho ta biết thông tin chi tiết về hệ thống, rất thuận tiện khi ta muốn kiểm tra nhanh thông tin một hệ thống nào đó. Tuy nhiên thì Nmap do là một công cụ quét cổng khá mạnh, nên cũng được các hacker thường xuyên dùng để quét lỗi và xâm nhập vào các hệ thống nạn nhân, thậm chí gửi các gói tin làm tràn hệ thống đích.

Zenmap là công cụ mang giao diện đồ hoạ của Nmap, dễ sử dụng với chỉ vài thao tác click chuột. Chúng ta không cần phải nắm các lệnh và tham số khó nhớ, phức tạp của Nmap, vì các lựa chọn và thông tin đã có sẵn.

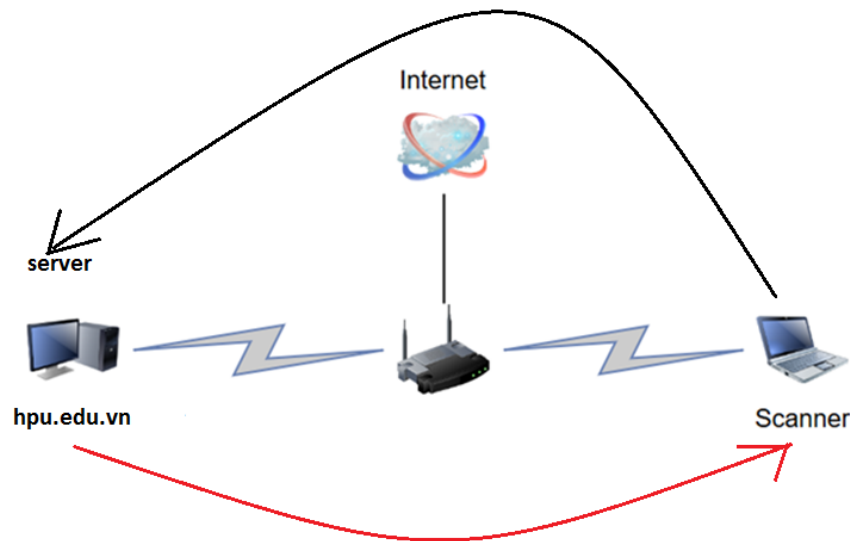
#### 3.1.1 Mô hình

Xây dựng mô hình quét Zenmap gồm có:

- Một máy chủ hoặc một máy client
- Mạng Internet
- Một máy quét ( có thể lap top, pc hoặc máy ảo )

Ta có mô hình mẫu sau:





Hình 3-1: Mô hình Zenmap

Máy tính nạn nhân không cần phải là máy sử dụng hệ điều hành cho Server, nó có thể là một máy client bất kỳ nào đó. Máy scanner cần cài đặt sẵn Nmap/Zenmap và các driver cần thiết.

Với mô hình này ta sẽ bắt đầu từ máy scanner đã cài đặt sẵn Zenmap và khởi động nó lên để quét với trang web hpu.edu.vn và rồi kết quả sẽ trả cho chúng ta những cổng tcp đang mở, đóng, tên hệ điều hành, tên máy nạn nhân, hay thậm chí cả địa chỉ IP của trang web. Điều cần thiết hơn cả đó là cả 2 phải cùng kết nối Internet. Nếu port mà mở càng nhiều thì nguy cơ bị hacker tấn công để thu thập thông tin càng cao. Biện pháp tốt nhất có lẽ là chúng ta nên đóng bớt cổng không sử dụng hoặc tìm cách để cổng ẩn để tránh bị tấn công. Chúng ta có thể sử dụng công cụ này để phòng ngừa những lỗ hổng an ninh mạng máy tính rất hiệu quả.

