Hacker Mũ Trắng

Mục lục

Chương 1: Tổng quan về Hacker mũ trắng

Hacking: tóm lược lịch sử

Hacker là một trong những khái niệm bị sử dụng và hiểu sai nhiều nhất trong ngành công nghiệp bảo mật. Nó gần như trở thành tương đương với kỹ thuật của 1 kẻ xấu, cái mà mọi người hoặc sợ hãi hoặc bỏ qua. Vậy hacker là gì và chúng ta ở đâu khi là Hacker mũ trắng? Để trả lời câu hỏi này, chúng ta hãy xem lịch sử của hacking cùng với các sự kiện đáng chú ý.

Thủa sơ khai của Hacking

Như một câu chuyện, những hacker đầu tiên là 1 nhóm những người có đam mê và tò mò về công nghệ mới. Họ là những cá nhân tương đồng như ngày nay – những người không chỉ muốn các công nghệ mới nhất, như điện thoại thông mình hay iPhone, mà còn muốn học tất các chi tiết lý thú mà các thiết bị có và kiểu những điều không được tài liệu hóa mà họ có thể làm. Từ những ngày đầu những thứ đã phát triển một cách đáng kể: những cá nhâ đã trở nên nâng cao hơn, sáng tạo hơn và được truy cập tới nhiều công cụ mạnh mẽ và mới hơn.

Các Hacker hay những người đam mê đã luôn làm việc với những công nghệ tốt nhất có thể theo thời gian. Trong những năm 1970, đó là các máy chủ mainframe được giới thiệu ở các trường đại học và các doanh nghiệp lớn. Sau đó, trong những năm 1980, PC trở thành mảng công nghệ mới, và các hacker đã chuyển sang môi trường này. Những năm 1980 đã chứng kiến hacker chuyển sang các hoạt động có hại hơn và sau đó là độc hại; các cuộc tấn công của họ giờ được sử dụng để chống lại nhiều hệ thống hơn vì nhiều người được truy cập PC hơn. Trong những năm 1990, mạng Internet đã tạo ra khả năng truy cập tới công cộng và các hệ thống được kết nối; nhưng một hệ quả, sự tò mò và nghịch ngợm dễ dàng lây lan qua một tập nhỏ các hệ thống và trở thành toàn cầu. Từ năm 2000, điện thoại di động, máy tính bảng, Bluetooth, và các công nghệ khác đã được đưa vào các thiết bị và các công nghệ mà các hacker hướng đến. Như sự phát triển của các hacker, họ thực hiện các cuộc tấn công.

Khi mạng Internet đã trở nên phổ biến trên diện rộng, việc tấn công mạng (hacking) và các hacker không còn ở xa phía sau. Khi thế hệ đầu tiên của các trình duyệt trở nên khả dụng trong khoảng đầu những năm 1990, các cuộc tấn công phát triển trong dạng deface các website và 1 số dạng lừa đảo khác. Đột phá đầu

tiên về phá hoại trong không gian mạng xuất phát từ những trò đùa, tuy nhiên sau đó các cuộc tấn công có chủ đích hơn bắt đầu xuất hiện. Các sự cố như phá hoại các website các hãng phim, chính phủ là một trong những ví dụ đầu tiên. Cho đến đầu những năm 2000, tấn công deface website vẫn còn phổ biến đến nỗi nhiều trong số các sự cố đó không còn được nhắc đến.

Các sự phát triển hiện tại

Trong những năm đầu 2000, nhiều hành động độc hại hơn bắt đầu xuất hiện trong dạng các cuộc tấn công nâng cao hơn. Thực tế, trong một số năm đầu của thiên niên kỷ mới tính tấn công của các cuộc tấn công gia tăng, với nhiều cuộc tấn công với động cơ tội phạm. Các tấn công nguy hại đã xảy ra dưới đây là một số trong số rất nhiều nữa:

- Các tấn công từ chối dịch vụ
- Điều khiển giá cổ phiếu
- Đánh cắp định danh
- Phá hoại văn hóa
- Ăn cắp thẻ tín dụng
- Xuất bản lậu
- Ăn cắp dịch vụ

Một trong nhiều tình huống mà đã đóng góp trong việc gia tăng của phá hoại mngj và tội phạm mạng là số lượng lớn thông tin được truyên qua và phụ thuộc vào mạng Internet và các thiết bị số. Trải qua thập kỷ vừa qua số lượng các giao dịch thương mại đã tăng lên, đang tạo ra mục tiêu hấp dẫn cho các kẻ lừa đảo. Cùng với đó, sự mở của các thiết bị hiện đại như điện thoại thông minh và các công nghệ như Bluetooth đang làm cho việc phá hoại và ăn cắp thông tin dễ dàng hơn. Cuối cùng, chúng ta cũng có thể nhắc đến số lượng các thiết bị kết nối được Internet như máy tính bảng và các thiết bị khác mà các cá nhân mang theo tăng nhanh về số lượng. Mỗi một trường hợp trong các ví dụ này đã thu hút sự chú ý của các tội phạm với sự hấp dẫn của việc ăn cắp chưa bao giờ có trước khi nghe về tổng số tiền, dữ liệu và các tài nguyên khác. Cũng như các luật về tội phạm máy tính bắt đầu được thông qua, các quyền về sự công bố việc hack các website trở nên kém hấp dẫn. Các hành động đùa cợt dường như giảm xuống trong khi hành động tội phạm thực tăng lên. Với thương mại trực tuyến, các kỹ năng bắt

đầu đi tới người trả giá cao nhất, với các nhóm tội phạm, tổ chức tội phạm và các quốc gia với lợi ích thù địch đang sử dụng mạng Internet như một phương thức tấn công.

Hacking: trò đùa hay tội phạm?

Bắt đầu sớm hơn, hacking không có nghĩa là một hiện tượng mới; nó đã tồn tại trong 1 dạng khác từ những năm 1960. Nó chỉ được xác định thời gian kể từ khi khái niệm hacking được nhìn như là tội pham và 1 tình huống mà nó cần phải được chỉ ra.

Dưới đây là một số vụ hack nổi tiếng:

- Năm 1988, Robert T.Morris, Jr – một sinh viên đại học Cornell, đã tạo ra cái mà được xem là sâu (worm) Internet đầu tiên. Theo Morris, sâu của anh được thiết kế để đếm số lượng các hệ thống kết nối Internet. Do mỗi lỗi (lỗ hổng) thiết kế, sâu này đã nhân bản nhanh và bừa bãi, gây ra sự chậm chạm lan rộng toàn cầu. Morris bị kết án theo luật Gian lận và lạm dụng máy tính 1986 và phải làm lao động công ích thay vì phải ngồi tù.
- Năm 1999, David L.Smith tạo ra virus Melissa, cái được thiết kế cho email của bản thân Davd để truy nhập vào một danh sách tài khoản người dùng và sau đó xóa các file trên hệ thống bị nhiễm.
- Năm 2001, Jan de Wit tạo ra virus Anna Kournikova, nó được thiết kế để đọc tất cả các mục của danh sách địa chỉ người dùng Outlook và tự gửi email nó tới mỗi địa chỉ đó.
- Năm 2004: Adam Botbyl, cùng với 2 người bạn, âm mưu ăn cắp thông tin thẻ tín dụng từ chuỗi phần cứng Lowe.
- Năm 2005, Cameron LaCroix đã xâm nhập vào hệ thống điện thoại của Paris Hiltan và cũng tham gia vao vụ tấn công chống lại trang LexisNexis, một trang thu thập thông tin xã hội trực tuyến, cuối cùng làm lộ hàng ngàn thông tin cá nhân.
- Năm 2011, nhóm hacker Lulzsec thực hiện một số vụ tấn công nổi tiếng chống lại các mục tiêu như Sony, CNN và Fox.com. Nhóm này dường như vẫn hoạt động bất chấp tuyên bố của họ về việc đã về hưu.

- Trong năm 2010 cho đến thời điểm này, nhóm hacker Anonymous cũng tấn công nhiều mục tiêu, bao gồm các mạng nội bộ chính phủ, các cơ quan mới, và các đối tượng khác. Nhóm này hiện nay vẫn đang hoạt động.

Những ví dụ trên đại diện một số sự cố nổi tiếng đã xảy ra, nhưng với bất cứ câu chuyện hay sự kiện mới nào mà làm nó vào trong ý thức cộng đồng, còn nhiều hơn những gì đã làm. Lưu ý rằng bất cứ sự cố nào mà nó đã được thông báo, chỉ một số nhỏ những cá nhân mà thực hiện nó bị bắt giữ, và thậm chí một số nhỏ hơn nữa bị truy cứu về tội phạm mạng. Trong mọi trường hợp, hacking thực sự là tội phạm, và bất cứ ai liên quan đến các hành động như vậy có thể bị truy cứu bởi luật pháp cái mà khác nhau giữa nơi này và nơi khác. Số lượng, tần suất, và độ nguy hiểm của các vụ tấn công chỉ có tăng lên và sẽ tiếp tục tăng cùng với sự phát triển của công nghệ.

Dưới đây là một số ví dụ về loại tội phạm mạng:

- Đánh cắp mật khẩu và tên người dùng, hoặc sử dụng các lỗ hổng trong một hệ thống để thực hiện truy cập, thuộc thể loại hành vi ăn cắp của sự truy cập và lấy cắp dịch vụ và tài nguyên mà một bên sẽ không được nếu không được phép truy cập. Trong một số trường hợp lấy cắp thông tin quan trọng mà không dùng cũng đủ để bị xem là tội phạm mạng. Ở một số ít quốc gia, thậm chí việc chia sẻ tên người dùng và mật khẩu với bạn bè hoặc thành viên trong gia đình cũng là phạm tội.
- Các xâm nhập mạng là một dạng của tội xâm phạm số khi một bên tới một số nơi mà họ không được đến nếu không được phép truy cập. Truy cập tới bất cứ hệ thống hoặc nhóm các hệ thống mà ở đó một bên thường không được phép truy cập được xem là một sự vi phạm về mạng và do đó là một tội phạm mạng. Trong một số trường hợp xâm nhập thực tế có thể không liên quan tới các công cụ hacking; hành vi đăng nhập vào 1 tài khoản khách có thể đủ để bị xem là một sự xâm nhập.
- Social Engineering (tạm dịch là kỹ thuật tấn công phi kỹ thuật) vừa là đơn giản nhất đồng thời cũng là phức tạp nhất của phương pháp hacking hay khai thác một hệ thống bằng việc tân công vào điểm nhiếu nhất của nó, thành phần con người. Một mặt, nó là dễ dàng để tấn công vì con người đang là thành phần dễ truy cập nhất nhiều lần của một hệ thống và là đơn giản nhất để tương tác với. Mặt khác, sẽ là rất khó khăn để đọc tín hiệu đọc

được và không đọc được để lý thông tin mà có thể được sử dụng cho kẻ tấn công.

- Việc đăng/truyền các thông tin bất hợp pháp đang trở thành một vấn đề khó để giải quyết và đối phó trong thập niên vừa qua. Với sư gia tăng của việc sử dụng môi trường xã hội và các dịch vụ liên quan tới Internet khác, thông tin bất hợp pháp có thể lan truyền từ một góc của thế giới sang góc bên kia trong một khoảng thời gian rất ngắn
- Gian lận (Fraud) là một lừa gạt của một bên hoặc các bên để lấy thông tin hoặc truy cập thường là cho lợi ích tài chính hoặc mục đích phá hoại.
- •Vi phạm bản quyền phần mềm là việc chiếm hữu, trùng lặp, hoặc phân phối các phần mềm vi phạm một thỏa thuận cấp phép, hoặc các hành động bảo vệ chống sao chép cơ chế hoặc giấy phép thực thi khác. Một lần nữa điều này đã trở thành một vấn đề lớn với sự gia tăng của các dịch vụ chia sẻ tập tin và các cơ chế khác được thiết kế để dễ dàng chia sẻ và phân phối; trong nhiều trường hợp các hệ thống được sử dụng để phân phối mà không có sự đồng ý của chủ sở hữu của hệ thống.
- Dumpter diving là một cách đơn giản và lâu đời nhất để thu thập thông tin từ những tài liệu đã được loại bỏ hoặc để trong đồ đựng không có bảo đảm hoặc không bảo mật. Thông thường, các dữ liệu đã bị xóa bỏ có thể được ráp lại với nhau để tái tạo lại thông tin nhạy cảm.
- Mã độc hại là khái niệm chỉ các hạng mục như virus, sâu, spyware, adware, rootkit, và các loại phần mềm độc hại. Tội phạm này bao gồm bất kỳ loại phần mềm cố tình viết để tàn phá và hủy diệt hoặc gián đoạn.
- Tiêu hủy hoặc thay đổi thông tin trái phép bao gồm các thay đổi, phá hủy hoặc làm xáo trộn thông tin mà không được phép.
- • Tham ô là một hình thức gian lận tài chính có liên quan đến hành vi trộm cắp hoặc chuyển hướng của các quỹ do vi phạm một vị trí của sự tin tưởng. Các tội phạm đã được thực hiện dễ dàng hơn thông qua việc sử dụng các phương tiện kỹ thuật số hiện đại.
- Data-diddling (dữ liệu lừa gạt) chính là những thay đổi thông tin trái phép để bao che cho các hoạt động.
- Denial-of-Service (DoS: tấn công từ chối dịch vụ) và Distributed Denial-of-Service (DdoS: tấn công từ chối dịch vụ phân tán) là cách làm quá tải tài

nguyên của hệ thống, do đó không thể cung cấp các dịch vụ cần thiết cho người sử dụng hợp pháp.

Sự phát triển và tăng trưởng của Hacking

Các cuộc tấn công và chiến lược đã được cải thiện và phát triển qua nhiều năm theo những cách bạn có thể không nhận thức được. Những kẻ tấn công đã liên tục tìm cách "nâng cấp" trò chơi của họ với chiến thuật và chiến lược mới để bao gồm các loại phần mềm độc hại mới như worm, spam, spyware, adware, và thậm chí cả rootkit.

Các hacker cũng đã bắt đầu nhận ra rằng nó có thể sử dụng kỹ năng của họ để tạo ra tiền bằng nhiều cách thú vị. Ví dụ, những kẻ tấn công đã sử dụng các kỹ thuật để chuyển hướng trình duyệt web đến các trang cụ thể mà tạo ra doanh thu cho mình. Một ví dụ khác là một spammer gửi ra hàng ngàn hàng ngàn tin nhắn e-mail quảng cáo cho một sản phẩm hoặc dịch vụ.

Hacker mũ trắng là gì?

Hacker mũ trắng (hay hacker có đạo đức) được tuyển dụng hoặc thông qua hợp đồng hoặc làm việc trực tiếp để kiểm tra sự an toàn của một tổ chức. Họ sử dụng những kỹ năng và chiến thuật giống như một hacker, nhưng với sự cho phép của chủ sở hữu hệ thống để thực hiện cuộc tấn công của họ chống lại hệ thống. Ngoài ra, một hacker mũ trắng không tiết lộ những điểm yếu của một hệ thống mà mình đánh giá cho bất cứ ai khác ngoài chủ sở hữu của hệ thống. Cuối cùng, các hacker có đạo đức làm việc theo hợp đồng cho một công ty hoặc khách hàng, và các hợp đồng của họ chỉ định giới hạn là gì và những gì họ đang dự kiến sẽ làm. Nó phụ thuộc vào nhu cầu cụ thể của một tổ chức cụ thể. Trong thực tế, một số tổ chức có đội nhân viên đặc biệt để tham gia vào các hoạt động hacking đạo đức.

Các loại hacker

- Black Hat: Người có kỹ năng tính toán xuất sắc ,có hành động phá hoại như là cracker
- White Hat: Người biết nhiều kỹ năng của hacker và sử dụng chúng cho các hành vi phòng thủ ví dụ như là chuyên gia phân tích an ninh
- Suicide hackers: Người tấn công các cơ sở hạ tầng quan trọng quy mô rộng mà không cần quan tâm đến thiệt hại và trách nhiệm về việc đó

- Gray Hat: Người làm việc cả 2 việc tấn công và phòng thủ ở những thời điểm khác nhau
- Script Kiddies Các hacker có rất hạn chế hoặc thậm chí không được đào tạo và chỉ biết cách sử dụng các kỹ thuật hoặc các công cụ cơ bản. Thậm chí sau đó họ có thể không hiểu bất kỳ hoặc tất cả những gì họ đang làm.

Ethical Hacking and Penetration Testing

Hacker mũ trắng tham gia vào việc tấn công được phép - đó là, tấn công với sự cho phép của chủ sở hữu của hệ thống. Trong thế giới của hacker mũ trắng, hầu hết có xu hướng sử dụng khái niệm kiểm thử - pen tester. Người kiểm thử chỉ đơn giản là: thâm nhập vào các hệ thống như một hacker, nhưng với mục đích lành tính.

Là một hacker mũ trắng và ứng cử viên kiểm thử trong tương lai, bạn phải trở nên quen thuộc với các biệt ngữ của thương mại. Dưới đây là một số các điều khoản mà bạn sẽ gặp phải trong bút thử nghiệm:

Hack Value Thuật ngữ này mô tả một mục tiêu có thể thu hút sự chú ý với mức độ trên trung bình của một kẻ tấn công. Có lẽ vì mục tiêu này là hấp dẫn, nó có giá trị hơn cho một kẻ tấn công vì những gì nó có thể chứa.

Target of Evaluation (TOE) Một TOE là một hệ thống hoặc tài nguyên đang được đánh giá lỗ hổng. Một TOE sẽ được quy định trong hợp đồng với khách hàng.

Attack Đây là một hành động với mục tiêu nằm trong TOE.

Exploit Đây là một cách để xác định rõ ràng vi phạm an ninh của hệ thống.

Zero Day Đây là một threat hoặc một vulnerability mà không được biết đến bởi các nhà phát triển và cũng chưa được giải quyết. Nó được coi là một vấn đề nghiêm trọng trong nhiều trường hợp.

Security Nó được mô tả là một trạng thái "hạnh phúc" trong một môi trường mà ở đó chỉ những hành động đã được định nghĩa được cho phép.

Threat Là một nguy cơ về an ninh thông tin.

Vulnerability Là một điểm yếu của hệ thống mà có thể bị tấn công và sử dụng như một điểm để xâm nhập một môi trường.

Daisy Chaining Là hành động cho phép thực hiện nhiều vụ tấn công liên tục với mỗi hành động dựa tiếp theo dựa trên kết quả của hành động trước đó.

Phương thức hack

Phương pháp hack là đề cập đến các phương pháp tiếp cận từng bước được sử dụng bởi một kẻ xâm lược để tấn công một mục tiêu như một mạng máy tính. Không có phương pháp tiếp cận từng bước cụ thể được sử dụng bởi tất cả các tin tặc. Như có thể mong đợi khi một nhóm hoạt động bên ngoài các quy tắc như hacker làm, quy định này không áp dụng cùng một cách. Một sự khác biệt lớn giữa một hacker và một hacker mũ trắng là những quy tắc đạo đức.

Một số bước hack thường thấy:

Footprinting: Trinh sát

Footprinting có nghĩa là bạn đang sử dụng các phương pháp chủ yếu là thụ động thu thập thông tin từ một mục tiêu trước khi thực hiện các biện pháp chủ động sau này. Thông thường, bạn duy trì tương tác với các mục tiêu của bạn đến mức tối thiểu để tránh bị phát hiện, vì nó có thể cảnh báo các mục tiêu là có một cái gì đó đang đến theo hướng của họ.

Scanning: Quét

Scanning là giai đoạn mà trong đó bạn có những thông tin thu thập được từ giai đoạn Footprinting và sử dụng nó để nhắm mục tiêu tấn công của bạn chính xác hơn nhiều.

Enumeration: Liệt kê

Enumeration là giai đoạn tiếp theo nơi bạn trích xuất thông tin chi tiết hơn nữa về những gì bạn phát hiện trong giai đoạn Scanning để xác định tính hữu dụng của nó.

System Hacking: tấn công hệ thống

System hacking là bước sau Enumeration. Bây giờ bạn có thể lập kế hoạch và thực hiện một cuộc tấn công dựa trên các thông tin mà bạn phát hiện ra. Bạn có thể, ví dụ, bắt đầu chọn tài khoản người dùng để tấn công dựa trên những phát hiện trong giai đoạn điều tra. Bạn cũng có thể bắt đầu việc tạo một cuộc tấn công dựa trên các thông tin dịch vụ phát hiện bằng cách lấy các banner từ các ứng dụng hoặc dịch vụ.

Escalation of privilege: leo thang đặc quyền

Nếu giai đoạn hack thành công, bạn có thể bắt đầu để có được đặc quyền được cấp tài khoản để có đặc quyền cao hơn quyền của tài khoản đột nhập vào ban đầu. Tùy thuộc vào kỹ năng của bạn tại bước này, nó có thể di chuyển từ một tài khoản cấp thấp như một tài khoản khách lên quyền quản trị hoặc truy cập hệ thống.

Covering tracks: Xóa dấu vết

Covering tracks là giai đoạn khi bạn cố gắng để loại bỏ các bằng chứng về sự hiện diện của bạn trong một hệ thống. Bạn tẩy log file và phá hủy bằng chứng khác có thể cho những manh mối có giá trị cần thiết cho chủ sở hữu hệ thống để xác định một cuộc tấn công xảy ra.

Planting Backdoors: Cài đặt cửa hậu

Mục đích của việc cài đặt backdoors là để lại một cái gì đó đằng sau đó sẽ cho phép bạn quay lại sau nếu bạn muốn. Các hạng mục như các tài khoản đặc biệt, Trojan...

Chương 3: Footprinting và Reconnaissance

Các bước tấn công mạng

Để bắt đầu tấn công hệ thống, bạn cần thực hiện 4 bước

- Footprinting
- Scanning
- Enumeration
- System Hacking

Các bước trên áp dụng cho bất kỳ cuộc tấn công trên mạng nào. Hacker phải ra sức thu thập càng nhiều thông tin càng tốt về mọi góc cạnh bảo mật của tổ chức. Kết quả thu được sẽ giúp cuộc tấn công trót lọt hơn. Bằng cách dò theo dấu chân, những bộ lưu trữ trên internet, truy cập từ xa, cùngvới sự hiện diện của internet kẽ tấn công có thể góp nhặt một cách có hệ thống các thông tin từ nhiều nguồn khác nhau về một tổ chức nào đó.

FootPrinting là gì ?

Footprinting là một phần của giai đoạn tấn công có chuẩn bị trước và bao gồm việc tích lũy dữ liệu về môi trường của một mục tiêu và kiến trúc, thông thường với mục đích tìm cách để xâm nhập vào môi trường đó. Footprinting có thể tiết lộ các lỗ hổng hệ thống và xác định dễ dàng mà chúng có thể được khai thác. Đây là cách dễ nhất cho các hacker để thu thập thông tin về những hệ thống máy tính và các công ty mà họ thuộc về. Mục đích của giai đoạn chuẩn bị này là để tìm hiểu càng nhiều càng tốt như bạn có thể về một hệ thống, khả năng truy cập từ xa của nó, port và dịch vụ của mình, và bất kỳ khía cạnh cụ thể về bảo mật của nó.

Các kỹ thuật Footprinting

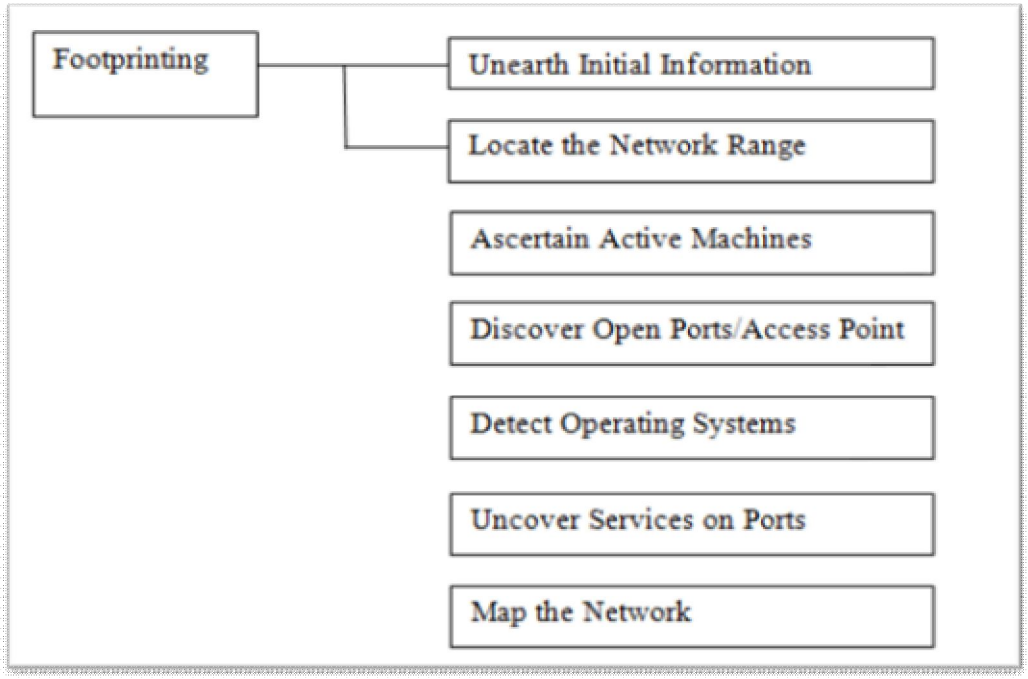
Phương pháp thu thập thông tin

Tổng hợp thông tin có thể được hiện trong 7 bước như mô tả của hình 3.1. Quá trình Footprinting được thực hiện trong 2 bước đầu của việc khám phá thông tin ban đầu và định vị phạm vi mạng

Một số nguồn thông thường được sử dụng để thu thập thông tin bao gồm sau đây:

- Domain name lookup

- Whois
- Nslookup
- Sam Spade



Bảy bước của việc tổng hợp thông tin

Trước khi chúng ta thảo luận những công cụ này, Hãy nhớ rằng thông tin nguồn mở có thể mang lại sự giàu có của thông tin về một mục tiêu, ví dụ như những số điện thoại và địa chỉ. Thực hiện những yêu cầu của Whois, tìm kiếm trong bảng Domain Name System (DNS). Hầu hết thông tin này là dễ dàng có được và hợp pháp để có được.

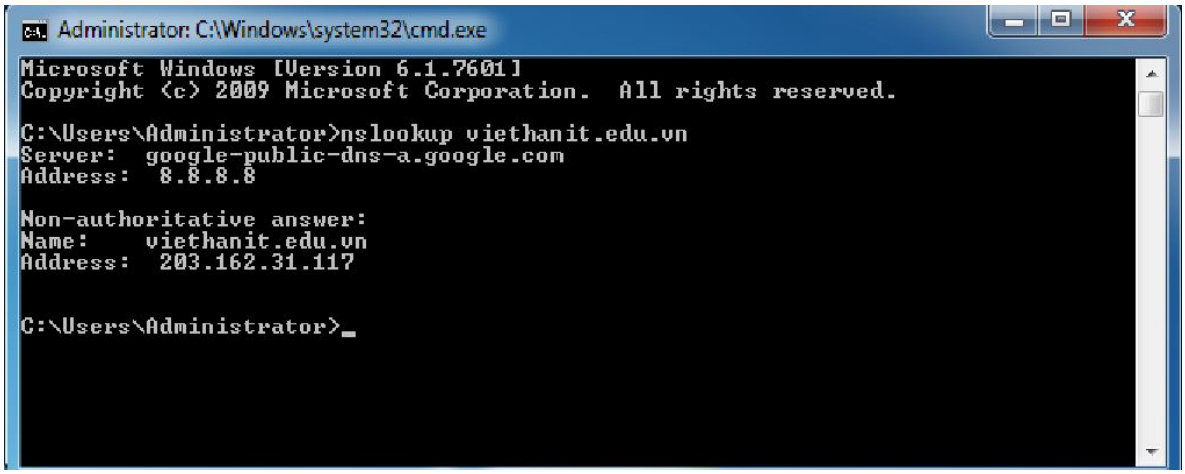
Chi tiết về cách hoạt động DNS và cụ thể của bản dịch DNS là ngoài phạm vi của cuốn sách này và sẽ không được thảo luận chi tiết. Duy nhất chi tiết quan trong nhất liên quan cụ thể tới thông tin được nằm trong cuốn sách này. Đó là khuyến cáo rằng tất cả các ứng cử viên CEH có một sự hiểu biết về DNS và cách phân tên công việc trên Internet.

