TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG

1. Cơ bản về tấn công và phòng thủ hệ thống
   1. Khái niệm cơ bản

Một hacker có đạo đức tuân theo các quy trình tương tự như quy trình của một hacker độc hại. Các bước để giành và duy trì quyền truy cập vào hệ thống máy tính là tương tự nhau bất kể ý định của tin tặc.

* 1. Mô hình tấn công và phòng thủ hệ thống

Mô hình này giúp các tổ chức hiểu được các mối đe dọa khác nhau có thể xảy ra ở mọi giai đoạn của một cuộc tấn công và các biện pháp đối phó cần thiết để chống lại các cuộc tấn công đó. Ngoài ra, cung cấp cho các chuyên gia bảo mật cái nhìn sâu sắc rõ ràng về chiến lược tấn công mà kẻ thù sử dụng để có thể triển khai các mức kiểm soát bảo mật khác nhau nhằm bảo vệ cơ sở hạ tầng CNTT của tổ chức.

Phương pháp chuỗi tiêu diệt mạng là một thành phần của hệ thống phòng thủ dựa trên trí thông minh để xác định và ngăn chặn các hoạt động xâm nhập nguy hiểm. Phương pháp này giúp các chuyên gia bảo mật xác định các bước mà kẻ thù tuân theo để đạt được mục tiêu của họ.

Chuỗi tiêu diệt trên mạng là một khuôn khổ được phát triển để bảo vệ không gian mạng dựa trên khái niệm chuỗi tiêu diệt quân sự. Phương pháp này nhằm mục đích chủ động tăng cường khả năng phát hiện và phản ứng xâm nhập. Chuỗi tiêu diệt mạng được trang bị cơ chế bảo vệ bảy giai đoạn để giảm thiểu và giảm thiểu các mối đe dọa trên mạng.

Theo Lockheed Martin, các cuộc tấn công mạng có thể xảy ra theo 7 giai đoạn khác nhau, từ trinh sát cho đến hoàn thành mục tiêu cuối cùng. Sự hiểu biết về phương pháp chuỗi tiêu diệt mạng giúp các chuyên gia bảo mật tận dụng các biện pháp kiểm soát bảo mật ở các giai đoạn khác nhau của một cuộc tấn công và giúp họ ngăn chặn cuộc tấn công trước khi nó thành công. Nó cũng cung cấp cái nhìn sâu sắc hơn về các giai đoạn tấn công, giúp hiểu trước các TTP của đối thủ.

* 1. Quy trình tấn công hệ thống

1. Reconnaissance:- Là bước thu thập thông tin có liên quan đến victim bằng cách dùng tool dùng để dò quét,…

2. Weaponization:- Dựa vào những thông tin có được từ bước Reconnaissance chẳng hạn như các lỗ hổng. Sau đó hacker sẽ tạo phần mềm độc hại dựa vào những thông tin có được

3. Delivery:- Đây là giai đoạn phân phối, hacker dùng những gì đã tạo ở bước trên và tiến hành phân phối bằng nhiều cách, chẳng hạn phishing email có chứa malware

4. Exploitation:- Đây là giai đoạn khai thác sau khi đã Delivery malware, lợi dụng lỗ hổng để vào sâu vào trong hệthống.

5. Installation:- Giai đoạn này hacker sẽ cố cài đặt malware vào hệ thống mạng victim để chiếm quyền kiểm soát

6. Command and Control:- Giai đoạn này hacker sẽ kết nối với malware đã cài đặt để điều khiển các công cụ thực hiện mục tiêucủa nó.

7. Actions on Objectives:- Bước này tùy thuộc vào mục đích của hacker khi tấn công vào mạng có thể DDos, đánh cắp data, mã hóa tống tiền.

* 1. Cơ sở pháp lý

Luật pháp là một hệ thống các quy tắc và hướng dẫn được thực thi bởi một quốc gia hoặc cộng đồng cụ thể để điều chỉnh hành vi. Tiêu chuẩn là một "tài liệu được thiết lập theo sự đồng thuận và được phê duyệt bởi một cơ quan được công nhận cung cấp, để sử dụng chung và lặp đi lặp lại, các quy tắc, hướng dẫn hoặc đặc điểm cho các hoạt động hoặc kết quả của chúng, nhằm đạt được mức độ trật tự tối ưu trong một bối cảnh nhất định ." Phần này đề cập đến các luật và tiêu chuẩn khác nhau liên quan đến bảo mật thông tin ở các quốc gia khác nhau.

**Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS)**

Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) là một tiêu chuẩn bảo mật thông tin độc quyền dành cho các tổ chức xử lý thông tin chủ thẻ cho thẻ ghi nợ, tín dụng, trả trước, ví điện tử, thẻ ATM và thẻ POS chính. Tiêu chuẩn này cung cấp các tiêu chuẩn và tài liệu hỗ trợ mạnh mẽ và toàn diện để tăng cường bảo mật dữ liệu thẻ thanh toán. Những tài liệu này bao gồm khung thông số kỹ thuật, công cụ, phép đo và tài nguyên hỗ trợ để giúp các tổ chức đảm bảo xử lý an toàn thông tin chủ thẻ. PCI DSS áp dụng cho tất cả các thực thể liên quan đến xử lý thẻ thanh toán, bao gồm người bán, bộ xử lý, người mua, nhà phát hành và nhà cung cấp dịch vụ, cũng như tất cả các thực thể khác lưu trữ, xử lý hoặc truyền dữ liệu chủ thẻ. PCI DSS bao gồm một bộ yêu cầu tối thiểu để bảo vệ dữ liệu của chủ thẻ. Hội đồng tiêu chuẩn bảo mật ngành thẻ thanh toán (PCI) đã phát triển và duy trì tổng quan cấp cao về các yêu cầu PCI DSS.

Việc không đáp ứng các yêu cầu PCI DSS có thể dẫn đến bị phạt tiền hoặc chấm dứt đặc quyền xử lý thẻ thanh toán.

**ISO/IEC 27001:2013**

ISO/IEC 27001:2013 quy định các yêu cầu để thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý bảo mật thông tin trong bối cảnh của một tổ chức. Nó bao gồm các yêu cầu để đánh giá và xử lý các rủi ro bảo mật thông tin phù hợp với nhu cầu của tổ chức.

Quy định này nhằm mục đích phù hợp cho một số mục đích sử dụng khác nhau, bao gồm:

* Sử dụng trong các tổ chức để xây dựng các yêu cầu và mục tiêu bảo mật
* Sử dụng trong các tổ chức như một cách để đảm bảo rằng các rủi ro bảo mật được quản lý hiệu quả về mặt chi phí
* Sử dụng trong các tổ chức để đảm bảo tuân thủ luật pháp và quy định
* Xác định các quy trình quản lý bảo mật thông tin mới
* Xác định và làm rõ các quy trình quản lý bảo mật thông tin hiện có
* Sử dụng bởi ban quản lý của các tổ chức để xác định trạng thái của các hoạt động quản lý bảo mật thông tin
* Triển khai bảo mật thông tin hỗ trợ kinh doanh
* Tổ chức sử dụng để cung cấp thông tin liên quan về bảo mật thông tin cho khách hàng

**Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế (HIPAA)**

Quy tắc về quyền riêng tư của HIPAA cung cấp các biện pháp bảo vệ của liên bang đối với thông tin sức khỏe có thể nhận dạng cá nhân do các thực thể được bảo hiểm và đối tác kinh doanh của họ nắm giữ, đồng thời trao cho bệnh nhân nhiều quyền đối với thông tin đó. Đồng thời, Quy tắc Quyền riêng tư cho phép tiết lộ thông tin sức khỏe cần thiết cho việc chăm sóc bệnh nhân và các mục đích cần thiết khác.

Quy tắc bảo mật chỉ định một loạt các biện pháp bảo vệ hành chính, vật lý và kỹ thuật cho các thực thể được bảo vệ và các đối tác kinh doanh của họ sử dụng để đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin sức khỏe được bảo vệ bằng điện tử.

Văn phòng dân quyền đã triển khai Quy chế và Quy tắc Đơn giản hóa Hành chính của HIPAA, như được thảo luận dưới đây:

* Giao dịch điện tử và tiêu chuẩn bộ mã

Giao dịch là trao đổi điện tử liên quan đến việc chuyển thông tin giữa hai bên cho các mục đích cụ thể. Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế năm 1996 (HIPAA) đã chỉ định một số loại tổ chức nhất định là thực thể được bảo hiểm, bao gồm các chương trình bảo hiểm sức khỏe, trung tâm thanh toán bù trừ chăm sóc sức khỏe và một số nhà cung cấp dịch vụ chăm sóc sức khỏe. Trong các quy định của HIPAA, Bộ trưởng Bộ Y tế và Dịch vụ Nhân sinh (HHS) đã thông qua một số giao dịch tiêu chuẩn nhất định cho Trao đổi Dữ liệu Điện tử (EDI) về dữ liệu chăm sóc sức khỏe. Các giao dịch này là yêu cầu và thông tin gặp phải, tư vấn thanh toán và chuyển tiền, trạng thái yêu cầu, tính đủ điều kiện, đăng ký và hủy đăng ký, giới thiệu và ủy quyền, điều phối các lợi ích và thanh toán phí bảo hiểm. Theo HIPAA, nếu một thực thể được điều chỉnh thực hiện điện tử một trong các giao dịch được thông qua, họ phải sử dụng tiêu chuẩn được thông qua-từ ASC, X12N hoặc NCPDP (đối với một số giao dịch dược phẩm). Các thực thể được bảo hiểm phải tuân thủ các yêu cầu về nội dung và định dạng của từng giao dịch. Mọi nhà cung cấp thực hiện kinh doanh điện tử đều phải sử dụng các giao dịch chăm sóc sức khỏe, bộ mã và số nhận dạng giống nhau.

* Quy tắc bảo vệ sự riêng tư

Quy tắc về quyền riêng tư của HIPAA thiết lập các tiêu chuẩn quốc gia để bảo vệ hồ sơ y tế của mọi người và thông tin sức khỏe cá nhân khác, đồng thời áp dụng cho các chương trình bảo hiểm sức khỏe, trung tâm thanh toán bù trừ chăm sóc sức khỏe và nhà cung cấp dịch vụ chăm sóc sức khỏe thực hiện một số giao dịch chăm sóc sức khỏe bằng điện tử. Quy tắc yêu cầu các biện pháp bảo vệ thích hợp để bảo vệ quyền riêng tư của thông tin sức khỏe cá nhân. Nó đặt ra các giới hạn và điều kiện về việc sử dụng và tiết lộ có thể được thực hiện đối với thông tin đó mà không có sự cho phép của bệnh nhân. Quy tắc này cũng trao cho bệnh nhân các quyền đối với thông tin sức khỏe của họ, bao gồm quyền kiểm tra và lấy một bản sao hồ sơ sức khỏe của họ và yêu cầu chỉnh sửa.

