**LỜI MỞ ĐẦU**

Những năm gần đây, trong xu thế của cuộc cách mạng công nghiệp 4.0, cùng với việc CNTT được ứng dụng ngày càng sâu rộng vào mọi mặt của đời sống, các chuyên gia đều có chung nhận định, tình hình an toàn thông tin mạng trên thế giới nói chung và Việt Nam nói riêng ngày càng diễn biến phức tạp. Không nằm ngoài xu thế chung trên toàn cầu, công tác đảm bảo an toàn thông tin mạng của các cơ quan, tổ chức, doanh nghiệp tại Việt Nam đã và đang phải đối mặt với rất nhiều thách thức, bởi các cuộc tấn công mạng vào hệ thống thông tin gia tăng mạnh mẽ cả về quy mô cũng như mức độ phức tạp, tinh vi, khó dự đoán.

Cũng trong tháng đầu tiên năm 2019, hệ thống của Trung tâm đã ghi nhận 1.025.104 địa chỉ IP của Việt Nam thường xuyên nằm trong các mạng máy tính ma (botnet).

Trước đó, theo số liệu từ Trung tâm Giám sát an toàn không gian mạng quốc gia, năm 2018, có 10.220 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam, giảm 1.023 cuộc so với năm 2017 (tương đương 10%).

Trong đó có 5.932 cuộc tấn công lừa đảo, 3.198 cuộc tấn công thay đổi giao diện và 1.090 cuộc tấn công cài cắm mã độc. Cuối năm 2018, sau khi Bộ TT&TT phối hợp với các một số Bộ, ngành, địa phương và các doanh nghiệp tiến hành rà soát, bóc gỡ mã độc, số lượng địa chỉ IP Việt Nam nằm trong mạng máy tính ma đã giảm khoảng 6% so với năm 2017, còn trên 4.181.000 địa chỉ.

Năm 2019 trong Quý này có 620 cuộc tấn công mạng nhằm vào các hệ thống thông tin ở Việt Nam. Dựa vào việc khai thác các lỗ hổng thông tin, lừa đảo trên mạng xã hội và đánh cắp thông tin khách hàng.

Trend Micro, công ty dẫn đầu trong các giải pháp an ninh mạng, hôm nay đã công bố Báo cáo dự đoán tình hình hiểm họa năm 2019, cảnh báo rằng sẽ có các phương thức tấn công an ninh mạng tinh vi hơn trong năm 2019.

Từ trước đến nay vấn đề bảo mật trong mạng luôn là vấn đề cấp thiết . Công nghệ càng phát triển nhu cầu sử dụng trao đổi thông tin qua mạng càng nhiều và trở nên tất yếu. Cũng vì vậy mà các tài nguyên, dữ liệu rất rất bị rò rỉ và đánh cắp thông tin.

Việc tấn công các hổng đánh cắp thông tin của nạn nhân càng ngày càng tinh vinh thì việc tìm kiếm lỗ hổng bảo mật từng ngày được hoàn thiện hơn.

**LỜI CẢM ƠN**

I. TỔNG QUAN VỀ AN NINH MẠNG.

I.1. Bảo mật thông tin là gì?

Bảo mật là sự hạn chế khả năng lạm dụng tài nguyên và tài sản. Bảo mật trở nên đặc biệt phức tạp trong quản lý, vận hành những hệ thống thông tin có sử dụng các công cụ tin học, nơi có thể xảy ra và lan tràn nhanh chóng việc lạm dụng tài nguyên (các thông tin di chuyển vô hình trên mạng hoặc lưu trữ hữu hình trong các vật liệu) và lạm dụng tài sản (các máy tính, thiết bị mạng, thiết bị ngoại vi, các phần mềm của cơ quan hoặc người sở hữu hệ thống). Hạn chế ở đây có ý rằng không thể triệt phá hết ngay việc lạm dụng, cho nên cần sẵn sàng đề phòng mọi khả năng xấu với các phương cách thích hợp và chuẩn bị xử lý các sự cố nếu có việc lạm dụng xảy ra.

I.2. An ninh mạng là gì?

An ninh mạng (cybersecurity), an ninh máy tính (computer security), bảo mật công nghệ thông tin (IT security) hay an ninh mạng máy tính là việc bảo vệ hệ thống mạng máy tính từ các hành vi trộm cắp hoặc làm hư hỏng phần cứng, phần mềm hoặc các dữ liệu, cũng như từ sự gián đoạn hoặc chuyển lạc hướng của các dịch vụ được cung cấp.

Network Security sẽ bảo vệ chống lại mọi hoạt động tấn công mạng từ phía bên trong và phía bên ngoài . Đó có thể là hành vi tấn công vào hệ thống an ninh mạng của công ty từ những nhân viên hoặc người lạ sử dụng usb của nhân viên trong công ty và biết được mật khẩu của nhân viên trong công ty, sau đó thực hiện hành vi tấn công. Hoặc có những trường hợp tin tặc sẽ tấn công từ bên ngoài tường lửa của doanh nghiệp của bạn. Một hệ thống an ninh hiệu quả sẽ giám sát tất cả các hoạt động mạng, cảnh báo về những hành động vi phạm trái phép và thực hiện những sự thay đổi, ăn cắp dữ liệu… (những hành động trái phép).

I.3. Sự kiện bảo mật năm 2011 và các cuộc tấn công lớn

I.3.1. VietNamNet bị tấn công DDoS lớn chưa từng có .

Trong vài ngày qua, báo VietNamNet đã phải hứng chịu một cuộc tấn công từ chối dịch vụ phân tán (DDoS) ở quy mô lớn chưa từng có tại Việt Nam, xuất phát từ một mạng lưới khổng lồ gồm hàng chục ngàn máy tính bị nhiễm vi rút. Bắt đầu từ cuối ngày 4/1/2011, lưu lượng truy cập vào trang chủ báo VietNamNet tại địa chỉ http://vietnamnet.vn tăng nhanh một cách bất thường, lên tới hàng trăm ngàn kết nối tại một thời điểm.