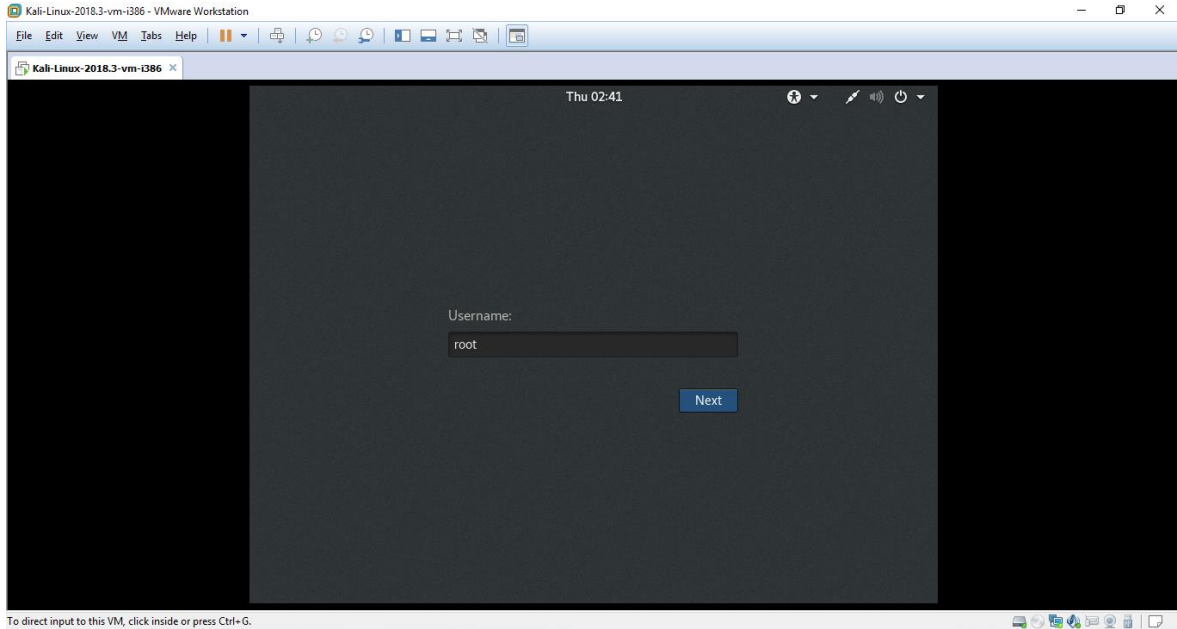
### 3.1.2 Các bước thực hiện

- Triển khai Zenmap
- Kiểm tra, phân tích một số lỗi phổ biến

### 3.1.3 Triển khai

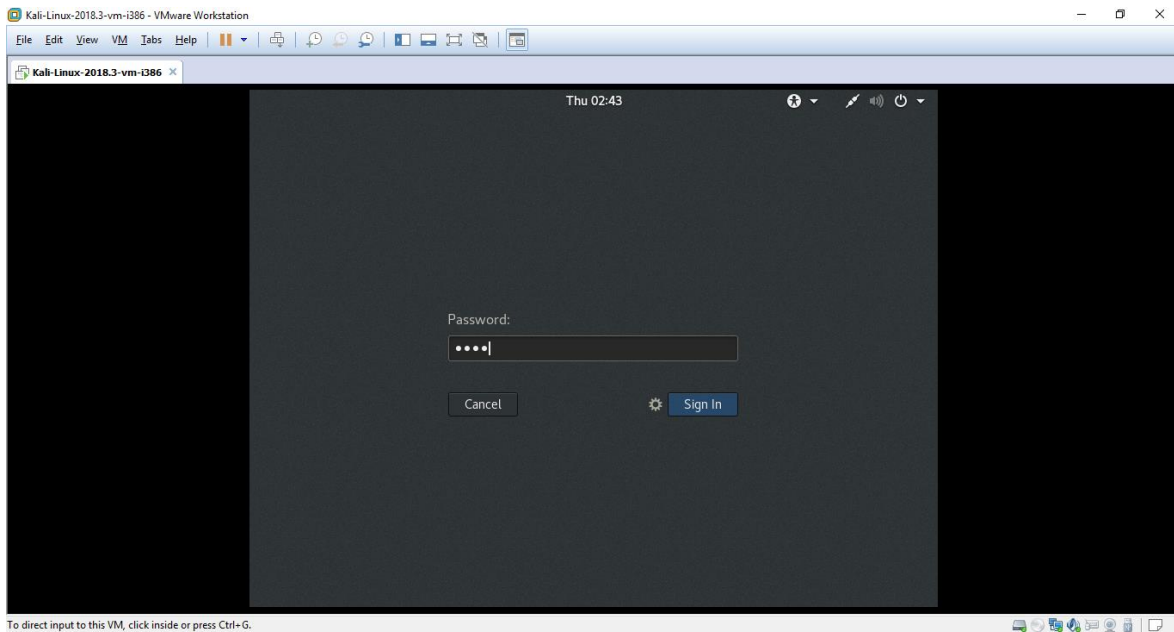
Bước 1: Đăng nhập vào Kali Linux

- Login : root



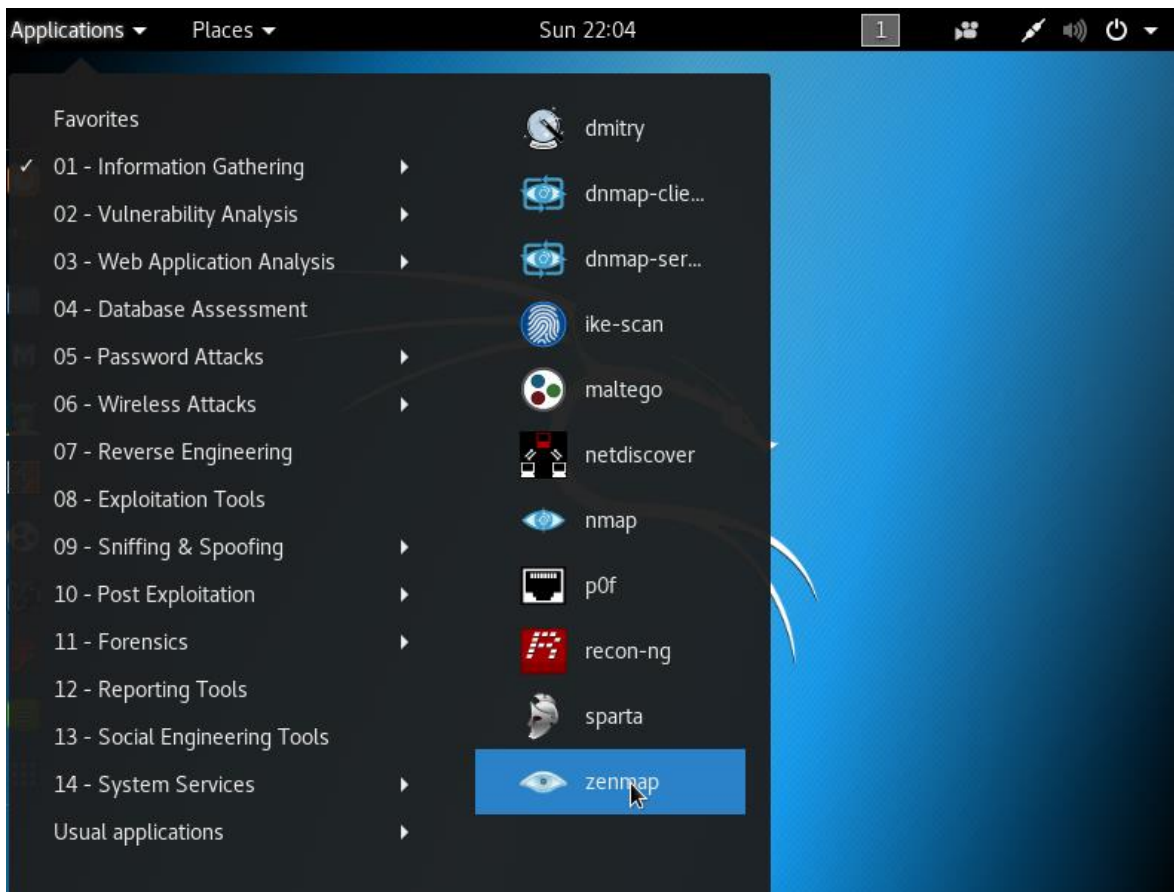