* Quy tắc bảo mật

Quy tắc bảo mật HIPAA thiết lập các tiêu chuẩn quốc gia để bảo vệ thông tin sức khỏe cá nhân điện tử của các cá nhân được tạo, nhận, sử dụng hoặc duy trì bởi một thực thể được bảo hiểm. Quy tắc bảo mật yêu cầu các biện pháp bảo vệ hành chính, vật lý và kỹ thuật phù hợp để đảm bảo tính bảo mật, tính toàn vẹn và an ninh của thông tin sức khỏe được bảo vệ bằng điện tử.

* Tiêu chuẩn định danh nhà tuyển dụng

HIPAA yêu cầu mỗi chủ lao động phải có một số quốc gia tiêu chuẩn để xác định họ trên các giao dịch tiêu chuẩn.

* Tiêu chuẩn nhận dạng nhà cung cấp quốc gia (NPI)

Mã định danh Nhà cung cấp Quốc gia (NPI) là một Tiêu chuẩn Đơn giản hóa Hành chính của HIPAA. NPI là một số nhận dạng duy nhất được chỉ định cho các nhà cung cấp dịch vụ chăm sóc sức khỏe được bảo hiểm. Các nhà cung cấp dịch vụ chăm sóc sức khỏe được bảo hiểm và tất cả các chương trình sức khỏe và trung tâm thanh toán bù trừ chăm sóc sức khỏe phải sử dụng NPI trong các giao dịch hành chính và tài chính được thông qua theo HIPAA. NPI là một mã định danh số 10 vị trí, không có thông tin tình báo (số có 10 chữ số). Điều này có nghĩa là các con số không mang thông tin khác về các nhà cung cấp dịch vụ chăm sóc sức khỏe, chẳng hạn như tiểu bang nơi họ sinh sống hoặc chuyên môn y tế của họ.

* Quy tắc thực thi

Quy tắc Thực thi HIPAA bao gồm các điều khoản liên quan đến việc tuân thủ và điều tra, cũng như việc áp dụng các hình phạt tiền tệ dân sự đối với hành vi vi phạm Quy tắc Đơn giản hóa Hành chính của HIPAA và thủ tục điều trần.

**Đạo luật Sarbanes Oxley (SOX)**

Được ban hành vào năm 2002, Đạo luật Sarbanes-Oxley nhằm mục đích bảo vệ công chúng và các nhà đầu tư bằng cách tăng tính chính xác và độ tin cậy của các thông tin công bố của công ty. Đạo luật này không giải thích cách một tổ chức phải lưu trữ hồ sơ nhưng mô tả các hồ sơ mà tổ chức phải lưu trữ và thời hạn lưu trữ của chúng. Đạo luật bắt buộc thực hiện một số cải cách để nâng cao trách nhiệm của công ty, tăng cường công khai tài chính và chống gian lận kế toán và doanh nghiệp.

Các yêu cầu và quy định chính của SOX được sắp xếp thành 11 Mục:

* Mục I: Ban giám sát kế toán công ty đại chúng (PCAOB)

Mục I bao gồm chín phần và thành lập Ban Giám sát Kế toán Công ty Đại chúng để giám sát độc lập các công ty kế toán công cung cấp dịch vụ kiểm toán ("kiểm toán viên"). Nó cũng tạo ra một ban giám sát trung tâm được giao nhiệm vụ đăng ký dịch vụ kiểm toán, xác định các quy trình và thủ tục cụ thể cho kiểm toán tuân thủ, kiểm tra và lập chính sách về hành vi và kiểm soát chất lượng, đồng thời thực thi việc tuân thủ các nhiệm vụ cụ thể của SOX.

* Mục II: Kiểm toán độc lập

Mục II bao gồm chín phần và thiết lập các tiêu chuẩn cho sự độc lập của kiểm toán viên bên ngoài để hạn chế xung đột lợi ích. Nó cũng giải quyết các yêu cầu phê duyệt kiểm toán viên mới, luân chuyển đối tác kiểm toán và yêu cầu báo cáo kiểm toán viên. Nó hạn chế các công ty kiểm toán cung cấp các dịch vụ phi kiểm toán (chẳng hạn như tư vấn) cho cùng một khách hàng.

* Mục III: Trách Nhiệm Doanh Nghiệp

Mục III bao gồm tám phần và yêu cầu các giám đốc điều hành cấp cao chịu trách nhiệm cá nhân về tính chính xác và đầy đủ của các báo cáo tài chính doanh nghiệp. Nó xác định sự tương tác giữa các kiểm toán viên bên ngoài và ủy ban kiểm toán của công ty và quy định trách nhiệm của các cán bộ công ty về tính chính xác và hợp lệ của các báo cáo tài chính của công ty. Nó liệt kê các giới hạn cụ thể đối với hành vi của các quan chức doanh nghiệp và mô tả các hình thức tước quyền lợi cụ thể và các hình phạt dân sự đối với việc không tuân thủ.

* Mục IV: Tăng cường Tiết lộ Tài chính

Mục IV bao gồm chín phần. Nó mô tả các yêu cầu báo cáo nâng cao đối với các giao dịch tài chính, bao gồm các giao dịch ngoại bảng, số liệu theo mẫu và các giao dịch chứng khoán của các quan chức công ty. Nó yêu cầu các biện pháp kiểm soát nội bộ để đảm bảo tính chính xác của các báo cáo tài chính và công bố thông tin, đồng thời yêu cầu cả kiểm toán và báo cáo về các biện pháp kiểm soát đó. Nó cũng yêu cầu báo cáo kịp thời về những thay đổi quan trọng trong điều kiện tài chính và đánh giá nâng cao cụ thể về các báo cáo của công ty bởi SEC hoặc các đại lý của nó.

* Mục V: Xung đột lợi ích của nhà phân tích

Mục V chỉ bao gồm một phần thảo luận về các biện pháp được thiết kế để giúp khôi phục niềm tin của nhà đầu tư vào báo cáo của các nhà phân tích chứng khoán. Nó xác định quy tắc ứng xử cho các nhà phân tích chứng khoán và yêu cầu họ tiết lộ mọi xung đột lợi ích có thể biết được.

* Mục VI: Nguồn lực và Thẩm quyền của Ủy ban

Mục VI bao gồm bốn phần và xác định các thông lệ nhằm khôi phục niềm tin của nhà đầu tư đối với các nhà phân tích chứng khoán. Nó cũng xác định thẩm quyền của SEC để kiểm duyệt hoặc cấm các chuyên gia chứng khoán hành nghề và xác định các điều kiện để cấm một người hành nghề với tư cách là nhà môi giới, cố vấn hoặc đại lý.

* Mục VII: Nghiên cứu và Báo cáo

Mục VII bao gồm năm phần và yêu cầu Tổng kiểm soát và Ủy ban Chứng khoán và Hối đoái (SEC) thực hiện các nghiên cứu khác nhau và báo cáo những phát hiện của họ. Các nghiên cứu và báo cáo bắt buộc bao gồm tác động của việc hợp nhất các công ty kế toán công, vai trò của các cơ quan xếp hạng tín dụng trong hoạt động của thị trường chứng khoán, vi phạm chứng khoán, hành động thực thi và liệu các ngân hàng đầu tư có hỗ trợ Enron, Global Crossing và các tổ chức khác thao túng thu nhập hay không và làm xáo trộn các điều kiện tài chính thực sự.

* Mục VIII: Trách nhiệm giải trình đối với gian lận hình sự và doanh nghiệp

Mục VIII, còn được gọi là "Đạo luật trách nhiệm giải trình về gian lận hình sự và doanh nghiệp năm 2002," bao gồm bảy phần. Nó mô tả các hình phạt hình sự cụ thể đối với việc thao túng, phá hủy hoặc thay đổi hồ sơ tài chính hoặc can thiệp vào các cuộc điều tra, đồng thời cung cấp các biện pháp bảo vệ nhất định cho người tố cáo.

* Mục IX: Tăng cường hình phạt cho tội phạm cổ áo trắng

Mục IX, còn được gọi là "Đạo luật tăng cường hình phạt cho tội phạm cổ áo trắng năm 2002," bao gồm sáu phần. Mục này làm tăng hình phạt hình sự liên quan đến âm mưu và tội phạm cổ cồn trắng. Nó khuyến nghị các hướng dẫn kết án mạnh mẽ hơn và đặc biệt bổ sung việc không chứng nhận các báo cáo tài chính của công ty là một tội hình sự.

* Mục X: Tờ khai thuế doanh nghiệp

Mục X bao gồm một phần quy định rằng Giám đốc điều hành phải ký vào tờ khai thuế của công ty.

* Mục XI: Trách nhiệm giải trình gian lận của công ty

Mục XI bao gồm bảy phần. Mục 1101 đề xuất tên sau đây cho Mục: "Đạo luật trách nhiệm giải trình gian lận của công ty năm 2002." Nó xác định hành vi gian lận của công ty và giả mạo hồ sơ là tội hình sự và kết hợp các tội đó với các hình phạt cụ thể. Nó cũng sửa đổi các hướng dẫn kết án và tăng cường hình phạt. Làm như vậy cho phép SEC tạm thời đóng băng các giao dịch hoặc khoản thanh toán "lớn" hoặc "bất thường".