Với lượng độc giả truy cập hàng ngày, số lượng kết nối tại một thời điểm chỉ ở

mức dưới một trăm ngàn. Nên việc tại một thời điểm có tới hàng trăm ngàn kết nối liên tục (bao gồm cả của các độc giả thông thường) tới máy chủ web đã khiến băng thông đường truyền mạng bị quá tải. Do vậy, độc giả truy cập vào báo VietNamNet sẽ bị tắc nghẽn ngay từ đường truyền và báo lỗi không tìm thấy máy chủ, phải truy cập vài lần mới mở được trang web.

Trên thực tế, báo VietNamNet đã từng bị tấn công DDoS nhiều lần nhưng ở quy

mô vài chục ngàn kết nối tại một thời điểm nên băng thông hệ thống và công suất các máy chủ vẫn có thể chịu đựng được. Trong cuộc tấn công DDoS đang diễn ra, kẻ thủ ác đã thể hiện khả năng rất chuyên nghiệp khi huy động một mạng lưới botnet với lượng máy lên tới hàng chục ngàn máy tính.

I.3.2. "Hacktivism" nổi dậy

Hacktivism là thuật ngữ diễn tả hành động tấn công, đột nhập vào một hệ thống máy tính nhằm mục đích chính trị. Trên thế giới hiện nay, những nhóm hacker mang "mác" hacktivism nổi tiếng có thể kể đến bao gồm Anonymous, LulzSec (đã gác kiếm), hay TeaMp0isoN. Trong suốt năm 2011 qua, các nhóm hacktivism đã tiến hành nhiều hoạt động khác nhau chống lại các cơ quan luật pháp, ngân hàng, chính phủ, các công ty bảo mật và những nhà cung cấp phần mềm như tấn công lỗ thủng an ninh các hệ thống của Tổ chức Liên hiệp quốc (UN), cơ quan tình báo bảo mật Straffor, CIA…

I.3.3. Các cuộc tấn công lớn khác ở Việt Nam:

I.3.3.1. Cuộc tấn công vào năm 2012 của Bkav:

Tháng 2/2012 Website bị deface, lộ hơn 100.000 địa chỉ email, mật khẩu diễn đàn, xuất hiện nhiều bài viết công kích.

Vài 13/02/2012, nhóm hacker tự nhiện là “Anoymous/LulzSec Việt Nam” đã tấn công diễn đàn Bkav và công khai toàn bộ dữ liệu của diễn đàn bao gồm hơn 100.000 địa chỉ email và toàn bộ dữ liệu cho đến tháng 02/2012. Ngày 24/02/2012, các hacker công bố 8 lỗi bảo mật nghiêm trọng trong hệ thống web của công ty trên một blog. Tuy nhiên, đại diện từ Bkav đã khắng định thông tin về số lỗ hổng này không xác định.

I.3.3.2 Cuộc tấn công vào năm 2014 của VCCrop.

Nhiều website lớn của Kênh14, Gamek, Genk, CafeF và một số website do VCCorp vận hành kỹ thuật như Dân Trí, Soha, Người Lao Động… ngưng hoạt động.

Trong khoảng 17-18/10, các website thuộc sở hữu của VCCorp và các đối tác công ty này liên tục không thể truy cập hoặc chuyển hướng về blog “VCCorp truyện”với nhiều thông tin tiêu cực về VCCrop. Báo Bantri và VnEconomy liên tiếp bị gián đoạn. Website giadinh.net nghi ngờ bị hacker xoá toàn bộ dữ liệu trên máy chủ. Sự cố đã gây thiệt hại cho VCCorp hàng chục tỷ đồng cà được coi như nghiêm trọng nhất từ ngày xảy ra cho đến nay.

I.3.3.3 Cuộc tấn công vào năm 2015 của VNG.

Ảnh hưởng đến thông tin cá nhân 163 triệu người dùng.

Vào ngày 26/4/2018, hơn 163 triệu tài khoản Zing ID bị phát hiện được rao bán trên một diễn đàn nước ngoài. VNG xác nhận sự kiện này xảy ta từ năm 2015 nhưng đã không có hành đồng công bố vụ việc, Các dữ liệu bị lộ gồm mật khẩu, tên đăng nhập, mã game, email, số điện thoại, họ tên đầy đủ, ngày sinh, địa chỉ, IP…Dữ liệu mật khẩu bị lộ được cộng đồng bảo mật đánh giá đã được mã hoá sơ sài và dễ dàng bị giải mã bởi hacker.

I.3.3.4 Cuộc tấn công vào năm 2016 của Airlines:

Ảnh hưởng đến thông tin của 411.000 người dùng, chiếm đoạt hệ thống thông báo sân bay.

Chiều ngày 29/07/2019, một số màn hình hiện thị thông tin chuyên bay của các Sân bay quốc tế Tân Sơn Nhất, Nội Bài, Đà Nẵng, Sân bay Phú Quốc bị chèn những nội dung xúc phạm Việt Nam và Philippines, xuyên tạc các nội dung về biển Đông. Website của Vietnam Airlines bị điều hướng đến trang khác và tiết lộ dữ liệu của 411.000 thành viên Golden Lotus – phần lớn các lãnh đạo, quản lý cơ quan nhà nước, ngân hàng, doanh nghiệp lớn…Những thông tin trong file bao gồm họ tên, ngày sinh, địa chỉ thường trú, đơn vị làm việc, số điện thoại, quốc tịch, ngày tham gia chương trình, điểm tích luỹ, mật khẩu GLP và có nguy cơ hacker giữ lại không công bố số thẻ ứng dụng. Hơn 1000 chuyến bay bị ảnh hưởng.