Phương pháp liệt kê DNS

NSlookup, DNSstuff, the American Registry for Internet Number (ARIN), và Whois có thể được sử dụng tất cả để đạt được thông tin mà kế đó được sử dụng để thực hiện DNS enumeration.

Nslookup and DNSstuff

Một công cụ mạnh mẽ bạn nên làm quen là nslookup (xem hình 2.2). Công cụ này truy vấn những DNS server để tìm thông tin. Nó được cài đặt trong Unix, Linux, và hệ đều hành Window. Công cụ hack Sam Spade bao gồm những công cụ nslookup.



Nslookup

Ngoài việc tìm thông tin tổng hợp từ Whois, bạn có thể sử dụng nslookup để tìm bổ sung địa chỉ IP cho những máy chủ và những host khác. Sử dụng tên máy chủ có thẩm quyền thông tin từ Whois *(AUTH1.NS.NYI.NET)*, bạn cần nhận ra địa chỉ IP của mail server.

Sự bùng nổ của việc sử dụng thành thạo các công cụ đã làm quá trình hack thật sự dễ dàng, nếu như bạn biết những công cụ nào để sử dụng. ***DNSwatch*** là một công cụ khác của những công cụ đó. Thay vì sử dụng dòng lệnh công cụ nslookup với những thiết bị chuyển mạch cổng kênh của nó để tổng hợp việc ghi thông tin DNS, chỉ cần truy cập website http://www.dnswatch.info, và bạn có thể làm một DNS record search online

Whois và ARIN Lookups

Whois đã phát triển từ hệ điều hành Unix, nhưng nó bây giờ có thể được tìm thấy trong nhiều hệ điều hành khác như trong hacking toolkits và trên Internet. Người xác định công cụ này phải đăng ký tên miền sử dụng cho email hoặc website. ***Uniform Resource Locator*** (URL), ví dụ www.Microsoft.com, chứa tên miền *(Microsoft.com)* và 1 tên host hoặc bí danh*(www)*.

Internet Corporation for Asigned Names and Numbers (ICANN) yêu cầu đăng ký tên miền để bảo đảm rằng chỉ có một công ty duy nhất sử dụng tên miền cụ thể đó. Công cụ Whois truy vấn việc đăng ký cơ sở dữ liệu để lấy thông tin liên lạc về cá nhân hoặc tổ chức đăng ký tên miền đó.

Whois thông minh là 1 chương trình thu thập thông tin cho phép bạn tìm tất cả thông tin giá trị về một địa chỉ IP, host name, hoặc domain, bao gồm đất nước, gồm có làng, tỉnh, thành phố, tên của người cung cấp mạng, administrator, và hỗ trợ kỹ thuật địa chỉ thông tin. Whois thông minh là 1 phiên bản đồ họa của chương trình Whois cơ sở.

ARIN là một cơ sở dữ liệu của thông tin bao gồm những thông tin như chủ sở hữu của địa chỉ IP tĩnh. Cơ sở dữ liệu ARIN có thể được truy vấn việc sử dụng công cụ Whois, ví dụ một vị trí tại http://centralops.net/

Tìm kiếm vùng địa chỉ mạng (network address range)

Mỗi hacker cần hiểu làm thế nào để tìm vùng địa chỉ mạng và subnet mask của hệ thống đích. Địa chỉ IP được sử dụng để xác định vị trí, scan, và kết nối đến hệ thống đích. Bạn có thể tìm địa chỉ IP đăng ký trên internet với ARIN hoặc với IANA(Internet Asigned Numbers Authority).

Hacker cũng cần phải tìm ra bảng đồ đường đi của hệ thống mạng mục tiêu. Nhiệm vụ này có thể thực hiện bằng cách gửi những gói tin thăm dò (bằng giao thức ICMP) đến địa chỉ IP đích. Bạn có thể sử dụng công cụ như Traceroute, VisualRouter và NeoTrace cho công việc này.

Ngoài ra, không chỉ có thông tin mạng đích, những thông tin khác cũng trở nên có giá trị. Ví dụ nhưng những địa chỉ mà hệ thống mạng này vừa truyền nhận gói tin, địa chỉ gateway…Nó sẽ có tác dụng trong một tiến trình tấn công khác.

Sự khác biệt của các loại bảng ghi DNS (DNS Record)

Dưới đây là các loại bảng ghi DNS mà chúng ta thường gặp. Việc nghiên cứu nó sẽ giúp chúng ta phân biệt rõ server mà chúng ta đang tìm có chức năng gì.

A (address): Ánh xạ hostname thành địa chỉ IP.

SOA (Start of Authoriy): Xác định bảng ghi thông tin của DNS Server.

CNAME (canonical name): Cung cấp những tên biệt danh (alias) cho tên miền đang có.

MX (mail exchange): Xác định mail server cho domain

SRV (service): Xác định những dịch vụ như những directory service

PTR (pointer): Ánh xạ địa chỉ ip thành hostname

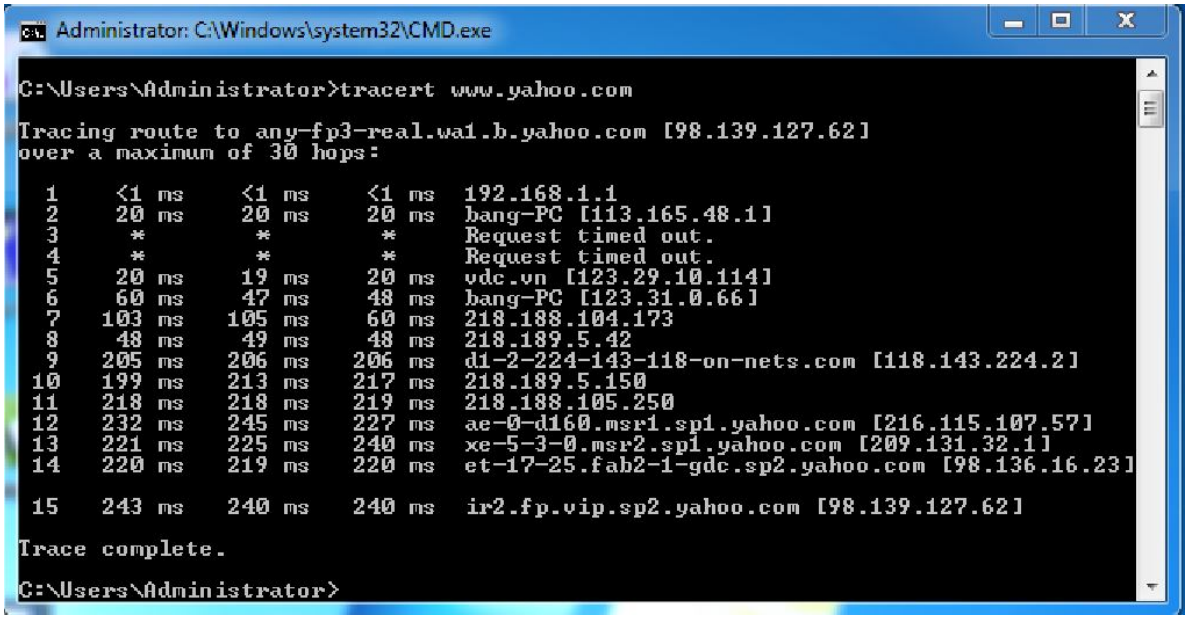
NS (name server): Xác định Name Server khác cho domain

Sử dụng traceroute trong kỹ thuật FootPrinting

Traceroute là gói công cụ được cài đặt sẵn trong hầu hết các hệ điều hành. Chức năng của nó là gửi một gói tin ICME Echo đến mỗi hop (router hoặc gateway), cho đến khi đến được đích. Khi gói tin ICMP gửi qua mỗi router, trường thời gian sống (Time To Live – TTL) được trừ đi xuống một mức. Chúng ta có thể đếm được có bao nhiêu Hop mà gói tin này đã đi qua, tức là để đến được đích phải qua bao nhiêu router. Ngoài ra, chúng ta sẽ thu được kết qua là những router mà gói tin đã đi qua.

Một vấn đề lớn khi sử dụng Traceroute là hết thời gian đợi (time out), khi gói tin đi qua tường lửa hoặc router có chức năng lọc gói tin. Mặc dù tường lửa sẽ chặn đứng việc gói tin ICMP đi qua, nhưng nó vẫn gửi cho hacker một thông báo cho biết sự hiện diện này, kế đến vài kỹ thuật vượt tường lửa có thể được sử dụng.

Sam Spade và nhiều công cụ hack khác bao gồm 1 phiên bản của traceroute. Những hệ điều hành Window sử dụng cú pháp ***tracert hostname*** để xác định một traceroute. Hình dưới là một ví dụ về traceroute hiển thị việc theo dõi theo http://www.yahoo.com



Kết quả của Traceroute cho www.yahoo.com

Theo dõi email (E-mail Tracking)

E-mail–tracking là chương trình cho phép người gửi biết được những việc đã làm của người nhận như reads, forwards, modifies, hay deletes. Hầu hết các chương trình E-mail–tracking hoạt động tại server của tên miền email. Một file đồ họa đơn bit được sử dụng để đính kèm vào email gửi cho người nhận, nhưng file này sẽ không được đọc. Khi một hành động tác động vảo email, file đính kèm đó sẽ gửi thông tin lại cho server cho biết hành động của server. Bạn thường thấy những file này đính kèm vào email với cái tên quen thuộc như noname, noread...

Emailtracking pro và mailtracking.com là những công cụ giúp hacker thực hiện chức năng theo dõi email. Khi sử dụng công cụ, tất cả những hoạt động như gửi mail, trả lời, chuyển tiếp, sửa mail đều được gửi đến người quản lý. Người gửi sẽ nhận được những thông báo này một cách tự động.

Thu thập thông tin qua Web (Web Spiders)

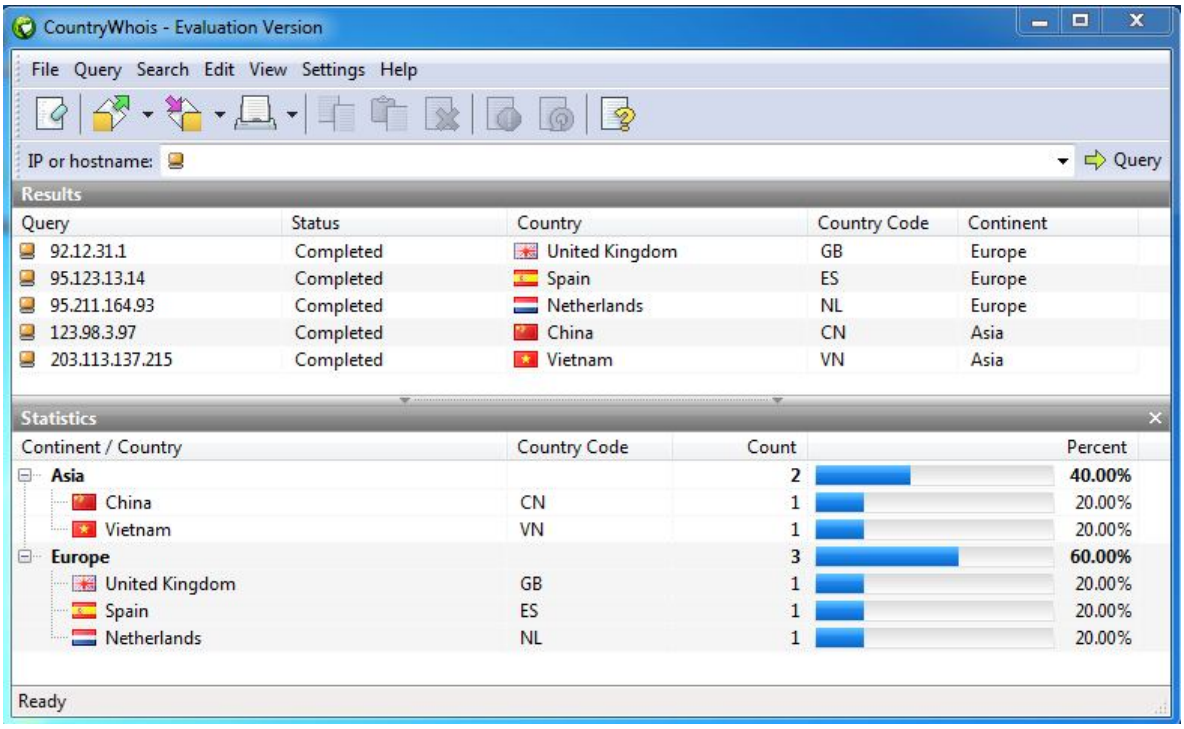
Web Spoder là công nghệ thu thập những thông tin từ internet. Đây là cách là spammer hoặc bất ai quan tâm đến email dùng để thu thập danh sách email hữu dụng. Web Spider sử dụng những cứu pháp, ví dụ như biểu tượng @, để xác định email hay, kế đến sao chép chúng vào cơ sở dữ liệu. Dữ liệu này được thu thập để phục vụ cho một mục đích khác. Hacker có thể sử dụng Web Spider để tổng hợp các loại thông tin trên internet. Có một phương pháp để ngăn chặn Spider là thêm file robots.txt trong thưc mục gốc của website với nội dung là danh sách các thư mục cần sự bảo vệ. Bạn sẽ tìm hiểu chủ đề này trong phần nói về Web Hacking.

1 email address spider và SpiderFoot là công cụ cho phép chúng ta thu thập email từ website theo những tên miền khác nhau. Những spammer sử dụng công cụ này để tiến hành thu thập hàng loạt email, phục vụ cho mục đích spam của họ.

MỘT SỐ VÍ DỤ ĐIỂN HÌNH VỀ FOOTPRINTING

Thông tin địa chỉ IP

Ngày nay công nghệ thông tin phát triển hầu hết các nước trên thế giới đều áp dụng công nghệ thông tin vào nhiều lĩnh lực. Khi chúng ta biết được một địa chỉ ip và muốn ip đó thuộc nước nào thì chúng ta có thể dùng phần mềm **CountryWhois** để tra cứu thông tin.



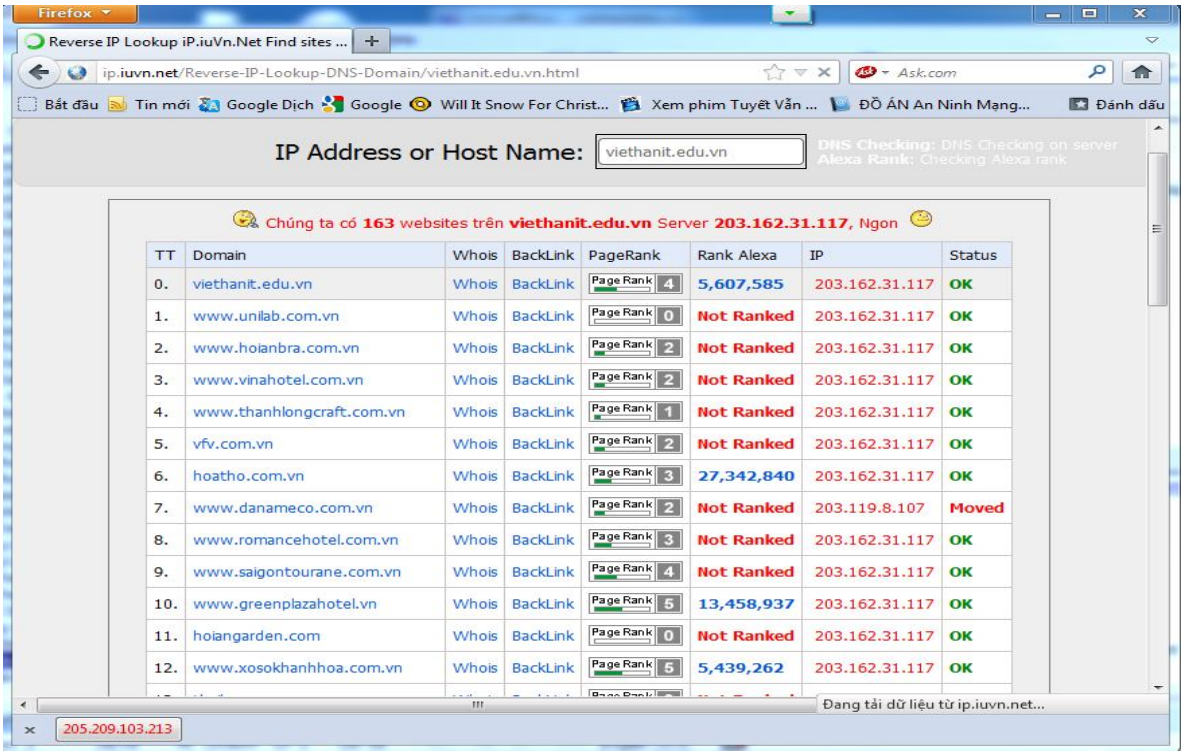
Hình: Thông tin về một địa chỉ IP

Xem thông tin domain name

Khi chúng ta biết một trang web thì chúng ta có thông tin của domain name và các trang web nằm trên cùng domain name đó.

Thông tin của domain name chúng ta dùng công cụ **Active Whois** hay trang web http://centralops.net

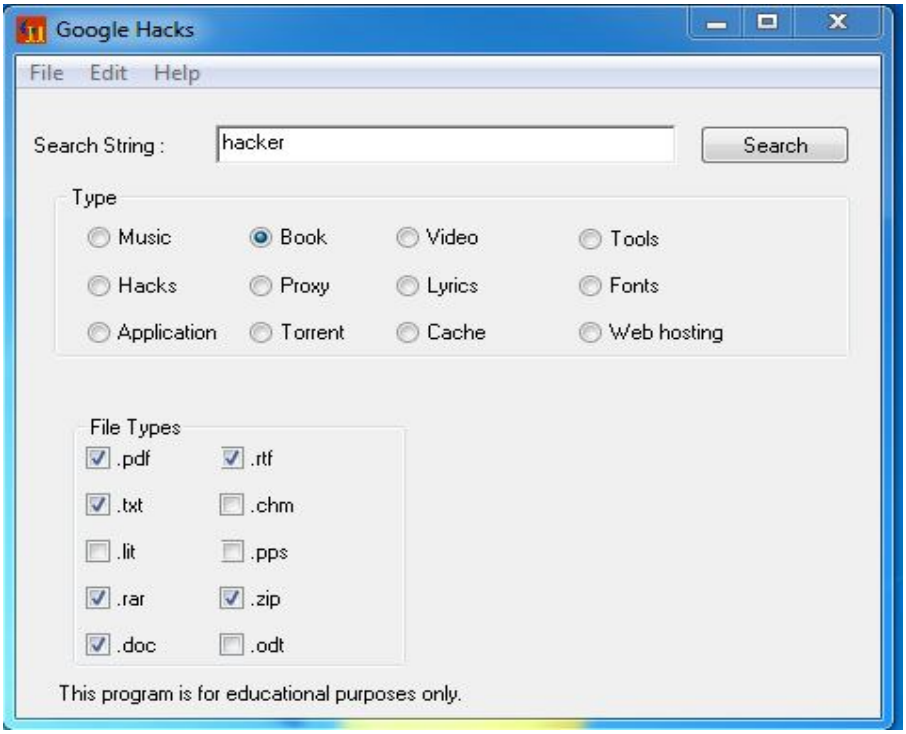
Các trang web nằm trên cùng domain name vào trang web http://ip.iuvn.net



Thông tin về các domain cùng nằm trên 1 server

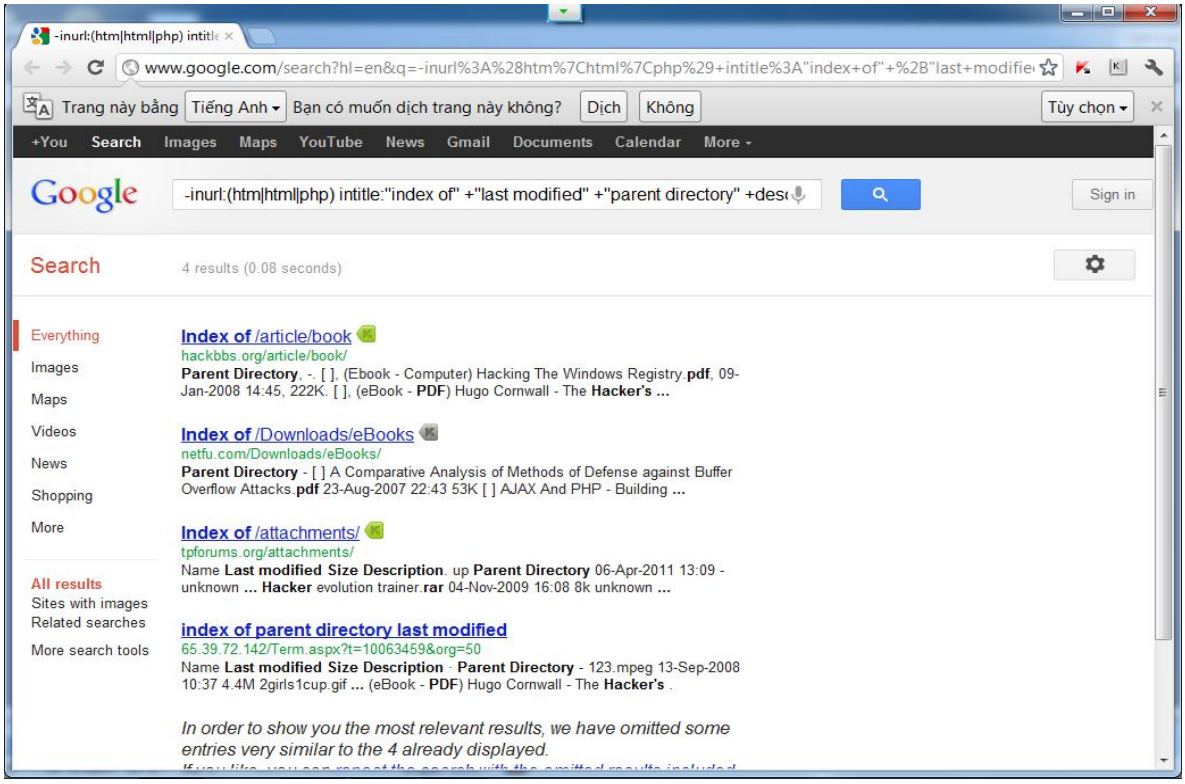
GOOGLE HACK

Thông qua google hack các hacker nhanh chóng tìm ra những thông tin mình cần



Công cụ google hacks

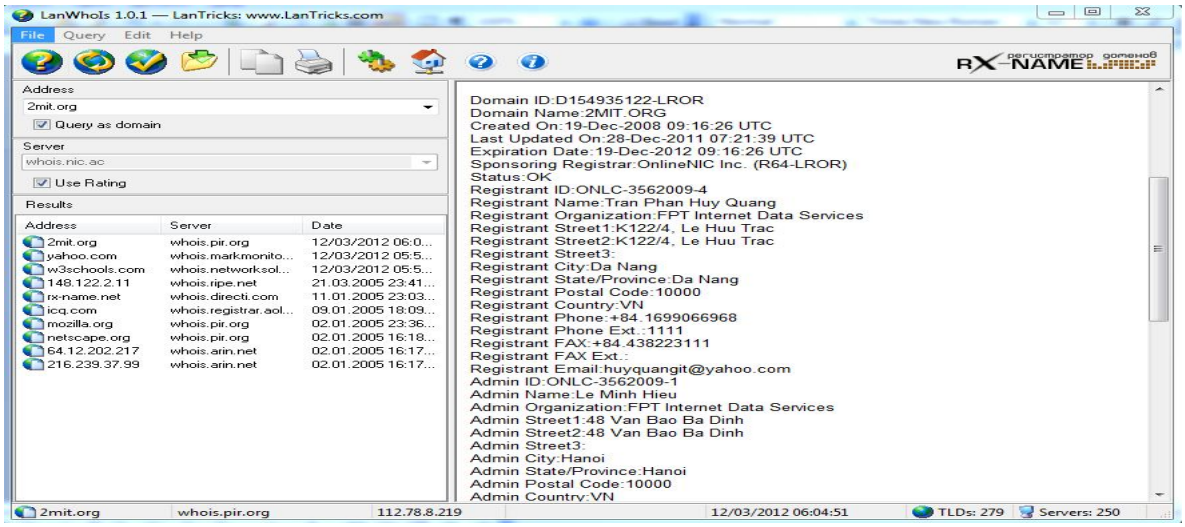
Các thông tin mà các hacker dùng google hacker tìm ra được



Thông tin từ công cụ google hacks

LAN WHOIS

Là chương trình này sẽ giúp các hacker tìm ra ai, ở đâu và khi đăng ký tên miền hoặc trang web mà các hacker đang quan tâm đến. LanWhoIs sẽ trả lời tất cả câu hỏi của hacker về tên miền (trang web) chủ sở hữu hoặc địa chỉ IP!



Hình: Thông tin về domain

Chương 4: Scanning Networks

Scanning là gì

Quét (Scanning) là một bước tiếp theo trong tiến trình tấn công hệ thống. Giai đoạn này giúp chúng ta xác định được nhiều thông tin của mục tiêu cần tấn công. Tức là sau khi chúng ta tìm được vài thông tin có liên quan đến máy tính cần tấn công, công đoạn tiếp theo là thu thập thông tin về máy tính đó. Những thông tin cần thu thập như tên máy (computer name), địa chỉ ip, cấu hình máy tính, hệ điều hành, dịch vụ đang chạy, port đang mở…Những thông tin này sẽ giúp cho hacker có kế hoạch tấn công hợp lý, cũng như việc chọn kỹ thuật tấn công nào. Quét giúp định vị hệ thống còn hoạt động trên mạng hay không. Một hacker chân chính sử dụng cách này đề tìm kiếm thông tin của hệ thống đích.

Phân loại Scanning

Port Scanning

Port scanning là quá trình xác định cổng TCP/IP mở và có sẵn trên một hệ thống. Công cụ Port scanning cho phép một hacker tìm hiểu về các dịch vụ có sẵn trên một hệ thống nhất định. Mỗi dịch vụ hay ứng dụng máy tính được kết hợp với một số cổng thông dụng. Ví dụ, một công cụ quét đó là xác định cổng 80 mở cho một web sever đang chạy trên đó. Hacker cần phải biết rõ với số cổng thông dụng.