Hình 3-2: Giao diện Username

- Password : root

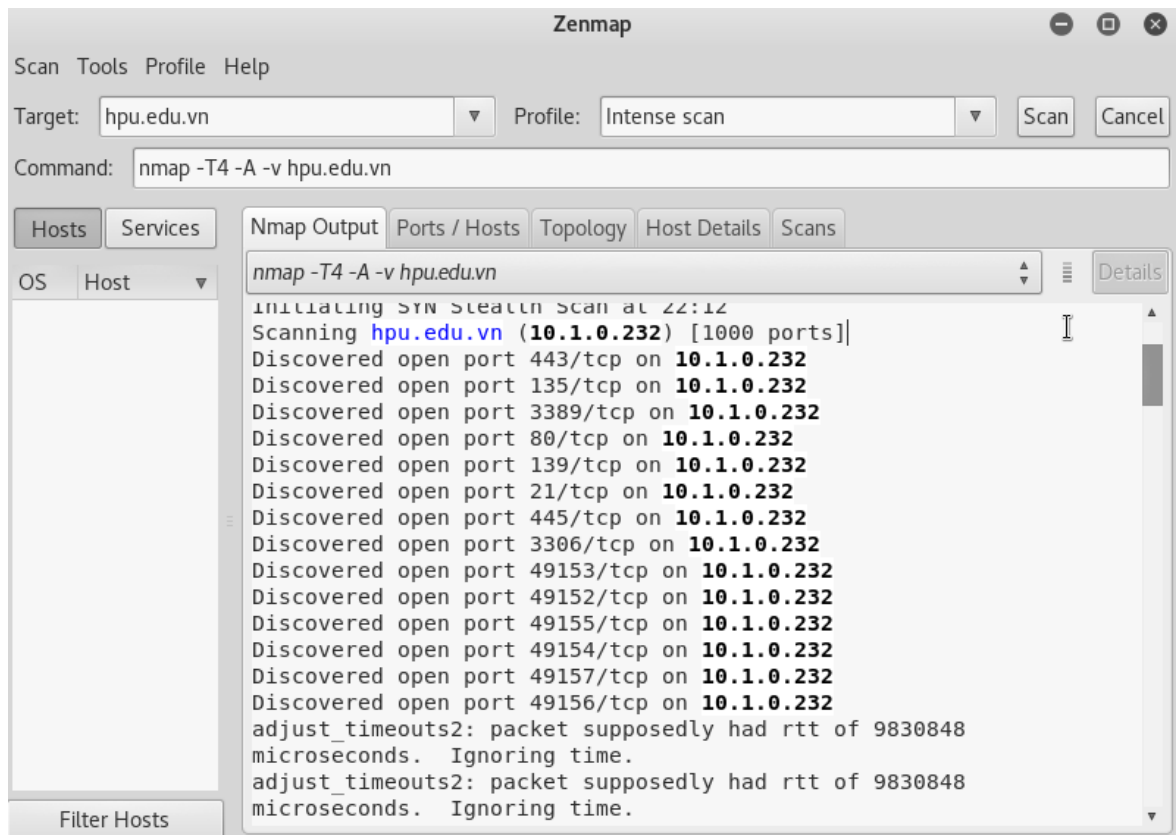


Hình 3-3: Giao diện Password

- Bước 2: Khởi động Zenmap
- Applications → Information Gathering → Zenmap



Hình 3-4: Giao diện khởi động Zenmap trong Kali Linux  
Bước 3: Tiến hành thực hiện quét vs trang web hpu.edu.vn