I.4. Các cuộc tấn công trên thế giới

I.4.1. Công ty cung cấp giải pháp bảo mật cho chính phủ Hoa Kỳ bị tấn công

Vào tháng 1-2011, những hacker thuộc Anonymous đã đột nhập máy chủ web của HBGary Federal – hbgaryfederal.com – thông qua việc sử dụng những đoạn mã SQL bất hợp pháp nhằm khai thác một lỗ hổng bảo mật tồn tại trong cơ sở dữ liệu của một ứng dụng. Sau đó trích xuất mã MD5 cho các mật khẩu thuộc sở hữu của giám đốc điều hành (CEO), Aaron Barr, và COO, Ted Vera. Cả hai đều dùng mật khẩu rất đơn giản: 6 kí tự thường và 2 con số.

Những mật khẩu như thế này cho phép những kẻ tấn công tiếp cận vào những tài liệu nghiên cứu của công ty và hàng chục ngàn email được lưu trữ trong Google Apps. Như vậy, việc sử dụng những mật khẩu thiếu an toàn cho hệ thống phần mềm cũ cộng với việc sử dụng điện toán đám mây đã gây ra cơn ác mộng đối với an ninh bảo mật.

I.4.2. Các cuộc tấn công nổi tiếng:

Tháng 2/2001, máy chủ của Cục tài chính Ireland bị một số sinh viên Đại học Maynooth ở nước này tấn công DDoS.

Ngày 15/8/2003, Microsoft chịu đợt tấn công DoS cực mạnh và làm gián đoạn websites trong vòng 2 giờ.

Tháng 2/2007, hơn 10.000 máy chủ của game trực tuyến như Return to Castle Wolfenstein, Halo, Counter-Strike …bị nhóm RUS tấn công với hệ thống điều khiển chủ yếu đặt tại Nga, Uzbekistan và Belarus.

Trong suốt các tuần đầu của cuộc chiến Nam Ossetia 2008, các trang web của chính phủ Georgia luôn trong tình trạng quá tải, gồm các trang web ngân hàng quốc gia và của tổng thống Georgia Mikhail Saakashvili. Chính phủ Nga phủ nhận mọi sự cáo buộc cho rằng họ đứng đằng sau vụ tấn công.

Tháng 8/2009, các vụ DDoS nhắm tới một loạt trang mạng xã hội đình đám

như Facebook, Twitter, LiveJournal và một số website của Google được thực hiện chỉ để "khóa miệng" một blogger có tên Cyxymu ở Georgia

Ngày 28/11/2010, WikiLeaks bị tê liệt vì DDoS ngay khi họ chuẩn bị tung ra những tài liệu mật của chính phủ Mỹ.

Ngày 7/12/2010, nhóm hacker có tên Anonymous đánh sập website Visa.com sau khi tổ chức những cuộc tấn công tương tự vào Mastercard và PayPal để trả đũa cho việc chủ WikiLeaks bị tạm giam ở Anh.

Ngày 3/3/2011, dịch vụ blog nổi tiếng thế giới WordPress bị tấn công.

Ngày 4/3/2011, 40 trang web của các cơ quan chính phủ Hàn Quốc bị tê liệt vì DDoS.

Năm 2013 – 2014. Ảnh hưởng đến: 3 tỉ tài khoản người dùng. Tại thời điểm tháng 9 năm 2016, khi Yahoo đang thương lượng việc bán lại cho Verizon, công ty này đã công bố thông tin về vụ lộ dữ liệu lớn nhất trong lịch sử – xảy ra từ năm 2014 với 500 triệu tài khoản bị ảnh hưởng. Chẳng bao lâu sau, Yahoo cập nhật thêm thông tin về một cuộc tấn công mạng khác vào năm 2013 với số tài khoản bị ảnh hưởng lên đến 1 tỉ. Lần này không chỉ tên, ngày sinh, địa chỉ email và mật khẩu (không được mã hóa chặt chẽ) mà cả câu hỏi bảo mật và đáp án cũng bị đánh cắp. Đến tháng 10 năm 2017, số lượng tài khoản bị ảnh hưởng cuối cùng cũng được chốt: 3 tỉ tài khoản.

Tháng 5/2014. Ảnh hưởng đến: 145 triệu tài khoản. Những hacker thực hiện cuộc tấn công mạng vào trang thương mại trực tuyến này đã xâm nhập vào hệ thống của eBay qua tài khoản của 3 nhân viên và có quyền truy cập nội bộ trong suốt 229 ngày. Toàn bộ 145 triệu người dùng bị lộ thông tin tài khoản bao gồm tên, địa chỉ, ngày sinh và mật khẩu đã mã hóa. Tuy thông tin thanh toán được lưu trữ riêng và không bị đánh cắp, eBay vẫn chịu sự chỉ trích vì đã không cảnh báo người dùng một cách rõ ràng.

Tháng 10/2016. Ảnh hưởng đến: hơn 412,2 triệu tài khoản. Mạng xã hội FriendFinder bao gồm các trang kết bạn và có nội dung người lớn (bao gồm Adult Friend Finder) đã bị lộ thông tin người dùng vào khoảng giữa tháng 10/2016. Dữ liệu trong 20 năm hoạt động bị mất trong cuộc tấn công mạng này bao gồm tên, địa chỉ email và mật khẩu. Do mã hóa không chặt chẽ, gần như toàn bộ số mật khẩu này đã bị giải mã tại thời điểm bài phân tích về số dữ liệu trên được đăng trên LeakedSource.com.

II. TỔNG QUAN VỀ HACKING.

II.1.Hacker là gì?

Hacker (còn được gọi là tin tặc) là người hiểu rõ hoạt động của hệ thống máy tính, mạng máy tính, có thể viết hay chỉnh sửa phần mềm, phần cứng máy tính để làm thay đổi, chỉnh sửa nó với nhiều mục đích tốt xấu khác nhau. Công việc của hacker bao gồm lập trình, quản trị và bảo mật.

Hacker là những người thực hiện hack. Họ sử dụng những kiến thức của họ để khai khác lỗi hỏng, điểm yếu. Hacker cũng được phân ra nhiều loại.

II.2. . Tại sao lại nghiên cứu về hacking và cần kỹ năng gì?

II.2.1. Tại sao phải nghiên cứu về hacking.