Network Scanning

Network scanning là một quy trình để xác định máy chủ đang hoạt động trên mạng, hoặc để tấn công chúng hoặc là đánh giá an ninh mạng. Máy chủ được xác định bởi IP cá nhân của chúng. Các công cụ network-scanning cố gắng xác định tất cả các máy chủ trực tiếp hoặc trả lời trên mạng và địa chỉ IP tương ứng của chúng.

Vulnerability scanning

Vulnerability scanning là quá trình chủ động xác định các lỗ hổng của hệ thống máy tính trên mạng. Thông thường, một máy quét lỗ hổng đầu tiên xác định các hệ điều hành và số phiên bản, bao gồm các gói dịch vụ có thể được cài đặt. Sau đó, máy quét lỗ hổng xác định các điểm yếu, lỗ hổng trong hệ điều hành.Trong

giai đoạn tấn công sau đó, một hacker có thể khai thác những điểm yếu để đạt được quyền truy cập vào hệ thống.

Các phương pháp Scanning

Kiểm tra hệ thống.

- **Quét ICMP**

Bản chất của quá trình này là gửi một gói ICMP Echo Request đến máy chủ đang muốn tấn công

Việc quét này rất hữu ích để định vị các thiết bị hoạt động hoặc xác định hệ thống có tường lửa hay không

- **Ping Sweep**

Ping Sweep được sử dụng để xác định các máy chủ còn "sống" từ một loạt các địa chỉ IP bằng cách gửi các gói ICMP Echo Request đến tất cả các IP đó. Nếu một máy chủ còn "sống" nó sẽ trả lại một gói tin ICMP Reply.

Kiểm tra các cổng mở

Kiểm tra các cổng đang mở là bước thứ hai trong tiến trình quét. Port scanning là phương pháp được sử dụng để kiểm tra các cổng đang mở. Quá trình quét bao gồm việc thăm dò mỗi cổng trên máy chủ để xác định các cổng đang mở. Thông thường Ports scanning có giá trị hơn một quá trình quét ping về máy chủ và các lỗ hổng trên hệ thống.

Các kĩ thuật quét :

- **XMAS**: XMAS scans gửi một gói với cờ FIN,URG, và PSH được thiết lập. Nếu cổng mở, không đáp lại; nếu đóng mục tiêu gửi lại gói RST/ACK. XMAS scan chỉ làm việc trên hệ thống máy đích theo RFC 793 của TCP/IP và không chống lại bất cứ version nào của Windows.
- **FIN**: FIN scan tương tự XMAS scan nhưng gửi gói dữ liệu chỉ với cờ FIN được thiết lập. FIN scan nhận trả lời và có giới hạn giống như XMAS scan.
- **NULL**: NULL scan cũng tương tự như XMAS và FIN trong giới hạn và trả lời, nhưng nó chỉ gửi một packet mà không có flag set.

- **IDLE:** IDLE scan sử dụng địa chỉ IP giả mạo để gửi một gói SYN đến mục tiêu. Phụ thuộc vào trả lời, cổng có thể được xác định là mở hoặc đóng. IDLE scans xác định phản ứng quét cổng bằng cách theo dõi số thứ tự IP header.

Kỹ thuật War DiaLing

War-Dialing là quá trình quay số modem để tìm một kết nối modem đang mở, kết nối này cung cấp truy cập từ xa vào mạng, để tấn công vào hệ thống đích. Thuật ngữ War dialing bắt nguồn từ những ngày đầu của Internet khi hầu hết các công ty đã được kết nối với Internet thông qua kết nối dial-up modem. War dialing được xem như là một phương pháp quét bởi vì nó tìm thấy một kết nối mạng mà có thể có bảo mật yếu hơn so với các kết nối Internet chính.

Công nghệ Banner Grabing và Operating System Fingerprint

Banner Grabbing cũng có thể định nghĩa là **Fingerprinting TCP/IP stack** – là bước thứ 4 trong phương pháp scanning. Quá trình fingerprinting cho phép hacker xác định vùng đặc biệt dế bị tổn thương của mục tiêu trên mạng. Banner grabbing là quá trình tạo kết nối và đọc biểu ngữ được gửi trả lời bởi ứng dụng. Nhiều server (mail, web, ftp…) sẽ trả lời đến một kết nối telnet với tên và version của software. Hacker có thể tìm thấy nhiều mối liên hệ giữa hệ điều hành và phần mềm ứng dụng. Ví dụ, Microsoft Exchange e-mail server chỉ cài được trên HĐH Windows.

OS Fingerprint là kỹ thuật xác định thông tin hệ điều hành chạy trên host đích. Có hai phương thức để thực hiện OS Fingerprint như sau:

Active stack fingerprinting là hình thức phổ biến nhất của fingerprinting. Nó bao gồm việc gửi dữ liệu đến hệ thống để xem cách hệ thống trả lời. Nó dựa trên thực tế là các nhà cung cấp hệ điều hành thực hiện các TCP stack khác nhau, và khác nhau dựa trên hệ điều hành. Các phản ứng này sau đó được so sánh với cơ sở dữ liệu để xác định hệ điều hành. *Active stack fingerprinting* bị phát hiện bởi vì nó cố gắng nhiều lần để kết nối với hệ thống mục tiêu.

Passive stack fingerprinting thì "tàng hình" hơn và bao gồm sự kiểm tra lưu lượng trên mạng để xác định hệ điều hành. Nó sử dụng kỹ thuật Sniffing thay vì kỹ thuật Scanning. *Passive stack fingerprinting* thường không phát hiện ra bởi IDS hoặc hệ thống bảo mật khác nhưng ít chính xác hơn *Active fingerprinting*.

Quét lỗ hổng

Quét lỗ hổng là để xác định lỗ hổng và điểm yếu của một hệ thống mạng và mạng lưới để xác định xem hệ thống đó có thể khai thác được như thế nào.

Thực hiện quét lỗ hổng sẽ được các kết quả :

- Cấu trúc liên kết mạng và các lỗ hổng hệ điều hành
- Các cổng mở và các dịch vụ đang chạy
- Ứng dụng và các lỗi cấu hình các dịch vụ
- Ứng dụng và các lỗ hổng dịch vụ

Triển khai Proxy Server để tấn công

Chuẩn bị máy chủ proxy là bước cuối cùng trong phương pháp quét CEH. Một proxy server là một máy tính hoạt động trung gian giữa hacker và máy tính đích.

Sử dụng một proxy server có thể cho phép hacker trở thành vô danh trên mạng. Hacker trước tiên kết nối tới máy proxy server rồi yêu cầu kết nối tới máy đích thông qua kết nối có sẵn đến proxy. Cơ bản, proxy yêu cầu truy cập đến mục tiêu mà không phải là máy tính của hacker. Điều này làm hacker lướt web vô danh hoặc ẩn trong cuộc tấn công.

Chương 5: Sniffers

Sniffing là gì

Sniffing (nghe lén) được hiểu đơn giản là một chương trình cố gắng nghe ngóng các lưu lượng thông tin trên một hệ thống mạng. Là một tiến trình cho phép giám sát cuộc gọi và hội thoại internet bởi thành phần thứ ba.

Người nghe lén để thiết bị lắng nghe giữa mạng mang thông tin như hai thiết bị điện thoại hoặc hai thiết bị đầu cuối trên internet. Nghe lén được sử dụng như công cụ để các nhà quản trị mạng theo dõi và bảo trì hệ thống mạng. Về mặt tiêu cực, nó được sử dụng như một công cụ với mục đích nghe lén các thông tin trên mạng để lấy các thông tin quan trọng.

Sniffing thường xảy ra ở đâu

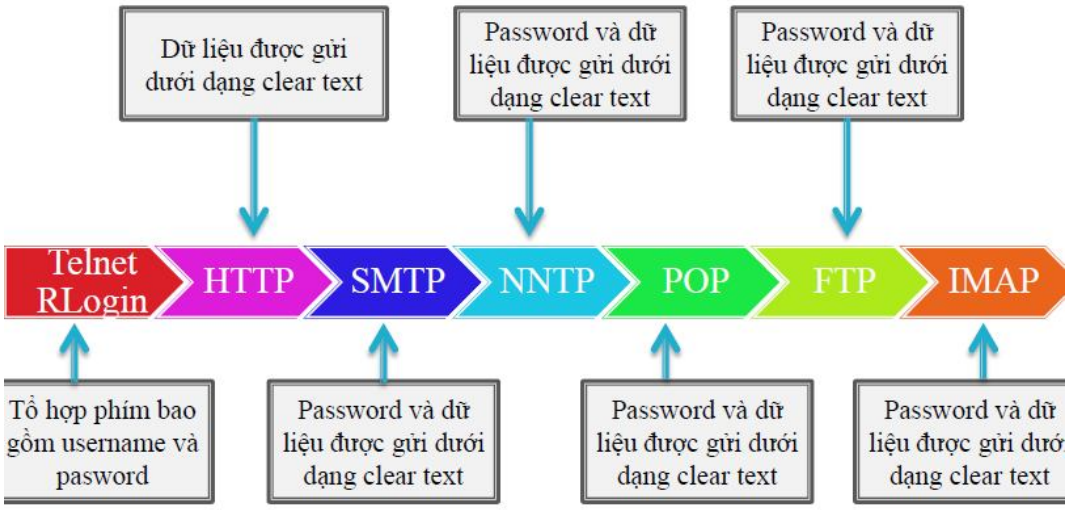
Nghe lén chủ yếu xảy ra ở mặt vật lý. Nghĩa là kẻ tấn công phải tiếp cận và có thể điều khiển một thành phần của hệ thống mạng, chẳng hạn như một máy tính nào đó. Trường hợp hệ thống máy tính nghe trộm và kẻ tấn công ở cách xa nhau, kẻ tấn công tìm cách điều khiển một máy tính nào đó trong hệ thống mạng rồi cài đặt trình nghe lén vào máy đó để thực hiện nghe trộm từ xa.

Các mối đe dọa về nghe lén

Bằng cách đặt gói tin trên mạng ở chế độ đa mode, kẻ tấn công có thể bắt và phân tích tất cả lưu lượng, thông tin mạng. Các gói tin nghe lén có thể chỉ bắt những thông tin trên cùng 1 miền mạng.

Sniffing trong môi trường Switch:

Khác với Hub, Switch chỉ chuyển tải các gói tin đến những địa chỉ cổng xác định trong bảng chuyển mạch nên nghe trộm kiểu "tự nhận" như ở Hub không thực hiện được. Tuy nhiên, kẻ tấn công có thể dùng các cơ chế khác để tấn công trong môi trường Switch như ARP spoofing, MAC spoofing, MAC duplicating, DNS spoofing, v.v…



Tấn công MAC

Switch thì có bộ nhớ giới hạn cho việc ánh xạ địa chỉ MAC và port vật lý trên switch. Tấn công MAC là tấn công làm ngập lụt switch với một số lượng lớn yêu cầu, lúc này switch hoạt động như hub và lúc này các gói tin sẽ được gửi ra tất cả các máy trên cùng miền mạng và kẻ tấn công có thể dễ dàng nghe lén. Ngập lụt MAC làm cho bộ nhớ giới hạn của switch đầy lên bằng cách giả mạo nhiều địa chỉ MAC khác nhau và gửi đến switch.

Một khi bảng CAM trên switch đầy thì các lưu lượng ARP request sẽ làm ngập lụt mỗi cổng của switch. Lúc này switch hoạt động cơ bản như hub, và tấn công lúc này sẽ làm đầy bảng CAM của switch.

Tấn công DHCP

DHCP làm việc khá đơn giản và xuyên suốt quá trình trao đổi thông điệp giữa server và client không hề có sự xác thực hay kiểm soát truy cập nào.

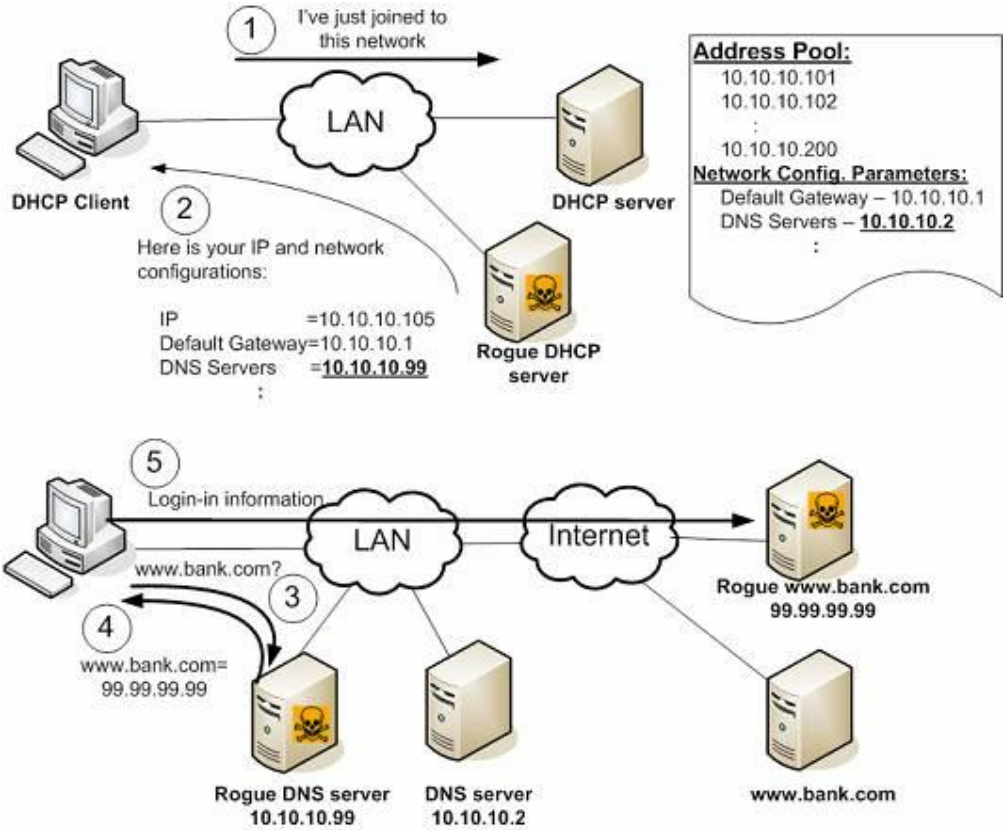
Server không có cách nào biết được rằng nó có đang liên lạc với một legitimate client (tạm dịch là máy hợp pháp, tức là một máy không bị điều khiển để thực hiện các mục đích xấu) hay không và ngược lại client cũng không thể biết được là nó có đang liên lạc với một legitimate server hay không.

Khả năng trong mạng xuất hiện các rogue DHCP client và rogue DHCP server (rogue tạm dịch là máy "DHCP giả", tức là một máy giả tạo, bị điều khiển để thực hiện các hành vi xấu) tạo ra nhiều vấn đề đáng quan tâm.

Một rogue server có thể cung cấp cho các legitimate client các thông số cấu hình TCP/IP giả và trái phép như: địa chỉ IP không hợp lệ, sai subnet mask, hoặc sai địa chỉ của default gateway, DNS server nhằm ngăn chặn client truy cập tài nguyên, dịch vụ trong mạng nội bộ hoặc Internet (đây là hình thức của tấn công DoS).

Việc thiết lập một rogue server như vậy có thể thực hiện được bằng cách sử dụng các kỹ thuật "social engineering" để có được khả năng tiếp cận vật lý rồi kết nối rouge server vào mạng.

Attacker có thể thoả hiệp thành công với một legitimate client nào đó trong mạng và thực hiện cài đặt rồi thực thi trên client này một chương trình có chức năng liên tục gửi tới DHCP server các gói tin yêu cầu xin cấp IP với các địa chỉ MAC nguồn không có thực cho tới khi toàn bộ dải IP trong scope của DHCP server này bị nó "thuê" hết. Điều này dẫn tới server không còn IP nào để có thể cấp phát cho các legitimate client khác. Hậu quả là các client này không thể truy cập vào mạng.



Tấn công đầu độc ARP

ARP là giao thức ánh xạ địa chỉ IP đến địa chỉ vật lý được nhận diện. Giao thức ARP sẽ quảng bá miền mạng của máy để tìm địa chỉ vật lý. Khi một máy cần giao tiếp với máy khác, và nó tìm trong bảng ARP của mình, nếu địa chỉ MAC không được tìm thấy trong bảng, giao thức ARP sẽ quảng bá ra toàn miền mạng. Tất cả các máy trong miền mạng sẽ so sánh địa chỉ IP đến địa chỉ MAC của chúng. Nếu một trong những máy đó, xác định được đó chính là địa chỉ của mình, nó sẽ gửi gói ARP hồi đáp và địa chỉ này sẽ được lưu trong bảng ARP và quá trình giao tiếp diễn ra.

Tấn công đầu độc ARP là hình thức tấn công mà gói tin ARP có thể bị giả mạo để gửi dữ liệu đến máy của kẻ tấn công. Kẻ tấn công làm ngập lụt bộ nhớ cache chứa địa chỉ ARP của máy mục tiêu bằng các địa chỉ ARP giả mạo, phương thức này còn được gọi là đầu độc. Giả mạo ARP liên quan đến việc xây dựng một số lượng lớn ARP Request giả mạo và gói ARP Reply liên tục được phản hồi dẫn đến tình trạng quá tải switch. Cuối cùng sau khi bảng ARP bị đầy thì switch sẽ hoạt động ở chế độ forwarding, lúc này thì kẻ tấn công có thể dễ dàng nghe lén mọi hoạt động trong mạng.

Giả mạo ARP giúp kẻ tấn công có thể chuyển hướng tất cả giao tiếp giữa hai máy, khi đó tất cả lưu lượng được gửi thông qua máy của kẻ tấn công. Các mối de dọa về tấn công ARP như: tấn công từ chối dịch vụ, Ăn cắp thông tin dữ liệu, Nghe lén cuộc gọi, Ăn cắp password, Thao tác dữ liệu

Chương 6: Cryptography

Giới thiệu tổng quan về mã hóa

Tìm hiểu mã hóa

Mã hóa là một quá trình xáo trộn nội dung của một phai hoặc một bản tin sao cho chỉ có đối tượng sở hữu khóa giải mã mới có thể đọc được nội dung đã được mã hóa.

Mã hóa được sử dụng để bảo vệ e-mail, thông tin thẻ tín dụng và các dữ liệu của công ty.

Mục tiêu mã hóa

- Tính bảo mật
- Tính toàn vẹn
- Tính sác thực
- Tính không khước từ

Các loại mã hóa

- Mã hóa đối xứng: sử dụng cùng một chìa khóa cho việc mã hóa và giải mã
- Mã hóa bất đối xứng: khóa dùng để mã hóa và giải mã là khác nhau. Có hai loại khóa là khóa bí mật và khóa công khai.
- Hàm băm (Hash Fuction): không sử dụng chìa khóa để mã hóa và giải mã

Cơ chế hoạt động

Mã hóa đối xứng

mã hóa đối xứng : tức là cả hai quá trình mã hóa và giải mã đều dùng một chìa khóa. Để đảm bảo tính an toàn, chìa khóa này phải được giữ bí mật. Vì thế các thuật toán loại này còn có tên gọi khác là secret key cryptography (hay private key cryptography), tức là thuật toán mã hóa dùng chìa khóa riêng (hay bí mật). Các thuật toán loại này lý tưởng cho mục đích mã hóa dữ liệu của cá nhân hay tổ chức đơn lẻ nhưng bộc lộ hạn chế khi thông tin đó phải được chia sẻ với một bên thứ hai.

Mã hóa đối xứng có thể phân thành hai nhóm phụ:

- Block ciphers: thuật toán khối – trong đó từng khối dữ liệu trong văn bản ban đầu được thay thế bằng một khối dữ liệu khác có cùng độ dài. Độ dài mỗi khối gọi là block size, thường được tính bằng đơn vị bit. Ví dụ thuật toán 3-Way có kích thước khối bằng 96 bit.
- Stream ciphers: thuật toán dòng – trong đó dữ liệu đầu vào được mã hóa từng bit một. Các thuật toán dòng có tốc độ nhanh hơn các thuật toán khối, được dùng khi khối lượng dữ liệu cần mã hóa chưa được biết trước, ví dụ trong kết nối không dây. Có thể coi thuật toán dòng là thuật toán khối với kích thước mỗi khối là 1 bit.

Mã hóa bất đối xứng

Mã hóa bất đối xứng : sử dụng một cặp chìa khóa có liên quan với nhau về mặt toán học, một chìa công khai dùng để mã hoá (public key) và một chìa bí mật dùng để giải mã (private key). Một thông điệp sau khi được mã hóa bởi chìa công khai sẽ chỉ có thể được giải mã với chìa bí mật tương ứng. Do các thuật toán loại này sử dụng một chìa khóa công khai (không bí mật) nên còn có tên gọi khác là public-key cryptography (thuật toán mã hóa dùng chìa khóa công khai).

Một trong những hạn chế của các thuật toán mã hóa bất đối xứng là tốc độ chậm, do đó trong thực tế người ta thường sử dụng một hệ thống lai tạp trong đó dữ liệu được mã hóa bởi một thuật toán đối xứng, chỉ có chìa dùng để thực hiện việc mã hóa này mới được mã hóa bằng thuật toán bất đối xứng.

Thuật toán AES

AES viết tắt của Advance Encryption Standard. Tháng 12 năm 1997, viện tiêu chuẩn và công nghệ Mỹ (NIST – National Institute of Standard and Technology) kêu gọi phát triển một thuật toán mới thay thế cho 3DES (một biến thể an toàn hơn của DES với chìa khóa dài 112 bit). Thuật toán được chọn phải là thuật toán khối có kích thước khối là 128 bit, hỗ trợ chìa khóa có kích thước 128 bit, 192 bit và 256 bit.

15 thuật toán được gửi đến từ nhiều nơi trên thế giới, 5 thuật toán lọt vào vòng hai: Rijndael, Twofish, Serpent, RC6 và MARS. Tháng 11 năm 2001, Rijndael được chọn làm AES (một phần nhờ có tốc độ nhanh hơn so với các đối thủ), chính thức thay thế DES trong vai trò chuẩn mã hóa dữ liệu.

Thuật toán DES

DES viết tắt của Data Encryption Standard. DES là một thuật toán khối với kích thước khối 64 bit và kích thước chìa 56 bit. Tiền thân của nó là Lucifer, một thuật toán do IBM phát triển. Cuối năm 1976, DES được chọn làm chuẩn mã hóa dữ liệu của nước Mỹ, sau đó được sử dụng rộng rãi trên toàn thế giới. DES cùng với mã hóa bất đối xứng đã mở ra một thời kì mới cho ngành mã hóa thông tin. Trước DES, việc nghiên cứu và sử dụng mã hóa dữ liệu chỉ giới hạn trong chính phủ và quân đội. Từ khi có DES, các sản phẩm sử dụng nó tràn ngập thị trường. Đồng thời, việc nghiên cứu mã hóa thông tin cũng không còn là bí mật nữa mà đã trở thành một ngành khoa học máy tính bình thường.

Trong khoảng 20 năm sau đó, DES đã trải qua nhiều khảo sát, phân tích kỹ lưỡng và được công nhận là an toàn đối với các dạng tấn công (tất nhiên, ngoại trừ brute-force).

Tới tháng 7 năm 1998, EFF (Electronic Frontier Foundation) đã "brute-force" thành công DES trong 56 giờ. Ít lâu sau đó cùng với mạng tính toán ngang hàng Distribute.net, tổ chức này đã lập nên kỉ lục mới là 22 giờ 15 phút. Sự kiện này chứng tỏ cỡ chìa 56 bit của DES đã lỗi thời và cần được thay thế.

Thuật toán RSA

RSA là 1 là một thuật toán mã hóa bất đối xứng được sử dụng rất rộng rãi trong giao dịch điện tử. Nó sử dụng phép tính số học và lý thuyết mô-đun số tiểu để thực hiện tính toán bằng cách sử dụng hai số nguyên tố lớn hơn

Mã hóa RSA được sử dụng rộng rãi và là tiêu chuẩn mã hóa phổ biến.

Cái tên RSA có nguồn gốc từ ba chữ cái đầu của tên ba người đồng thiết kế ra nó: Ronald Rivest, Adi Shamir và Leonard Adleman.

Trước đó, vào năm 1973, Clifford Cocks, một nhà toán học người Anh làm việc tại GCHQ, đã mô tả một thuật toán tương tự. Với khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm 1997 vì được xếp vào loại tuyệt mật.

Hàm băm (hashing)

Hàm băm tính toán kích thước cố định của chuỗi ký tự được gọi là băm giá trị của bất kỳkhối thông tin tùy ý. Nếu bất kỳ bit đầu vào của hàm được thay đổi, tất

cả các bit đầu ra có 50% cơ hội thay đổi.Nó khả thi về mặt có 2 tập tin với cùng 1 giá trị Message Digest

Hàm băm thường được gọi là một chiều vì chúng tạo giá trị rất khó để dịch ngược

Thuật toán hàm băm MD5

MD5 (Message-Digest algorithm 5) là một hàm băm mật mã được sử dụng phổ biến, được thiết kế bởi Giáo sư Ronald L. Rivest tại trường MIT vào năm 1991 để thay thế cho hàm băm trước đó là MD4 (1990). Là một chuẩn Internet (RFC 1321), MD5 đã được dùng trong nhiều ứng dụng bảo mật và cũng được dùng phổ biến để kiểm tra tính toàn vẹn của tập tin. Cũng như các hàm băm khác như MD4 và SHS (Secure Hash Standard), MD5 là phương pháp có ưu điểm tốc độ xử lý rất nhanh, thích hợp với các thông điệp dài và cho ra giá trị băm dài 128 bit.

Trong MD5, thông điệp ban đầu X sẽ được mở rộng thành dãy bit X có độ dài là bội của 512. Dãy bit X gồm các thành phần được sắp thứ tự như sau: Dãy bit X ban đầu, một bit 1, dãy d bit 0 (d được tính sao cho dãy X cuối cùng là bội của 512), dãy 64 bit l biểu diễn chiều dài của thông điệp. Đơn vị xử lý trong MD5 là các từ 32-bit, nên dãy bit X ở trên sẽ được biểu diễn thành dãy các từ X[i] 32-bit sau:

$$X=X[0]\ X[1]\ X[2]\ \ldots X[\mathbf{N}-1]\text{ , với }\mathbf{N}\text{ là bội của 16.[5]}$$

MD5 không có khả năng chịu va chạm,nên sử dụng các thuật toán như SHA-1 và SHA-2

MD5 là một số thập lục phân 32-chữ số, nó được sử dụng rộng rãi cho các ứng dụng chữ ký số, kiểm tra toàn vẹn tập tin và lưu trữ mật khẩu

Giao thức SSL

Việc kết nối giữa một Web browser tới bất kỳ điểm nào trên mạng Internet đi qua rất nhiều các hệ thống độc lập mà không có bất kỳ sự bảo vệ nào với các thông tin trên đường truyền. Không một ai kể cả người sử dụng lẫn Web server có bất kỳ sự kiểm soát nào đối với đường đi của dữ liệu hay có thể kiểm soát được liệu có ai đó thâm nhập vào thông tin trên đường truyền. Để bảo vệ những thông tin mật trên mạng Internet hay bất kỳ mạng TCP/IP nào, SSL đã kết hợp những yếu tố sau để thiết lập được một giao dịch an toàn:

Xác thực: đảm bảo tính xác thực của trang mà bạn sẽ làm việc ở đầu kia của kết nối. Cũng như vậy, các trang Web cũng cần phải kiểm tra tính xác thực của người sử dụng.