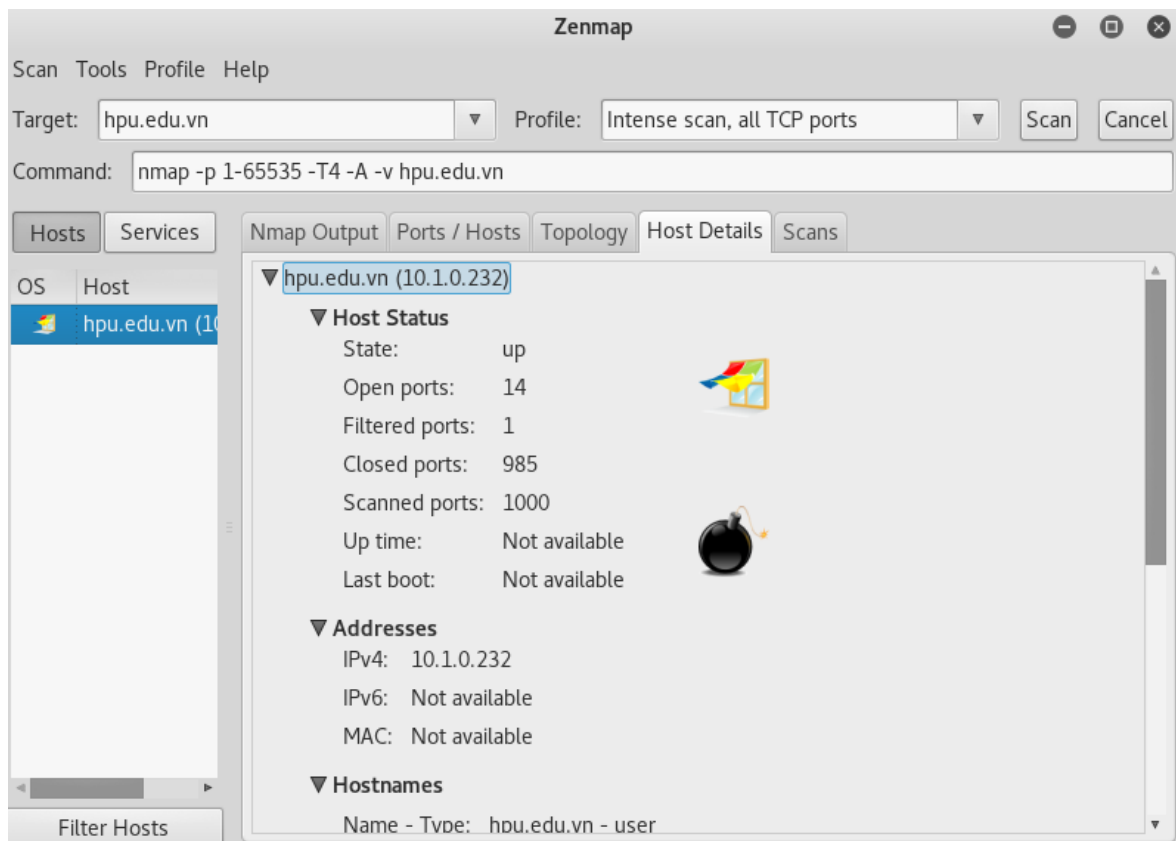


Hình 3-5: Giao diện các cổng tcp đang mở

Kiểu scan này có 3 option:

- -A ra lệnh cho Nmap cố gắng tìm phiên bản của hệ điều hành đích, các dịch vụ và các thông số chi tiết giúp nhận dạng hệ điều hành đích. Option này cũng thực hiện traceroute (tìm đường đi) và dùng các mã lệnh NSE để tìm thêm các thông tin phụ trợ. Option này khiến cách scan này không được bí mật vì nó cộng khá nhiều kiểu scan vào 1 lần scan.
- -v giúp hiển thị thông tin scan một cách tường minh hơn, dễ hiểu hơn.
- -T4 là tùy chọn về mẫu tính thời gian (timing template) với các giá trị T khác nhau, từ T0 đến T5, T5 là nhanh nhất. Tùy chọn này chính là cách chúng ta cho Nmap biết chúng ta muốn Nmap làm việc nhanh hay chậm. Tốc độ khác nhau sẽ dùng cho các mục đích khác nhau.

Như kết quả trên hình các chúng ta thấy, Intense Scan đã phát hiện ra được 14 cổng TCP đang mở trên hệ thống đích, port 80, port 135, port 3389, port 139, port 21, port 445, port 3306, port 49153, port 49152, port 49155, port 49154, port 49157, port 49156 và port 443.



Hình 3-6: Giao diện thông tin về máy nạn nhân

Click sang phần Host Details, các chúng ta có thể thấy những thông tin về máy nạn nhân mà Nmap đã lọc ra:

- Host Status: bao gồm state (trạng thái, up hoặc down), tổng số port đang mở, các port đã đóng, các port đã được scan, thời gian mà hệ thống đã được mở, lần cuối cùng hệ thống nạn nhân được bật là khi nào.
- Addresses: IPv4, IPv6 và địa chỉ MAC của hệ thống nạn nhân.
- Hostname: tên máy nạn nhân, thông tin domain của máy nạn nhân.

- Operating System: tên hệ điều hành kèm theo khả năng chính xác bao nhiêu phần trăm do Nmap đánh giá dựa vào quá trình scan. Sau đó là thông tin các service đang được bật, các port trên hệ thống nguồn, port nào đóng, port nào mở.