Để biết điểm yếu của hệ thống. Nhận ra điểm yếu để kiểm soát chúng là điều cần thiết nhưng điều đó không có nghĩa là điểm yếu luôn gây tổn hại. Tìm ra các lỗ hổng từ hệ thống giúp ta có thể phòng trừ và sửa chữa chúng.

Giúp hệ thống an toàn hơn. Việc đảm bảo tính sẵn sàng và hoạt động đúng đắn của hệ thống máy tính mà không quan tâm đến thông tin được lưu trữ, xử lý bởi chúng. Đảm bảo thông tin tập trung vào lý do đảm bảo rằng thông tin được bảo vệ và vì thế nó là lý do để thực hiện an toàn thông tin.

II.2.2. Các kỹ năng căn bản cần thiết để nghiên cứu hacking:

Có kiến thức ở nhiều nền tảng (Linux, Unix, Windows..).

* UNIX là hệ điều hành đa nhiệm và đa người dùng, được thiết kế để mang lại độ tin cậy và bảo mật cho bất kỳ hệ thống nào sử dụng nó. UNIX được phát triển bởi một nhóm nghiên cứu viên tại AT&T Bell Lab. Nắm rõ kiến thức mạng (network), kĩ thuật máy tính, bảo mật.
* Một số lượng rất rất lớn web server đang chạy các hệ điều hành nhân UNIX. Do đó việc sử dụng thành thạo và hiểu được design của UNIX là một kỹ năng không thể thiếu của lập trình viên nói chung và hacker nói riêng.
* Ngoài tượng đài UNIX, các hệ điều hành Window cũng là một mục tiêu thú vị để tìm hiểu. Có 2 lý do để học window đó là: các máy tính cá nhân phần lớn đều sử dụng window và hệ điều hành này có rất nhiều lỗ hổng.
* Việc thực hành khai thác lỗ hổng vừa mang lại kỹ năng hacking căn bản, vừa cho biết sự quý giá và tầm quan trọng của việc cập nhật Windows nói riêng và các phần mềm khác nói chung.

Lập trình C và các ngôn ngữ lập trình khác

* C là một ngôn ngữ lập trình mạnh mẽ bậc nhất. Thành thạo ngôn ngữ C là rất cần thiết đối với lập trình viên nói chung và hacker nói riêng. C là ngôn ngữ lập trình hướng cấu trúc. Với ngôn ngữ C, các tác vụ được chia thành từng phần nhỏ hơn và các phần nhỏ này được hoàn thành bởi một số đoạn mã.
* Với Hacker, ngoài C, vẫn cần thêm các công cụ đắc lực khác. Một trong số các công cụ đó là những ngôn ngữ lập trình bậc cao như Java, Perl, và đặc biệt là Python. Học thêm các ngôn ngữ lập trình khác ngoài C giúp ích rất nhiều cho việc khai thác cũng như vá lỗ hổng của các ứng dụng. Nó được biết đến như là ngôn ngữ ổn định, manh mẽ, linh hoạt cùng với độ bảo mật rất cao. Tìm hiểu mô hình bảo mật áp dụng trong Java là cách nhanh nhất giúp nắm được những nền tảng bảo mật áp dụng trong ngôn ngữ lập trình.
* Perl là ngôn ngữ lập trình đa dụng khá linh hoạt, một số tính năng của Perl đưjc lấy ý tưởng từ C. Python nổi tiếng với cú pháp ngắn gọn, dễ học. Tuy cú pháp đơn giản nhưng Python có thể làm được nhiều thứ hơn bạn nghĩ: lập trình web, lập trình big data, viết tool automation,…

Khởi động bằng các tutorial

* Để trở thành Hacker, con đường ngắn nhất là …. bắt tay vào hack. Tuy nhiên “động chạm” vào các hệ thống lớn không phải là chuyện dễ dàng khi có rất nhiều rào cản cả về mặt pháp lý lẫn chuyên môn đối với newbie. Do đó, con đường tối ưu nhất là “tập hack” theo các kịch bản có sẵn.

II.3. Phân loại hacker:

Về cơ bản có 4 loại hacker: hacker mũ trắng, hacker mũ xám, hacker mũ đen, hacker mũ xanh. Nhưng thực tế còn nhiều loại hacker khác.

II.3.1 Hacker mũ trắng (White Hat):

Hacker mũ trắng ho thường là những chuyên gia an nunh mạng, hỗ trợ chính phủ và các tổ chức bằng cách thâm nhập hệ thống để kiểm tra dữ liệu có lỗ hổng nào trong hàng rào bảo mật không. Trong nhiều trường hợp họ cũng xoá vius, phần mềm độc hại cũng như chống lại hacker mỹ đen và các tội phạm mạng khác. Về cơ bản họ được xem là các hacker “có đạo đức”.

II.3.2. Hacker mũ đen (Back Hat):

Khác với hacker mũ trắng, hacker mũ đen là những kẻ gây hại tới cộng đồng. Họ thường tìm các lỗ hổng trong máy tính cá nhân, các tổ chức ngân hàng, doanh nghiệp… để đánh cắp thông tin, dữ liệu, tài chính nhằm chuộc lợi cho cá nhân hoặc một tổ chức nào đó.

II.3.3. Hacker mũ xám (Grey Hat):

Hacker mũ xám nằm giữa hacker mũ đen và hacker mũ trắng. Họ không ăn cấp tiền hay thông tin nhưng họ cũng không giúp ích được cho người khác. Một hacker mũ xám có thể khai thác lỗ hổng, nhưng thay vì sử dụng nó cho mục đích cá nhân, họ có thể nói cho hacker mũ trắng hoặc mũ đen biết để khám phá, cũng có khi họ nói với tổ chức liên quan để sửa chữa vấn đề. Những hacker này chiếm một số lượng lớn trong giới hacker, dù cho hacker mũ xám mới là những hacker chiếm được hầu hết sự chú ý của giới truyền thông.