Mã hoá: đảm bảo thông tin không thể bị truy cập bởi đối tượng thứ ba. Để loại trừ việc nghe trộm những thông tin "nhạy cảm" khi nó được truyền qua Internet, dữ liệu phải được mã hoá để không thể bị đọc được bởi những người khác ngoài người gửi và người nhận.

Toàn vẹn dữ liệu: đảm bảo thông tin không bị sai lệch và nó phải thể hiện chính xác thông tin gốc gửi đến.

Với việc sử dụng SSL, các Web site có thể cung cấp khả năng bảo mật thông tin, xác thực và toàn vẹn dữ liệu đến người dùng. SSL được tích hợp sẵn vào các browser và Web server, cho phép người sử dụng làm việc với các trang Web ở chế độ an toàn. Khi Web browser sử dụng kết nối SSL tới server, biểu tượng ổ khóa sẽ xuất hiện trên thanh trạng thái của cửa sổ browser và dòng "http" trong hộp nhập địa chỉ URL sẽ đổi thành "https". Một phiên giao dịch HTTPS sử dụng cổng 443 thay vì sử dụng cổng 80 như dùng cho HTTP.

Được phát triển bởi Netscape, ngày nay giao thức Secure Socket Layer (SSL) đã được sử dụng rộng rãi trên World Wide Web trong việc xác thực và mã hoá thông tin giữa client và server. Tổ chức IETF (Internet Engineering Task Force) đã chuẩn hoá SSL và đặt lại tên là TLS (Transport Layer Security). Mặc dù là có sự thay đổi về tên nhưng TSL chỉ là một phiên bản mới của SSL. Phiên bản TSL 1.0 tương đương với phiên bản SSL 3.1. Tuy nhiên SSL là thuật ngữ được sử dụng rộng rãi hơn.

SSL được thiết kế như là một giao thức riêng cho vấn đề bảo mật có thể hỗ trợ cho rất nhiều ứng dụng. Giao thức SSL hoạt động bên trên TCP/IP và bên dưới các giao thức ứng dụng tầng cao hơn như là HTTP (Hyper Text Transport Protocol), IMAP (Internet Messaging Access Protocol) và FTP (File Transport Protocol). Trong khi SSL có thể sử dụng để hỗ trợ các giao dịch an toàn cho rất nhiều ứng dụng khác nhau trên Internet, thì hiện nay SSL được sử dụng chính cho các giao dịch trên Web.

SSL không phải là một giao thức đơn lẻ, mà là một tập các thủ tục đã được chuẩn hoá để thực hiện các nhiệm vụ bảo mật như xác thực server, xác thực client và mã hóa kết nối.

Giao thức SSL bao gồm 2 giao thức con: giao thức SSL record và giao thức SSL handshake. Giao thức SSL record xác định các định dạng dùng để truyền dữ liệu. Giao thức SSL handshake (gọi là giao thức bắt tay) sẽ sử dụng SSL record protocol để trao đổi một số thông tin giữa server và client vào lần đầu tiên thiết lập kết nối SSL.

Chương 7: Enumeration of Services

Enumeration là gì?

Là quá trình trích xuất tên người dùng, tên máy, tài nguyên mạng, các chia sẻ, và cá dịch vụ từ một hệ thống.

Kỹ thuật này được tiến hành trong một môi trường mạng nội bộ.

Các kỹ thuật liệt kê

- Trích xuất tên người dùng sử dụng ID thư điện tử.
- Trích xuất tên người dùng sử dụng SNMP.
- Trích xuất tên người dùng từ Windows.
- Trích xuất thông tin sử dụng từ các mật khẩu mặc định.
- Chiếm Active Directory.
- Trích xuất thông tin sử dụng vùng thuyên chuyển DNS.

Liệt kê NetBIOS

NetBIOS là gì?

NetBIOS (Network Basic Input Output System) là một giao thức cho các máy khách kết nối tới tài nguyên các máy trong mạng LAN, NetBIOS được thiết kế bởi tập đoàn máy tính IBM và Sytek.

Nó được thiết kế trong môi trường mạng LAN để chia sẻ tài nguyên (như dùng chung các File, Folder, máy in và nhiều tài nguyên khác....Mô hình này rất giống mô hình mạng ngang hàng Peer to Peer).

Thông thường thì một mạng dùng giao thức Netbios thường là Netbios Datagram Service (Port 138), Netbios Session Service (Port 139) hoặc cả 2.

Liệt kê NetBIOS

Kẻ tấn công có được các liệt kê:

- Danh sách máy tính thuộc một miền mạng.
- Danh sách các chia sẻ của các máy tính trên một miền mạng.
- Các chính sách và các mật khẩu

Các công cụ liệt kê NetBIOS

- SuperScan
- NetBios Enumertor

Các công cụ liệt kê tài khoản người dùng

- Ps Tools
- Trong Ps Tools có rất nhìu công cụ nhỏ như:
  - PsExec
  - PsFile
  - PsGetSid
  - PsKill
  - PsInfo
  - PsList
  - PsLoggedOn
  - PsLogList

Công cụ liệt kê hệ thống sử dụng các mật khẩu mặc định

- Trang web http://www.defaultpassword.com

Liệt kê SNMP

SNMP là gì?

SNMP (Simple Network Management Protocol) là một tập hợp các giao thức không chỉ cho phép kiểm tra nhằm đảm bảo các thiết bị mạng như router, switch hay server đang vận hành mà còn vận hành một cách tối ưu, ngoài ra SNMP còn cho phép quản lý các thiết bị mạng từ xa.

Một hệ thống sử dụng SNMP bao gồm 2 thành phần chính:

- Manager: Là một máy tính chạy chương trình quản lý mạng. Manager còn được gọi là một NMS (Network Management Station). Nhiệm vụ của một manager là truy vấn các agent và xử lý thông tin nhận được từ agent.
- Agent: Là một chương trình chạy trên thiết bị mạng cần được quản lý. Agent có thể là một chương trình riêng biệt (ví dụ như daemon trên Unix) hay được tích hợp vào hệ điều hành, ví dụ như IOS (Internetwork Operation System) của Cisco. Nhiệm vụ của agent là thông tin cho manager.

Liệt kê SNMP

Kẻ tấn công liệt kê SNMP để trích xuất thông tin về tai nguyên mạng chẳng hạn như: máy chủ, bộ định truyến, bộ chuyển mạch, các thiết bị, chia sẻ,..v..v.,

Sử dụng tập hợp chuỗi mặc định để trích xuất thông tin về một thiết bị sử dụng tập hợp chuỗi "public".

Ngoài ra còn có thể liệt kê được MIB (cơ sở dữ liệu ảo chứa thông tin các đối tượng mạng).

Các công cụ liệt kê SNMP

- Getif SNMP MIB Browser.
- iReasoning MIB Browser.
- LoriotPro.
- Nsauditor Network Security Auditor.
- OidView SNMP MIB Browser.
- OpUtils Network Monitoring Toolset.
- SNMP SCANNER.
- SNScan.
- SoftPerfect Network Scanner.
- Solarwind Engineer's Toolset.

Liệt kê Unix/Linux

Linux là gì?

Linux là một hệ điều hành mã nguồn mở dạng Unix được xây dựng bởi Linus Torvalds và sau đó được phát triển bởi cộng đồng lập trình mã nguồn mở trên toàn thế giới thành nhiều nhiều phiên bản khác nhau. Phần lớn các phiên bản Linux đều miễn phí nhưng hiện nay có một số công ty đã cho ra đời một số phiên bản Linux thương mại.

Khác với Windows, Linux được tạo thành bởi các modul hoạt động độc lập với nhau, người dùng có thể tự xây dựng kernel (nhân) cho hệ điều hành của mình bằng cách thêm những modul cần thiết vào. Vì vậy hệ thống Linux có tính linh hoạt cao hơn Windows. Thường Linux được sử dụng làm máy chủ nhiều hơn là làm máy trạm vì việc cấu hình cho Linux phức tạp hơn nhiều vì thường phải dùng command line để cấu hình chứ không có giao diện đồ hoạ như Windows.

Hệ thống chạy trên Linux thường nhanh hơn và ổn định hơn là chạy trên Windows. Sở dĩ Linux chưa được dùng nhiều cho máy tính cá nhân vì nó hỗ trợ giao diện đồ hoạ chưa tốt.

Liệt kê trên Unix

Lệnh sử dụng để liệt kê tài nguyên mạng của Unix gồm những lệnh sau:

- Showmount: dùng để tìm các thư mục chia sẻ trên máy tính.

  [root$] showmount –e 19x.16x.xxx.xx

- Finger: dùng để liệt kê về người dùng và máy chủ, cho phép xem thời gian đăng nhập của người sử dụng thư mục, thời gian nhàn rỗi, vị trí văn phòng, và thời gian cuối cùng cả hai đều nhận được hoặc đọc thư.

  [root$] finger –l @target.hackme.com

- Rpcclient: dùng để điều tra được tên người dùng trên Linux và OS X.

  [root$] rpcclient $> netshareenum

- Rpcinfo (RPC): dùng liệt kê giao thức RPC (gọi hàm từ xa), giao thức RPC cho phép các ứng dụng giao tiếp với nhau qua mạng.

  [root$] rpcinfo –p 19x.16x.xxx.xx

Công cụ liệt kê Linux

- Enum4linux.

Liệt kê LDAP

LDAP là gì?

LDAP (Lightweight Directory Access Protocol) là giao thức sử dụng truy cập thư mục với Active Directory hoặc từ dịch vụ thư mục khác, và hoạt động ở port 389

Trong hệ thông sử dụng LDAP thư mục được định dạng phân cấp hợp lý, giống như quản lý các nhân viên trong một công ty.

Nó được găn vào hệ thống tên miền và cho phép tích hợp các tìm kiếm nhanh và phân giải nhanh chóng các truy vấn.

Các công cụ liệt kê LDAP

- Jxplorer.
- LDAP Account Manager.
- LDAP Admin tool Professional.
- LDAP Explorer Tool.
- Ldp.exe
- LEX – The LDAP Explorer.
- Softerra LDAP Administor.
- Symlabs LDAP Browser.

Liệt kê NTP

NTP là gì?

NTP (Network Time Protocol) là giao thức thời gian mạng được thiết kế để đồng bộ thời gian của các máy tính nối mạng với nhau, và sử dụng port 123.

Các máy tính trong mạng công cộng có thể chênh lệch nhau 10mili giây.

Và chênh lệch 200 micro giây hoặc ít hơn trong mạng cục bộ ở điều kiện lý tưởng.

Các công cụ liệt kê NTP

- NTP Server Scanner.
- PresenTense Time Server.
- PresenTense Time Client.
- LAN Time Analyser.
- NTP Server Checker.
- Time Watch.
- PresenTense NTP Auditor.
- NTP Time Server Monitor.
- AtomSync.
- Ngoài ra còn có các lệnh để liệt kê NTP như ntpdate, ntptrace, ntpdc, ntpq.

Liệt kê SMTP

SMTP là gì?

SMTP (Simple Mail Transfer Protocol) là giao thức dùng để gửi thư điện tử giữa các máy tính với nhau và dùng port 25.

Công cụ liệt kê SMTP

- NetScanTools Pro.

Liệt kê DNS

DNS là gì?

DNS(Domain Name Server) là hệ thống dùng để phân giải tên miền dùng port 53.

Liệt kê DNS Zone Transfer

Sử dụng lệnh nslookup để xác đinh máy chủ DNS và hồ sơ của một mạng mục tiêu.Kẻ tấn công có thê thu thập được các thông tin giá trị như máy chủ DNS, tên máy chủ, tên người dùng,…v..v

Sử dụng công cụ Men & Mice Suite

Chương 8: System Hacking

Quá trình tấn công hệ thống (System hacking)

Quá trình tấn công có thể được khái quát qua 3 giai đoạn sau :

Giai đoạn 1 : Thu thập thông tin

Giai đoạn 2 : Phân tích và hành động

Giai đoạn 3 : Dừng và xoá dấu vết

Giai đoạn thu thập thông tin

Footprinting

Đây là bước mà kẻ tấn công nắm được càng nhiều thông tin càng tốt về đối tượng như Domain Name, Địa chỉ IP, giao thức mạng sử dụng (IP , IPX , DecNet ...)… Các thông tin cá nhân về người quản trị: Số điện thoại, địa chỉ, chức vụ, các chi nhánh của công ty… Đây là một bước quan trọng cho hacker nhiều thông tin, đôi khi với những thông tin này hacker đã có thể làm chủ hệ thống.

Scanning

Khi đã có những thông tin cần thiết, thì tiếp đến là đánh giá và định danh những dịch vụ mà mục tiêu có. Việc này bao gồm:

- Quét cổng, xác định hệ điều hành
- Tìm hiểu kĩ hơn về hệ thống đối tượng
- Xác định hệ thống có đang chạy ko
- Tìm hiểu các dịch vụ đang chạy hay đang lắng nghe
- Tìm hiểu các lỗ hổng
- Kiểm tra các cổng
- Xác địng các dịch vụ sử dụng giao thức TCP và UDP
- Tìm hiểu về hệ điều hành của hệ thống

Enumeration

Bước thứ ba là tìm kiếm những tài nguyên được bảo vệ kém hoặc tài khoản người dùng mà có thể sử dụng để xâm nhập. Nó bao gồm các mật khẩu mặc định, các script và dich vụ mặc định. Rất nhiều người quản trị mạng không biết đến hoặc không sửa đổi lại các giá trị này.

Đến bước này, các hacker bắt đầu kiểm soát server nội bộ, xác định các tài khoản trên server, mức độ bảo vệ, tài nguyên chia sẻ…

Giai đoạn phân tích và hành động

Gainning Access (Đột nhập hệ thống)

Với các thông tin thu thập được hacker có thể sử dụng một kĩ thuật nào đó để biết được mật khẩu của tài khoản trên hệ thống.

Privilege Escalation (Nâng quyền hệ thống)

Đây là một giai đoạn thực sự khó vì việc nâng quyền đòi hỏi sự can thiệp không chính tắc vào hệ điều hành hoặc vào hệ thống phần mềm.

Ví dụ trong trường hợp hacker xâm nhập được vào mạng với tài khoản guest,

thì họ sẽ tìm cách kiểm soát toàn bộ hệ thống. Hacker sẽ tìm cách crack password của admin, hoặc sử dụng lỗ hổng để tăng đặc quyền trên hệ thống.

Pilfering (Khai thác hệ thống)

Thêm một lần nữa các máy tìm kiếm lại được sử dụng để tìm các phương pháp truy cập vào mạng. Những tập tin lưu trữ mật khẩu hay các cơ chế không an toàn khác có thể giúp cho hacker khai thác hệ thống, định vị server và điều khiển server.

Dừng và xóa dấu vết

Backdoors

Hacker để lại "Back Doors", tức là một cơ chế cho phép hacker truy cập trở lại bằng con đường bí mật không phải tốn nhiều công sức, bằng việc cài đặt Trojan hay tạo user mới (đối với tổ chức có nhiều user).

Covering Tracks (Xoá dấu vết)

Vì hệ thống luôn ghi nhận những hành động những gì đã xảy ra. Sau khi đã có những thông tin cần thiết, hacker tìm cách xoá dấu vết, xoá các file log của hệ điều hành làm cho người quản lý không nhận ra hệ thống đã bị xâm nhập hoặc có biêt cũng không tìm ra kẻ xâm nhập là ai.

Bẻ khóa mật khẩu

Các loại mật khẩu

Chỉ là chữ cái: *POTHMYDE*

Chỉ là số: *23698217*

Chỉ là những ký tự đặc biệt: *&*#@!(%)*

Chữ cái và số: *meetl 23*

Chỉ là số và ký tự đặc biệt: *123@$45*

Chữ cái ,số, và ký tự đặc biệt: *ap1@52*

Chữ cái và các ký tự đặc biệt: *bob&ba*

Các loại tấn công mật khẩu

Tấn công thụ động trực tuyến (Passive Online Attacks)

Một cuộc tấn công thụ động trực tuyến là đánh hơi (sniffing) để tìm các dấu vết, các mật khẩu trên một mạng. Mật khẩu bị bắt (capture) trong quá trình xác thực và sau đó có thể được so sánh với một từ điển (dictionary) hoặc là danh sách mật khẩu (word list). Tài khoản người dùng có mật khẩu thường được băm (hashed) hoặc mã hóa (encrypted) trước khi gửi lên mạng để ngăn chặn truy cập trái phép và sử dụng. Nếu mật khẩu được bảo vệ bằng cách trên, một số công cụ đặc biệt giúp hacker có thể phá vỡ các thuật toán mã hóa mật khẩu.

Tấn công chủ động trực tuyến (Actice Online Attacks)

Cách dễ nhất để đạt được cấp độ truy cập của một quản trị viên hệ thống là đoán mật khẩu. Mật khẩu đoán là để tấn công. Tấn công chủ động trực tuyến dựa trên các yếu tố con người tham gia vào việc tạo ra mật khẩu và cách tấn công này chỉ hữu dụng với những mật khẩu yếu.

Tấn công không trực tuyến

Cuộc tấn công không trực tuyến được thực hiện tại một máy khác. Cuộc tấn công không trực tuyến yêu cầu phần cứng để truy cập vật lý vào máy tính và sao chép các tập tin mật khẩu từ hệ thống lên phương tiện di động. Sau đó kẻ tấn công có tập tin mật khẩu đó và tiếp tục khai thác lỗ hổng bảo mật.

Tấn công không công nghệ

Là cuộc tấn công mà không sử dụng bất kỳ kiến thức kỹ thuật nào. Nó lợi dụng qua sự giao tiếp, kẻ tấn công có thể có được thông tin của nạn nhân và từ đó có thể tấn công mật khẩu. Loại tấn công có thể bao gồm các kỹ thuật như: Social Engineering, Shoulder Surfing, Dumpster Diving.

Tăng quyền hạn (Escalating Privileges)

Một kẻ tấn công có thể được truy cập vào mạng bằng cách sử dụng một tài khoản người dùng bình thường, và các bước tiếp theo sẽ là đạt được quyền quản trị.

Cái này được thực hiện bằng cách nắm lấy quyền truy cập bằng cách sử dụng một tài khoản người dùng không phải là quản trị viên. Thường bằng cách thu thập các tên người dùng và mật khẩu thông qua một bước trung gian để gia tăng các đặc quyền trên tài khoản với mức độ quản trị viên.

Một khi kẻ tấn công đã có một tài khoản người dùng hợp lệ và mật khẩu, các bước tiếp theo là để thực thi các ứng dụng nói chung kẻ tấn công cần phải có một tài khoản có quyền truy cập cấp quản trị viên để cài đặt chương trình. Đó là lý do tại sao tăng đặc quyền là rất quan trọng.

Thực thi ứng dụng (Executing Applications)

Một khi hacker đã có thể truy cập tài khoản với quyền quản trị, điều tiếp theo cần làm là thực thi các ứng dụng trên hệ thống đích. Mục đích của việc thực thi ứng dụng có thể cài đặt một cửa sau trên hệ thống, cài đặt một keylogger để thu thập thông tin bí mật, sao chép các tập tin, hoặc chỉ gây thiệt hại cơ bản cho hệ thống, bất cứ điều gì hacker muốn làm trên hệ thống.

Keylogger

Nếu tất cả những nỗ lực để thu thập mật khẩu không thành công, thì keylogger là công cụ lựa chọn cho các hacker. Được thực hiện như là phần mềm được cài đặt trên máy tính hoặc là phần cứng gắn vào máy tính. Keylogger là các phần mềm ẩn, ngồi giữa phần cứng (bàn phím) và hệ điều hành, để họ có thể ghi lại mọi phím tắt. Keylogger phần mềm có thể phá hoại hệ thống như Trojans hoặc viruses.

Keylogger là phần mềm gián điệp có dung lượng nhỏ, giúp kết nối các bàn phím máy tính và lưu tất cả các thao tác phím vào một file. Hacker có thể cài thêm tính năng là tự động gửi nội dung file đó đến máy chủ của hacker.

Spyware

Phần mềm gián điệp (Spyware) là một chương trình ghi lại sự tương tác của người sử dụng máy tính và internet mà người sử dụng không thể can thiệp. Spyware có thể gây mất ổn định ở hệ thống, lấy thông tin của người dùng và gửi đến kẻ tấn công, giám sát người dùng trực tuyến, giảm mức độ bảo vệ của máy tính, …

Che dấu vết tích

Một khi kẻ xâm nhập thành công, đã đạt được quyền truy cập quản trị viên trên một hệ thống, thì kẻ tấn công cố gắng che dấu vết tích ngăn chặn bị phát hiện. Một hacker cũng có thể cố gắng để loại bỏ các bằng chứng hoặc các hoạt động của họ trên hệ thống, để ngăn ngừa truy tìm danh tính hoặc vị trí của cơ quan hacker. Xóa bất kỳ thông báo lỗi hoặc các sự kiện an ninh đã được lưu lại, để tránh phát hiện.

Ẩn tập tin (Hiding Files)

Rootkits

Rootkit là một loại chương trình thường được sử dụng để che dấu các tiện ích trên hệ thống bị xâm nhập. Rootkit bao gồm cái gọi là *back doors*, nó giúp cho kẻ tấn công đó truy cập vào hệ thống sẽ dễ dàng hơn trong lần sau. Ví dụ, các rootkit có thể ẩn một ứng dụng, ứng dụng này có thể sinh ra một lệnh kết nối vào một cổng mạng cụ thể trên hệ thống. *Back door* cho phép các quá trình bắt đầu bởi một người không có đặc quyên, dùng để thực hiện chức năng thường dành cho các quản trị viên.

Luồng NTFS (NTFS Streaming)

Luồng NTFS có một tính năng gọi là *ADS* cho phép dữ liệu được lưu trữ trong các tập tin liên kết ẩn một cách bình thường, có thể nhìn thấy được tập tin. Không giới hạn về kích thước, hơn nữa một luồng có thể liên kết đến một file bình thường.

Steganography

Steganography là quá trình giấu dữ liệu trong các loại dữ liệu khác như hình ảnh hay tập tin văn bản.

Các phương pháp phổ biến nhất của dữ liệu ẩn trong các tập tin là sử dụng hình ảnh đồ họa như là nơi để cất giấu. Kẻ tấn công có thể nhúng các thông tin trong một tập tin hình ảnh bằng cách sử dụng steganography.

Chương 9: Trojans, Viruses, Worms, và Covert Channels

Trojan

Trojan Là loại mã độc hại được đặt theo sự tích "Ngựa thành Troy". Trojan là một chương trình mà trong đó chứa đựng nhưng mã nguy hiểm và độc hại ẩn dưới dạng nhưng dữ liệu hay nhưng chương trình dường như vô hại theo như tính năng này nó có thể điều khiển và gây hại, ví dụ như mở bảng phân bố tập tin trong đĩa cứng của bạn.

Mục đích của Trojan

- Ăn cắp thông tin như mật khẩu, mã bảo mật thẻ tín dụng thông tin bằng cách sử dụng keylogers
- Sử dụng máy tính của nạn nhân để tạo một mạng botnet (mạng máy tính ma) để thực hiện tấn công DDOS
- Xóa hoặc thay thế các file quan trọng của hệ thống
- Tạo một kết nối giả để tấn công DOS
- Tải Spyware Adwares và các file độc hại
- Vô hiệu hóa tường lửa và phần mềm chống virus
- Chụp màn hình, ghi âm, quay màn hình của máy nạn nhận
- lây nhiễm sang PC của nạn nhân như một máy chủ proxy cho các cuộc tấn công chuyển tiếp
- Sử dụng máy tính của nan nhân để phát tán thư rác và bom thư

Backdoor

Backdoor là một chương trình (program) hoặc có liên quan đến chương trình, được hacker sử dụng để cài đặt trên hệ thống đích, nhằm mục đích cho anh ta truy cập trở lại hệ thống vào lần sau. Mục đích của backdoor là xóa bỏ một cách minh chứng hệ thống ghi nhật ký. Nó cũng giúp hacker cầm cự trạng thái truy cập khi bị quản trị viên phát hiện và tìm cách khắc phục.

Phân loại Trojan

Command shell Trojan

- Lệnh Trojan Shell cho phép điều khiển từ xa lệnh Shell trên máy tính của nạn nhân
- Máy chủ Trojan được cài trên máy của nạn nhân, trong đó nó mở một cổng để cho Attacker kết nối đến.

Một máy trạm được trên máy của Attacker, trong đó nó được sử dụng để chạy lênh shell trên máy tính của nạn nhân

Email Trojans

- Attacker điều khiển tự xa máy tính của nạn nhân bằng cách gửi một email
- Attacker có thể lấy file hoặc thư mục bằng cách gủi lệnh thông qua email
- Attacker mở máy chủ relay SMTP và giả mạo email từ một trường để che giấu nguồn gốc

Botnet Trojans

- Trojan botnet lây nhiễm một số lượng lớn các máy tính trên một phạm vi địa lý rộng lớn, tạo ra một mạng bot được điều khiển thông qua Command và Control (C&C) trung tâm
- Botnet được sử dụng để phát động một cuộc tấn công khác nhau trên một nạn nhân bao gồm tấn công từ chối dich vụ, spamming, Click gian lân và trộm cắp thông tin tài chính

Proxy sever Trojans

- Trojan Proxy thường được sử dụng như một ứng dụng cho phép Attacker từ xa sử dụng máy tính của nạn nhân như một Proxy để kết nối Internet
- Proxy server Trojan, khi bị nhiễm, bắt đầu ẩn một Proxy server trên máy tính của nạn nhân
- Hàng ngàn máy tính trên Internet bị nhiễm với những Proxy server bằng cách sử dụng kỹ thuật này

FTP Trojans

- FTP Trojans cài đặt FTP server trên máy nạn nhân, nó mở cổng FTP

- Attacker có thể kết nối đến máy của nạn nhân bằng cách sử dụng cổng FTP để tải bất kỳ file nào tồn tại trên máy tính của nạn nhân.

VNC Trojans

VNC Trojan bắt đầu một VNC Server deamon trong hệ thông bị nhiễm. Nó kết nối đến nạn nhân bằng cách sử dụng bất kỳ VNC viewer nào với mật khẩu "secret". Khi chương trình VNC được xem xét kỹ lưỡng, thì Trojan sẽ không bao giờ bị phát hiện bởi trình chống Virus.

HTTP/HTTPS Trojans

- HTTP Trojan có thể vượt qua bất kỳ tường lửa nào và làm việc theo các đảo ngược một đường hầm HTTP tunnel
- Chúng được thực thi trên host nội bộ rồi tự nhân bản lên theo một chu kỳ được tính trước
- Chương trình con xuất hiện để người dùng tường lửa do đó cho phép truy cập Internet

Remote Access Trojan

Trojan làm việc giống như truy cập Remote Desktop. Hacker chiếm đoạt được hết GUI truy cập đến hệ thống từ xa

- Lây nhiễm máy tính(Rebecca's) với server.exe và Trojan kết nối ngược trở lại
- Trojan kết nối đến cổng 80 để Attacker tại Nga thiết lập một kết nối đảo ngược
- Jason, kẻ tấn công, có toàn quyền điều khiển máy của Rebecca

E-banking Trojans

E-Banking Trojan Đánh chặn các thông tin tài khoản của nạn nhân trước khi nó được mã hóa và gửi lệnh Trojan vào trung tâm điều khiển của kẻ tấn công.