### 3.2 Triển khai công cụ Nikto

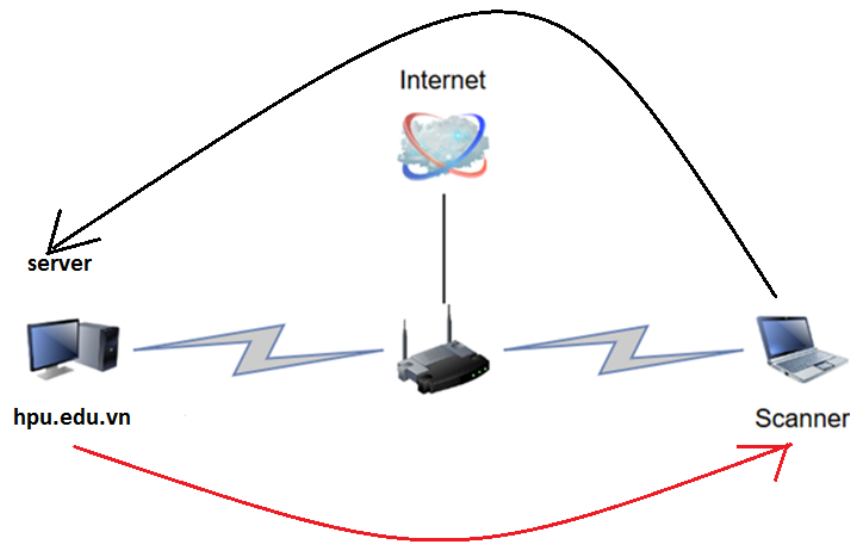
Nikto web server scanner là một công cụ bảo mật, nó kiểm tra một trang web để chỉ ra được hàng ngàn vấn đề bảo mật có thể xảy ra, bao gồm dangerous files, mis-configured services, vulnerable scripts và rất nhiều vấn đề khác nữa, kiểm tra các phiên bản lỗi thời của hơn 1250 máy chủ và các vấn đề cụ thể về phiên bản trên 270 máy chủ ( Apache, Nginx, OHS,...). Nikto là mã nguồn mở và được cấu trúc với các plugin giúp mở rộng khả năng. Các plugin này thường xuyên được cập nhật với các kiểm tra bảo mật mới. Và Nikto không phải là một công cụ tàng hình.

#### 3.2.1 Mô hình

Xây dựng mô hình quét Nikto gồm có:

- Một máy chủ.
- Mạng Internet.
- Một máy quét ( có thể lap top, pc hoặc máy ảo ).

Ta có mô hình mẫu sau:



Hình 3-7: Mô hình Nikto

Giống với Zenmap nhưng Nikto bắt buộc máy của nạn nhân phải là máy sử dụng hệ điều hành cho Server.

Với mô hình này ta bắt đầu quét từ máy scanner của mình đã cài sẵn có kết nối Internet cũng như sever ta chuẩn bị quét cũng phải kết nối Internet nhờ thế máy quét của ta có thể phát hiện ra những lỗi mà các hacker có thể tấn công được vào. Sau khi quét nó sẽ cung cấp cho ta biết máy chủ web là gì và liệt kê cho ta nhiều lỗ hổng bảo mật. Như vậy chúng ta có thể biết lỗi rất nhanh và sửa lỗi hiệu quả gây cho chúng ta ít thiệt hại hơn.

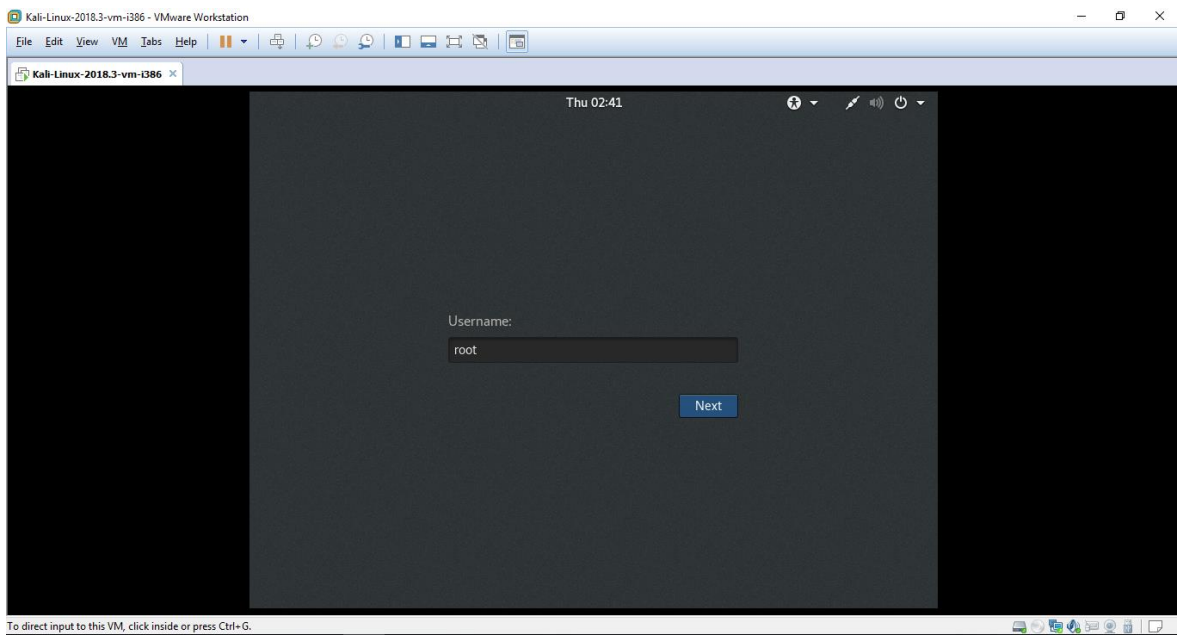
### 3.2.2 Các bước thực hiện

- Triển khai Nikto.
- Kiểm tra, phân tích một số lỗi phổ biến.