II.3.4. Hacker mũ xanh (Blue hat):

Hacker mũ xanh là họ là những chuyên gia lập trình tài năng được các công ty lớn mời về làm việc để chuyên tìm lỗi, khai thác lỗ hổng và sữa chữa.

Về nguyên tắc nói chùng mọi hacker đều là xấu và hành động của họ là trái với pháp luật.

II.4. Tấn công mạng:

II.4.1. 1. Tần công mạng là gì:

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

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

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

II.4.1.2. Đối tượng bị tấn công

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

II.4.1.3. Mục đích tấn công mạng

Tích cực: Tìm ra những lỗ hổng bảo mật, những nguy cơ tấn công mạng cho cá nhân và tổ chức từ đó chỉ ra các giải pháp phòng chống, ngăn chặn sự đe dọa từ tin tặc.

Tiêu cực: Phá hoại, lừa đảo tống tiền, mua vui, đe dọa nạn nhân.

II.4.2. Các phương pháp tấn công mạng điển hình

II.4.2.1. Tấn công do thám (Reconnaissance attack)

II.4.2.1.1. Khái niệm:

Tấn công do thám. Là hình thức tấn công nhằm thu thập các thông tin về hệ thống mục tiêu, từ đó phát hiện ra các điểm yếu. Tấn công do thám thường để làm bàn đạp cho cuộc tấn công truy cập hoặc tấn công từ chối dịch vụ về sau.

II.4.2.1.2. Các kỹ năng do thám thông dụng:

* Nghe lén
* Quét địa chỉ IP
* Quyét cổng
* Quét né tránh
* Xác định hệ điều hành

II.4.2.1.3. Các thông tin cần ghi nhận

* Địa chỉ IP
* Các dịch vụ mạng đang sử dụng
* Cổng của các ứng dụng nào đang mở
* Hệ điều hành đang sử dụng
* Phiên bản Web server nào…

II.4.2.2. Tấn công truy cập (Access attack)

II.4.2.2.1. Khái niệm

Tấn công truy cập là loại tấn công chiếm lấy tài nguyên trên hệ thống như file, mật khẩu, quyền điều khiển, thường khai thác các lỗ hổng của hệ thống nạn nhân. Các lỗ hổng này thường là: lỗ hổng trong các dịch vụ xác thực, dịch vụ FTP, dịch vụ web. Sau khi khai thác lỗ hổng, kẻ tấn công sẽ có quyền truy cập vào tài khoản web, database và các dữ liệu nhạy cảm khác. Kiểu tấn công này thường rất đa dạng về hình thức nhưng có điểm chung là kẻ tấn công thường dùng từ điển để đoán mật khẩu.

II.4.2.2.2. Các kỹ thuật tấn công truy cập

* Nghe lén.
* Sử dụng lại.
* Cướp giao dịch.
* Kẻ đứng giữa.
* Cổng sau.
* Đánh lừa.
* Khai thác lỗ hổng.
* Tấn công mật khẩu.

II.4.2.3. Tấn công từ chối dịch vụ (DoS)

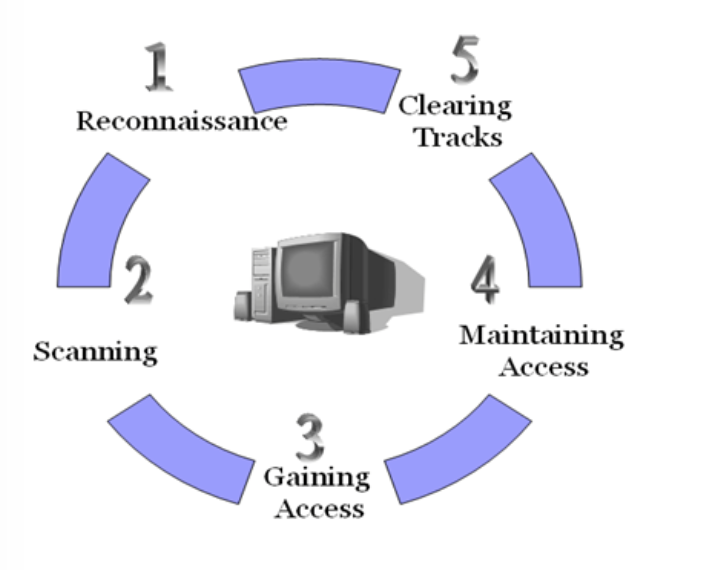
II.4.2.3.1. Khái niệm

Là tấn công phá hoại chứ không nhằm mục đích lấy được thông tin. Tấn công từ chối dịch vụ DoS có thể mô tả như hành động ngăn cản những người dùng hợp pháp khả năng truy cập và sử dụng vào một dịch vụ nào đó. Nó bao gồm làm tràn ngập mạng, mất kết nối với dịch vụ… mà mụcc đích cuối cùng là Server không thể đáp ứng đựng các yêu cầu từ Client.

II.4.2.3.2. Các kỹ thuật tấn công:

* Kỹ thuật làm lụt bằng SYN.
* Kỹ thuật làm lụt UDP.
* Kỹ thuật DoS phân tán (DDoS).

II.5. Các giai đoạn tấn công.



II.5.1. Thăm dò  (Reconnaissace)

Thăm dò mục tiêu là một trong những bước qua trọng để biết những thông tin trên hệ thống mục tiêu. Hacker sử dụng kỹ thuật này để khám phá hệ thống mục tiêu đang chạy trên hệ điều hành nào, có bao nhiêu dịch vụ đang chạy trên các dịch vụ đó, cổng dịch vụ nào đang đóng và cổng nào đang mở, gồm hai loại:

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

II.5.2. Quét hệ thống (Scanning)

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

II.5.3. Chiếm quyền điều khiển (Gainning access)

Đến đây hacker đã bắt đầu dần dần xâm nhập được hệ thống và tấn công nó, đã truy cập được nó bằng các lệnh khai thác. Các lệnh khai thác luôn ở bất cứ không gian nào, từ mạng LAN cho tới INTERNET và đã lan rộng ra mạng không dây.