Trojans phá hoại

- Đây là một loại nguy hiểm và phá hoại của Trojans
- Khi thực hiện Trojans này phá hủy các hệ điều hành
- Trojans định dạng tất cả các ổ đĩa nộ bộ và mạng
- Người sử dụng sẽ không thể khởi động hệ điều hành

Trojans mã hóa

- Trojan Mã Hóa: mã hóa tập tin dữ liệu trong hệ thống của nạn nhân và làm cho thông tin không sử dụng được
- Kẻ tấn công yêu cầu một khoản tiền chuộc hoặc nhân lực để mua hàng từ các cửa hàng thuốc trực tuyến của họ lại cho các mật khẩu để mở khóa

Overt channel và Covert channel?

Kênh công khai (overt channel) là kênh được khởi tạo một cách hợp pháp để các trương trình có thể giao tiếp với nhau trong hệ thống hoặc môi trường mạng. Các protocol là một ví dụ điển hình của overt channel

Kênh ẩn (covert channel) lại khởi tạo một cách bí mật đối với người sử dụng, các chương trình không trong sang, sẽ lấy môi trường này để có thể giao tiếp và trao đổi thông tin mà không cần có sự cho phép của người sử dụng

Virus

Đặc điểm cơ bản virus

Virus máy tính thực chất là các phần mềm tin học có khả năng gián tiếp tự kích hoạt, tự nhân bản sao chép chính nó vào các chương trình khác nhằm mục đích phá hoại, do thám hoặc cũng có thể chỉ là để vui đùa.Một số virus ảnh hưởng đến máy tính ngay sau khi mã của nó được thực hiện, một số virus khác nằm im cho đến khi một hoàn cảnh hợp lý rồi mới được kích hoạt. Để tiện đồ án, khi nói virus ta hiểu là virus máy tính.

Nguyên nhân Virus được tạo ra

- Gây thiệt hại cho các đối thủ cạnh tranh
- Lợi ích tài chính
- Dự án nghiên cứu
- Trò đùa
- Phá hoại
- Khủng bố mạng lưới
- Phân tấn các thông điệp trính trị

Dấu hiệu nhận biết bị nhiễm Virus

- Truy xuất tập tin, mở các chương trình ứng dụng chậm.
- Khi duyệt web có các trang web lạ tự động xuất hiện.
- Duyệt web chậm, nội dung các trang web hiển thị trên trình duyệt chậm.
- Các trang quảng cáo tự động hiện ra (pop up), màn hình Desktop bị thay đổi.
- Các file lạ tự động sinh ra khi bạn mở ổ đĩa USB.
- Xuất hiện các file có phần mở rộng .exe có tên trùng với tên các thư mục.và có dấu hiệu mất file và thư mục
- Nhẫn ổ đĩa bị thay đổi
- Ổ cứng bị truy xuất thường xuyên

B-virus

B-virus: Virus chỉ tấn công lên Master Boot hay Boot Sector.

Tùy thuộc vào độ lớn của đoạn mã virus mà B-virus được chia thành hai loại:

SB-virus.

Chương trình của SB-virus chỉ chiếm đúng một sector khởi động, các tác vụ của SB-virus không nhiều và tương đối đơn giản. Hiện nay số các virus loại này thường ít gặp.

DB-virus.

Đây là những loại virus mà đoạn mã của nó lớn hơn 512 byte (thường thấy). Vì thế mà chương trình virus được chia thành hai phần:

Phần đầu virus: Được cài đặt trong sector khởi động để chiếm quyền điều hiển khi quyền điều khiển được trao cho sector khởi động này. Nhiệm vụ duy nhất của phần đầu là: tải tiếp phần thân của virus vào vùng nhớ và trao quyền điều khiển cho phần thân đó. Vì nhiệm vụ đơn giản như vậy nên phần đầu của virus thường rất ngắn, và càng ngắn càng tốt vì càng ngắn thì sự khác biệt giữa sector khởi động chuẩn và sector khởi động đã bị nhiễm virus càng ít, giảm khả năng bị nghi ngờ.

Phần thân virus: Là phần chương trình chính của virus. Sau khi được phần đầu tải vào vùng nhớ và trao quyền, phần thân này sẽ tiến hành các tác vụ của mình, sau

khi tiến hành xong mới đọc sector khởi động chuẩn vào vùng nhớ và trao quyền cho nó để máy tính làm việc một cách bình thường như chưa có gì xảy ra cả.

Một số kỹ thuật cơ bản của B-virus.

Dù là SB-virus hay DB-virus, nhưng để tồn tại và lây lan, chúng đều có một số các kỹ thuật cơ bản như sau:

Kỹ thuật kiểm tra tính duy nhất.

Virus phải tồn tại trong bộ nhớ cũng như trên đĩa, song sự tồn tại quá nhiều bản sao của chính nó trên đĩa và trong bộ nhớ sẽ chỉ làm chậm quá trình Boot máy, cũng như chiếm quá nhiều vùng nhớ ảnh hưởng tới việc tải và thi hành các chương trình khác đồng thời cũng làm giảm tốc độ truy xuất đĩa. Chính vì thế, kỹ thuật này là một yêu cầu nghiêm ngặt với B-virus.

Kỹ thuật lưu trú.

Sau khi thực hiện xong chương trình POST, giá trị tổng số vùng nhớ vừa được Test sẽ được lưu vào vùng BIOS Data ở địa chỉ 0:413h. Khi hệ điều hành nhận quyền điều khiển, nó sẽ coi vùng nhớ mà nó kiểm soát là giá trị trong địa chỉ này. Vì vậy để lưu trú, mọi B-virus đều áp dụng kỹ thuật sau đây: Sau khi tải phần lưu trú của mình lên vùng nhớ cao, nó sẽ giảm giá trị vùng nhớ do DOS quản lý tại 0:413h đi một lượng đúng bông kích thước của virus. Tuy nhiên nếu không kiểm tra tốt sự có mặt trong vùng nhớ, khi bị Boot mềm liên tục, giá trị tổng số vùng nhớ này sẽ bị giảm nhiều lần, ảnh hưởng tới việc thực hiện của các chương trình sau này. Chính vì thế, các virus được thiết kế tốt phải kiểm tra sự tồn tại của mình trong bộ nhớ, nếu đã có mặt trong bộ nhớ thì không giảm dung lượng vùng nhớ nữa.

Kỹ thuật lây lan.

Đoạn mã thực hiện nhiệm vụ lây lan là đoạn mã quan trọng trong chương trình virus. Để đảm bảo việc lây lan, virus khống chế ngắt quan trọng nhất trong việc đọc/ghi vùng hệ thống: đó là ngắt 13h, tuy nhiên để đảm bảo tốc độ truy xuất đĩa, chỉ các chức năng 2 và 3 (đọc/ghi) là dẫn tới việc lây lan. Việc lây lan bông cách đọc Boot Sector (Master Boot) lên và kiểm tra xem đã bị lây chưa (kỹ thuật kiểm tra đã nói ở trên). Nếu sector khởi động đó chưa bị nhiễm thì virus sẽ tạo một sector khởi động mới với các tham số tương ứng của đoạn mã virus rồi ghi trở lại vào vị trí của nó trên đĩa. Còn sector khởi động vừa đọc lên cùng với thân của virus (loại DB-virus) sẽ được ghi vào vùng xác định trên đĩa. Ngoài ra một số

virus còn chiếm ngắt 21 của DOS để lây nhiễm và phá hoại trên các file mà ngắt 21 làm việc.

Kỹ thuật ngụy trang và gây nhiễu.

Kỹ thuật này ra đời khá muộn về sau này, do khuynh hướng chống lại sự phát hiện của người sử dụng và những lập trình viên đối với virus. Vì kích thước của virus khá nhỏ bé cho nên các lậptrình viên hoàn toàn có thể dò từng bước xem cơ chế của virus hoạt động như thế nào, cho nên các virus tìm mọi cách lắt léo để chống lại sự theo dõi của các lập trình viên.

Kỹ thuật phá hoại.

Đã là virus thì bao giờ cũng có tính phá hoại. Có thể phá hoại ở mức đùa cho vui, cũng có thể là phá hoại ở mức độ nghiêm trọng, gây mất mát và đình trệ đối với thông tin trên đĩa.

Kỹ thuật dành quyền điều khuyển của B-virus.

Khi máy tính bắt đầu khởi động (Power on), các thanh ghi phân đoạn đều được đặt về 0FFFFh,còn mọi thanh ghi khác đều được đặt về 0. Như vậy, quyền điều khiển ban đầu được trao cho đoạn mã tại 0FFFFh: 0h, đoạn mã này thực ra chỉ là lệnh nhảy JMP FAR đến một đoạn chương trình trong ROM, đoạn chương trình này thực hiện quá trình POST (Power On Self Test - Tự kiểm tra khi khởi động).

Quá trình POST sẽ lần lượt kiểm tra các thanh ghi, kiểm tra bộ nhớ, khởi tạo các Chip điều khiển DMA, bộ điều khiển ngắt, bộ điều khiển đĩa... Sau đó nó sẽ dò tìm các Card thiết bị gắn thêm để trao quyền điều khiển cho chúng tự khởi tạo rồi lấy lại quyền điều khiển. Chú ý rông đây là đoạn chương trình trong ROM (Read Only Memory) nên không thể sửa đổi, cũng như không thể chèn thêm một đoạn mã nào khác.

Sau quá trình POST, đoạn chương trình trong ROM tiến hành đọc Boot Sector trên đĩa A hoặc Master Boot trên đĩa cứng vào RAM (Random Acess Memory) tại địa chỉ 0:7C00h và trao quyền điều khiển cho đoạn mã đó bông lệnh JMP FAR 0:7C00h. Đây là chỗ mà B-virus lợi dụng để tấn công vào Boot Sector (Master Boot), nghĩa là nó sẽ thay Boot Sector (Master Boot) chuẩn bông đoạn mã virus, vì thế quyền điều khiển được trao cho virus, nó sẽ tiến hành các hoạt động của mình trước, rồi sau đó mới tiến hành các thao tác như thông thường: Đọc Boot Sector (Master Boot) chuẩn mà nó cất giấu ở đâu đó vào 0:7C00h rồi trao quyền

điều khiển cho đoạn mã chuẩn này, và người sử dụng có cảm giác rông máy tính của mình vẫn hoạt động bình thường.

F-Virus

F-virus: Virus chỉ tấn công lên các file khả thi.

Phân loại F-Virus

So với B-virus thì số lượng F-virus đông đảo hơn nhiều, có lẽ do các tác vụ đĩa với sự hỗ trợ của Int 21 đã trở nên cực kỳ dễ dàng và thoải mái, đó là điều kiện phát triển cho các F-virus. Thường thì các F-virus chỉ lây lan trên các file khả thi (có đuôi .COM hoặc .EXE), tuy nhiên một nguyên tắc mà virus phải tuân thủ là: Khi thi hành một file khả thi bị lây nhiễm, quyền điều khiển phải nôm trong tay virus trước khi virus trả nó lại cho file bị nhiễm, và khi file nhận lại quyền điều khiển, tất cả mọi dữ liệu của file phải được bảo toàn.

Đối với F-virus, có một số kỹ thuật được nêu ra ở đây:

Kỹ thuật lây lan

Các F-virus chủ yếu sử dụng hai kỹ thuật:

- Thêm vào đầu file.
- Thêm vào cuối file.

Kỹ thuật đảm bảo tính tồn tại duy nhất.

Cũng giống như B-virus, một yêu cầu nghiêm ngặt đặt ra đối với F-virus là tính tồn tại duy nhất của mình trong bộ nhớ cũng như trên file. Trong vùng nhớ, thông thường các F-virus sử dụng hai kỹ thuật chính:

Thứ nhất là tạo thêm chức năng cho DOS, bông cách sử dụng một chức năng con nào đó trong đó đặt chức năng lớn hơn chức năng cao nhất mà DOS có. Để kiểm tra chỉ cần gọi chức năng này, giá trị trả lại trong thanh ghi quyết định sự tồn tại của virus trong bộ nhớ hay chưa.

Cách thứ hai là so sánh mộtđoạn mã trong vùng nhớ ấn định với đoạn mã của virus, nếu có sự chênh lệch thì có nghĩa là virus chưa có mặt trong vùng nhớ và sẽ tiến hành lây lan. Trên file, có thể có các cách kiểm tra như kiểm tra bông test logic nào đó với các thông tin của Entry trong thư mục của file này. Cách này không đảm bảo tính chính xác tuyệt đối song nếu thiết kế tốt thì khả năng trùng lặp cũng hạn chế, hầu như không có, ngoài ra một ưu điểm là tốc thực hiện kiểm tra rất nhanh. Ngoài ra có thể kiểm tra bông cách dò một đoạn mã đặc trưng (key

value) của virus tại vị trí ấn định nào đó trên file, ví dụ trên các byte cuối cùng của file.

Kỹ thuật thường trú

Đây là một kỹ thuật khó khăn, lý do là DOS chỉ cung cấp chức năng thường trú cho chương trình, nghĩa là chỉ cho phép cả chương trình thường trú. Vì vậy nếu sử dụng chức năng của DOS, chương trình virus muốn thường trú thì cả file đối tượng cũng phải thường trú, mà điều này thì không thể được nếu kích thước của file đối tượng quá lớn. Chính vì lý do trên, hầu hết các chương trình virus muốn thường trú đều phải thao tác qua mặt DOS trên chuỗi MCB bông phương pháp "thủ công". Căn cứ vào việc thường trú được thực hiện trước hay sau khi chương trình đối tượng thi hành, có thể chia kỹ thuật thường trú thành hai nhóm:

Thường trú trước khi trả quyền điều khiển.

Như đã nói ở trên, DOS không cung cấp một chức năng nào cho kiểu thường trú này, cho nên chương trình virus phải tự thu xếp. Các cách sau đây đã được virus dùng đến:

- Thao tác trên MCB để tách một khối vùng nhớ ra khỏi quyền điều khiển của DOS, rồi dùng vùng này để chứa chương trình virus.
- Tự định vị vị trí trong bộ nhớ để tải phần thường trú của virus vào, thường thì các virus chọn ở vùng nhớ cao, phía dưới phần tạm trú của file command.com để tránh bị ghi đè khi hệ thống tải lại command.com. Vì không cấp phát bọ nhớ cho phần chương trình virus đang thường trú, cho nên command.com hoàn toàn có quyền cấp phát vùng nhớ đó cho các chương trình khác, nghĩa là chương trình thương trú của virus phải chấp nhận sự mất mát do may rủi.
- Thường trú bông chức năng thường trú 31h: Đây là một kỹ thuật phức tạp, tiến trình cần thực hiện được mô tả như sau: Khi chương trình virus được trao quyền, nó sẽ tạo ra một MCB được khai báo là phần tử trung gian trong chuỗi MCB để chứa chương trình virus, sau đó lại tạo tiếp một MCB mới để cho chương trình bị nhiễm bông cách dời chương trình xuống vùng mới này. Để thay đổi PSP mà DOS đang lưu giữ thành PSP mà chương trình virus tạo ra cho chương trình đối tượng, phải sử dụng chức năng 50h của ngắt 21h.

Thường trú sau khi đoạt lại quyền điều khiển.

Chương trình virus lấy tên chương trình đang thi hành trong môi trường của DOS, rồi nó thi hành ngay chính bản thân mình. Sau khi thi hành xong, quyền điều khiển lại được trả về cho virus, và khi đó nó mới tiến hành thường trú một cách bình thường bông chức năng 31h của ngắt 21h.

Kỹ thuật ngụy trang và gây nhiễu

Một nhược điểm không tránh khỏi là file đối tượng bị lây nhiễm virus sẽ bị tăng kích thước. Một số virus ngụy trang bông cách khi sử dụng chức năng DIR của DOS, virus chi phối chức năng tìm kiếm file (chức năng 11h và 12h của ngắt 21h) để giảm kích thước của file bị lây nhiễm xuống, vì thế khi virus đang chi phối máy tính, nếu sử dụng lệnh DIR của DOS, hoặc các lệnh sử dụng chức năng tìm kiếm file ở trên để có thông tin về entry trong bảng thư mục, thì thấy kích thước file bị lây nhiễm vẫn bông kích thước của file ban đầu, điều này đánh lừa người sử dụng về sự trong sạch của file này.

Một số virus còn gây nhiễu bông cách mã hoá phần lớn chương trình virus, chỉ khi nào vào vùng nhớ, chương trình mới được giải mã ngược lại. Một số virus anti-debug bông cách chiếm ngắt 1 và ngắt 3. Bởi vì các chương trình debug thực chất phải dùng ngắt 1 và ngắt 3 để thi hành từng bước một, cho nên khi virus chiếm các ngắt này rồi mà người lập trình dùng debug để theo dõi virus thì kết quả không lường trước được.

Kỹ thuật phá hoại

Thông thường, các F-virus cũng sử dụng cách thức và kỹ thuật phá hoại giống như B-virus. Có thể phá hoại một cách định thời, liên tục hoặc ngẫu nhiên. Đối tượng phá hoại có thể là màn hình, loa, đĩa,...

Worm

Sâu máy tính (worm) là một chương trình máy tính có khả năng tự nhân bản giống như virus máy tính. Trong khi virus máy tính bám vào và trở thành một phần của mã máy tính để có thể thi hành thì sâu máy tính là một chương trình độc lập không nhất thiết phải là một phần của một chương trình máy tính khác để có thể lây nhiễm. Sâu máy tính thường được thiết kế để khai thác khả năng truyền thông tin có trên những máy tính có các đặc điểm chung - cùng hệ điều hành hoặc cùng chạy một phần mềm mạng - và được nối mạng với nhau.

Hầu hết worm được tạo chỉ có thể tái tạo và lây lan thông qua mạng, tiêu thụ tài nguyên máy tính, tuy nhiên 1 vài worm mang 1 payload tàn phá hệ thống

Kẻ tấn công sử dụng worm payload để cài đặt vào cửa sau của máy tính bị nhiễm, sẽ bật chúng trở thành thây ma và tạo botnet; những botnet này có thể sử dụng để mang tấn công đến không gian mạng

Giới thiệu một số worm cơ bản

W32/Netsky

Đặc điểm

W32/Netsky là một sâu lây lan sử dụng email và và chia sẻ qua mạng Windows Nó tìm tất cả ánh xạ ổ đĩa của file có phần mở rộng để tìm thấy địa chỉ email Worm cũng sẽ cố gắng sao chép chính nó vào trong thư mục root của ổ đĩa C

Thực thi

Khi một file được giải nén và mở thì virus có thể hiện thị dòng tin nhắn "The file could not be opend " W32/Netsky-A sao chép chính nó vào trong thư mục Windows như services.exe. Để tự động chạy mỗi khi Windows khởi động W32/Netsky-A tạo một registry

W32/Bagle.GE

Đặc điểm

Worm W32/Bagle.GE được nhúng trong file đính kèm email, và lây lan sử dụng mạng email đã bị lây nhiễm. Nó tự ẩn mình và các thành phần Bagle khác sử dụng kĩ thuật rookit .

Thực thi

- Nó cố gắng ngăn chặn nhiều Anti-Virus và các phần mềm liên quan đến an ninh khác.
- Bagle.GE tải một ổ đĩa chế độ kernel(m_hook.sys) được nó sử dụng để tự ẩn mình và Bagle các phần mềm độc hại khác, Email-Worm/Bagle.GF
- Xử lý file và thư mục, khóa registry và các value

Worm Conficker

Đặc điểm

- Worm Conficker là một worm máy tính có thể lây nhiễm và tự nó lây lan sang các máy tính khác thông qua mạng một cách tự động, mà không tương tác con người
- File autorun.inf được đặt trong thư mục thùng rác
- Người dùng bị khóa bên ngoài của thư mục
- Truy cập an toàn-liên quan trang web bị chặn
- Lưu lượng truy cập được gửi qua port 445 trên máy chủ non-Directory Service(DS)
- Truy cập với quyền admin vào ổ đĩa chia sẽ bị từ chối.

Thực thi

- Worm Conficker có thể vô hiệu hóa các dịch vụ quan trọng trong máy tính của bạn
- Trong hộp thoại autoplay, lựa chọn Open folder to view files – Publisher not specified được thêm vào bởi worm
- Lựa chọn đánh dấu, Open folder to view files – using Windows explore là lựa chọn windows có thể cung cấp và lựa chọn cho bạn sử dụng
- Nếu bạn chọn lựa chọn đầu tiên, sâu sẽ thực thi và bắt đầu tự lây lan qua các máy khác

Chương 10: Denial of Service

Hiểu về DoS

Tấn công từ chối dịch vụ - DoS

Tấn công từ chối dịch vụ là kiểu tấn công vào máy tính hoặc một mạng để ngăn chặn sự truy cập hợp pháp.

Trên kiểu tấn công DoS, attackers làm tràn ngập hệ thống của victim với luồng yêu cầu dịch vụ không hợp pháp làm quá tải nguồn (Server), ngăn chặn server thực hiện nhiệm vụ hợp lệ.

Tấn công từ chối dịch vụ phân tán

Tấn công từ chối dịch vụ phân tán hay DDoS bao gồm các thỏa hiệp của hệ thống để tấn công mục tiêu duy nhất, là nguyên nhân người sử dụng bị từ chối dịch vụ của hệ thống.

Để khởi động một cuộc tấn công DDoS, một kẻ tấn công sử dụng botnet và tấn công một hệ thống duy nhất.

Dấu hiệu khi bị tấn công DoS

- Thông thường thì hiệu suất mạng sẽ rất chậm.
- Không thể sử dụng website.
- Không truy cập được bất kỳ website nào.
- Tăng lượng thư rác nhanh chóng.

Các mục đích của tấn công DoS

- Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (flood), khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường.
- Cố gắng làm ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy cập vào dịch vụ.
- Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó.
- Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy cập vào.

- Khi tấn công DoS xảy ra người dùng có cảm giác khi truy cập vào dịch vụ đó như bị:
    - Tắt mạng .
    - Tổ chức không hoạt động.
    - Tài chính bị mất.

Các kỹ thuật tấn công DoS

Tấn công băng thông

Tấn công băng thông nhằm làm tràn ngập mạng mục tiêu với những traffic không cần thiết, với mục đích làm giảm tối thiểu khả năng của các traffic hợp lệ đến được hệ thống cung cấp dịch vụ của mục tiêu.

Có hai loại BandWith Depletion Attack:

- Flood attack: Điều khiển các Agent gởi một lượng lớn traffic đến hệ thống dịch vụ của mục tiêu, làm dịch vụ này bị hết khả năng về băng thông.
- Amplification attack: Điều khiển các agent hay client tự gửi message đến một địa chỉ IP broadcast, làm cho tất cả các máy trong subnet này gửi message đến hệ thống dịch vụ của mục tiêu. Phương pháp này làm gia tăng traffic không cần thiết, làm suy giảm băng thông của mục tiêu.

Tấn công tràn ngập yêu cầu dịch vụ

Một kẻ tấn công hoặc nhóm zombie cố gắng làm cạn kiệt tài nguyên máy chủ bằng cách thiết lập và phá hủy các kết nối TCP. Nó bắt đầu gửi yêu cầu trên tất cả kết nối và nguồn gốc từ server kết nối tốc độ cao.

Tấn công tràn ngập SYN

Attacker gởi một SYN packet đến nạn nhân với địa chỉ bên gởi là giả mạo, kết quả là nạn nhân gởi SYN/ACK REPLY đến một địa chỉ khác và sẽ không bao giờ nhận được ACK packet cuối cùng, cho đến hết thời gian timeout nạn nhân mới nhận ra được điều này và giải phóng các tài nguyên hệ thống. Tuy nhiên, nếu lượng SYN packet giả mạo đến với số lượng nhiều và dồn dập, hệ thống của nạn nhân có thể bị hết tài nguyên.

Tấn công tràn ngập ICMP

Kiểu tấn công ICMP là thủ phạm gửi số lượng lớn của gói tin giả mạo địa chỉ nguồn tới server đích để phá hủy nó và gây ra ngừng đáp ứng yêu cầu TCP/IP.

Sau khi đến ngưỡng ICMP đạt đến, các router từ chối yêu cầu phản hồi ICMP từ tất cả địa chỉ trên cùng vùng an toàn cho phần còn lại.

Tấn công điểm nối điểm

Dùng điểm nối điểm để tấn công, kẻ tấn công chỉ đạo clients của mô hình điểm nối điểm chia sẽ file trung tâm gây ngắt kết nối từ mạng của họ và kết nối tới website giả mạo của victim.

Kẻ tấn công khai thác lỗ hổng tìm thấy trên mạng dùng giao thức DC++(kết nối trực tiếp), cho phép hoán đổi file giữa các tin nhắn clients ngay lập tức.

Dùng phương pháp này, kẻ tấn công chạy tấn công DoS rất lớn và làm hại website.

Tấn công cố định DoS

Tấn công cố định DoS hay PDoS còn được gọi như phlashing, là một cuộc tấn công gây tổn thương một hệ thống nhiều đến nổi nó đòi hỏi phải thay thế hoặc cài đặt lại phần cứng, Không giống như các cuộc tấn công DDoS, PDoS một cuộc tấn công khai thác lỗ hổng bảo mật cho phép quản trị từ xa trên các giao diện quản lý phần cứng của nạn nhân, chẳng hạn như router, máy in, hoặc phần cứng mạng khác.

Tấn công thực hiện dùng phương pháp như "xây dựng hệ thống". Dùng phương pháp này, kẻ tấn công gửi cập nhập phần cứng lừa đảo tới victim.

Tấn công tràn ngập ở cấp độ dịch vụ

Tấn công làm tràn ở cấp độ ứng dụng là kết quả mất dịch vụ của mạng đặc biệt như là: email, tài nguyên mạng, tạm thời ngừng ứng dụng và dịch vụ,... Dùng kiểu tấn công này, kẻ tấn công phá hủy mã nguồn chương trình và file làm ảnh hưởng tới hệ thống máy tính.

Tấn công làm tràn ngập ở cấp độ ứng dụng, kẻ tấn công cố gắng:

- Tràn ngập ứng dụng web tới lưu lượng người sử dụng hợp lệ.
- Ngắt dịch vụ cụ thể của hệ thống hoặc con người.

- Làm tắt nghẽn cơ sở dữ liệu của ứng dụng kết nối bằng truy vấn thủ công nguy hiểm SQL.

DDoS

Khái niệm botnet

Botnet là từ chỉ một tập hợp các rô bôt phần mềm hoặc các con bot hoạt động một cách tự chủ. Từ này còn được dùng để chỉ một mạng các máy tính sử dụng phần mềm tính toán phân tán.

Hoạt động

Tuy từ "botnet" có thể dùng để chỉ một nhóm bot bất kỳ, chẳng hạn IRC bot, từ này thường được dùng để chỉ một tập hợp các máy tính đã bị tấn công và thỏa hiệp và đang chạy các chương trình độc hại, thường là sâu máy tính, trojan horse hay backdoor, dưới cùng một hạ tầng cơ sở lệnh và điều khiển. Một chương trình chỉ huy botnet có thể điều khiển cả nhóm bot từ xa, thường là qua một phương tiện chẳng hạn như IRC, và thường là nhằm các mục đích bất chính. Mỗi con bot thường chạy ẩn và tuân theo chuẩn RFC 1459 (IRC). Thông thường, kẻ tạo botnet trước đó đã thỏa hiệp một loạt hệ thống bằng nhiều công cụ đa dạng (tràn bộ nhớ đệm, ...). Các bot mới hơn có thể tự động quét môi trường của chúng và tự lan truyền bản thân bằng cách sử dụng các lỗ hổng an ninh và mật khẩu yếu. Nếu một con bot có thể quét và tự lan truyền qua càng nhiều lỗ hổng an ninh, thì nó càng trở nên giá trị đối với một cộng đồng điều khiển botnet.