**Đạo luật bản quyền kỹ thuật số thiên niên kỷ (DMCA)**

DMCA là luật bản quyền của Hoa Kỳ thực thi hai hiệp ước năm 1996 của Tổ chức Sở hữu Trí tuệ Thế giới (WIPO): Hiệp ước Bản quyền WIPO và Hiệp ước Biểu diễn và Bản ghi âm của WIPO. Để thực hiện các nghĩa vụ theo hiệp ước của Hoa Kỳ, DMCA xác định các quy định cấm hợp pháp đối với việc lách các biện pháp bảo vệ bằng công nghệ mà chủ sở hữu bản quyền sử dụng để bảo vệ tác phẩm của họ và đối với việc xóa hoặc thay đổi thông tin quản lý bản quyền. DMCA chứa năm mục:

* Mục I: THỰC HIỆN HIỆP ĐỊNH WIPO

Mục I thực hiện các hiệp ước WIPO. Đầu tiên, nó thực hiện một số sửa đổi kỹ thuật đối với luật pháp Hoa Kỳ để cung cấp các tài liệu tham khảo và liên kết phù hợp với các điều ước. Thứ hai, nó tạo ra hai điều cấm mới trong Mục 17 của Bộ luật Hoa Kỳ - một là phá vỡ các biện pháp công nghệ được sử dụng bởi chủ sở hữu bản quyền để bảo vệ tác phẩm của họ và một là giả mạo thông tin quản lý bản quyền - và bổ sung các biện pháp dân sự và hình phạt hình sự nếu vi phạm các điều cấm.

* Mục II: GIỚI HẠN TRÁCH NHIỆM VI PHẠM BẢN QUYỀN TRỰC TUYẾN

Mục II của DMCA bổ sung mục 512 mới vào Đạo luật bản quyền để tạo ra bốn giới hạn mới về trách nhiệm pháp lý đối với hành vi vi phạm bản quyền của các nhà cung cấp dịch vụ trực tuyến. Nhà cung cấp dịch vụ căn cứ vào những hạn chế này dựa trên bốn loại hành vi sau:

* + Thông tin liên lạc tạm thời
  + Bộ nhớ đệm hệ thống
  + Lưu trữ thông tin do người dùng định hướng trên hệ thống hoặc mạng
  + Công cụ định vị thông tin

Mục 512 mới cũng bao gồm các quy tắc đặc biệt liên quan đến việc áp dụng các hạn chế này đối với các tổ chức giáo dục phi lợi nhuận.

* Mục III: BẢO TRÌ HOẶC SỬA CHỮA MÁY TÍNH

Mục III của DMCA cho phép chủ sở hữu bản sao của chương trình sao chép hoặc điều chỉnh khi cần thiết để sử dụng chương trình kết hợp với máy tính. Việc sửa đổi cho phép chủ sở hữu hoặc người thuê máy tính tạo hoặc cho phép tạo một bản sao của chương trình máy tính trong quá trình bảo trì hoặc sửa chữa máy tính đó.

* Mục IV: NHỮNG QUY ĐỊNH KHÁC

Mục IV có sáu điều khoản linh tinh. Điều khoản thứ nhất thông báo về việc làm rõ thẩm quyền của Cục bản quyền tác giả; quyền thứ hai miễn trừ cho việc tạo "bản ghi tạm thời"; thứ ba thúc đẩy nghiên cứu bằng giáo dục từ xa; thứ tư cung cấp miễn trừ cho các Thư viện và Lưu trữ Phi lợi nhuận; điều khoản thứ năm cho phép Sửa đổi Webcasting đối với Quyền biểu diễn kỹ thuật số trong Bản ghi âm và cuối cùng, điều khoản thứ sáu giải quyết những lo ngại về khả năng của các nhà biên kịch, đạo diễn và diễn viên màn ảnh trong việc thu được các khoản thanh toán còn lại cho việc khai thác các hình ảnh chuyển động trong các tình huống mà nhà sản xuất không có có thể thực hiện các khoản thanh toán này lâu hơn.

* Mục V: BẢO VỆ MỘT SỐ THIẾT KẾ GỐC

Mục V của DMCA, cho phép Đạo luật bảo vệ thiết kế thân tàu (VHDPA). Đạo luật này tạo ra một hệ thống mới để bảo vệ các thiết kế ban đầu của một số vật phẩm hữu ích giúp cho vật phẩm đó có vẻ ngoài hấp dẫn hoặc khác biệt. Đối với các mục đích của VHDPA, "các vật phẩm hữu ích" được giới hạn ở thân tàu (bao gồm cả boong) của các tàu không dài hơn 200 feet.

**Đạo luật quản lý bảo mật thông tin liên bang (FISMA)**

Đạo luật quản lý bảo mật thông tin liên bang năm 2002 được ban hành để tạo ra một số tiêu chuẩn và hướng dẫn bảo mật chính theo yêu cầu của luật pháp Quốc hội. FISMA cung cấp một khuôn khổ toàn diện để đảm bảo tính hiệu quả của các biện pháp kiểm soát an ninh thông tin đối với các nguồn thông tin hỗ trợ các hoạt động và tài sản của liên bang. Nó yêu cầu mỗi cơ quan liên bang phát triển, lập tài liệu và triển khai chương trình toàn cơ quan để cung cấp bảo mật thông tin cho thông tin và hệ thống thông tin hỗ trợ các hoạt động và tài sản của cơ quan, bao gồm cả những thứ được cung cấp hoặc quản lý bởi cơ quan, nhà thầu hoặc người khác nguồn. Khung FISMA bao gồm:

* Tiêu chuẩn phân loại thông tin và hệ thống thông tin theo nhiệm vụ tác động
* Tiêu chuẩn về yêu cầu bảo mật tối thiểu đối với thông tin và hệ thống thông tin
* Hướng dẫn lựa chọn biện pháp kiểm soát an ninh phù hợp cho hệ thống thông tin
* Hướng dẫn đánh giá các biện pháp kiểm soát an ninh trong hệ thống thông tin và xác định hiệu quả của chúng
* Hướng dẫn cấp phép bảo mật hệ thống thông tin

Câu hỏi và bài tập

1. Thu thập thông tin
   1. Khái niệm cơ bản

**Khái niệm thu thập thông tin**

Hack đạo đức về bản chất là hợp pháp và được thực hiện để đánh giá tính bảo mật của cơ sở hạ tầng CNTT của tổ chức mục tiêu với sự đồng ý của họ. Thu thập thông tin, nơi kẻ tấn công cố gắng thu thập thông tin về mục tiêu, là bước đầu tiên trong hack đạo đức. Bước này đóng vai trò như một giai đoạn chuẩn bị cho kẻ tấn công, những kẻ cần thu thập càng nhiều thông tin càng tốt để dễ dàng tìm cách xâm nhập vào mạng mục tiêu.

**Thu thập thông tin là gì?**

Một khía cạnh thiết yếu của thu thập thông tin là xác định mức độ rủi ro liên quan đến thông tin có thể truy cập công khai của tổ chức. Thu thập thông tin, bước đầu tiên trong hack đạo đức, đề cập đến quá trình thu thập thông tin về mạng mục tiêu và môi trường của nó. Sử dụng thu thập thông tin, bạn có thể tìm thấy một số cơ hội để thâm nhập và đánh giá mạng của tổ chức mục tiêu.

Sau khi bạn hoàn thành quy trình đánh dấu vết theo phương pháp, bạn sẽ có được bản thiết kế hồ sơ bảo mật của tổ chức mục tiêu. Ở đây, thuật ngữ "bản thiết kế" đề cập đến hồ sơ hệ thống duy nhất của tổ chức mục tiêu có được bằng cách theo dõi.

Không có một phương pháp duy nhất nào cho việc đánh dấu vết, vì thông tin có thể được truy tìm theo một số cách. Tuy nhiên, hoạt động này rất quan trọng vì bạn cần thu thập tất cả thông tin quan trọng về tổ chức mục tiêu trước khi bắt đầu giai đoạn hack. Vì lý do này, thu thập thông tin cần phải được thực hiện một cách có tổ chức. Thông tin được thu thập trong bước này giúp phát hiện ra các lỗ hổng tồn tại trong mạng mục tiêu và xác định các cách khác nhau để khai thác các lỗ hổng này.

**Các loại thu thập thông tin**

Thu thập thông tin có thể được phân loại thành thu thập thông tin bị động và thu thập thông tin chủ động.

* Thu thập thông tin bị động

Thu thập thông tin bị động liên quan đến việc thu thập thông tin về mục tiêu mà không cần tương tác trực tiếp. Nó chủ yếu hữu ích khi các hoạt động thu thập thông tin không bị mục tiêu phát hiện. Việc thực hiện thu thập thông tin bị động là khó khăn về mặt kỹ thuật, vì lưu lượng truy cập chủ động không được gửi đến tổ chức mục tiêu từ máy chủ hoặc máy chủ hoặc dịch vụ ẩn danh qua Internet. Chúng tôi chỉ có thể thu thập thông tin được lưu trữ và lưu trữ về mục tiêu bằng cách sử dụng các công cụ tìm kiếm, các trang mạng xã hội, v.v.

Các kỹ thuật thu thập thông tin bị động bao gồm:

* + Tìm kiếm thông tin qua công cụ tìm kiếm
  + Tìm Tên miền cấp cao nhất (TLD) và tên miền phụ của mục tiêu thông qua các dịch vụ web
  + Thu thập thông tin vị trí trên mục tiêu thông qua các dịch vụ web
  + Thực hiện tìm kiếm người sử dụng các trang mạng xã hội và dịch vụ tìm kiếm người
  + Thu thập thông tin tài chính về mục tiêu thông qua các dịch vụ tài chính
  + Thu thập chi tiết cơ sở hạ tầng của tổ chức mục tiêu thông qua các trang web việc làm
  + Thu thập thông tin thông qua thu thập thông tin web sâu và tối
  + Xác định các hệ điều hành được sử dụng bởi tổ chức mục tiêu
  + Thực hiện tình báo cạnh tranh
  + Giám sát mục tiêu bằng các dịch vụ cảnh báo
  + thập thông tin qua các nhóm, diễn đàn, blog, nhóm tin NNTP Usenet
  + Thu thập thông tin thông qua kỹ thuật xã hội trên các trang mạng xã hội
  + Xác định các hệ điều hành được sử dụng bởi tổ chức mục tiêu
  + Thực hiện tình báo cạnh tranh
  + Giám sát mục tiêu bằng các dịch vụ cảnh báo
  + Thu thập thông tin qua các nhóm, diễn đàn, blog, nhóm tin NNTP Usenet
  + Thu thập thông tin thông qua kỹ thuật xã hội trên các trang mạng xã hội
  + Trích xuất thông tin về mục tiêu bằng cách sử dụng kho lưu trữ trên Internet
  + Thu thập thông tin bằng cách sử dụng các trang web hồ sơ doanh nghiệp
  + Giám sát lưu lượng truy cập trang web của mục tiêu
  + Theo dõi danh tiếng trực tuyến của mục tiêu
* Thu thập thông tin chủ động

Thu thập thông tin chủ động liên quan đến việc thu thập thông tin về mục tiêu với sự tương tác trực tiếp. Trong thu thập thông tin chủ động, mục tiêu có thể nhận ra quá trình thu thập thông tin đang diễn ra, khi chúng ta tương tác công khai với mạng mục tiêu. Thu thập thông tin chủ động đòi hỏi nhiều sự chuẩn bị hơn so với thu thập thông tin bị động, vì nó có thể để lại dấu vết có thể cảnh báo cho tổ chức mục tiêu.