### 3.2.3 Triển khai

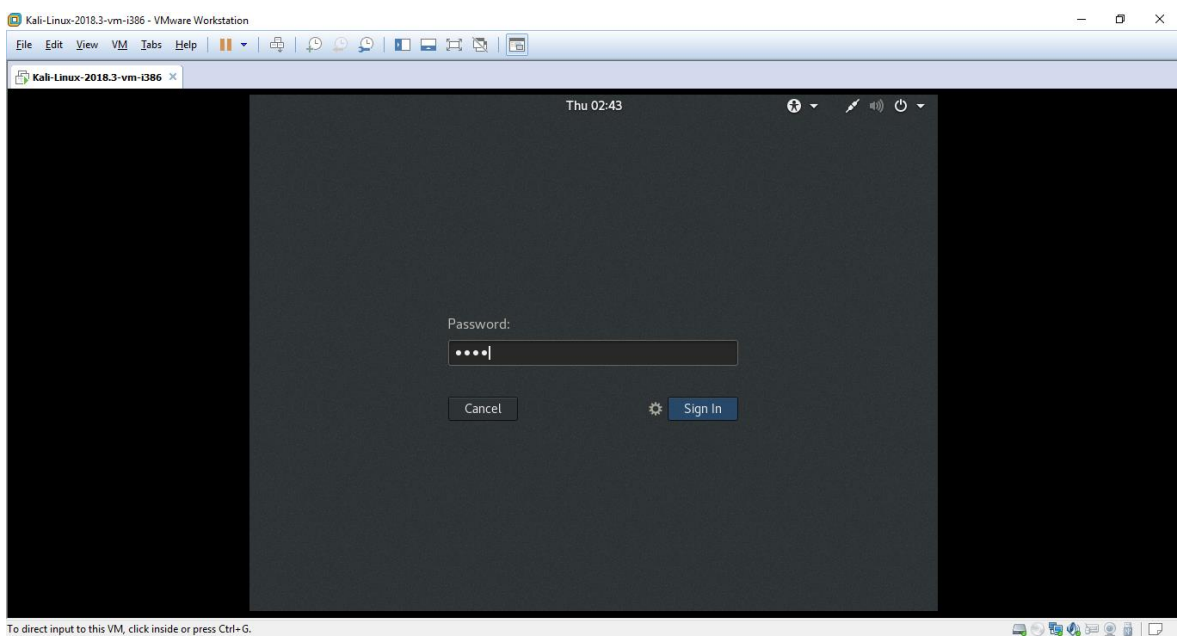
Bước 1: Đăng nhập vào Kali Linux.