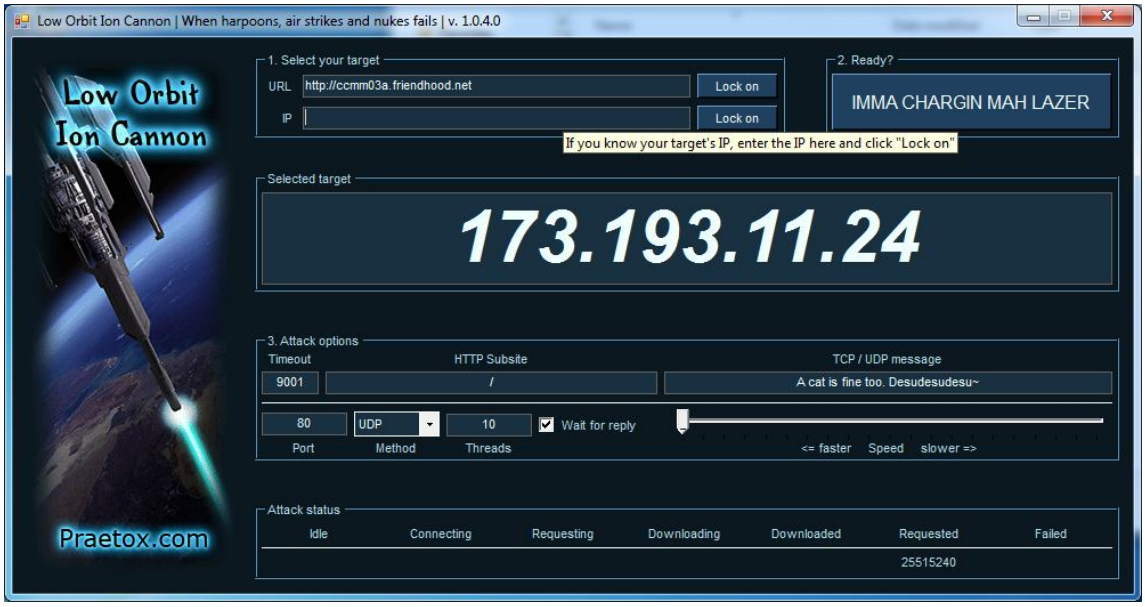
Hoạt động botnet

Các botnet đã trở nên một phần quan trọng của Internet, tuy chúng ngày càng ẩn kĩ. Do đa số các mạng IRC truyền thống thực hiện các biện pháp cấm truy nhập đối với các botnet đã từng ngụ tại đó, những người điều khiển botnet phải tự tìm các server cho mình. Một botnet thường bao gồm nhiều kết nối, chẳng hạn quay số, ADSL và cáp, và nhiều loại mạng máy tính, chẳng hạn mạng giáo dục, công ty, chính phủ và thậm chí quân sự. Đôi khi, một người điều khiển giấu một cài đặt IRC server trên một site công ty hoặc giáo dục, nơi các đường kết nối tốc độ cao có thể hỗ trợ một số lớn các bot khác. Chỉ đến gần đây, phương pháp sử dụng bot để chỉ huy các bot khác mới phát triển mạnh, do đa số hacker không chuyên không đủ kiến thức để sử dụng phương pháp này.

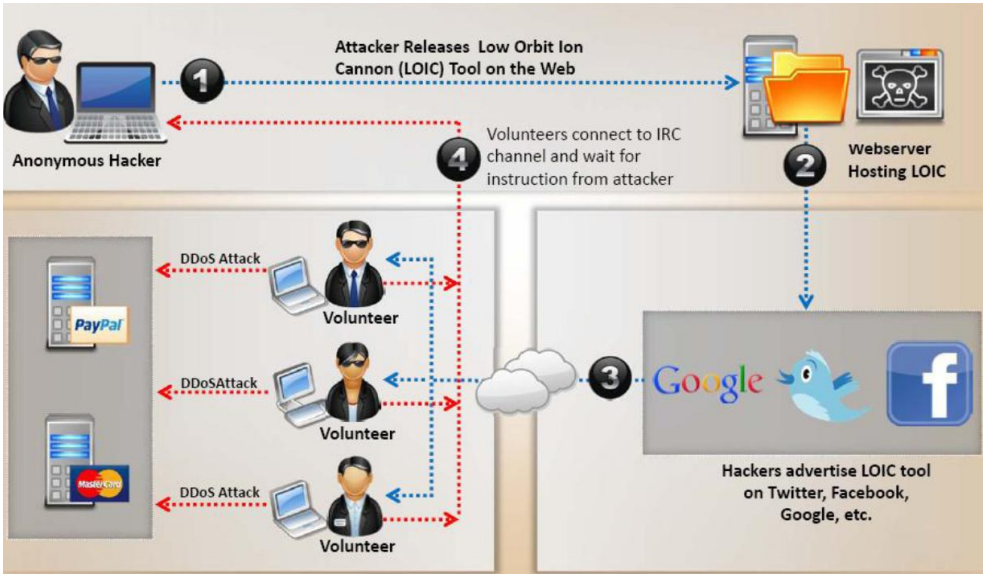
Một số công cụ tấn công

LOIC

LOIC là ứng dụng tấn công từ chối dịch vụ, được viết bằng C#. Loic thực hiện tấn công từ chối dịch vụ tấn công (hoặc khi được sử dụng bởi nhiều cá nhân, một cuộc tấn công DDoS) trên một trang web mục tiêu làm lũ lụt các máy chủ với các gói tin TCP hoặc UDP với ý định làm gián đoạn dịch vụ của một máy chủ cụ thể. Công cụ LOIC là một botnet tình nguyện kết nối đến một máy chủ từ xa mà chỉ đạo các cuộc tấn công. Hiện nay, có 40.000 người kết nối với botnet.



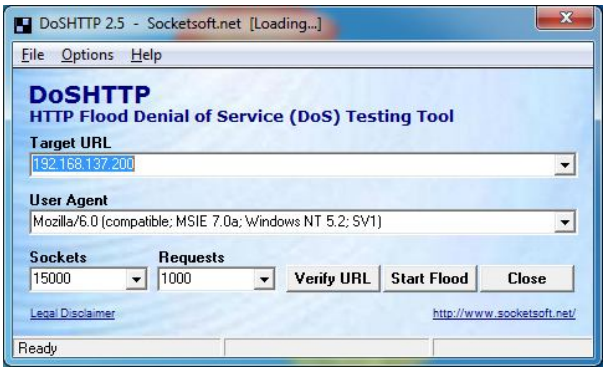
Công cụ LOIC



Dùng LOIC tấn công DDoS

DoSHTTP

DoSHTTP là một phần mềm sử dụng dễ dàng, mạnh mẽ để tấn công tràn ngập HTTP nhằm mục đích kiểm thử trên Windows. DoSHTTP bao gồm xác nhận URL, chuyển hướng HTTP và giám sát hiệu suất. Công cụ DoSHTTP có thể giúp các chuyên gia CNTT thử nghiệm hiệu năng máy chủ web và đánh giá độ bảo mật.



Biện pháp đối phó chiến lược DoS/ DdoS

- Hấp thụ cuộc tấn công: Dùng khả năng phụ để hấp thụ tấn công, yêu cầu kế hoạch trước.
- Làm giảm dịch vụ: Nhận biết dịch vụ nguy hiểm và dừng dịch vụ không nguy hiểm.
- Tắt dịch vụ: Tắt tất cả dịch vụ cho tới khi cuộc tấn công giảm bớt.

Biện pháp đối phó tấn công DoS/ DDoS

Bảo vệ thứ cấp victims

- Cài đặt phần mềm anti-virus, anti-Trojan và cập nhập bản mới.
- Tăng nhận thức về vấn đề bảo mật và kỹ thuật ngăn chặn người sử dụng từ tất cả nguồn trên internet.
- Tắt dịch vụ không cần thiết, gỡ bỏ ứng dụng không sử dụng, và quét tất cả files nhận từ nguồn bên ngoài.
- Cấu hình và thường xuyên cập nhập xây dựng cơ cấu phòng thủ trên lõi phần cứng và phần mềm hệ thống.

Phát hiện và vô hiệu hóa handers

- **Phân tích lưu lượng mạng**: Nghiên cứu giao tiếp giao thức và mô hình giữa handlers và client hoặc handlers và agents để nhận biết node mạng có thể lây với các handler.
- **Vô hiệu hóa botnet handler**: Thông thường vài DDoS handler được triển khai gần bằng so với số lượng agent. Vô hiệu hóa một vài handler có thể làm cho nhiều agent không hữu dụng, để cản trở cuộc tấn công DDoS.
- **Giả mạo địa chỉ nguồn**: Có một xác suất lớn giả mạo địa chỉ nguồn gói tin tấn công DDoS sẽ không hiện giá trị địa chỉ nguồn của mạng cụ thể.

Phát hiện tiềm năng tấn công

- **Bộ lọc xâm nhập**: Bảo vệ từ tấn công tràn ngập có nguồn gốc từ các tiền tố hợp lệ. Nó cho phép người khởi tạo truy tìm nguồn gốc thực sự.
- **Bộ lọc đi ra**: Quét header gói tin của gói tin IP ra một mạng. Bộ lọc đi ra không chứng thực hoặc lưu lượng nguy hiểm không được ra khỏi mạng bên ngoài.
- **Ngắt TCP**: Cấu hình ngắt TCP ngăn ngừa tấn công bằng cách ngắt và yêu cầu kết nối TCP hợp lệ.

Làm lệch hướng tấn công

- Hệ thống thiết lập với giới hạn bảo mật, cũng biết như là honeypot, hoạt động cám dỗ đối với kẻ tấn công.

- Phục vụ có nghĩa là giành thông tin từ kẻ tấn công bằng cách lưu trữ một bản ghi các hoạt động, học kiểu tấn công và công cụ phần mềm kẻ tấn công sử dụng.
- Dùng phòng thủ chiều sâu tiếp cận với IPSec tại điểm mạng khác nhau chuyển hướng đáng ngờ luồng DoS đến vài honeypot.

Honeypot là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng đánh lừa những kẻ sử dụng và xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn không cho chúng tiếp xúc với hệ thống thật.

Làm dịu cuộc tấn công

- Cân bằng tải:
  - Nhà cung cấp tăng băng thông trên kết nối quan trọng để ngăn ngừa và giảm xuống tấn công.
  - Nhân bản máy chủ có thể cung cấp thêm bảo vệ an toàn.
  - Cân bằng tải cho mỗi server trên cấu trúc nhiều server có thể cải tiến hiệu suất bình thường như là giảm ảnh hưởng của cuộc tấn công DoS.
- Hoạt động điều chỉnh:
  - Thiết lập cách thức router truy cập một server với điều chỉnh logic lưu lượng đi vào tới mức độ sẽ an toàn để server xử lý.
  - Bộ xử lý có thể ngăn ngừa tràn ngập thiệt hại tới server.
  - Bộ xử lý này có thể mở rộng để điều chỉnh luồng tấn công DDoS đối lập lưu lượng hợp pháp của người sử dụng cho kết quả tốt hơn.

Pháp lý

- Phân tích router, firewall, và IDS logs để nhận biết nguồn của lưu lượng DoS. Mặc dù kẻ tấn công thông thường giả mạo địa chỉ nguồn, dấu vết IP trả lại với trợ giúp ngay lập tức của ISP và thực thi pháp luật các cơ quan có thể cho phép bắt các thủ phạm.
- Phân tích mẫu lưu lượng: Dữ liệu có thể được phân tích-sau tấn công-để tìm kiếm đặc điểm riêng biệt trong lưu lượng tấn công.
- Mẫu lưu lượng tấn công DDoS có thể giúp người quản trị mạng phát triển kỹ thuật lọc để ngăn ngừa đi vào hoặc đi ra mạng

- Dùng những đặc điểm, dữ liệu có thể được dùng để cập nhập cân bằng tải và điều chỉnh biện pháp đối phó.

Kỹ thuật để phòng thủ chống lại botnet

- **Lọc:** Các gói tin cần phải được có nguồn gốc hợp lệ, cho phép địa chỉ trống, bao gồm tôpô và cấp phát không gian. Bất kỳ lưu lượng vào không sử dụng hoặc địa chỉ ip dành riêng không thật và nên lọc tại ISP trước khi vào đường link internet.
- **Lọc lỗ đen:** Lỗ đen là nơi trên một một mạng, nơi đó lưu lượng được chuyển tiếp hoặc hủy bỏ. Kỹ thuật lọc này dùng giao thức cập nhập định tuyến để điều khiển bảng định tuyến tại biên một mạng để hủy lưu lượng không thích nghi trước nó xâm nhập vào mạng của nhà cung cấp dịch vụ.
- **Lọc nguồn ip uy tín trên Cisco IPS:** IPS cisco nhận đe dọa cập nhập từ mạng Cisco SensorBase (trung tâm kiểm soát tấn công) chứa thông tin chi tiết nhân biệt mối đe dọa trên internet, bao gồm tuần tự kẻ tấn công, botnet harvester, malware bùng phát và dark net.
- **Cung cấp dịch vụ phòng chống DDoS từ ISP:** Bật bảo vệ IP nguồn trên switch ngăn ngừa một host gửi gói tin giả mạo trở thành bot.

Biện pháp đối phó DoS/ DdoS

Một số biện pháp như:

- Hiệu quả của cơ chế mã hóa cần đề xuất cho mỗi công nghệ băng thông rộng.
- Cải tiến giao thức định tuyến được kỳ vọng, đặc biệt là cho nhiều hop WMN.
- Tắt những dịch vụ không sử dụng và không bảo mật.
- Khóa tất cả gói tin có nguồn đi vào từ cổng dịch vụ để khóa lưu lượng ánh xạ từ server.
- Cập nhập kernel tới phiên bản mới nhất.
- Ngăn ngừa truyền địa chỉ gói tin lậu ở mức độ ISP.
- Thực hiện nhận biệt vô tuyến ở lớp vật lý để xử lý gây nhiễu và xáo trộn cuộc tấn công.

- Cấu hình firewall để từ chối dòng truy cập giao thức điều khiển thông điệp internet (ICMP).
- Ngăn ngừa dùng chức năng không cấp thiết như get, strcpy,...
- Đảm bảo an toàn cho người quản trị từ xa và kiểm tra kết nối.
- Ngăn chặn địa chị trả lại không bị ghi đè.
- Dữ liệu được xử lý bởi kẻ tấn công nên dừng lại trước khi chạy.
- Thực hiện triệt để giá trị nhập vào.
- Các card mạng là gateway của gói tin vì vậy nên dùng card mạng tốt hơn để xử lý số lượng lớn gói tin.

Chương 11: Social Engineering

Social Engeering là gì

Social engineering sử dụng sự ảnh hưởng và sự thuyết phục để đánh lừa người dùng nhằm khai tác các thông tin có lợi cho các cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó. Social engineer (người thực hiện công việc tấn công bằng phương pháp socal engineering) thường sử dụng điện thoại hoặc internet để dụ dỗ người dùng tiết lộ thông tin nhạy cảm hoặc để có được họ có thể làm một chuyện gì đó để chống lại các chính sách an ninh của tổ chức. Bằng phuong pháp này, Social engineer tiến hành khai thác các thói quen tự nhiên của người dùng, hơn là tìm các lỗ hổng bảo mật của hệ thống. Điều này có nghĩa là người dùng với kiến thức bảo mật kém cõi sẽ là cơ hội cho kỹ thuật tấn công này hành động.

Nghệ thuật thao túng

Social Engineering bao gồm việc đạt được những thông tin mật hay truy cập trái phép, bằng cách xây dựng mối quan hệ với một số người. Kết quả của social engineer là lừa một người nào đó cung cấp thông tin có giá trị. Nó tác động lên phẩm chất vốn có của con người, chẳng hạn như mong muốn trở thành người có ích, tin tưởng mọi người và sợ những rắc rối.

Social engineering vận dụng những thủ thuật và kỹ thuật làm cho một người nào đó đồng ý làm theo những gì mà Social engineer muốn. Nó không phải là cách điều khiển suy nghĩ người khác, và nó không cho phép Social engineer làm cho người nào đó làm những việc vượt quá tư cách đạo đức thông thường. Và trên hết, nó không dễ thực hiện chút nào. Tuy nhiên, đó là một phương pháp mà hầu hết Attackers dùng để tấn công vào công ty. Có 2 loại rất thông dụng :

- **Social engineering** là việc lấy được thông tin cần thiết từ một người nào đó hơn là phá hủy hệ thống.
- **Psychological subversion**: mục đích của hacker hay attacker khi sử dụng PsychSub (một kỹ thuật thiên về tâm lý) thì phức tạp hơn và bao gồm sự chuẩn bị, phân tích tình huống, và suy nghĩ cẩn thận, chính xác những từ sử dụng và giọng điệu khi nói, và nó thường sử dụng trong quân đội.

Điểm yếu của mọi người

Mọi người thường mắc phải nhiều điểm yếu trong các vấn đề bảo mật. Để đề phòng thành công thì chúng ta phải dựa vào các chính sách tốt và huấn luyện nhân viên thực hiện tốt các chính sách đó. Social engineering là phương pháp khó phòng chống nhất vì nó không thể dùng phần cứng hay phần mềm để chống lại.

Một người nào đó khi truy cập vào bất cứ phần nào của hệ thống thì các thiết bị vật lý và vấn đề cấp điện có thể là một trở ngại lớn. Bất cứ thông tin nào thu thập được đều có thể dùng phương pháp Social engineering để thu thập thêm thông tin. Có nghĩa là một người không nằm trong chính sách bảo mật cũng có thể phá hủy hệ thống bảo mật. Các chuyên gia bảo mật cho rằng cách bảo mật giấu đi thông tin là rất yếu. Trong trường hợp của Social engineering, hoàn toàn không có sự bảo mật nào vì không thể che giấu việc ai đang sử dụng hệ thống và khả năng ảnh hưởng của họ tới hệ thống.

Có nhiều cách để hoàn thành mục tiêu đề ra. Cách đơn giản nhất là yêu cầu trực tiếp, đó là đặt câu hỏi trực tiếp. Mặc dù cách này rất khó thành công, nhưng đây là phương pháp dễ nhất, đơn giản nhất. Người đó biết chính xác họ cần gì.

Cách thứ hai, tạo ra một tình huống mà nạn nhân có liên quan đến. Với các nhân tố khác nhau cần được yêu cầu xem xét, làm thế nào để nạn nhân dễ dàng dính bẩy nhất, bởi vì attacker có thể tạo ra những lý do thuyết phục hơn những người bình thường. Attacker càng nỗ lực thì khả năng thành công càng cao, thông tin thu được càng nhiều. Không có nghĩa là các tình huống này không dựa trên thực tế. Càng giống sự thật thì khả năng thành công càng cao.

Một trong những công cụ quan trọng được sử dụng trong Social engineering là một trí nhớ tốt để thu thập các sự kiện. Đó là điều mà các hacker và sysadmin nổi trội hơn, đặc biệt khi nói đến những vấn đề liên quan đến lĩnh vực của họ.

Phân loại kỹ thuật Social Egnieering

Social engineering có thể được chia thành hai loại phổ biến:

Human-based: Kỹ thuật Social engineering liên quan đến sự tương tác giữa con người với con người để thu được thông tin mong muốn. Ví dụ như chúng ta phải gọi điện thoại đến phòng Help Desk để truy tìm mật khẩu.

Computer-based: Kỹ thuật này liên quan đến việc sử dụng các phần mềm để cố gắng thu thập thông tin cần thiết. Ví dụ bạn gửi email và yêu cầu người dùng nhập lại mật khẩu đăng nhập vào website. Kỹ thuật này còn được gọi là Phishing (lừa đảo).

Các đe dọa từ tính chất con người

Impersonation: Mạo danh là nhân viên hoặc người dùng hợp lệ. Trong kỹ thuật này, kẽ tấn công sẽ giả dạng thành nhân viên công ty hoặc người dùng hợp lệ của hệ thống. Hacker mạo danh mình là người gác công, nhân viên, đối tác, để độp nhập công ty. Một khi đã vào được bên trong, chúng tiến hành thu thập các thông tin từ thùng rác, máy tính để bàn, hoặc các hệ thống máy tính, hoặc là hỏi thăm những người đồng nghiệp.

Posing as Important User: Trong vai trò của một người sử dụng quan trọng như người quan lý cấp cao, trưởng phòng, hoặc những người cần trợ giúp ngay lập tức, hacker có thể dụ dỗ người dùng cung cấp cho chúng mật khẩu truy cập vào hệ thống.

Third-person Authorization: Lấy danh nghĩa được sự cho phép của một người nào đó để truy cập vào hệ thống. Ví dụ một tên hacker nói anh được sự ủy quyền của giám đốc dùng tài khoản của giám đốc để truy cập vào hệ thống.

Calling Technical Support: Gọi điện thoại đến phòng tư vấn kỹ thuật là một phương pháp cổ điển của kỹ thuật tấn công Social engineering. Help-desk và phòng hổ trợ kỹ thuật được lập ra để giúp cho người dùng, đó cũng là con mồi ngon cho hacker.

Shoulder Surfing là kỹ thuật thu thập thông tin bằng cách xem file ghi nhật ký hệ thống. Thông thường khi đăng nhập vào hệ thống, quá trình đăng nhập được ghi nhận lại, thông tin ghi lại có thể giúp ích nhiều cho hacker.

Dumpster Diving là kỹ thuật thu thập thông tin trong thùng rác. Nghe có vẽ "đê tiện" vì phải lôi thùng rác của người ta ra để tìm kiếm thông tin, nhưng vì đại cuộc phải chấp nhận hi sinh. Nói vui vậy, thu thập thông tin trong thùng rác của các công ty lớn, thông tin mà chúng ta cần thu có thể là password, username, filename hoặc những thông tin mật khác.

Phising: Thuật ngữ này áp dụng cho một email xuất hiện đến từ một công ty kinh doanh, ngân hàng hoặc thẻ tín dụng yêu cầu chứng thực thông tin và cảnh báo sẽ xảy ra hậu quả nghiêm trọng nếu việc này không được làm. Lá thư thường chứa một đường link đến một trang web giả mạo trông hợp pháp với logo của công ty và nội dung có chứa form để yêu cầu username, password, số thẻ tín dụng hoặc số pin.

Vishing: Thuật ngữ là sự kết hợp của "voice" và phishing. Đây cũng là một dạng phising, nhưng kẻ tấn công sẽ trực tiếp gọi điện cho nạn nhân thay vì gởi email. Người sử dụng sẽ nhận được một thông điệp tự động với nội dung cảnh báo vấn đề liên quan đến tài khoản ngân hàng. Thông điệp này hướng dẫn họ gọi đến một số điện thoại để khắc phục vấn đề. Sau khi gọi, số điện thoại này sẽ kết nối người được gọi tới một hệ thống hỗ trợ giả, yêu cầu họ phải nhập mã thẻ tín dụng. Và Voip tiếp tay đắc lực thêm cho dạng tấn công mới này vì giá rẻ và khó giám sát một cuộc gọi bằng Voip.

Pop-up Windows: Một cửa sổ sẽ xuất hiện trên màn hình nói với user là anh ta đã mất kết nối và cần phải nhập lại username và password. Một chương trình đã được cài đặt trước đó bởi kẻ xâm nhập sau đó sẽ email thông tin đến một website ở xa.

Mail attachments: Có 2 hình thức thông thường có thể được sử dụng. Đầu tiên là mã độc hại. Mã này sẽ luôn luôn ẩn trong một file đính kèm trong email. Với mục đích là một user không nghi ngờ sẽ click hay mở file đó. Thứ hai cũng có hiệu quả tương tự, bao gồm gởi một file đánh lừa hỏi user để xóa file hợp pháp. Chúng được lập kế hoạch để làm tắc nghẽn hệ thống mail bằng cách báo cáo một sự đe dọa không tồn tại và yêu cầu người nhận chuyển tiếp một bản sao đến tất cả bạn và đồng nghiệp của họ. Điều này có thể tạo ra một hiệu ứng gọi là hiệu ứng quả cầu tuyết.

Websites: Một mưu mẹo để làm cho user không chú ý để lộ ra dữ liệu nhạy cảm, chẳng hạn như password họ sử dụng tại nơi làm việc. Ví dụ, một website có thể tạo ra một cuộc thi hư cấu, đòi hỏi user điền vào địa chỉ email và password. Password điền vào có thể tương tự với password được sử dụng cá nhân tại nơi làm việc. Nhiều nhân viên sẽ điền vào password giống với password họ sử dụng tại nơi làm việc, vì thế social engineer có username hợp lệ và password để truy xuất vào hệ thống mạng tổ chức.

Interesting Software: Trong trường hợp này nạn nhân được thuyết phục tải về và cài đặt các chương trình hay ứng dụng hữu ích như cải thiện hiệu suất của CPU, RAM, hoặc các tiện ích hệ thống hoặc như một crack để sử dụng các phần mềm có bản quyền. Và một Spyware hay Malware (chẳng hạn như Keylogger) sẽ được cài đặt thông qua một chương trình độc hại ngụy trang dưới một chương trình hợp pháp.

Identity Theft

Một hacker có thể giả danh một nhân viên hoặc ăn cấp danh tính của một nhân viên để thâm nhập vào hệ thống. Thông tin được thu thập thông qua kỹ thuật Dumpster Diving hoặc Shoulder Surfing kết hợp với việc tạo ID giả (fake ID) có thể giúp các hacker xâm nhập vào tổ chức. Việc tạo tài khoản xâm nhập vào hệ thống mà không bị phản đối gì hết như thế được ví von là ăn trộm hợp pháp (Identity Theft).

Biện pháp đối phó Social Engineering

Để xác định được phương pháp đối phó với Social Engineering là điều rất quan trọng trong các kỹ thuật phòng thủ và tấn công. Nó có liên quan đến vấn đề về xã hội nên việc phòng chống nó có chút rắc rối về cách tư cách của con người. Có một số cách để làm điều này.

Chính sách (policy) an ninh trong công ty quyết định vấn đề an toàn của hệ thống. Bạn cần đặt ra những quy định, giới hạn quyền truy cập cho các nhân viên trong công ty.

Huấn luyện tốt cho nhân viên về an ninh là điều rất cần thiết. Khi nhân viên của bạn hiểu ra các vấn đề an ninh, họ sẽ tự trách các rủi ro trước khi có sự can thiệt của phòng an ninh.

Vấn đề về con người cũng không kém quan trọng. Vì kỹ thuật tấn công này chủ yếu liên quan đến tư tưởng con người. Sự lơ là của nhân viên, sự mất lòng tin của nhân viên cũng là nguy cơ mất an toàn cho hệ thống.

Xây dựng một framework quản lý an ninh: Phải xác định tập hợp các mục đích của an ninh social engineering và đội ngũ nhân viên những người chịu trách nhiệm cho việc phân phối những mục đích này.