* + Các kỹ thuật đánh dấu chủ động bao gồm:
  + Truy vấn máy chủ tên đã xuất bản của mục tiêu
  + Tìm kiếm các tập tin kỹ thuật số
  + Trích xuất các liên kết trang web và thu thập danh sách từ từ trang web mục tiêu
  + Trích xuất siêu dữ liệu của các tài liệu và tệp đã xuất bản
  + Thu thập thông tin trang web bằng cách sử dụng các công cụ sao chép và sao chép trang web
  + Thu thập thông tin qua theo dõi email
  + Thu hoạch danh sách email
  + Thực hiện tra cứu Whois
  + Trích xuất thông tin DNS
  + Thực hiện phân tích theo dõi
  + Thực hiện kỹ thuật xã hội

**Thông tin thu được trong Thu thập thông tin**

Các mục tiêu chính của thu thập thông tin bao gồm thu thập thông tin mạng, thông tin hệ thống và thông tin tổ chức của mục tiêu. Bằng cách tiến hành đánh dấu vết trên các cấp độ mạng khác nhau, bạn có thể thu được thông tin như khối mạng, địa chỉ IP cụ thể, chi tiết nhân viên, v.v. Những thông tin như vậy có thể giúp kẻ tấn công giành được quyền truy cập vào dữ liệu nhạy cảm hoặc thực hiện các cuộc tấn công khác nhau vào mạng mục tiêu.

* Thông tin về Tổ chức: Những thông tin như vậy về một tổ chức có sẵn trên trang web của tổ chức đó. Ngoài ra, bạn có thể truy vấn tên miền của mục tiêu đối với cơ sở dữ liệu Whois và lấy thông tin có giá trị. Các thông tin được thu thập bao gồm:
  + Thông tin chi tiết về nhân viên (tên nhân viên, địa chỉ liên lạc, chức danh và kinh nghiệm làm việc)
  + Địa chỉ và số điện thoại di động/điện thoại
  + Thông tin chi nhánh và vị trí
  + Các đối tác của tổ chức
  + Liên kết web đến các trang web khác có liên quan đến công ty
  + Bối cảnh của tổ chức
  + Công nghệ web
  + Các bài báo, thông cáo báo chí và các tài liệu liên quan
  + Văn bản pháp luật liên quan đến tổ chức
  + Bằng sáng chế và thương hiệu liên quan đến tổ chức

Những kẻ tấn công có thể truy cập thông tin tổ chức và sử dụng thông tin đó để xác định nhân sự chủ chốt và khởi chạy các cuộc tấn công kỹ thuật xã hội để trích xuất dữ liệu nhạy cảm về thực thể.

* Thông tin mạng: Bạn có thể thu thập thông tin mạng bằng cách thực hiện phân tích cơ sở dữ liệu Whois, theo dõi định tuyến, v.v. Các thông tin được thu thập bao gồm:
  + Tên miền và tên miền phụ
  + Khối mạng
  + Cấu trúc liên kết mạng, bộ định tuyến đáng tin cậy và tường lửa
  + Địa chỉ IP của các hệ thống có thể truy cập
  + Hồ sơ Whois
  + Bản ghi DNS và thông tin liên quan
* Thông tin hệ thống: Bạn có thể thu thập thông tin hệ thống bằng cách thực hiện theo dõi mạng, theo dõi DNS, theo dõi trang web, theo dõi email, v.v. Các thông tin được thu thập bao gồm:
  + Hệ điều hành máy chủ web
  + Vị trí của máy chủ web
  + Địa chỉ email có sẵn công khai
  + Tên người dùng, mật khẩu, v.v.

**Mục tiêu của Footprinting**

Để xây dựng chiến lược tấn công, kẻ tấn công cần thu thập thông tin về mạng của tổ chức mục tiêu. Sau đó, họ sử dụng những thông tin đó để xác định cách dễ dàng nhất để vượt qua vành đai an ninh của tổ chức. Như đã đề cập trước đây, phương pháp đánh dấu dấu vết giúp dễ dàng thu thập thông tin về tổ chức mục tiêu; điều này đóng một vai trò quan trọng trong quá trình hack.

**Thu thập thông tin giúp:**

* Biết trạng thái bảo mật: Thực hiện thu thập thông tin trên tổ chức mục tiêu cung cấp hồ sơ đầy đủ về trạng thái bảo mật của tổ chức. Sau đó, tin tặc có thể phân tích báo cáo để xác định các lỗ hổng trong tình trạng bảo mật của tổ chức mục tiêu và xây dựng kế hoạch tấn công phù hợp.
* Giảm phạm vi tập trung: Bằng cách sử dụng kết hợp các công cụ và kỹ thuật, kẻ tấn công có thể lấy một thực thể không xác định (ví dụ: Tổ chức XYZ) và giảm phạm vi đó thành một phạm vi tên miền, khối mạng và địa chỉ IP riêng lẻ của các hệ thống được kết nối trực tiếp với Internet, cũng như nhiều chi tiết khác liên quan đến tình hình bảo mật của nó.
* Xác định các lỗ hổng bảo mật: Thu thập thông tin chi tiết cung cấp thông tin tối đa về tổ chức mục tiêu. Nó cho phép kẻ tấn công xác định các lỗ hổng trong hệ thống mục tiêu để chọn cách khai thác thích hợp. Những kẻ tấn công có thể xây dựng cơ sở dữ liệu thông tin của riêng chúng về các điểm yếu bảo mật của tổ chức mục tiêu. Cơ sở dữ liệu như vậy sau đó có thể giúp xác định liên kết yếu nhất trong vành đai bảo mật của tổ chức.
* Vẽ bản đồ mạng: Kết hợp các kỹ thuật dấu vết với các công cụ như Tracert cho phép kẻ tấn công tạo ra các biểu diễn sơ đồ về sự hiện diện mạng của tổ chức đích. Cụ thể, nó cho phép kẻ tấn công vẽ bản đồ hoặc phác thảo cơ sở hạ tầng mạng của tổ chức mục tiêu để biết về môi trường thực tế mà chúng sẽ đột nhập. Bản đồ mạng sẽ mô tả sự hiểu biết của kẻ tấn công về thu thập thông tin Internet của mục tiêu. Các sơ đồ mạng này có thể hướng dẫn kẻ tấn công thực hiện một cuộc tấn công.

**Các mối đe dọa về thu thập thông tin**

Những kẻ tấn công thực hiện thu thập thông tin như bước đầu tiên của bất kỳ cuộc tấn công nào vào hệ thống thông tin. Trong giai đoạn này, những kẻ tấn công cố gắng thu thập thông tin có giá trị ở cấp hệ thống như chi tiết tài khoản, hệ điều hành và các phiên bản phần mềm khác, tên máy chủ, chi tiết lược đồ cơ sở dữ liệu, v.v., những thông tin này sẽ hữu ích trong quá trình hack.

Sau đây là các loại mối đe dọa có thể thực hiện được thông qua thu thập thông tin:

* Kỹ thuật xã hội: Không sử dụng bất kỳ phương pháp xâm nhập nào, tin tặc trực tiếp và gián tiếp thu thập thông tin thông qua thuyết phục và các phương tiện khác. Tin tặc thu thập thông tin quan trọng từ những nhân viên sẵn sàng không biết về ý định của tin tặc.
* Tấn công hệ thống và mạng: Footprinting cho phép kẻ tấn công thực hiện các cuộc tấn công hệ thống và mạng. Do đó, kẻ tấn công có thể thu thập thông tin liên quan đến cấu hình hệ thống của tổ chức mục tiêu, hệ điều hành đang chạy trên máy, v.v. Sử dụng thông tin này, kẻ tấn công có thể tìm thấy các lỗ hổng trong hệ thống đích và sau đó khai thác các lỗ hổng đó. Sau đó, họ có thể kiểm soát một hệ thống mục tiêu hoặc toàn bộ mạng.
* Rò rỉ thông tin: Rò rỉ thông tin gây ra mối đe dọa cho bất kỳ tổ chức nào. Nếu thông tin nhạy cảm của một thực thể rơi vào tay kẻ tấn công, chúng có thể thực hiện một cuộc tấn công dựa trên thông tin hoặc sử dụng nó để thu lợi tiền tệ.
* Mất quyền riêng tư: Thông qua thu thập thông tin, tin tặc có thể truy cập vào các hệ thống và mạng của tổ chức và thậm chí leo thang các đặc quyền lên cấp quản trị viên, dẫn đến mất quyền riêng tư cho toàn bộ tổ chức và cho từng nhân viên của tổ chức.
* Gián điệp doanh nghiệp: Gián điệp doanh nghiệp là mối đe dọa chính đối với các tổ chức, vì các đối thủ cạnh tranh thường cố gắng bảo mật dữ liệu nhạy cảm thông qua dấu vết. Thông qua cách tiếp cận này, các đối thủ cạnh tranh có thể tung ra các sản phẩm tương tự trên thị trường, thay đổi giá cả và nói chung là làm suy yếu vị thế thị trường của một tổ chức mục tiêu.
* Tổn thất kinh doanh: Thu thập thông tin có thể ảnh hưởng lớn đến các tổ chức như doanh nghiệp trực tuyến và các trang web thương mại điện tử khác cũng như các doanh nghiệp liên quan đến ngân hàng và tài chính. Hàng tỷ đô la bị mất mỗi năm do các cuộc tấn công nguy hiểm của tin tặc.
  1. Phương pháp thu thập thông tin

**Phương pháp thu thập thông tin**

Bây giờ bạn đã quen thuộc với các khái niệm về thu thập thông tin và các mối đe dọa tiềm ẩn, chúng ta sẽ thảo luận về phương pháp thu thập thông tin. Phương pháp đánh dấu thu thập thông tin là một quy trình thu thập thông tin về một tổ chức mục tiêu từ tất cả các nguồn có sẵn. Nó liên quan đến việc thu thập thông tin về một tổ chức mục tiêu, chẳng hạn như URL, vị trí, chi tiết cơ sở, số lượng nhân viên, phạm vi tên miền cụ thể, thông tin liên hệ và các thông tin liên quan khác. Những kẻ tấn công thu thập thông tin này từ các nguồn có thể truy cập công khai như công cụ tìm kiếm, trang mạng xã hội, cơ sở dữ liệu Whois, v.v.