- Login : root



Hình 3-8: Giao diện Username

- Password : toor

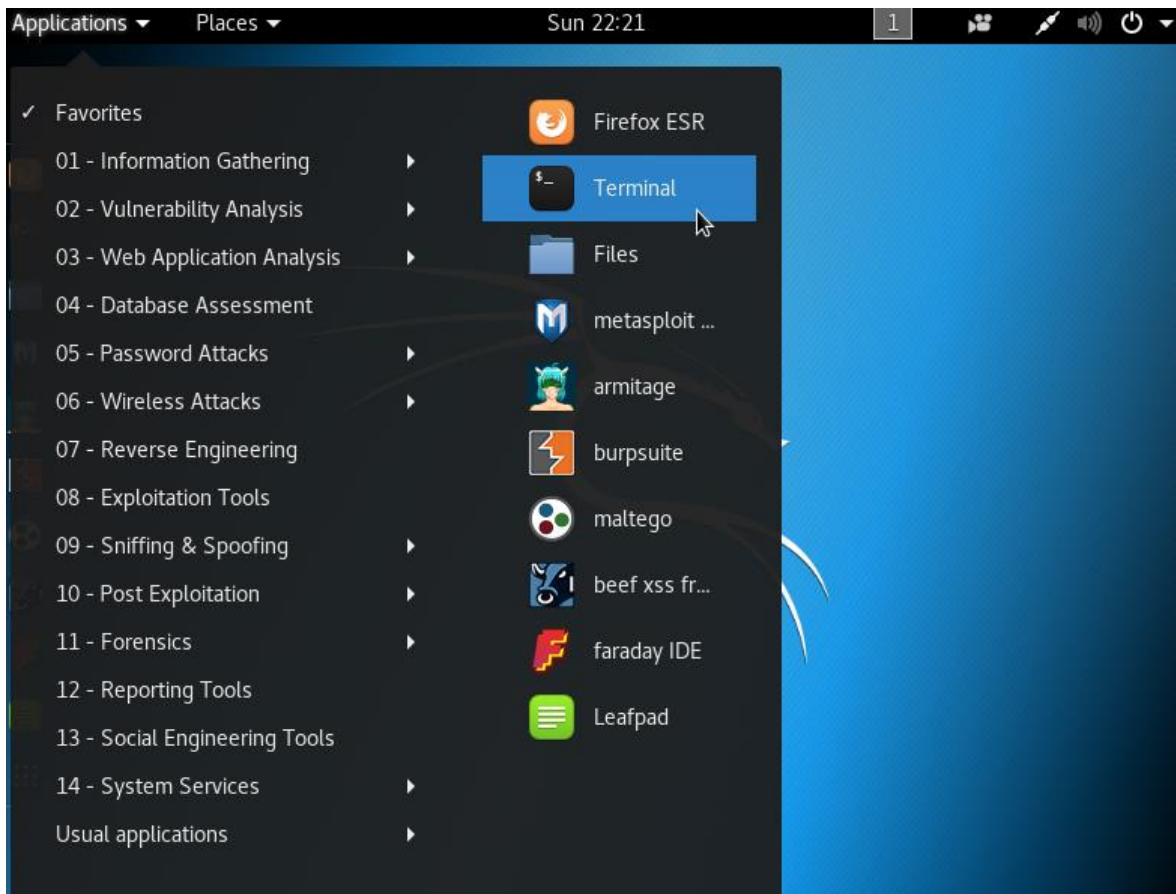


Hình 3-9: Giao diện Password

Bước 2: Khởi động Terminal.

- Applications → Favorites → Terminal





Hình 3-10: Giao diện khởi động Terminal

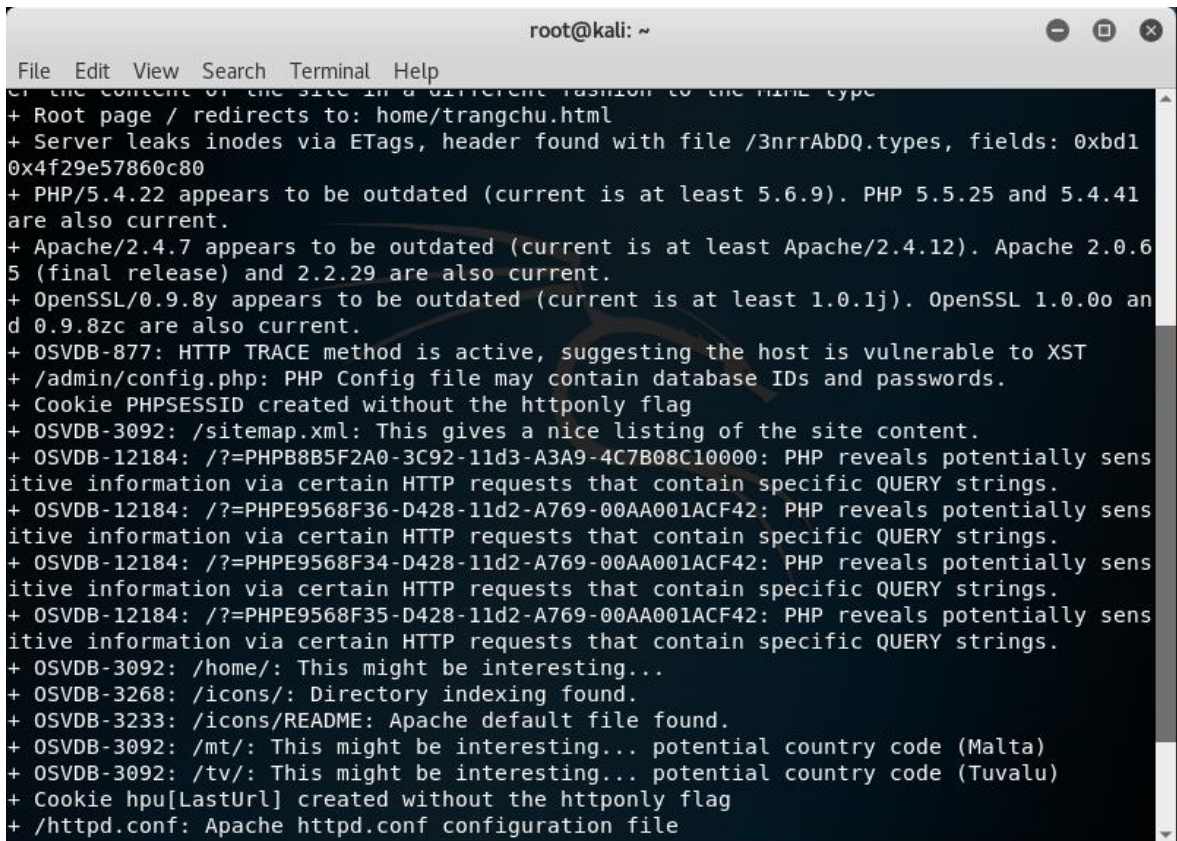
Bước 3: Tiến hành quét với trang web hpu.edu.vn bằng Nikto.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nikto -h hpu.edu.vn  
- Nikto v2.1.6  
-----  
+ Target IP: 10.1.0.232  
+ Target Hostname: hpu.edu.vn  
+ Target Port: 80  
+ Start Time: 2019-05-19 22:24:00 (GMT-4)  
-----  
+ Server: Apache/2.4.7 (Win32) OpenSSL/0.9.8y PHP/5.4.22  
+ Retrieved x-powered-by header: PHP/5.4.22  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Root page / redirects to: home/trangchu.html  
+ Server leaks inodes via ETags, header found with file /UwRZ65Ry.render_css, fields: 0xbd1 0x4f29e57860c80  
+ OpenSSL/0.9.8y appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.  
+ PHP/5.4.22 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
```

Hình 3-11: Giao diện quét với Nikto

Kết quả.

- Apache Web Sever
- Phiên bản PHP/5.4.22