Đánh giá rủi ro: Các mối đe dọa không thể hiện cùng một mức độ rủi ro cho các công ty khác nhau. Ta phải xem xét lại mỗi một mối đe dọa social engineering và hợp lý hóa mối nguy hiểm trong tổ chức.

Social engineering trong chính sách an ninh: Phát triển một văn bản thiết lập các chính sách và thủ tục quy định nhân viên xử trí tình huống mà có thể là tấn công social engineering. Bước này giả định là chính sách bảo mật đã có, bên ngoài những mối đe dọa của social engineering. Nếu hiện tại không có chính sách bảo mật, thì cần phải phát triển chúng.

Chapter 12: Session Hijacking

Tìm hiểu về kỹ thuật tấn công Session Hijacking

Thuật ngữ chiếm quyền điều khiển session (session hijacking) chứa đựng một loạt các tấn công khác nhau. Nhìn chung, các tấn công có liên quan đến sự khai thác session giữa các thiết bị đều được coi là chiếm quyền điều khiển session. Khi đề cập đến một session, chúng ta sẽ nói về kết nối giữa các thiết bị mà trong đó có trạng thái đàm thoại được thiết lập khi kết nối chính thức được tạo, kết nối này được duy trì và phải sử dụng một quá trình nào đó để ngắt nó.

Session Hijacking là quá trình chiếm lấy một session đang hoạt động, nhằm mục đích vượt qua quá trình chứng thực truy cập bất hợp lệ vào thông tin hoặc dịch vụ của một hệ thống máy tính.

Khi một user thực hiện kết nối tới server qua quá trình xác thực, bằng cách cung cấp ID người dùng và mật khẩu của mình. Sau khi người dùng xác thực, họ có quyền truy cập đến máy chủ và hoạt động bình thường.

Trong quá trình hoạt động, người dùng không cần phải chứng thực lại. Kẻ tấn công lợi dụng điều này để cướp session đang hoạt động của người dùng và làm cho người dùng không kết nối được với hệ thống. Sau đó kẻ tấn công mạo danh người dùng bằng session vừa cướp được, truy cập đến máy chủ mà không cần phải đăng nhập vào hệ thống.

Khi cướp được session của người dùng, kẻ tấn công có thể vượt qua quá trình chứng thực dùng, có thể ghi lại phiên làm việc và xem lại mọi thứ đã diễn ra. Đối với cơ quan pháp lý, có thể dung làm bằng chứng để truy tố, đối với kẻ tấn công, có thể dùng thu thập thông tin như ID người dùng và mật khẩu. Điều này gây nhiều nguy hại đến người dùng.

Lý do Session Hijacking thành công

- ✓ Các ứng dụng không khóa các tài khoản cho các Session ID không hợp lệ.
- ✓ Session ID có hệ thuật toán đơn giản khiến việc dò tìm dễ dàng.
- ✓ Phiên hoạt động trên ứng dụng thì không giới hạn thời gian kết thúc.
- ✓ Cách truyền dữ liệu qua lại bằng văn bản tường minh không được mã hóa.
- ✓ Các Session ID nhỏ.

- ✓ Xử lí không an toàn.

Brute Forcing

Kẻ tấn công cố thử các ID khác nhau cho đến khi hắn thành công.

Các Session ID có thể bị lấy cắp bằng cách dùng những kỹ thuật khác nhau như:

1. Sử dụng giao thức HTTP giới thiệu tiêu đề.
2. Kiểm tra lưu lượng mạng.
3. Sử dụng các cuộc tấn công Cross-Site Scripting.
4. Gửi Trojans trong các máy khách.

Stealing

Kẻ tấn công dùng các kỹ thuật khác nhau để lấy cắp các Session ID.

Calculating

Kẻ tấn công sẽ cố gắng tính toán để có một Session ID đúng chỉ đơn giản bằng cách tìm kiếm một session ID đang tồn tại rồi sau đó tính ra chuỗi số.

So sánh giữa Spoofing và Hijacking

Spoofing và Hijacking thì tương tự nhau, nhưng có một vài điểm phân biệt giữa chúng.

Tấn công Spoofing khác hijacking ở chỗ kẻ tấn công không thực hiện được tấn công khi người dùng không hoạt động. Kẻ tấn công giả dạng người dùng để truy cập.

Trong khi thực hiện, người bị tấn công có thể là ở nhà hoặc ở bất kỳ nơi nào đó, người bị tấn công không có vai trò gì trong cuộc tấn công đó.

Đối với Hijacking, kẻ tấn công chiếm session sau khi người dùng đã chứng thực với hệ thống máy tính. Bằng cách này, kẻ tấn công có thể truy cập vào hệ thống một cách hợp lệ, sử dụng phiên làm việc của người dùng hợp lệ để giao tiếp với server.

Điểm khác biệt chính giữa Spoofing và Hijacking là: Spoofing chỉ liên quan đến kẻ tấn công và Server. Đối với Session Hijacking, kẻ tấn công phải đợi nạn nhân kết nối với server, chứng thực với server rồi mới tấn công để lấy session của nạn nhân. Lúc này, kẻ tấn công giả dạng nạn nhân để giao tiếp với server. Hình minh họa, ví dụ về tấn công Session Hijacking.

Tấn công Active và Passive

- **Active**

Trong 1 tấn công active, kẻ tấn công tìm phiên đang hoạt động và chiếm nó.

- **Passive**

Với tấn công passive, kẻ tấn công chiếm quyền điều khiển 1 phiên, nhưng ngừng lại, xem và ghi lại tất cả các lưu lượng truy cập được gửi ra.

Session Hijacking mức ứng dụng

Khi cố thử chiếm một session tại lớp ứng dụng, hacker có thể chọn một trong số các phương pháp tấn công hữu hiệu như dưới đây.

Thăm dò phiên

Kẻ tấn công dùng thăm dò để chiếm 1 mã thông báo hợp lệ gọi là "Session ID".

Kẻ tấn công lúc này dùng mã thông báo phiên hợp lệ để truy cập trái phép vào máy chủ web.

Dự đoán Session Token

Nhiều trang web có thể dễ dàng dự đoán được cơ chế thực hiện chứng thực dựa vào các session hợp lệ đã có.

Tấn công Man-in-the-Middle

Kiểu tấn công man-in-the-middle là dùng để xâm nhập vào một kết nối hiện tại giữa các hệ thống và chặn các tin nhắn được trao đổi.

Kiểu tấn công Man-in-the-Browser

Tấn công Man-in-the-browser dùng Trojan, Cross-site scripting và JavaScript để chặn các cuộc gọi của trình duyệt và các cơ chế bảo mật hoặc thư viện.

Cross-site scripting

Cross-Site Scripting (XSS) là một trong những kĩ thuật tấn công phổ biến nhất hiên nay, đồng thời nó cũng là một trong những vấn đề bảo mật quan trọng đối với các nhà phát triển web và cả những người sử dụng web. Bất kì một website nào cho phép người sử dụng đăng thông tin mà không có sự kiểm tra chặt chẽ các đoạn mã nguy hiểm thì đều có thể tiềm ẩn các lỗi XSS.

Một số khái niếm quan trọng

Blind Hijacking: Là kiểu tấn công chiếm session ngay cả trong trường hợp hacker không thể chụp được traffic từ máy kết nối – đó là lý do gọi là Blind.

IP Spoofing: là phương thức mà kẻ tấn công cố thử bằng cách giả mạo như một người dùng hợp lệ bằng cách giả địa chỉ IP của người đó.

Source Routing: là cơ chế hacker can thiệp vào việc định tuyến bằng việc đưa thông tin về địa chỉ nguồn gói tin giả mạo.

DNS Spoofing: là kỹ thuạt mà kẻ tấn công điều hướng dữ liệu của nạn nhân tới một địa chỉ giả.

Session Hijacking mức mạng

Mức mạng có thể định nghĩa là đánh chặn các gói tin trong quá trình truyền tải giữa máy chủ và máy khách trên 1 phiên TCP và UDP.

Tấn công mức mạng được thực hiện trên dòng chảy dữ liệu của giao thức chia sẻ bởi tất cả các ứng dụng web.

Bằng cách tấn công các phiên mức mạng, kẻ tấn công tập hợp một số thông tin quan trọng được sử dụng để tấn công các phiên mức ứng dụng.

Tấn công TCP/IP

Tấn công TCP / IP là một kỹ thuật tấn công sử dụng các gói tin giả mạo để tiếp nhận một kết nối giữa một nạn nhân và một máy mục tiêu.

Kết nối của nạn nhân bị treo và kẻ tấn công sau đó có thể giao tiếp với máy chủ như kẻ tấn công là nạn nhân.

Để khởi động tấn công chiếm TCP / IP, kẻ tấn công phải trên cùng 1 lớp mạng với nạn nhân.

Mục tiêu và nạn nhân có thể ở bất cứ đâu.

Tấn công Man-in-the-Middle

Các gói dữ liệu giữa máy khách và máy chủ được chuyển qua máy chủ của kẻ tấn công bằng cách sử dụng hai kỹ thuật.

Sử dụng giả mạo giao thức tạo thông điệp điều khiển của Internet (ICMP) - Đó là một phần mở rộng của IP để gửi các thông báo lỗi nơi mà kẻ tấn công có thể gửi tin nhắn để đánh lừa các máy khách và máy chủ.

Sử dụng giao thức phân giải địa chỉ (ARP) giả mạo- ARP dùng để ánh xạ địa chỉ IP cục bộ để địa chỉ phần cứng hoặc các địa chỉ MAC.

Tấn công UDP

Cách tấn công UDP đòi hỏi phải có 2 hệ thống máy cùng tham gia. Hackers sẽ làm cho hệ thống của mình đi vào một vòng lặp trao đổi các dữ liệu qua giao thức UDP. Và giả mạo địa chỉ ip của các gói tin là địa chỉ loopback (127.0.0.1), rồi gởi gói tin này đến hệ thống của nạn nhân trên cổng UDP echo (7). Hệ thống của nạn nhân sẽ trả lời lại các messages do 127.0.0.1 (chính nó) gởi đến, kết quả là nó sẽ đi vòng một vòng lặp vô tận. Tuy nhiên, có nhiều hệ thống không cho dùng địa chỉ loopback nên hacker sẽ giả mạo một địa chỉ ip của một máy tính nào đó trên mạng nạn nhân và tiến hành ngập UDP trên hệ thống của nạn nhân. Nếu làm cách này không thành công thì chính máy ấy sẽ bị tràn.

Chiến lược phòng chống Session Hijacking

- Mã hóa dữ liệu mạng.
- Sử dụng các thiết bị giám sát mạng như IDS, IPS
- Cấu hình các thiết bị để chặn các thông tin giả mạo như địa chỉ IP
- Xóa các thông tin rác trong các trình duyệt
- Sử dụng các hệ thống xác thực mạnh như Kerberos
- Sử dụng các kỹ thuật như IPSec và SSL
- Phòng thủ theo chiều sâu

Chương 13: Máy chủ Web và Ứng dụng Web

Tràn bộ nhớ đệm (Buffer Overflow)

Một khối lượng dữ liệu được gửi vào ứng dụng vượt quá lượng dữ liệu được cấp phát khiến cho ứng dụng không thực thi được câu lệnh dự định kế tiếp mà thay vào đó phải thực thi một đoạn mã bất kì do Hacker đưa vào hệ thống. Nghiêm trọng hơn nếu ứng dụng được cấu hình để thực thi với quyền root trên hệ thống thì coi như Hacker đã chiếm được toàn bộ hệ thống máy chủ web.

Tấn công từ chối dịch vụ DoS

Tấn công DoS là kiểu tấn công làm cho dịch vụ mạng bị tê liệt, không còn đáp ứng được yêu cầu nữa. Loại tấn công này ảnh hưởng đến nhiều hệ thống mạng, rất dễ thực hiện và lại rất khó bảo vệ hệ thống khỏi tấn công DoS. Thực chất của DoS là Attacker sẽ chiếm dụng một lượng lớn tài nguyên mạng như băng thông, bộ nhớ,... và làm mất khả năng xử lý các yêu cầu dịch vụ đến các máy khách khác.

Tấn công DDoS

DDoS có nghĩa là nhiều Hacker cùng đánh vào một máy chủ hay một hệ thống mạng nào đấy. Tuy mạng của mỗi Hacker không có tài nguyên lớn như máy chủ nhưng số lượng gói tin gởi đến máy chủ thì lại bị tắt nghẽn chỗ tiếp xúc giữa mạng Internet và mạng cục bộ của máy chủ dẫn đến tình trạng nghẽn mạng và hệ thống mạng sụp hoàn toàn.

Cross Site Scripting (XSS)

Kỹ thuật tấn công Cross Site Scripting (được viết tắt là XSS) là phương pháp tấn công băng cách chèn thêm những đoạn mã lệnh có khả năng đánh cắp hay thiết lập được những thông tin quan trọng như Cookie, mật khẩu,... vào nguồn ứng dụng web để từ đó chúng được chạy như là một phần của ứng dụng WEB và có chức năng cung cấp hoặc thực hiện những điều Hacker muốn.

Phương pháp này không nhằm vào máy chủ của hệ thống mà chủ yếu tấn công trên chính máy người sử dụng. Hacker sẽ lợi dụng sự kiểm tra không chặt chẽ từ ứng dụng và hiểu biết hạn chế của người dùng cũng như biết đánh vào sự tò của họ dẫn đến người dùng bị mất thông tin một cách dễ dàng.

Tấn công Directory Traversal.

Directory traversal hay còn được biết với một số tên khác như “dot-dot-slash”, “path Traversal”,”directory clumbing” và “backtracking” là hình thức tấn công truy cập đến những file và thư mục mà được lưu bên ngoài thư mục webroot. Hình thức tấn công này không cần sử dụng một công cụ nào mà chỉ đơn thuần thao tác các biến với (dot-dot-slash) để truy cập đến file, thư mục, bao gồm cả source code, những file hệ thống, …

Chương 14: SQL Injection

Giới thiệu về SQL Injection

SQL Injection là gì?

SQL Injection là 1 kỹ thuật cho phép những kẻ tấn công lợi dụng vào lổ hỏng trong việc kiểm tra các dữ liệu trong các ứng dụng website và các thông báo lỗi của hệ quản trị cơ sở dữ liệu để "tiêm vào" (inject) và thi hành các câu lệnh SQL bất hợp pháp (do người viết phần mềm ứng dụng họ không lường trước). Hậu quả của nó rất tai hại vì nó cho phép những kẻ tấn công có thể thực hiện các thao tác xóa, hiệu chỉnh, … trực tiếp trên ứng dụng như là 1 người quản trị, do có toàn quyền trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy.

Lỗi này thường xảy ra trên các ứng dụng website có dữ liệu được quản lí bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase.

Các dạng tấn công SQL Injection.

✓Có bốn dạng thông thường bao gồm:

- Vượt qua kiểm tra lúc đăng nhập (Aauthorization bypass)
- Sử dụng câu lệnh SELECT
- Sử dụng câu lệnh INSERT
- Sử dụng các stored-procedures

Dạng tấn công vượt qua kiểm tra đăng nhập.

- Với dạng tấn công này, tin tặc có thể dễ dàng vượt qua các trang đăng nhập nhờ vào lỗi khi dùng các câu lệnh SQL thao tác trên cơ sở dữ liệu của ứng dụng web.
- Sau khi người dùng nhập thông tin vào, hệ thống sẽ kiểm tra tên đăng nhập và mật khẩu có hợp lệ hay không để quyết định cho phép hay từ chối thực hiện tiếp.

Tấn công sử dụng câu lệnh SELECT.

- Dạng tấn công này phức tạp hơn. Để thực hiện được kiểu tấn công này, kẻ tấn công phải có khả năng hiểu và lợi dụng các sơ hở trong các thông báo lỗi từ hệ thống để dò tìm các điểm yếu khởi đầu cho việc tấn công.

- Tấn công kiểu select này tuy phức tạp nhưng thường được hacker sử dụng, hacker thường khai thác lỗi này để lấy cắp tài khoản chùa hoặc chiếm quyền Admin của một website nào đó.

Tấn công sử dụng câu lệnh INSERT

- Thông thường các ứng dụng web cho phép người dùng đăng kí một tài khoản để tham gia. Chức năng không thể thiếu là sau khi đăng kí thành công, người dùng có thể xem và hiệu chỉnh thông tin của mình. SQL injection có thể được dùng khi hệ thống không kiểm tra tính hợp lệ của thông tin nhập vào.

Dạng tấn công Stored – Procedures

- Việc tấn công bằng stored-procedures sẽ gây tác hại rất lớn nếu ứng dụng được thực thi với quyền quản trị hệ thống 'sa'.

- Ví dụ, nếu ta thay đoạn mã tiêm vào dạng: **' ; EXEC xp_cmdshell 'cmd.exe dir C: '**.

- Lúc này hệ thống sẽ thực hiện lệnh liệt kê thư mục trên ổ đĩa C:\ cài đặt server. Việc phá hoại kiểu nào tuỳ thuộc vào câu lệnh đằng sau cmd.exe.

Phòng tránh tấn công SQL Injection

Lọc bỏ các ký tự và từ khóa nguy hiểm như: -- , select , where , drop, shutdown …

Kiểm soát chặt chẽ tất cả các dữ liệu nhập nhận được từ đối tượng Request (Request, Request.QueryString),

Cần có cơ chế kiểm soát chặt chẽ và giới hạn quyền xử lí dữ liệu đến tài khoản người dùng mà ứng dụng web đang sử dụng. Các ứng dụng thông thường nên tránh dùng đến các quyền như dbo hay sa. Quyền càng bị hạn chế, thiệt hại càng ít.

Ngoài ra để tránh các nguy cơ từ SQL Injection attack, nên chú ý loại bỏ bất kì thông tin kĩ thuật nào chứa trong thông điệp chuyển xuống cho người dùng khi ứng dụng có lỗi. Các thông báo lỗi thông thường tiết lộ các chi tiết kĩ thuật có thể cho phép kẻ tấn công biết được điểm yếu của hệ thống.

Chương 15: Mạng không dây - Wireless Networking

Mạng không dây là gì?

Giới thiệu

Thuật ngữ "mạng máy tính không dây" nói đến công nghệ cho phép hai hay nhiều máy tính giao tiếp với nhau dùng những giao thức mạng chuẩn nhưng không cần dây cáp mạng. Nó là một hệ thống mạng dữ liệu linh hoạt được thực hiện như một sự mở rộng hoặc một sự lựa chọn mới cho mạng máy tính hữu tuyến (hay còn gọi là mạng có dây).

Các mạng máy tính không dây sử dụng các sóng điện từ không gian (sóng vô tuyến hoặc sóng ánh sáng) thu, phát dữ liệu qua không khí, giảm thiểu nhu cầu về kết nối bằng dây. Vì vậy, các mạng máy tính không dây kết hợp liên kết dữ liệu với tính di động của người sử dụng.

Ưu điểm của mạng máy tính không dây

Mạng máy tính không dây đang nhanh chóng trở thành một mạng cốt lõi trong các mạng máy tính và đang phát triển vượt trội. Với công nghệ này, những người sử dụng có thể truy cập thông tin dùng chung mà không phải tìm kiếm chỗ để nối dây mạng, chúng ta có thể mở rộng phạm vi mạng mà không cần lắp đặt hoặc di chuyển dây. Các mạng máy tính không dây có ưu điểm về hiệu suất, sự thuận lợi, cụ thể như sau:

- *Tính di động* : những người sử dụng mạng máy tính không dây có thể truy nhập nguồn thông tin ở bất kỳ nơi nào. Tính di động này sẽ tăng năng suất và tính kịp thời thỏa mãn nhu cầu về thông tin mà các mạng hữu tuyến không thể có được.
- *Tính đơn giản* : lắp đặt, thiết lập, kết nối một mạng máy tính không dây là rất dễ dàng, đơn giản và có thể tránh được việc kéo cáp qua các bức tường và trần nhà.
- *Tính linh hoạt* : có thể triển khai ở những nơi mà mạng hữu tuyến không thể triển khai được.
- *Tiết kiệm chi phí lâu dài* : Trong khi đầu tư cần thiết ban đầu đối với phần cứng của một mạng máy tính không dây có thể cao hơn chi phí phần cứng

của một mạng hữu tuyến nhưng toàn bộ phí tổn lắp đặt và các chi phí về thời gian tồn tại có thể thấp hơn đáng kể. Chi phí dài hạn có lợi nhất trong các môi trường động cần phải di chuyển và thay đổi thường xuyên.

- *Khả năng vô hướng* : các mạng máy tính không dây có thể được cấu hình theo các topo khác nhau để đáp ứng các nhu cầu ứng dụng và lắp đặt cụ thể. Các cấu hình dễ dàng thay đổi từ các mạng ngang hàng thích hợp cho một số lượng nhỏ người sử dụng đến các mạng có cơ sở hạ tầng đầy đủ dành cho hàng nghìn người sử dụng mà có khả năng di chuyển trên một vùng rộng.

Hoạt động của mạng máy tính không dây

Các mạng máy tính không dây sử dụng các sóng điện từ không gian (vô tuyến hoặc ánh sáng) để truyền thông tin từ một điểm tới điểm khác. Các sóng vô tuyến thường được xem như các sóng mang vô tuyến do chúng chỉ thực hiện chức năng cung cấp năng lượng cho một máy thu ở xa. Dữ liệu đang được phát được điều chế trên sóng mang vô tuyến (thường được gọi là điều chế sóng mang nhờ thông tin đang được phát) sao cho có thể được khôi phục chính xác tại máy thu.

Nhiễu sóng mang vô tuyến có thể tồn tại trong cùng không gian, tại cùng thời điểm mà không can nhiễu lẫn nhau nếu các sóng vô tuyến được phát trên các tần số vô tuyến khác nhau. Để nhận lại dữ liệu, máy thu vô tuyến sẽ thu trên tần số vô tuyến của máy phát tương ứng

Trong một cấu hình mạng máy tính không dây tiêu chuẩn, một thiết bị thu/phát (bộ thu/phát) được gọi là một điểm truy cập, nối với mạng hữu tuyến từ một vị trí cố định sử dụng cáp tiêu chuẩn. Chức năng tối thiểu của điểm truy cập là thu, làm đệm, và phát dữ liệu giữa mạng máy tính không dây và cơ sở hạ tầng mạng hữu tuyến. Một điểm truy cập đơn có thể hỗ trợ một nhóm nhỏ người sử dụng và có thể thực hiện chức năng trong một phạm vi từ một trăm đến vài trăm feet. Điểm truy cập (hoặc anten được gắn vào điểm truy cập) thường được đặt cao nhưng về cơ bản có thể được đặt ở bất kỳ chỗ nào miễn là đạt được vùng phủ sóng mong muốn.

Những người sử dụng truy cập vào mạng máy tính không dây thông qua các bộ thích ứng máy tính không dây như các Card mạng không dây trong các vi máy tính, các máy Palm, PDA. Các bộ thích ứng máy tính không dây cung cấp một giao diện giữa hệ thống điều hành mạng (NOS – Network Operation System)

của máy khách và các sóng không gian qua một anten. Bản chất của kết nối không dây là trong suốt đối với hệ điều hành mạng.

Một số khái niệm

Mạng Ad – hoc

Mỗi máy tính trong mạng giao tiếp trực tiếp với nhau thông qua các thiết bị card mạng không dây mà không dùng đến các thiết bị định tuyến hay thu phát không dây.

Mạng Infrastructure

Các máy tính trong hệ thống mạng sử dụng một hoặc nhiều các thiết bị định tuyến hay thiết bị thu phát để thực hiện các hoạt động trao đổi dữ liệu với nhau và các hoạt động khác.

WEP

WEP (Wired Equivalen Privacy) : thực chất là một giao thức sử dụng trong mạng lan được định nghĩa trong chuẩn 802.11.WEP được xây dựng nhằm bảo vệ sự trao đổi thông tin chống sự nghe trôm, chống lại những kết nối mạng không được cho phép cũng như chống lại việc thay đổi làm nhiễu thông tin

+ *Các tính năng của WEP*

WEP sử dụng thủ công để tạo ra một khoá giống nhau ở các client và ở các Access Point. WEP đưa ra 3 mức an toàn : Mức OFF (no sencurity) ,64-bit (Weak security) và 128-bit (Stronger security) với các thiết bị truyền thông không dây thì tất cả phải sử dụng cùng kiểu mã hoá.

WEP sử dụng stream cipher RC4 cùng với một mã 40 bit hoặc 104 bit và một số ngẫu nhiên 24 bit (initialization vector-IV) để mã hoá thông tin.Thông tin mã hoá được tạo ra bằng cách thực hiện operation XOR giữa keystream và plain text. Thông tin mã hoá và IV sẽ được gữi đến người nhận.Người nhận sẽ giải mã thông tin dựa vào IV và khoá WEP đã biết trước.

WEP IV (Initialization Vector) là giá trị độ dài 24 bit được thay đổi ngẫu nhiên theo từng gói dữ liệu, vì vậy thực tế WEP key chúng ta chỉ định trong các AP chỉ còn 40bit với kieur mã hoá 64bit 104bit với kiểu mã hoá 128 bit

WEP với độ dài 24bit giá tri dao đồng trong khoảng 16.777.216 trường hợp nên sẽ có hiện tượng xung đột IV xảy ra khi sử dụng cùng một IV và khoá WEP kết quả là cùng một chuỗi khoá được sử dụng để mã hoá fram.

WPA

WPA là một chuẩn wifi được thiết kế để nâng cao các tính năng công nghệ WEP. WPA mã hoá đầy đủ 128 bit và IV có chiều dài 48 bit. Một trong những cải tiến quan trọng nhất cảu WPA là sử dụng hàm thay đổi khoá TKIP (Temprora Key Integrity Protocol)

WPA TKIP thay đổi khoá cùng AP và user một cách tự động trong quá trình trao đổi thông tin. Vì vậy các công cụ thu thập các gói tin để phá khoá đều không thực hiện được bởi WPA

WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin MIC là một message 64 bit được dựa trên thuật toán Michael.

WPA có 2 loại: WPA Presonal và WPA Enterprise, sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu. WPA Presonal thích hợp cho mạng gia đình và văn phòng nhỏ. WPA Enterprise cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc

Ưu điểm của WPA: nó cung cấp khả năng bảo mật rất tốt cho mạng không dây thêm vào đó tính xác thực

Nhược điểm WPA: cài đặt phức tạp, trong hầu hết các trường hợp nó yêu cầu cập nhập phần cơ sở (firmware) cho các sản phẩm chính.

WPA2

WPA2 (Wifi Protected Access – version 2) thường được gọi là 802.11i , là phiên bản kế tiếp của WPA. WPA2 sử dụng thuật toán mã hoá dựa trên AES, được xem là an toàn tuyệt đối.

WPA2 được kiểm định lần đầu tiên vào ngày 1/9/2004. WPA2 sử đụng thuật toán mã hoá Advance Encryption Standar (AES). WPA2 cũng có cấp độ bảo mật rất cao tương tự như chuẩn WPA, nhằm bảo vệ cho người dùng và người quản trị đối với tài khoản dữ liệu

WPA2 sử dụng thuật toán mã hoá AES thay vì RC4 như trong WPA. Mã khoá cảu AES có kích thước là 128, 192 hoặc 256 bit. WPA2 cũng có 2 phiên bản giống như WPA là Enterprise và Personal

Chương 16: Evading IDSs, Firewalls, and Honeypots

IDS

Một hệ thống phát hiện xâm nhập IDS (Intrusion Detection Systems) là một thiết bị hoặc một ứng dụng được sử dụng để theo dõi hoạt động của hệ thống mạng. Có chức năng tự động theo dõi các sự kiện xảy ra trên hệ thống máy tính, phân tích để phát hiện ra các vấn đề liên quan đến an ninh, bảo mật. IDS cũng có thể phân biệt giữa những tấn công bên trong từ bên trong (từ những người trong công ty) hay tấn công từ bên ngoài (từ các hacker). IDS phát hiện dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết (giống như cách các phần mềm diệt virus dựa vào các dấu hiệu đặc biệt để phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (thông số đo đạc chuẩn của hệ thống) để tìm ra các dấu hiệu khác thường.