Kỹ thuật thu thập thông tin:

* Thu thập thông tin thông qua các công cụ tìm kiếm
* Thu thập thông tin thông qua các dịch vụ web
* Thu thập thông tin thông qua các trang mạng xã hội
* Thu thập thông tin trang web
* Thu thập thông tin email
* Thu thập thông tin whois
* Thu thập thông tin DNS
* Thu thập thông tin mạng
* Thu thập thông tin thông qua kỹ thuật xã hội
  1. Kỹ thuật tấn công thăm dò
     1. Thu thập thông tin thông qua các công cụ tìm kiếm
* Thu thập thông tin bằng cách sử dụng các kỹ thuật hack nâng cao của Google
* Google Hacking Database (<https://www.exploit-db.com>)
* Thu thập thông tin bằng Tìm kiếm nâng cao của Google, Tìm kiếm hình ảnh nâng cao và Tìm kiếm hình ảnh đảo ngược
* Thu thập thông tin từ Công cụ tìm kiếm video
* Thu thập thông tin từ Meta Search Engines
* Thu thập thông tin từ Công cụ tìm kiếm FTP
* Thu thập thông tin từ các công cụ tìm kiếm IoT
  + 1. Thu thập thông tin thông qua các dịch vụ web
* Tìm tên miền cấp cao nhất (TLD) và tên miền phụ của công ty
* Công cụ tìm kiếm tên miền phụ của công ty
  1. Netcraft
  2. Sublist3r
  3. Pentest-Tools Tìm tên miền phụ (<https://pentest-tools.com>)
* Thu thập thông tin từ dịch vụ tài chính
* Thu thập thông tin bằng trang web hồ sơ doanh nghiệp
* Giám sát mục tiêu sử dụng cảnh báo
  1. Google Alerts
* Theo dõi danh tiếng trực tuyến của mục tiêu
* Thu thập thông tin bằng cách sử dụng Nhóm, Diễn đàn và Blog
* Thu thập Thông tin Sử dụng Nhóm tin NNTP Usenet
* Dịch vụ tìm người – Intelius (<https://www.intelius.com>)
* Thu thập thông tin từ LinkedIn
  1. theHarvester (<http://www.edge-security.com>)
* Thu thập thông tin thông qua các trang web việc làm
  + 1. Thu thập thông tin thông qua các trang mạng xã hội
* BuzzSumo
* Folowerwonk
* Sherlock
* Social Searcher
  + 1. Thu thập thông tin trang web
* Burf Suite
* Web Spiders
* Mirroring Entire Website
* Trích xuất thông tin trang web từ <https://archive.org>
* Trích xuất các đường link website
* Thu thập Từ điển từ website
* Trích xuất siêu dữ liệu của tài liệu công khai
* …
  + 1. Thu thập thông tin email
* Theo dõi liên lạc qua email
* Thu thập thông tin từ mục email
* Tools:
  + Infoga
  + eMailTrackerPro
    1. Thu thập thông tin whois
* Kết quả tra cứu Whois
* Tìm thông tin định vị địa lý IP
  + 1. Thu thập thông tin DNS
* Trích xuất thông tin DNS
* Tra cứu DNS đảo ngược
  + 1. Thu thập thông tin mạng
* Xác định phạm vi mạng
* Phân tích Traceroute
  + 1. Thu thập thông tin thông qua kỹ thuật xã hội
* Nghe lén
* Lướt vai
* Bới thùng rác
* Mạo danh
  1. Dò quét lỗ hổng bảo mật

Khái niệm

Quét là quá trình thu thập thông tin chi tiết bổ sung về mục tiêu bằng cách sử dụng các kỹ thuật trinh sát cực kỳ phức tạp và tích cực. Quét mạng đề cập đến một tập hợp các thủ tục được sử dụng để xác định máy chủ, cổng và dịch vụ trong mạng. Quét mạng cũng được sử dụng để khám phá các máy đang hoạt động trong mạng và xác định hệ điều hành đang chạy trên máy mục tiêu. Đây là một trong những giai đoạn thu thập thông tin tình báo quan trọng nhất đối với kẻ tấn công, cho phép kẻ tấn công tạo hồ sơ về tổ chức mục tiêu. Trong quá trình quét, kẻ tấn công cố gắng thu thập thông tin, bao gồm các địa chỉ IP cụ thể có thể được truy cập qua mạng, kiến trúc hệ thống và hệ điều hành của mục tiêu cũng như các cổng cùng với các dịch vụ tương ứng chạy trên mỗi máy tính.

Mục đích của việc quét là khám phá các kênh liên lạc có thể khai thác, thăm dò càng nhiều người nghe nhất có thể và theo dõi những thứ đáp ứng hoặc hữu ích cho nhu cầu cụ thể của kẻ tấn công. Trong giai đoạn quét của một cuộc tấn công, kẻ tấn công cố gắng tìm nhiều cách khác nhau để xâm nhập vào hệ thống mục tiêu. Kẻ tấn công cũng cố gắng khám phá thêm thông tin về hệ thống đích để xác định sự hiện diện của bất kỳ lỗi cấu hình nào. Kẻ tấn công sau đó sử dụng thông tin thu được để phát triển một chiến lược tấn công.

**Các loại quét**

Quét cổng - Liệt kê các cổng và dịch vụ đang mở. Quét cổng là quá trình kiểm tra các dịch vụ đang chạy trên máy tính đích bằng cách gửi một chuỗi các thông báo nhằm cố gắng đột nhập. Quét cổng liên quan đến việc kết nối hoặc thăm dò các cổng TCP và UDP của hệ thống đích để xác định xem các dịch vụ có đang chạy hay không. đang ở trạng thái lắng nghe. Trạng thái lắng nghe cung cấp thông tin về HĐH và ứng dụng hiện đang được sử dụng. Đôi khi, các dịch vụ đang hoạt động đang lắng nghe có thể cho phép người dùng trái phép định cấu hình sai hệ thống hoặc chạy phần mềm có lỗ hổng bảo mật.

Quét mạng - Liệt kê các máy chủ và địa chỉ IP đang hoạt động. Quét mạng là một thủ tục để xác định các máy chủ đang hoạt động trên mạng, để tấn công chúng hoặc đánh giá tính bảo mật của mạng.

Vulnerability Scanning Cho thấy sự hiện diện của các điểm yếu đã biết. Tính dễ bị tổn thương - quét là một phương pháp để kiểm tra xem một hệ thống có thể bị khai thác hay không bằng cách xác định các lỗ hổng của nó. Một trình quét lỗ hổng bao gồm một công cụ quét và một danh mục. Danh mục này bao gồm danh sách các tệp phổ biến có các lỗ hổng đã biết và các cách khai thác phổ biến cho một loạt máy chủ. Ví dụ, một trình quét lỗ hổng có thể tìm kiếm các tệp sao lưu hoặc khai thác duyệt thư mục. Công cụ quét duy trì logic để đọc danh sách khai thác, chuyển yêu cầu đến máy chủ web và phân tích các yêu cầu để đảm bảo an toàn cho máy chủ. Các công cụ này thường nhắm mục tiêu vào các lỗ hổng mà cấu hình máy chủ bảo mật có thể khắc phục dễ dàng thông qua các bản vá bảo mật được cập nhật và tài liệu web sạch.

Một tên trộm muốn đột nhập vào một ngôi nhà sẽ tìm kiếm các lối vào như cửa ra vào và cửa sổ. Đây thường là những điểm dễ bị tổn thương của ngôi nhà, vì chúng có thể dễ dàng tiếp cận. Khi nói đến hệ thống máy tính và mạng, cổng là cửa ra vào và cửa sổ của hệ thống mà kẻ xâm nhập sử dụng để truy cập. Một nguyên tắc chung cho các hệ thống máy tính là số lượng cổng mở trên hệ thống càng nhiều thì hệ thống càng dễ bị tấn công. Tuy nhiên, có những trường hợp trong đó một hệ thống có ít cổng mở hơn máy khác sẽ có mức độ dễ bị tổn thương cao hơn nhiều.

**Mục tiêu của việc quét mạng**

Càng có nhiều thông tin về một tổ chức mục tiêu, thì cơ hội biết được các lỗ hổng bảo mật của mạng càng cao và do đó, có được quyền truy cập trái phép vào mạng đó.

**Một số mục tiêu để quét mạng như sau:**

* Khám phá các máy chủ trực tiếp, địa chỉ IP và cổng mở của các máy chủ trực tiếp của mạng. Sử dụng các cổng mở, kẻ tấn công sẽ xác định phương tiện tốt nhất để xâm nhập vào hệ thống.
* Khám phá hệ điều hành và kiến trúc hệ thống của mục tiêu. Điều này còn được gọi là lấy dấu vân tay. Kẻ tấn công có thể xây dựng chiến lược tấn công dựa trên các lỗ hổng của HĐH.
* Khám phá các dịch vụ đang chạy/nghe trên hệ thống đích. Làm như vậy sẽ cung cấp cho kẻ tấn công dấu hiệu về các lỗ hổng (dựa trên dịch vụ) có thể bị khai thác để giành quyền truy cập vào hệ thống đích.
* Xác định các ứng dụng hoặc phiên bản cụ thể của một dịch vụ cụ thể.
* Xác định các lỗ hổng trong bất kỳ hệ thống mạng nào. Điều này giúp kẻ tấn công xâm phạm hệ thống hoặc mạng đích thông qua nhiều cách khai thác khác nhau.
  1. Kỹ thuật liệt kê

**Liệt kê là gì?**

Liệt kê là quá trình trích xuất tên người dùng, tên máy, tài nguyên mạng, chia sẻ và dịch vụ từ một hệ thống hoặc mạng. Trong giai đoạn liệt kê, kẻ tấn công tạo các kết nối tích cực với hệ thống và gửi các truy vấn trực tiếp để lấy thêm thông tin về mục tiêu. Kẻ tấn công sử dụng thông tin được thu thập bằng cách liệt kê để xác định các lỗ hổng trong bảo mật hệ thống, giúp chúng khai thác hệ thống mục tiêu. Đổi lại, phép liệt kê cho phép kẻ tấn công thực hiện các cuộc tấn công bằng mật khẩu để giành quyền truy cập trái phép vào tài nguyên hệ thống thông tin. Kỹ thuật liệt kê hoạt động trong môi trường mạng nội bộ.