```
File Edit View Search Terminal Help
+ Root page / redirects to: home/trangchu.html
+ Server leaks inodes via ETags, header found with file /3nrrAbDQ.types, fields: 0xbd1
0x4f29e57860c80
+ PHP/5.4.22 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41
are also current.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.6
5 (final release) and 2.2.29 are also current.
+ OpenSSL/0.9.8y appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o an
d 0.9.8zc are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /admin/config.php: PHP Config file may contain database IDs and passwords.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sens
itive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sens
itive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sens
itive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sens
itive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /home/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /mt/: This might be interesting... potential country code (Malta)
+ OSVDB-3092: /tv/: This might be interesting... potential country code (Tuvalu)
+ Cookie hpu[LastUrl] created without the httponly flag
+ /httpd.conf: Apache httpd.conf configuration file
```

Hình 3-12: Giao diện lỗi OSVDB

Có tất cả 11 lỗi OSVDB:

- OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST.
- OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
- OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

- OSVDB-12184:/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42:  
PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- OSVDB-12184:/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42:  
PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- OSVDB-12184:/?=PHPE9568F35-D428-11d2-A769-90AA001ACF42: PHP reveals potentially sens.
- OSVDB-3092: /home/: This might be interesting...
- OSVDB-3268: /icons/: Directory indexing found.
- OSVDB-3233: /icons/README: Apache default file found.
- OSVDB-3092: /mt/: This might be interesting... potential country code (Malta).
- OSVDB-3092: /tv/: This might be interesting... potential country code (Tuvalu).

## KẾT LUẬN

Phát hiện bảo mật nói chung và phát hiện bảo mật website nói riêng luôn là vấn đề cấp thiết và cần được giải quyết triệt để. Ngày nay, khi ngành công nghệ thông tin phát triển với một tốc độ chóng mặt thì vấn đề về kiểm thử bảo mật càng trở nên cấp thiết hơn và khó khăn hơn. Điều này thể hiện rõ ràng qua con số thống kê về số lượng website thương mại điện tử, kẻ tấn công tấn công mỗi ngày một tăng lên, quy mô các cuộc tấn công và mức độ thiệt hại ngày càng lớn hơn.

Tuy nhiên bên cạnh những điều đạt được, đề tài còn tồn tại một vài điểm hạn chế sau: Hạn chế đầu tiên của chuyên đề là, những lỗi bảo mật mà đề tài nêu ra chỉ là những lỗi bảo mật phổ biến chứ chưa bao phủ được hết toàn bộ các lỗi bảo mật hiện nay. Trên cơ sở nghiên cứu các tư liệu và kết quả thực nghiệm cho thấy kiểm thử bảo mật website là rất quan trọng, việc thực hiện kiểm thử sớm sẽ làm giảm thời gian kiểm thử cho các giai đoạn sau và tăng chất lượng của sản phẩm. Việc thực hiện kiểm thử bảo mật (kiểm thử ngay từ giai đoạn phân tích thiết kế hệ thống ) là rất tốt.

## TÀI LIỆU THAM KHẢO

- [1]. <https://tailieu.vn/doc/de-tai-tim-hieu-ve-bao-mat-mang-lan-va-su-dung-cong-cu-nessus-quet-lo-hong-bao-mat-trong-mang-lan-1749290.html>
- [2]. <https://123doc.org//document/4003918-do-an-tot-nghiep-danh-gia-bao-mat-he-thong-mang-cong-cu-kali-linux.htm>
- [3]. <https://text.123doc.org/document/3474246-nghien-cuu-mot-so-dang-lo-hong-bao-mat-cong-cu-phat-hien-va-ung-dung-de-kiem-thu-an-ninh-website.htm>
- [4]. <https://anonyviet.com/quet-lo-hong-bao-mat-trang-web-voi-nikto/>
- [5]. <https://123doc.org/document/3153469-nghien-cuu-mot-so-lo-hong-thieu-an-ninh-trong-ung-dung-cong-nghe-thong-tin-phuong-phap-va-cong-cu-kiem-soat-xu-ly-lo-hong.htm>
- [6]. <https://123doc.org//document/1616951-tim-hieu-cong-cu-quet-mang-nmap.htm>
- [7]. <https://www.mystown.com/2016/03/huong-dan-su-dung-nmap-e-scan-port-tren.html>
- [8]. <https://oktot.net/huong-dan-scan-port-voi-zenmap/>
- [9]. <https://cuongquach.com/nikto-cong-cu-tim-loi-co-ban.html>
- [10]. <http://hacking1993.blogspot.com/2016/09/quet-lo-hong-smb-bang-nmap-kali-linux.html>