Hacker có thể chiếm quyền điều khiển tại:

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

II.5.4. Duy trì điều khiển hệ thống (Maitaining access)

Đến đây hacker bắt đầu phá hỏng làm hại, hoặc có thể cài trojan, rootkit,

backdoor để lấy thông tin thêm. Thường được thấy sử dụng để đánh cắp tài khoản tín dụng, ngân hàng...

II.5.5. Xoá dấu vết (Clearning tracks)

Được đề cập đến hoạt động được thực hiện bằng cách hacker cố tình che dấu hành động xâm nhập của mình. Hacker phải tìm cách xóa đi dấu vết mỗi khi đột nhập bằng các phương thức như Steganography, tunneling, and altering log file.

III. TỔNG QUAN VỀ METASPLOIT.

III.1. Giới thiệu

III.1.1. Khái niệm về lỗ hổng

Các lổ hỗng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lổ hỗng cũng có thể nằm ngay trên các dịch vụ cung cấp như sendmail, web, ftp… Ngoài ra các lổ hỗng còn tồn tại ngay chính tại hệ điều hành như trong Windows NT, Win 95, UNIX hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng như trong processing, các hệ database…

III.1.2. Vòng đời phát hiện và khai thác lỗ hổng.

Discovery (phát hiện): Một nhà nghiên cứu bảo mật hoặc cung cấp phát hiện ra một khả năng dễ bị tổn thương trong phần mềm.

Disclosure (tiết lộ): Nhà nghiên cứu bảo mật thông báo cho nhà cung cấp.

Analysis (phân tích): các nhà nghiên cứu hoặc những người khác trên toàn thế giới bắt đầu phân tích lổ hỗng để xác định khả năng khai thác của nó. Nó có thể được khai thác hay không? Hay là khai thác từ xa? Chiều dài của đoạn mã khai thác được tiêm vào làm gì? Giai đoạn này cũng bao gồm việc gỡ lỗi ứng dụng dễ bị thương tổn.

Exploit development (phát triển khai thác): một câu trả lời cho những câu hỏi quan trọng đã được xác định, quán trình phát triển khai thác bắt đầu. Điều này đòi hỏi sự hiểu biết sâu sắc về các thanh ghi của bộ xử lý, mã assembly, địa chỉ offsets và payload.

Testing (Kiểm tra): Sau khi khai thác được thực nghiệm và các thông số cụ thể cần thiết cho nó thực thi thành công đã được xác định, coder sẽ phát hành khai thác hoặc riêng tư hoặc trên diễn đàn công cộng. Thỉnh thoảng khai thác sẽ được tinh chỉnh.

Metasploit là một dự án bảo mật máy tính cung cấp các thông tin vấn đề lỗ hổng bảo mật cũng như giúp đỡ về kiểm tra xâm nhập và phát triển hệ thống phát hiện xâm nhập. Một dự án con rất nổi tiếng của Metasploit là Metasploit Framework.

III.1.3. Lịch sử của Metasploit

Metasploit project là một dự án máy an ninh máy tính mã nguồn mở cung cấp thông tin về lỗ hổng bảo mật và hỗ trợ việc thử nghiệm thâm nhập và phát triển IDS (Intrusion Detection Systems\_Hệ thống phát hiện xâm nhập) signature. Tiểu project nổi tiếng nhất của nó là Metasploit Framework, một công cụ để phát triển và thực thi exploit code (mã khai thác) đối với một máy tính mục tiêu từ xa. Các tiểu project quan trọng khác bao gồm: Database Opcode, lưu trữ shellcode, và nghiên cứu bảo mật.

Metasploit project cũng nổi tiếng với các công cụ anti-forensic và evasion, một số trong đó được xây dựng vào Metasploit Framework.

Metasploit đã được tạo ra bởi HD Moore vào năm 2003 như một công cụ mạng di động bằng cách sử dụng ngôn ngữ kịch bản Perl.Sau đó, Metasploit Framework đã được viết lại hoàn toàn bằng ngôn ngữ lập trình Ruby và đã trở thành project Ruby lớn nhất thế giới, với hơn 700,000 dòng code. nó là một công cụ mạnh mẽ cho các nhà nghiên cứu an ninh của bên thứ ba để điều tra lỗ hổng bảo mật tiềm năng.

Sau nhiều năm thành công trong cộng đồng hacker/penetration tester. Ngày 21 Tháng 10 năm 2009 có công bố nói rằng Metasploit project đã được mua lại bởi Rapid7, một công ty bảo mật cung cấp các giải pháp quản lý lỗ hổng. Giống như các sản phẩm thương mại tương đương như Canvas của Immunity hoặc Core Impact của Core Security Technologies, Metasploit có thể được sử dụng để kiểm tra lỗ hổng của các hệ thống máy tính để bảo vệ chúng, và nó có thể được sử dụng để đột nhập vào hệ thống từ xa. Cũng như nhiều công cụ bảo mật thông tin khác, Metasploit cũng có thể được sử dụng cho cả các hoạt động hợp pháp và các hoạt động trái phép.

Sau đó, Metasploit framework được chia thành ba phiên bản, trong đó có hai phiên bản Metasploit Express và Metasploit Professional là phiên bản thương mại, Metasploit Professional được bán với giá 1.800$. Cả hai đều sở hữu một giao diện khá đẹp nhiều bells và whistles, bao gồm cả chức năng tự động hóa một số cuộc tấn công. Ngoài ra còn có một phiên bản là open source community edition được gọi là Metasploit Community.

May mắn thay, một số nhà phát triển độc lập tại Armitage đã tạo ra một GUI nguồn mở miễn phí cho Metasploit, giao diện khá đẹp và thanh lịch, thích hợp sử dụng cho những người thích chế độ hoạt động point-and-click.

Metasploit phiên bản dành cho Windows, sở hữu nhiều tính năng (raw IP packet injection, wireless driver exploitation, SMB relaying attacks ...) không có sẵn trong môi trường Windows, hạn chế này có thể khắc phục bằng cách sử dụng Cygwin hoặc chạy Windows trong môi trường ảo trên Linux.