Cụ thể, phép liệt kê cho phép kẻ tấn công thu thập các thông tin sau:

* Tài nguyên mạng
* Chia sẻ mạng
* Bảng định tuyến
* Cài đặt kiểm toán và dịch vụ
* SNMP và chi tiết tên miền đủ điều kiện (FQDN)
* Tên máy
* Người dùng và nhóm
* Ứng dụng và biểu ngữ

Trong quá trình liệt kê, những kẻ tấn công có thể tình cờ phát hiện ra một chia sẻ liên lạc giữa các quá trình (IPC) từ xa, chẳng hạn như IPC$ trong Windows, chúng có thể thăm dò thêm để kết nối với một chia sẻ quản trị bằng thông tin xác thực của quản trị viên và lấy thông tin đầy đủ về tệp- danh sách hệ thống mà chia sẻ đại diện.

Các mô-đun trước đã nêu bật cách những kẻ tấn công thu thập thông tin cần thiết về mục tiêu mà không có bất kỳ hoạt động bất hợp pháp nào. Tuy nhiên, các hoạt động điều tra có thể là bất hợp pháp tùy thuộc vào chính sách của tổ chức và các luật có hiệu lực. Một hacker hoặc pen tester có đạo đức phải luôn có được sự cho phép thích hợp trước khi thực hiện việc liệt kê.

**Kỹ thuật liệt kê**

Các kỹ thuật sau đây được sử dụng để trích xuất thông tin về mục tiêu.

* Trích xuất tên người dùng bằng ID email

Mỗi địa chỉ email chứa hai phần, tên người dùng và tên miền, ở định dạng "tên người dùng@tên miền."

* Trích xuất thông tin bằng mật khẩu mặc định

Nhiều tài nguyên trực tuyến cung cấp danh sách mật khẩu mặc định do nhà sản xuất gán cho sản phẩm của họ. Người dùng thường bỏ qua các đề xuất thay đổi tên người dùng và mật khẩu mặc định do nhà sản xuất hoặc nhà phát triển sản phẩm cung cấp. Điều này giúp kẻ tấn công dễ dàng liệt kê và khai thác hệ thống mục tiêu.

* Lực lượng vét cạn Active Directory

Microsoft Active Directory dễ bị liệt kê tên người dùng tại thời điểm xác minh đầu vào do người dùng cung cấp. Đây là lỗi thiết kế trong triển khai Microsoft Active Directory. Nếu người dùng bật tính năng "giờ đăng nhập" thì tất cả các nỗ lực xác thực dịch vụ đều dẫn đến các thông báo lỗi khác nhau. Những kẻ tấn công lợi dụng điều này để liệt kê tên người dùng hợp lệ. Kẻ tấn công thành công trong việc trích xuất tên người dùng hợp lệ có thể tiến hành một cuộc tấn công vét cạn để bẻ khóa các mật khẩu tương ứng.

* Trích xuất thông tin bằng DNS Zone Transfer

Quản trị viên mạng có thể sử dụng chuyển vùng DNS để sao chép dữ liệu DNS trên một số máy chủ DNS hoặc sao lưu các tệp DNS. Với mục đích này, quản trị viên cần thực hiện một yêu cầu chuyển vùng cụ thể tới máy chủ định danh. Nếu máy chủ định danh cho phép chuyển vùng, nó sẽ chuyển đổi tất cả tên DNS và địa chỉ IP do máy chủ đó lưu trữ thành văn bản ASCII.

Nếu quản trị viên mạng không định cấu hình máy chủ DNS đúng cách, chuyển vùng DNS có thể là một phương pháp hiệu quả để lấy thông tin về mạng của tổ chức. Thông tin này có thể bao gồm danh sách tất cả các máy chủ được đặt tên, vùng phụ và địa chỉ IP liên quan. Người dùng có thể thực hiện chuyển vùng DNS bằng các lệnh nslookup và dig.

* Trích xuất nhóm người dùng từ Windows

Để trích xuất các nhóm người dùng từ Windows, kẻ tấn công phải có ID đã đăng ký với tư cách là người dùng trong Active Directory. Sau đó, kẻ tấn công có thể trích xuất thông tin từ các nhóm mà người dùng là thành viên bằng cách sử dụng giao diện Windows hoặc phương pháp dòng lệnh.

* Trích xuất tên người dùng bằng SNMP

Những kẻ tấn công có thể dễ dàng đoán các chuỗi cộng đồng chỉ đọc hoặc đọc-ghi bằng cách sử dụng giao diện lập trình ứng dụng (API) SNMP để trích xuất tên người dùng.

* 1. Giải pháp phòng chống
     1. Phòng chống thu thập thông tin

Một số biện pháp đối phó với thu thập thông tin như sau:

* + Hạn chế quyền truy cập của nhân viên vào các trang mạng xã hội từ mạng của tổ chức
  + Cấu hình máy chủ web để tránh rò rỉ thông tin
  + Giáo dục nhân viên sử dụng bút danh trên blog, nhóm và diễn đàn
  + Không tiết lộ thông tin quan trọng trong thông cáo báo chí, báo cáo hàng năm, danh mục sản phẩm, v.v.
  + Giới hạn số lượng thông tin mà bạn đang xuất bản trên trang web/Internet
  + Sử dụng các kỹ thuật thu thập thông tin để khám phá và xóa mọi thông tin nhạy cảm có sẵn công khai
  + Ngăn các công cụ tìm kiếm lưu vào bộ nhớ đệm một trang web và sử dụng các dịch vụ đăng ký ẩn danh
  + Xây dựng và thực thi các chính sách bảo mật như chính sách bảo mật thông tin, chính sách mật khẩu, v.v., để điều chỉnh thông tin mà nhân viên có thể tiết lộ cho bên thứ ba
  + Đặt riêng DNS bên trong và bên ngoài hoặc sử dụng DNS phân tách và hạn chế chuyển vùng đến các máy chủ được ủy quyền
  + Vô hiệu hóa danh sách thư mục trong máy chủ web
  + Tiến hành đào tạo nâng cao nhận thức bảo mật định kỳ để giáo dục nhân viên về các thủ thuật và rủi ro kỹ thuật xã hội khác nhau
  + Chọn tham gia các dịch vụ bảo mật trên cơ sở dữ liệu tra cứu Whois
  + Tránh liên kết chéo cấp miền cho các nội dung quan trọng
  + Mã hóa và bảo vệ mật khẩu thông tin nhạy cảm
  + Không kích hoạt các giao thức không cần thiết
  + Luôn sử dụng bộ lọc TCP/IP và IPSec để bảo vệ chuyên sâu
  + Định cấu hình IIS để tránh lộ thông tin do lấy banner
  + Ẩn địa chỉ IP và thông tin liên quan bằng cách triển khai VPN hoặc giữ máy chủ đằng sau một proxy an toàn
  + Yêu cầu archive.org xóa lịch sử của trang web khỏi cơ sở dữ liệu lưu trữ
  + Giữ hồ sơ tên miền riêng tư
  + Đặt các tài liệu quan trọng như kế hoạch kinh doanh và tài liệu độc quyền ngoại tuyến để ngăn chặn việc khai thác
  + Đào tạo nhân viên để ngăn chặn các kỹ thuật và tấn công kỹ thuật xã hội
  + Vệ sinh các chi tiết được cung cấp cho các nhà đăng ký Internet để ẩn các chi tiết liên hệ trực tiếp của tổ chức
  + Vô hiệu hóa chức năng gắn thẻ địa lý trên máy ảnh để ngăn theo dõi vị trí địa lý
  + Tránh tiết lộ vị trí hoặc kế hoạch du lịch của một người trên các trang mạng xã hội
  + Tắt quyền truy cập định vị địa lý trên tất cả các thiết bị di động khi không cần thiết
  + Đảm bảo rằng không có thông tin quan trọng nào như kế hoạch chiến lược, thông tin sản phẩm và dự báo bán hàng được hiển thị trên bảng thông báo hoặc tường
    1. Phòng chống kỹ thuật liệt kê
* Các biện pháp đối phó liệt kê SNMP
* Xóa tác nhân SNMP hoặc tắt dịch vụ SNMP.
* Nếu tắt SNMP không phải là một tùy chọn, hãy thay đổi tên chuỗi cộng đồng mặc định.
* Nâng cấp lên SNMP3, mã hóa mật khẩu và tin nhắn.
* Triển khai tùy chọn bảo mật Chính sách Nhóm được gọi là "Hạn chế bổ sung cho các kết nối ẩn danh."
* Đảm bảo rằng quyền truy cập vào các ống phiên không có giá trị, chia sẻ phiên không có giá trị và lọc IPsec bị hạn chế.
* Chặn quyền truy cập vào cổng TCP/UDP 161.
* Không cài đặt thành phần Windows quản lý và giám sát trừ khi được yêu cầu.
* Mã hóa hoặc xác thực bằng IPsec.
* Không cấu hình sai dịch vụ SNMP với quyền đọc-ghi.
* Các biện pháp đối phó với việc liệt kê DNS
* Vô hiệu hóa việc chuyển vùng DNS tới các máy chủ không đáng tin cậy.
* Đảm bảo rằng các máy chủ riêng và địa chỉ IP của chúng không được công bố trong các tệp vùng DNS của máy chủ DNS công cộng.
* Sử dụng các dịch vụ đăng ký DNS cao cấp để ẩn thông tin nhạy cảm như thông tin máy chủ (HINFO) khỏi công chúng.
* Sử dụng địa chỉ liên hệ quản trị mạng tiêu chuẩn để đăng ký DNS để tránh các cuộc tấn công kỹ thuật xã hội.
* Cắt bớt các tệp vùng DNS để tránh tiết lộ thông tin không cần thiết.
* Các biện pháp đối phó liệt kê SMTP
* Máy chủ SMTP nên được cấu hình theo cách sau.
* Bỏ qua thư điện tử cho những người nhận không xác định.
* Loại trừ thông tin nhạy cảm trên máy chủ thư và máy chủ cục bộ trong phản hồi thư.
* Tắt tính năng rơle mở.
* Giới hạn số lượng kết nối được chấp nhận từ một nguồn để ngăn chặn các cuộc tấn công vét cạn.
* Vô hiệu hóa các lệnh EXPN, VRFY và RCPT TO hoặc hạn chế chúng đối với người dùng xác thực.
* Bỏ qua email cho người nhận không xác định bằng cách định cấu hình máy chủ SMTP.
* Biện pháp đối phó liệt kê LDAP
* Theo mặc định, lưu lượng LDAP được truyền không an toàn; do đó, hãy sử dụng công nghệ Lớp cổng bảo mật (SSL) hoặc STARTTLS để mã hóa lưu lượng.
* Chọn tên người dùng khác với địa chỉ email và bật khóa tài khoản.
* Hạn chế quyền truy cập vào Active Directory bằng cách sử dụng phần mềm như Citrix.
* Sử dụng NTLM hoặc bất kỳ cơ chế xác thực cơ bản nào để giới hạn quyền truy cập đối với người dùng hợp pháp.
* Các biện pháp đối phó trong việc liệt kê SMB