IDS bao gồm các thành phần chính:

- Thành phần thu thập thông tin gói tin
- Thành phần phát hiện gói tin
- Thành phần xử lý (phản hồi).

Thành phần thu thập thông tin gói tin

Thành phần này có nhiệm vụ lấy tất các gói tin đi đến mạng. Thông thường các gói tin có địa chỉ không phải của một card mạng thì sẽ bị card mạng đó huỷ bỏ nhưng card mạng của IDS được đặt ở chế độ thu nhận tất cả. Tất cả các gói tin qua chúng đều được sao lưu, xử lý, phân tích đến từng trường thông tin. Bộ phận thu thập gói tin sẽ đọc thông tin từng trường trong gói tin, xác định chúng thuộc kiểu gói tin nào, dịch vụ gì... Các thông tin này được chuyển đến thành phần phát hiện tấn công.

Thành phần phát hiện gói tin

Ở thành phần này, các bộ cảm biến đóng vai trò quyết định. Vai trò của bộ cảm biến là dùng để lọc thông tin và loại bỏ những thông tin dữ liệu không tương thích đạt được từ các sự kiện liên quan tới hệ thống bảo vệ, vì vậy có thể phát hiện được các hành động nghi ngờ.

Thành phần xử lý

Khi có dấu hiệu của sự tấn công hoặc thâm nhập, thành phần phát hiện tấn công sẽ gửi tín hiệu báo hiệu (alert) có sự tấn công hoặc thâm nhập đến thành phần phản ứng. Lúc đó thành phần phản ứng sẽ kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo tới người quản trị.

Một số kỹ thuật ngăn chặn.

- Cảnh báo thời gian thực Gửi các cảnh báo thời gian thực đến người quản trị để họ nắm được chi tiết các cuộc tấn công, các đặc điểm và thông tin về chúng.
- Ghi lại vào tập tin Các dữ liệu của các gói tin sẽ được lưu trữ trong hệ thống các tập tin log. Mục đích là để những người quản trị có thể theo dõi các luồng thông tin và là nguồn thông tin giúp cho module phát hiện tấn công hoạt động.
- Ngăn chặn, thay đổi gói tin Khi một gói tin khớp với dấu hiệu tấn công thì IDS sẽ phản hồi bằng cách xóa bỏ, từ chối hay thay đổi nội dung của gói tin, làm cho gói tin trở nên không bình thường.

Phân loại IDS

Có 2 loại IDS là Network Based IDS(NIDS) và Host Based IDS (HIDS).

Network Based IDS

Hệ thống IDS dựa trên mạng sử dụng bộ dò và bộ bộ cảm biến cài đặt trên toàn mạng. Những bộ dò này theo dõi trên mạng nhằm tìm kiếm những lưu lượng trùng với những mô tả sơ lược được định nghĩa hay là những dấu hiệu. Những bộ bộ cảm biến thu nhận và phân tích lưu lượng trong thời gian thực. Khi ghi nhận được một mẫu lưu lượng hay dấu hiệu, bộ cảm biến gửi tín hiệu cảnh báo đến trạm quản trị và có thể được cấu hình nhằm tìm ra biện pháp ngăn chặn những xâm nhập xa hơn. NIDS là tập nhiều sensor được đặt ở toàn mạng để theo dõi những gói tin trong mạng so sánh với với mẫu đã được định nghĩa để phát hiện đó là tấn công hay không.

Lợi thế của Network Based IDS

- Quản lý được cả một network segment (gồm nhiều host).
- Cài đặt và bảo trì đơn giản, không ảnh hưởng tới mạng.

- Tránh DOS ảnh hưởng tới một host nào đó.
- Có khả năng xác định lỗi ở tầng Network (trong mô hình OSI).
- Độc lập với hệ điều hành.

Hạn chế của Network Based IDS

- Có thể xảy ra trường hợp báo động giả (false positive), tức không có intrusion mà NIDS báo là có intrusion.
- NIDS đòi hỏi phải được cập nhật các signature mới nhất để thực sự an toàn.
- Có độ trễ giữa thời điểm bị attack với thời điểm phát báo động. Khi báo động được phát ra, hệ thống có thể đã bị tổn hại.
- Hạn chế về giới hạn băng thông. Hacker có thể tấn công bằng cách chia nhỏ dữ liệu ra để xâm nhập vào hệ thống.
- Không cho biết việc attack có thành công hay không

Host Based IDS

HIDS là hệ thống phát hiện xâm phạm máy chủ được cài đặt cục bộ trên một máy tính nhất định làm cho nó trở nên linh hoạt hơn nhiều so với NIDS. Kiểm soát lưu lượng vào ra trên một máy tính, có thể được triển khai trên nhiều máy tính trong hệ thống mạng. HIDS có thể được cài đặt trên nhiều dạng máy tính khác nhau cụ thể như các máy chủ, máy trạm, máy tính xách tay.

Lợi thế của Host Based IDS

- Có khả năng xác đinh user liên quan tới một sự kiện (event).
- HIDS có khả năng phát hiện các cuộc tấn công diễn ra trên một máy, NIDS không có khả năng này.
- Có thể phân tích các dữ liệu mã hoá.
- Cung cấp các thông tin về host trong lúc cuộc tấn công diễn ra trên host này.

Hạn chế của Host Based IDS

- Thông tin từ HIDS là không đáng tin cậy ngay khi sự tấn công vào host này thành công.
- Khi hệ điều hành bị "hạ" do tấn công, đồng thời HIDS cũng bị "hạ".
- HIDS phải được thiết lập trên từng host cần giám sát.

- HIDS không có khả năng phát hiện các cuộc dò quét mạng (Nmap, Netcat…).
- HIDS cần tài nguyên trên host để hoạt động.

Tường lửa - FIREWALL

Khái niệm

Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn. Cũng có thể hiểu rằng Firewall là một cơ chế để bảo vệ mạng tin tưởng (trusted network) khỏi mạng không tin tưởng (untrusted network).

Một Firewall có thể lọc các lưu lượng Internet nguy hiểm như hacker, các loại sâu, và một số loại virus trước khi chúng có thể gây ra trục trặc trên hệ thống. Ngoài ra, Firewall có thể giúp cho máy tính tránh tham gia các cuộc tấn công vào các máy tính khác mà không hay biết. Việc sử dụng một Firewall là cực kỳ quan trọng đối với các máy tính luôn kết nối Internet, như trường hợp có một kết nối băng thông rộng hoặc kết nối DSL/ADSL.

Các lựa chọn Firewall

Firewall phần cứng

Về tổng thể, Firewall phần cứng cung cấp mức độ bảo vệ cao hơn so với Firewall phần mềm và dễ bảo trì hơn. Firewall phần cứng cũng có một ưu điểm khác là không chiếm dụng tài nguyên hệ thống trên máy tính như Firewall phần mềm.

Firewall phần cứng là một lựa chọn rất tốt đối với các doanh nghiệp nhỏ, đặc biệt cho những công ty có chia sẻ kết nối Internet. Có thể kết hợp Firewall và một bộ định tuyến trên cùng một hệ thống phần cứng và sử dụng hệ thống này để bảo vệ cho toàn bộ mạng. Firewall phần cứng có thể là một lựa chọn đỡ tốn chi phí hơn so với Firewall phần mềm thường phải cài trên mọi máy tính cá nhân trong mạng.

Firewall phần mềm

So với Firewall phần cứng, Firewall phần mềm cho phép linh động hơn, nhất là khi cần đặt lại các thiết lập cho phù hợp hơn với nhu cầu riêng của từng công ty. Chúng có thể hoạt động tốt trên nhiều hệ thống khác nhau, khác với Firewall phần cứng tích hợp với bộ định tuyến chỉ làm việc tốt trong mạng có qui mô nhỏ.

Firewall phần mềm cũng là một lựa chọn phù hợp đối với máy tính xách tay vì máy tính sẽ vẫn được bảo vệ cho dù mang máy tính đi bất kỳ nơi nào.

Chức năng FIREWALL

Firewall được đặt giữa mạng bên trong (Intranet) của một công ty, tổ chức, ngành hay một quốc gia, và Internet. Vai trò chính là bảo mật thông tin, ngăn chặn sự truy nhập không mong muốn từ bên ngoài (Internet) và cấm truy nhập từ bên trong (Intranet) tới một số địa chỉ nhất định trên Internet.

Phân loại Firewall theo cơ chế hoạt động

Một Firewall bao gồm một hay nhiều các thành phần sau đây:

- Bộ lọc packet (packet filtering router)
- Cổng ứng dụng (application-level gateway hay proxy firewall)
- Cổng mạch (circuite level gateway)

Packet Filtering Firewall

Là hệ thống tường lửa giữa các thành phần bên trong mạng và bên ngoài mạng có kiểm soát. Firewall mức mạng thường hoạt động theo nguyên tắc router hay còn được gọi là router, tức là tạo ra các luật lệ về quyền truy cập mạng dựa trên mức mạng. Mô hình này hoạt động theo nguyên tắc lọc gói tin. Ở kiểu hoạt động này các gói tin đều được kiểm tra địa chỉ nguồn nơi chúng xuất phát. Sau khi địa chỉ IP nguồn được xác định, nó sẽ tiếp tục được kiểm tra với các luật đã đặt ra trên router.

Ưu điểm

Đa số các hệ thống firewall đều sử dụng bộ lọc packet. Một trong những ưu điểm của phương pháp dùng bộ lọc packet là chi phí thấp vì cơ chế loc packet đã được bao gồm trong mỗi phần mềm router.

Hạn chế

Do làm việc dựa trên header của packet, rõ ràng là bộ lọc packet không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ lấy cắp thông tin hay phá hoại của kẻ xấu.

Application-proxy firewall

Khi mộ kết nối từ một người dùng nào đó đến mạng sử dụng Firewall kiểu này thì kết nối đó sẽ bị chặn lại, sau đó Firewall sẽ kiểm tra các trường có liên quan của gói tin yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các luật đặt ra trên Firewall thì Firewall sẽ tạo mộ cầu kết nối cho gói tin đi qua.

Ưu điểm

- Không có chức năng chuyển tiếp các gói tin IP.
- Cho phép người quản trị hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy cập được bởi các dịch vụ.
- Đưa ra công cụ cho phép ghi lại quá trình kết nối.

Nhược điểm

- Tốc độ xử lý khá chậm.
- Sự chuyển tiếp các gói tin IP khi mộ máy chủ nhận được mộ yêu cầu từ mạng ngoài rồi chuyển chúng vào mạng trong chính là lỗ hổng cho hacker xâm nhập.
- Kiểu firewall này hoạt động dựa trên ứng dựng phần mềm nên phải tạo cho mỗi dịch vụ trên mạng một trình ứng dựng uỷ quyền (proxy) trên Firewall (Ftp proxy, Http proxy).

Circuit Level Gateway

Là một chức năng đặc biệt có thể thực hiện được bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.

Hạn chế của Firewall

Firewall không đủ thông minh để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó.

Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-drivent attack).

Honeypots

Khái niệm

Honeypot là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng đánh lừa những kẻ sử dụng và xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn không cho chúng tiếp xúc với hệ thống thật.

Hệ thống tài nguyên thông tin có nghĩa là Honeypot có thể giả dạng bất cứ loại máy chủ tài nguyên nào như là Mail Server, Domain Name Server, Web Server… Honeypot sẽ trực tiếp tương tác với tin tặc và tìm cách khai thác thông tin về tin tặc như hình thức tấn công, công cụ tấn công hay cách thức tiến hành thay vì bị tấn công.

Phân loại Honeypots

Gồm hai loại chính: Tương tác thấp và Tương tác cao

- Tương tác thấp: Mô phỏng giả các dịch vụ, ứng dụng, và hệ điều hành. Mức độ rủi ro thấp, dễ triển khai và bảo dưỡng nhưng bị giới hạn về dịch vụ.
- Tương tác cao: Là các dịch vụ, ứng dụng và hệ điều hành thực. Mức độ thông tin thu thập được cao. Nhưng rủi ro cao và tốn thời gian để vận hành và bảo dưỡng.

Chương 18: Pentration Testing

Giới thiệu về Penetration Testing.

Penetration Testing là gì.

Penetration Testing là 1 phương thức nhằm đánh giá, ước chừng độ an toàn và tin cậy của 1 hệ thống máy tính hay 1 môi trường mạng bằng cách giả lập (simulating) 1 cuộc tấn công từ hacker.

Tiến trình này bao gồm 1 quá trình phân tích linh hoạt (active analysis) trên hệ thống về bất kỳ điểm yếu, lỗ hổng nào.

Quá trình phân tích này được tiến hành từ vai trò của 1 attacker, và có thể bao gồm việc lợi dụng các lỗ hổng về bảo mật.

Khi phát hiện thấy bất kỳ vấn đề nào liên quan tới security nó sẽ hiển thị cho admin của hệ thống biết, đồng thời cũng đưa ra đánh giá những tác động của chúng và đi kèm với những đề xuất, giải pháp kỹ thuật thay thế.

Đánh giá bảo mật

Mỗi tổ chức đều sử dụng các mức đánh giá an ninh khác nhau để xác nhận mức độ an toàn về tài nguyên mạng

Kiểm tra an ninh là giai đoạn đầu tiên mà một nhà tư vấn an ninh thực hiện trong việc cung cấp dịch vụ tư vấn cho một doanh nghiệp. Tuy nhiên, ngoài các cuộc kiểm tra xây dựng nền tảng, các doanh nghiệp cũng phải thực hiện kiểm tra an ninh mạng hoặc đánh giá một cách thường xuyên để đảm bảo hiệu suất tối ưu.

Các mức đánh giá bao gồm:

1. **Kiểm tra an ninh:**

Trong giai đoạn ban đầu, kiểm tra viên kiểm kê toàn bộ mạng cả về thể chất và vận hành. Đối với phần cứng tồn kho, kiểm toán viên thu thập dữ liệu liên quan đến phần cứng và các thông tin phần mềm như giấy phép phần mềm. Mục tiêu của giai đoạn này là để đạt được một bản kế hoạch chi tiết để bảo mật mạng và thông tin cá nhân một . Những thông tin này được dùng như là cơ sở cho các giai đoạn còn lại của đánh giá.

2. **Đánh giá lỗ hổng**

Ở giai đoạn này, kiểm tra viên tận dụng kế hoạch chi tiết mạng và thông tin mật cá nhân "tấn công" mạng lưới từ bên ngoài. Mục tiêu trong giai đoạn này là để xâm nhập vào các lỗ hổng của hệ thống nhằm thu được dữ liệu nhạy cảm.

Trình quét lỗ hổng có thể kiểm trai hệ thống và mạng lưới các thiết bị ảnh hưởng trực tiếp từ các cuộc tấn công thông thường.

Ngoài ra, trình quét lỗ hổng có thể xác định sai sót phổ biến của việc cấu hình bảo mật.

3. Kiểm thử thâm nhập.

Thâm nhập thử nghiệm và đánh giá có rất nhiều như giai đoạn II nhưng tập trung vào tấn công mạng nội bộ chứ không phải bên ngoài.

Mỗi loại hình đánh giá an toàn đòi hỏi người thực hiện việc đánh giá phải có kỹ năng khác nhau

Hạn chế của việt đánh giá bảo mật.

- Phần mềm đánh giá bảo mật bị giới hạn trong khả năng phát hiện các lỗ hổng tại một điểm nhất định trong thời gian nhất định.
- Nó phải được cập nhật khi các lỗ hổng mới được phát hiện hoặc các sửa đổi được của phần mềm đang được sử dụng.
- Phương pháp được sử dụng cũng như các phần mềm Vulnerability scanning đa dạng đánh giá an ninh khác nhau.

Những điểm cần lưu ý.

- Kiểm tra thâm nhập nếu không được hoàn thành một cách chuyện nghiệp có thể dẫn đến sự mất mát của các dịch vụ và sự gián đoạn sự ổn định trong kinh doanh.
- Kiểm tra thâm nhập đánh giá các mô hình bảo mật của tổ chức một cách tổng thể
- Một kiểm tra thâm nhập được phân biệt là một người tấn công có mục đính chính đáng và không ác ý.

Các loại của Penetration Testing.

Kiểm tra bên ngoài (Extranal Testing): Kiểm tra bên ngoài bao gồm phân tích các thông tin công khai sẵn có, một giai đoạn liệt kê mạng lưới, và hoạt động của các thiết bị phân tích an ninh.

Kiêm tra nội bộ (Internal Testing): Kiểm tra nội bộ sẽ được thực hiện từ một số điểm truy cập mạng, thể hiện cho có các logic và phân đoạn vật lý.

Kỹ thuật kiểm thử hộp đen (black-box).

Các nhân viên sẽ không được biết bất cứ thông tin gì từ phí doanh nghiệp, tổ chức.

Quá trình pen-test sẽ được tiến hành sau khi đã thu thập đủ thông tin từ nhiều phía và nghiên cứu.

Kiểu kiểm tra nay mô phỏng quá trình hành động của một hacker thực sự. Nó quyết định đáng kể đến việc phân bổ của quá trình, qua đó tìm ra bản chất của cơ sở hạ tầng và làm thế nào nó kết nối và liên hệ với nhau.

Đặc điểm:

- Kiểu kiểm tra nay mô phỏng quá trình hành động của một hacker thực sự.
- Tốn thời gian và là loại kiểm tra tốn kém.

Kỹ thuật kiểm thử hộp xám (Grey-box).

Trong kiểm thử hộp xám, thử nghiệm thường có thông thin hạn chế

Nó thực hiện đánh giá và kiểm tra an ninh bên trong

Phương pháp bảo mật cho ứng dụng bằng cách kiểm tra tất cả các lỗ hổng mà hacker có thể tìm thấy và khai thác.

Thực hiện chủ yếu khi ki thuật kiểm thử bắt đầu kiểm tra hộp đen trên các hệ thống được bảo vệ tốt và có được một ít kinh nghiệm cần thiết để tiến hành xem xét kỹ lưỡng.

Kỹ thuật kiểm thử hộp trắng (White-box).

Đây là quá trình hoàn thiện việc tìm hiểu về cớ sở hạ tầng.

Kiểm tra này mô phỏng các hoạt động của nhân viên của công ty.

Kiểm tra tự động.

Sử dụng các công cụ được lập trình sẵn kiểm tra hệ thống.

Tự động kiểm tra có thể tiết kiệm thời gian và tiết kiệm chi phí trong một thời gian dài, tuy nhiên, nó không thể thay thế kinh nghiệm của sự bảo mật chuyên nghiệp.

Với kiểm tra tự động , ở đó không tồi tại phạm vị kiểm tra cho bất kì thành phần kiến trúc.

Kiểm tra bằng tay.

Hướng dẫn kiểm tra là lựa chọn tốt nhất một tổ chức có thể chọn để hưởng lợi từ kinh nghiệm của một chuyên gia an ninh

Mục đích của các chuyên gia là đánh giá tình trạng bảo mật của tổ chức từ góc độ của một kẻ tấn công

Để tiếp cận hướng dẫn đòi hỏi có quy hoạch, kiểm tra thiết kế, lập kế hoạch,và chăm tìm tài liệu hướng dẫn để nắm bắt kết quả của quá trình kiểm định

Các Giai Đoạn Kiểm Tra Thâm Nhập.

Giai đoạn trước khi tấn công.

Mục đích của giai đoạn trước khi tấn công là đề cập đến chế độ của cuộc tấn công và mục tiêu phải đạt được

Do thám được coi là giai đoạn trong giai đoạn trước khi tấn công để xác định vị trí, thu thập, xác định và ghi thông tin về mục tiêu.

Hacker tìm kiếm để tìm hiểu càng nhiều thông tin của nan nhân càng tốt.

Hacker thu thập thông tin theo những cách khác nhau cho phép chúng xây dựng kế hoạch tấn công, có 2 cách:

- Trinh sát thụ động gắng với việc thu thập thông tin về mục tiêu từ các truy cập công cộng trong hoạt động trinh sát
- Kỹ thuật thu thập thông tin thông trên các nguồn công cộng, ghé thăm trên các trang web, phỏng vấn,và bảng câu hỏi

Thông tin lấy được trong giai đoạn này:

- Thông tin cạnh tranh.
- Thông tin đăng ký trên mạng.

- Thông tin DNS và mail server
- Thông tinh haoạt động hệ thống
- Thông tin của người dùng
- Thông tin Chứng nhận xác thực
- Kêt nối tương tự
- Thông tin liên lạc
- Thông tinh website
- Địa chỉ vật lý và logic của tổ chức
- Phạm vi sản phẩm và dịch vụ được cung cấp bởi công ty mục tiêu có trên mạng
- Bất kỳ thông tin nào khác có giá trị đều có thể khai thác

Giai đoạn tấn công.

Kiểm tra vòng ngoài.

Phương pháp kiểm tra cho an ninh vòng ngoài bao gồm nhưng không giới hạn:

- Kiểm tra danh sách kiểm soát truy cập bằng cách giả mạo các câu trả lời với các gói dữ liệu thủ công.
- Đánh giá các quy tắc lọc giao thức bằng cách cố gắng kết nối sử dụng các giao thức khác nhau chẳng hạn như SSH, FTP, và Telnet.
- Kiểm tra phản ứng của hệ thống an ninh vòng ngoài của web server bằng cách sử dụng nhiều phương pháp như POST, 9 DELETE, và COPY.
- Đánh giá báo cáo lỗi và quản lý lỗi với thăm dò ICMP.
- Xác định ngưỡng từ chối dịch vụ bằng cách cố gắng kết nối lên tục đến TCP,đánh giá các kết nối chuyển tiếp TCP ^ và cố gắng kết nối đến dòng UDP.
- Đánh giá khả năng của IDS bằng cách gởi mã độc hại (chẳng hạn như URL bị thay đổi) và quét các mục tiêu khác nhau để đáp ứng lưu lượng truy cập bất thường.

Liệt kê các thiết bị

Kiểm kê thiết bị là một tập hợp các thiết bị mạng cùng với một số thông tin liên quan về mỗi thiết bị được ghi lại trong một tài liệu.

Sau khi mạng đã được lập bản đồ và các tài sản kinh doanh được xác định, bước hợp lý tiếp theo là làm một bản kê cho các thiết bị.

Một kiểm tra vật lý có thể được thực hiện bổ sung để đảm bảo rằng việc liệt kê các thiết bị đã được cố định.

Thu thập mục tiêu

Thu thập một mục tiêu cần phải tập hợp các hoạt động được thự hiện bởi các tester với các đối tượng máy bị nghi ngờ đến nhiều các thử thách xâm nhập chẳng hạn như quét lỗ hổng và đánh giá an ninh.

Phương pháp thử nghiệm đạt được mục tiêu bao gồm những phần không hạn chế như:

- **Hoạt động của các cuộc tấn công thăm dò:** Sử dụng kết quả của việt quét mạng để thu thập thêm thông tin có thể dẫn đến một sự thỏa hiệp.
- **Quá trình chạy quét lỗ hổng:** Quá trình quét lỗ hổng được hoàn thành trong giai đoạn này.
- **Hệ thống đáng tin cậy và quá trình đánh giá độ tin cậy:** Cố gắng truy cập tài nguyên của máy bằng cách sữ dụng thông tin hợp pháp thu được thông qua kỹ thật giao tiếp hoặc các kỹ thuật khác.

Kỹ thuật leo thang đặc quyền

Một khi đã dành được mục tiêu, tester cố gắng khai thác hệ thống và truy cập các nguồn tài nguyên được bảo vệ

Các hoạt động bao gồm:

- Các tester có thể tận dụng lợi thế của các chính sách bảo mật kém và tận dụng lợi thế của email hoặc code web không an toàn để thu thập thông tin có thể dẫn đến sự leo thang các đặc quyền
- Sử dụng các kỹ thuật như brute force để đạt được đặc quyền.
- Sử dụng các Trojans và phân tích giao thức
- Sử dụng thông tin thu thập được thông qua các kỹ thuật như kỹ thuật giao tiếp để truy cập trái phép vào các nguồn tài nguyên đặc quyền

Giai đoạn sau tấn công và hoạt động

Giai đoạn này quan trọng đối với bất kỳ kiểm tra thâm nhập vì nó có trách nhiệm để khôi phục lại các hệ thống trước kia.

Các giai đoạn hoạt động tấn công bao gồm những điều sau:

- Loại bỏ tất cả các tập tin đã tải lên trên hệ thống.
- Làm sạch tất cả các mục đăng ký và loại bỏ lỗ hổng .
- Loại bỏ tất cả các công cụ và khai thác từ các hệ thống thử nghiệm.
- Khôi phục lại mạng lưới thử nghiệm bằng cách loại bỏ chia sẽ và kết nói.
- Phân tích tất cả các kết quả và trình bày cùng với các tổ chức.

Đánh giá an ninh mạng.

Quá trình này quét trên môi trường mạng để xác định các lỗ hổng và giúp cải thiện chính sách bảo mật của doanh nghiệp.

Việc đánh giá sẽ phát hiện ra lỗi an ninh mạng có thể dẫn đến dữ liệu hoặc thiết bị đang được khai thác hoặc bị phá hủy bởi các trojan, các cuộc tấn công từ chối dịch vụ , và sự xâm nhập khác.

Quá trình đảm bảo rằng việc thực hiện an ninh thực sự cung cấp sự bảo vệ mà doanh nghiệp yêu cầu khi bất kỳ cuộc tấn công diễn ra trên mạng, thường bởi "khai thác" một lỗ hổng hệ thống.

Quá trình được thực hiện bởi nhóm tìm cách đột nhập vào mạng hoặc máy chủ.

Cấp độ thỏa thận dịch vụ Pentest.

Một thỏa thuận cấp độ dịch vụ là một hợp đồng chi tiết về dịch vụ mà một người đảm nhận sẽ cung cấp.

Điểm máu chốt SLAs xác định mức tối thiểu sẵn có từ những người thử nghiệm và xác định những hành động này sẽ thực hiện trong trường hợp sự cố rối loạn nghiêm trọng .

SLAs thực hiện bởi các chuyên gia hoặc các người chuyên nghiệp có hể bao gồm cả các biện pháp khắc phục hậu quả và hình phạt.

Tư vấn kiểm tra thâm nhập.

Thuê các chuyên gia pen-test đủ điều kiện về chất lượng của thử nghiệm thâm nhập.

Một thử nghiệm xâm nhập của một mạng công ty sẽ kiểm tra rất nhiều máy chủ khác nhau (vớimột số hệ điều hành khác nhau), kiến trúc mạng, chính sách và thủ tục.

Mỗi khu vực của mạng phải kiểm tra chuyên sâu

Kỹ năng pen-test không thể có được mà không có nhiều năm kinh nghiệm trong các lĩnh vực, chẳng hạn như phát triển, hệ thống quản lý, tư vấn.