III.1.4. Khái niệm Mestasploit

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

Metasploit framework là một framework mã nguồn mở phát triển nhằm sử dụng các shellcode (payload) để tấn công máy có lỗ hổng. Cùng với một số bộ công cụ bảo mật khác, Metasploit có cơ sở dữ liệu chứa hàng ngàn shellcode, hàng ngàn exploit của các hệ điều hành, các chương trình hay dịch vụ. Trong quá trình phát triển metasploit liên tục cập nhật các Exploit...Nên càng ngày nó càng trở thành một bộ công cụ mạnh mẽ.

Metasploit framework là một bộ dự án sinh ra để kiểm tra độ an toàn (pentesting) nhưng đối với những attacker như chúng ta, thì nó thực sự là một công cụ vô cùng hữu ích (dùng để kiểm tra, khai thác lỗi ,exploit ).Thực sự theo mình nghĩ thì ai muốn làm hacker (hay script kidie đi chăng nữa ) thì cũng nên bỏ thời gian ra nghiên cứu kĩ về nó.

III.2. Các giai đoạn của Metasploit.

III.2.1. Giai đoạn 1: System exploitation/Khai thác hệ thống

System exploitation/Khai thác hệ thống - thuật ngữ gốc đằng sau meta 'sploit' - tức là khai thác

Thuật ngữ này chỉ ra rằng bạn đang cố gắng khai thác một lỗ hổng hệ thống, máy tính hoặc mạng. Về cơ bản là bạn đang cố gắng tìm kiếm trong một mạng và sau đó tìm ra máy tính có lỗ hổng (backdoor) có thể bị xâm phạm.

III.2.2: Giai đoạn 2. Payload/Tải trọng

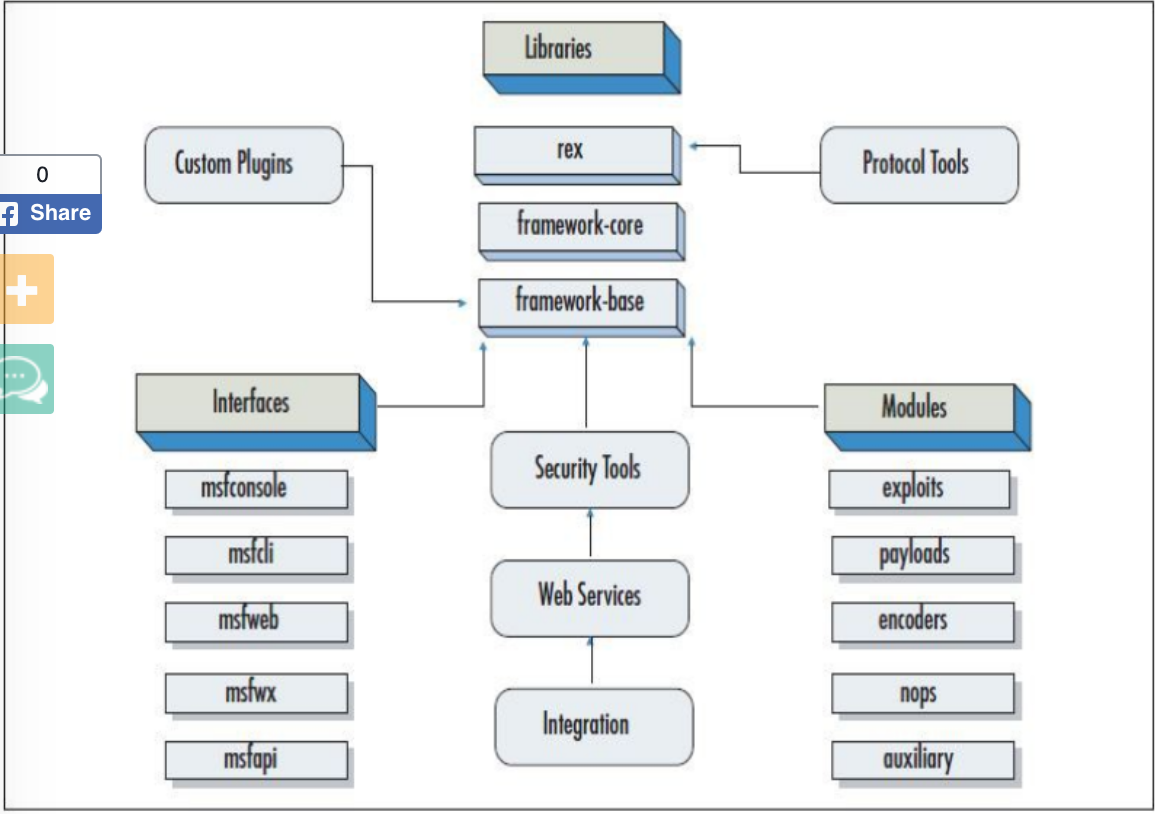
Một tính năng quan trọng của Metasploit là metasploit không chỉ quét mà còn thu thập thông tin về các hệ thống có thể được khai thác, và sau đó chạy mã code bên trong hệ thống bị xâm phạm. Tóm lại, đây là quá trình đưa code vào mà code đó nằm trong payload. Khi một payload được giải phóng, hacker hoặc penetration tester có thể chạy các lệnh và tác vụ sau đó. Mục tiêu là cần tạo ra một payload đủ lớn để có thể tạo mã shell. Shell là một giao diện dòng lệnh cung cấp cho người dùng quyền kiểm soát hoàn toàn đối với một máy bị xâm phạm.

Vì Metasploit là một framework nên user có thể tự tạo code và script riêng. Tuy nhiên, nếu bạn không rành về code thì cũng không cần quá lo lắng bởi đã có nhiều mô-đun được tạo ra để hỗ trợ bạn. Tất cả các module Metasploit đều rất cụ thể, qua đó chúng giúp thực hiện các tác vụ cụ thể. Ví dụ, các tác vụ như chạy quét mạng, mã độc ARP, packet sniffing vv… có thể đều đã có các module metasploit riêng.