Các dịch vụ chia sẻ chung hoặc các dịch vụ không sử dụng khác có thể cung cấp các cánh cửa cho kẻ tấn công đột nhập vào bảo mật của mạng. Mạng đang chạy SMB có nguy cơ liệt kê cao. Vì các máy chủ web và DNS không yêu cầu giao thức này, nên bạn nên tắt nó trên chúng. Giao thức SMB có thể bị vô hiệu hóa bằng cách vô hiệu hóa các thuộc tính Máy khách cho Mạng và Tệp và Máy in của Microsoft

Chia sẻ cho Mạng Microsoft trong Kết nối Mạng và Quay số. Trên các máy chủ có thể truy cập từ Internet, còn được gọi là máy chủ pháo đài, SMB có thể bị vô hiệu hóa bằng cách vô hiệu hóa hai thuộc tính giống nhau của hộp thoại thuộc tính TCP/IP. Một phương pháp khác để vô hiệu hóa giao thức SMB trên các máy chủ pháo đài mà không vô hiệu hóa nó một cách rõ ràng là chặn các cổng được sử dụng bởi dịch vụ SMB. Đây là các cổng TCP 139 và 445.

Vì việc vô hiệu hóa các dịch vụ SMB không phải lúc nào cũng là một lựa chọn khả thi nên có thể cần phải có các biện pháp đối phó khác đối với việc liệt kê SMB. Windows Registry có thể được cấu hình để hạn chế truy cập ẩn danh từ Internet vào một tập hợp tệp được chỉ định. Các tệp và thư mục này được chỉ định trong cài đặt Truy cập mạng: Đường ống được đặt tên có thể được truy cập ẩn danh và Truy cập mạng: Chia sẻ có thể được truy cập ẩn danh. Cấu hình này liên quan đến việc thêm tham số RestrictNullSessAccess vào khoá đăng ký:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Tham số RestrictNullSessAccess nhận các giá trị nhị phân, với 1 biểu thị đã bật và 0 biểu thị đã tắt. Việc đặt tham số này thành 1 hoặc được bật sẽ hạn chế quyền truy cập của người dùng ẩn danh vào các tệp được chỉ định trong cài đặt Truy cập mạng.

Sau đây là các biện pháp đối phó bổ sung để chống lại việc liệt kê SMB.

* Đảm bảo rằng Tường lửa của Windows hoặc các hệ thống bảo vệ điểm cuối tương tự được bật trên hệ thống.
* Cài đặt các bản vá bảo mật mới nhất cho Windows và phần mềm của bên thứ ba.
* Triển khai cơ chế xác thực phù hợp với chính sách mật khẩu mạnh.
* Triển khai các quyền mạnh mẽ để giữ an toàn cho thông tin được lưu trữ.
* Thực hiện kiểm toán thường xuyên nhật ký hệ thống.
* Thực hiện giám sát hệ thống tích cực để giám sát các hệ thống đối với bất kỳ sự cố độc hại nào.
* Các biện pháp đối phó liệt kê NFS
* Triển khai các quyền thích hợp (đọc/ghi phải được giới hạn cho những người dùng cụ thể) trong các hệ thống tệp đã xuất.
* Triển khai các quy tắc tường lửa để chặn cổng NFS 2049.
* Đảm bảo cấu hình đúng của các tệp như /etc/smb.conf, /etc/exports và etc/hosts.allow để bảo vệ dữ liệu được lưu trữ trong máy chủ.
* Ghi nhật ký các yêu cầu truy cập các tệp hệ thống trên máy chủ NFS.
* Luôn BẬT tùy chọn root\_squash trong tệp /etc/exports để không có yêu cầu nào được thực hiện với quyền root trên máy khách được tin cậy.
* Triển khai đường hầm NFS thông qua SSH để mã hóa lưu lượng NFS qua mạng.
* Các biện pháp đối phó liệt kê FTP
* Triển khai FTP an toàn (SFTP, sử dụng SSH) hoặc FTP an toàn (FTPS, sử dụng SSL) để mã hóa lưu lượng FTP qua mạng.
* Triển khai mật khẩu mạnh hoặc chính sách xác thực dựa trên chứng nhận.
* Đảm bảo rằng không cho phép tải lên không hạn chế các tệp trên máy chủ FTP.
* Vô hiệu hóa tài khoản FTP ẩn danh. Nếu không được, hãy thường xuyên theo dõi các tài khoản FTP ẩn danh.
* Hạn chế quyền truy cập theo IP hoặc tên miền vào máy chủ FTP.
* Định cấu hình kiểm soát truy cập trên tài khoản FTP đã xác thực với sự trợ giúp của danh sách kiểm soát truy cập (ACLS).
* Hạn chế số lần đăng nhập và thời gian.
* Định cấu hình quy tắc lọc cho các dịch vụ FTP.
* Sử dụng SSL/FTPS cho các tài khoản FTP đã được xác thực.

Câu hỏi ôn tập

1. Tấn công hệ thống
   1. Khái niệm cơ bản

Kẻ tấn công tham gia vào các nỗ lực xâm nhập hệ thống bằng cách sử dụng thông tin được thu thập trong các giai đoạn phân tích dấu vết, quét, liệt kê và lỗ hổng trước đó.

Những kẻ tấn công tuân theo một phương pháp nhất định để hack một hệ thống. Trước tiên, chúng lấy thông tin trong các giai đoạn phân tích dấu chân, quét, liệt kê và lỗ hổng, sau đó chúng sử dụng để khai thác hệ thống đích.

**Có bốn bước trong CHM:**

* Đạt được quyền truy cập

Các giai đoạn tấn công trước đó, bao gồm dấu chân và trinh sát, quét, liệt kê và đánh giá lỗ hổng, giúp kẻ tấn công xác định các lỗ hổng bảo mật và lỗ hổng bảo mật tồn tại trong tài sản CNTT của tổ chức mục tiêu. Những kẻ tấn công sử dụng thông tin này, cùng với các kỹ thuật như bẻ khóa mật khẩu và khai thác các lỗ hổng như lỗi tràn bộ đệm, để giành quyền truy cập vào hệ thống tổ chức mục tiêu.

Bẻ khóa mật khẩu liên quan đến việc giành quyền truy cập vào tài khoản người dùng có đặc quyền thấp bằng cách bẻ khóa mật khẩu bằng các kỹ thuật như cưỡng bức vét cạn, đoán mật khẩu và kỹ thuật xã hội. Những kẻ tấn công khai thác các lỗ hổng đã xác định, chẳng hạn như tràn bộ đệm, để giành quyền truy cập cấp gốc vào hệ thống đích.

* Nâng cao đặc quyền

Sau khi giành được quyền truy cập, kẻ tấn công sẽ nâng cấp đặc quyền của chúng lên cấp quản trị để thực hiện một hoạt động được bảo vệ. Những kẻ tấn công khai thác các lỗ hổng tồn tại trong PMNM và các ứng dụng phần mềm để leo thang đặc quyền.

* Duy trì quyền truy cập

Sau khi giành được thành công quyền truy cập và leo thang đặc quyền đối với hệ thống mục tiêu, kẻ tấn công đảm bảo rằng mức độ truy cập cao được duy trì để thực hiện các hoạt động độc hại như thực thi các ứng dụng độc hại và đánh cắp, che giấu hoặc can thiệp vào các tệp hệ thống nhạy cảm.

* Xóa nhật ký

Để duy trì quyền truy cập hệ thống trong tương lai, những kẻ tấn công cố gắng tránh sự công nhận của người dùng hệ thống hợp pháp. Để không bị phát hiện, kẻ tấn công xóa sạch các mục tương ứng với hoạt động của chúng trong nhật ký hệ thống, do đó tránh bị người dùng phát hiện.

**Mục tiêu tấn công hệ thống**

* Đạt được quyền truy cập

Trong hack hệ thống, trước tiên kẻ tấn công cố gắng giành quyền truy cập vào hệ thống mục tiêu bằng cách sử dụng thông tin thu được và các lỗ hổng được tìm thấy trong cơ chế kiểm soát truy cập của hệ thống. Khi kẻ tấn công thành công trong việc giành quyền truy cập vào hệ thống, chúng có thể tự do thực hiện nhiều hoạt động độc hại khác nhau như đánh cắp dữ liệu nhạy cảm, triển khai trình thám thính để nắm bắt lưu lượng mạng và lây nhiễm phần mềm độc hại vào hệ thống. Sau đó, kẻ tấn công có thể sử dụng các kỹ thuật như bẻ khóa mật khẩu, khai thác lỗ hổng và các chiến thuật kỹ thuật xã hội để giành quyền truy cập vào hệ thống đích.

* Nâng cao đặc quyền

Sau khi có quyền truy cập vào hệ thống bằng tài khoản người dùng thông thường có đặc quyền thấp, kẻ tấn công có thể cố gắng tăng đặc quyền quản trị viên của họ để thực hiện các hoạt động của hệ thống được bảo vệ, để họ có thể tiến tới cấp độ tiếp theo của giai đoạn tấn công hệ thống, đó là thực thi của các ứng dụng. Kẻ tấn công khai thác các lỗ hổng hệ thống đã biết để leo thang đặc quyền của người dùng.