III.2.3. Giai đoạn 3. Listening

Khả năng listening của metasploit được đánh giá rất cao. Trên thực tế, metasploit cũng giống như Wireshark lắng nghe rất tố các kết nối đến. Thế nhưng trong thế giới của các hacker, mọi thứ thường không xảy ra nhanh chóng, một hacker chuyên nghiệp có thể dành hàng tháng trời để xây dựng chiến lược và lên kế hoạch tấn công tốt nhất có thể. Bởi trong các cuộc tấn công, nghiên cứu đóng vai trò quan trọng nhất. PunkSPIDER và SHODAN là hai ví dụ về các dịch vụ mà một penetration tester có thể sử dụng trước khi dùng đến Metasploit. Cả PunkSPIDER và SHODAN đều hoạt động gần giống với một công cụ tìm kiếm. Sự khác biệt duy nhất là các công cụ này tìm kiếm các thông tin và lỗ hổng server. Metasploit có thể được triển khai để mở bất kỳ "cánh cửa khép hờ" nào.

III.3. Kiến trúc của Metasploit Framework



*Kiến trúc của Metasploit Framework.*

III.3.1. Các thành phần chính trong kiến trúc

III.3.1.1. Rex

Là thành phần cơ bản nhất của toàn bộ kiến trúc Framework. Rex là viết tắt của Ruby Extension Library, là một tập hợp các lớp, modum có thể được sử dụng bởi các nhà phát triển để phát triển các dự án hoặc các công cụ cho MSF (Metasploit Framework).

III.3.1.2. Framework Core (khung lõi)

Bao gồm một tập các hệ thống con như các modun quản lý, quản lý phiên, sự kiện điều phối… Lõi cũng như cung cấp cho ta một giao diện tới các modun, tiện ích bổ sung của Framework. Khung lõi bao gồm:

* Datastore: được hiểu như một môi trường, nó bao gồm một giá trị băm có thể được sử dụng bởi các modun tham chiếu đến các chương trình hay bằng các giá trị điều khiển. Biến môi trường là một trong những giá trị như vậy, nó được sử dụng bởi các modun khai thác hay bởi các framework để xác định chính xác các hành vi được thực hiện.
* Event Notification (thông báo sự kiện): cho phép các nhà phát triển đưa ra các hành động cụ thể với sự kiện ay hành động xảy ra.
* Framework Managers: có nhiệm vụ quản lý các modun, plugin, sessions.

III.3.1.3. Framework Base (khung cơ sở):

Được xây dựng dựa trên khuôn khổ của khung lõi, cung cấp giao fieenj có thể dễ dàng thực thi các lõi. Một số khung cơ sở:

* Configuration: duy trì một cấu hình liên tục và thu nhập thông tin về cấu trúc của tiến trình cài đặt chẳng hạn như thư mục gốc của quá trình cài đặt hay các thuộc tính khác.
* Sesions: những thông tin cơ bản về việc duy trì, kiểm soát các hành vi trong phiên làm việc của người dùng.
* Logging: là một tiện ích của MSF cho phép ghi lại các thông tin, các lỗi, gỡ lỗi một cách tổng quát và linh hoạt.

III.4. Các thành phần

III.4.1. Hỗ trợ giao diện người dùng

Console interface: Đây là giao diện sử dụng các dòng lệnh để cấu hình, kiểm tra do vậy tốc độ nhanh hơn và mềm dẻo hơn. Sử dụng file msfconsole.bat.

Web interface: Giao tiếp với người dùng thông qua giao diện web. Sử dụng file msfweb.bat.

III.4.2. Environment:

Global Environment: Được thực thi thông qua 2 câu lệnh setg và unsetg, những tùy chọn được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module khai thác.

Temporary Environment: Được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module khai thác đang load hiện tại, không ảnh hưởng đến các module khai thác khác.

Những thành phần nào có cấu hình giống nhau giữa các exploits module như là: LPORT, LHOST, PAYLOAD thì bạn nên cấu hình ở chế độ ở Global Environment để không phải cấu hình lại nhiều lần.

III.4.3. Các Module trong framework:

Exploits: là một phần của phần mềm, một đoạn dữ liệu, hoặc chuỗi các lệnh màlợi dụng một lỗi, lỗi hoặc lỗ hổng để gây ra hành vi không mong muốnhoặc không mong muốn xảy ra trên phần mềm máy tính, phần cứng, hoặc một cái gì đóthuộc điện tử (thường trên máy vi tính). Điều này thường bao gồm những thứ như giành quyền kiểm soát của một hệ thống máy tính hoặc cho phép nâng quyền hay một tấn công từ chối dịch vụ.

Payloads: là các phần của code được thực thi trên hệthống đích như một phần củanỗ lực khai thác.

III.4.4. Các loại payload Metasploit cung cấp

Lệnh Shell: cho phép người dùng chạy các kịch bản bộ sưu tập hoặc chạy các lệnh tùy ýđối với máy chủ.

Meterpreter cho phép người dùng điều khiển màn hình của thiết bị bằng cách sử dụngVNC và để trình duyệt tải lên và tải về tập tin.

NOP Generators: Thông thường, các vị trí chính xác của jump có thểkhông được biết đến, và các NOP cầnđược đưa vào trước để khai thác thực tế. Để tránh IDSes từ việc kích hoạttrên các mẫu lưu lượng truy cập, Các NOP Genergator cho phép làm bối rối các trình tự của NOPhoặc NOP sleds.

Encoders: Cũng giống như NOP sleds hayPayloadsđều có thể kích hoạt được IDS signatures. Các Encoders còn có thểthể tránh được bằng cách mã hóa các payload, vì vậy mà chúng vượt qua mà không bị phát hiện qua mạng, được giải mã vào mụctiêu, và thực hiện theo kế hoạch.

Auxiliary Modules: cung cấp chức năng tăng cường cho các thử nghiệm xâm nhập về vân tay và quét lỗ hổng.

III.4. Sử dụng Metasploit.