* Thực hiện các ứng dụng

Khi kẻ tấn công có đặc quyền của quản trị viên, chúng có thể cố gắng cài đặt các chương trình độc hại như Trojan, backdoor, rootkit và keylogger, những chương trình này cấp cho chúng quyền truy cập hệ thống từ xa và cho phép chúng thực thi mã độc từ xa. Cài đặt rootkit cho phép kẻ tấn công có quyền truy cập ở cấp hệ điều hành để thực hiện các hoạt động độc hại. Để duy trì quyền truy cập để sử dụng sau này, họ thậm chí có thể cài đặt các cửa hậu.

* Ẩn tập tin

Những kẻ tấn công sử dụng rootkit và các kỹ thuật lưu trữ dữ liệu để cố gắng che giấu các tệp độc hại mà chúng cài đặt trên hệ thống và do đó, các hoạt động của chúng.

* Xoá chứng cứ

Để không bị phát hiện, điều quan trọng là những kẻ tấn công phải xóa khỏi hệ thống tất cả bằng chứng về sự xâm phạm bảo mật. Để đạt được điều này, họ có thể sửa đổi hoặc xóa nhật ký trong hệ thống bằng cách sử dụng một số tiện ích xóa nhật ký nhất định, do đó xóa tất cả bằng chứng về sự hiện diện của họ.

* 1. Bẻ khóa mật khẩu

Bẻ khóa mật khẩu là quá trình khôi phục mật khẩu từ dữ liệu được truyền bởi hệ thống máy tính hoặc từ dữ liệu được lưu trữ trong đó. Mục đích của việc bẻ khóa mật khẩu có thể là để giúp người dùng khôi phục mật khẩu bị quên hoặc bị mất, như một biện pháp phòng ngừa của quản trị viên hệ thống để kiểm tra các mật khẩu dễ bị phá vỡ hoặc để kẻ tấn công sử dụng để giành quyền truy cập hệ thống trái phép.

Việc hack thường bắt đầu bằng các nỗ lực bẻ khóa mật khẩu. Mật khẩu là một phần thông tin quan trọng cần thiết để truy cập hệ thống. Do đó, hầu hết những kẻ tấn công sử dụng các kỹ thuật bẻ khóa mật khẩu để có được quyền truy cập trái phép. Kẻ tấn công có thể bẻ khóa mật khẩu theo cách thủ công bằng cách đoán hoặc sử dụng các công cụ và kỹ thuật tự động như từ điển hoặc phương pháp brute-force. Hầu hết các kỹ thuật bẻ khóa mật khẩu đều thành công nhờ mật khẩu yếu hoặc dễ đoán.

**Các loại tấn công mật khẩu**

Bẻ khóa mật khẩu là một trong những giai đoạn quan trọng của hack hệ thống. Các cơ chế bẻ khóa mật khẩu thường khai thác các phương tiện hợp pháp khác để giành quyền truy cập hệ thống trái phép, chẳng hạn như khôi phục mật khẩu đã quên của người dùng. Việc phân loại các cuộc tấn công mật khẩu phụ thuộc vào hành động của kẻ tấn công, có bốn loại sau:

* Tấn công phi điện tử: Trong hầu hết các trường hợp, đây là nỗ lực đầu tiên của kẻ tấn công nhằm lấy mật khẩu hệ thống mục tiêu. Các cuộc tấn công phi điện tử hoặc phi kỹ thuật không yêu cầu bất kỳ kiến thức kỹ thuật nào về hack hoặc khai thác hệ thống. Các kỹ thuật được sử dụng để thực hiện các cuộc tấn công phi điện tử bao gồm lướt vai, kỹ thuật xã hội, lặn biển, v.v.

Tấn công phi điện tử

Các cuộc tấn công phi điện tử hoặc phi kỹ thuật không yêu cầu kiến thức kỹ thuật về các phương pháp xâm nhập hệ thống. Có ba loại tấn công phi điện tử: kỹ thuật xã hội, vai

lướt sóng và bới thùng rác.

Kỹ thuật xã hội

Trong bảo mật máy tính, kỹ thuật xã hội được sử dụng để biểu thị một kiểu xâm nhập phi kỹ thuật khai thác hành vi của con người. Thông thường, nó chủ yếu dựa vào sự tương tác của con người và thường liên quan đến việc lừa người khác vi phạm các quy trình bảo mật thông thường. Một kỹ sư xã hội thực hiện một "trò lừa bịp" để phá vỡ các quy trình bảo mật. Ví dụ: kẻ tấn công sử dụng kỹ thuật xã hội để đột nhập vào mạng máy tính có thể cố gắng giành được sự tin tưởng của người dùng được ủy quyền để truy cập vào mạng mục tiêu và sau đó trích xuất thông tin để xâm phạm an ninh mạng. Trên thực tế, kỹ thuật xã hội là một phương thức được sử dụng để thu thập thông tin bí mật bằng cách lừa dối hoặc gây ảnh hưởng đến mọi người. Kẻ tấn công có thể cải trang thành người dùng hoặc quản trị viên hệ thống để lấy mật khẩu của người dùng. Các kỹ sư xã hội khai thác thực tế là mọi người nói chung cố gắng xây dựng mối quan hệ thân thiện với bạn bè và đồng nghiệp của họ và có xu hướng hữu ích và đáng tin cậy.

Một đặc điểm khác của kỹ thuật xã hội dựa trên việc con người không có khả năng theo kịp một nền văn hóa phụ thuộc nhiều vào công nghệ thông tin. Hầu hết mọi người không nhận thức được giá trị của thông tin mà họ sở hữu và do đó, chỉ một số ít quan tâm đến việc bảo vệ thông tin của họ. Các kỹ sư xã hội thường tìm kiếm các thùng rác để có được thông tin có giá trị. Hơn nữa, các kỹ sư xã hội thấy khó khăn hơn để có được sự kết hợp với két an toàn hoặc tủ khóa của câu lạc bộ sức khỏe so với trường hợp mật khẩu. Cách phòng thủ tốt nhất là giáo dục, đào tạo và nâng cao nhận thức về cuộc tấn công này cũng như giá trị của thông tin.

Lướt vai

Lướt vai là một kỹ thuật đánh cắp mật khẩu bằng cách di chuyển gần người dùng hợp pháp và xem họ nhập mật khẩu. Trong kiểu tấn công này, kẻ tấn công quan sát bàn phím hoặc màn hình của người dùng khi họ đăng nhập và theo dõi những gì người dùng đề cập đến khi nhập mật khẩu của họ, ví dụ: một đối tượng trên bàn của họ để viết mật khẩu hoặc ghi nhớ. Tuy nhiên, cuộc tấn công này chỉ có thể được thực hiện khi kẻ tấn công ở gần mục tiêu.

Cuộc tấn công này cũng có thể được thực hiện trong các hàng thanh toán của các cửa hàng tạp hóa, chẳng hạn như khi một nạn nhân tiềm năng quẹt thẻ ghi nợ và nhập mã PIN (Số nhận dạng cá nhân) được yêu cầu. Mã PIN thường có bốn chữ số và điều này khiến cuộc tấn công dễ dàng thực hiện.

Bới thùng rác

"Dumpsterdiving" là một phương pháp tấn công quan trọng sử dụng các lỗi đáng kể về bảo mật máy tính trong hệ thống mục tiêu. Thông tin nhạy cảm mà mọi người khao khát, bảo vệ và bảo mật tận tình có thể được truy cập bởi hầu hết mọi người sẵn sàng thực hiện tìm kiếm rác. Nhìn qua thùng rác là một kiểu tấn công công nghệ thấp với nhiều hệ lụy.

Lặn thùng rác khá phổ biến vào những năm 1980. Bản thân thuật ngữ này đề cập đến việc thu thập thông tin chung, hữu ích từ các bãi rác như thùng rác, thùng chứa bên lề đường và thùng rác. Thậm chí ngày nay, những kẻ tấn công tò mò và/hoặc ác ý đôi khi tìm thấy phương tiện bị loại bỏ cùng với các tệp mật khẩu, sách hướng dẫn, báo cáo, biên lai, số thẻ tín dụng hoặc các tài liệu nhạy cảm khác.

Việc kiểm tra các sản phẩm phế thải từ các bãi rác có thể giúp kẻ tấn công giành được quyền truy cập trái phép vào các hệ thống mục tiêu và có nhiều bằng chứng ủng hộ khái niệm này. Nhân viên hỗ trợ thường đổ thông tin nhạy cảm mà không để ý đến việc ai có thể truy cập thông tin đó sau này. Do đó, thông tin được thu thập sau đó có thể được sử dụng bởi những kẻ tấn công để thực hiện các loại tấn công khác, chẳng hạn như kỹ thuật xã hội.

* Tấn công active online: Đây là một trong những cách dễ dàng nhất để giành quyền truy cập hệ thống cấp quản trị viên trái phép. Tại đây, kẻ tấn công giao tiếp với máy mục tiêu để giành quyền truy cập bằng mật khẩu. Các kỹ thuật được sử dụng để thực hiện các cuộc tấn công active online bao gồm đoán mật khẩu, từ điển và tấn công vét cạn, tiêm băm, đầu độc LLMNR/NBT-NS, sử dụng Trojan/phần mềm gián điệp/keylogger, tấn công độc thoại nội bộ, tấn công chuỗi Markov, bẻ khóa mật khẩu Kerberos, v.v. .

Các cuộc tấn công active online

Tấn công từ điển

Trong kiểu tấn công này, một tệp từ điển được tải vào một ứng dụng bẻ khóa chạy trên tài khoản người dùng. Từ điển này là một tệp văn bản chứa một số từ điển thường được sử dụng làm mật khẩu. Chương trình sử dụng mọi từ có trong từ điển để tìm mật khẩu. Ngoài từ điển tiêu chuẩn, từ điển của kẻ tấn công chứa các mục có số và ký hiệu được thêm vào từ (ví dụ: "3 tháng 12!962"). Do đó, cuộn ngón tay trên bàn phím đơn giản ("qwer0987"), mà nhiều người tin rằng sẽ tạo ra mật khẩu ngẫu nhiên và an toàn, do đó được đưa vào một từ điển như vậy. Các cuộc tấn công từ điển hữu ích hơn các cuộc tấn công vét cạn, tuy nhiên, cuộc tấn công trước không thể thực hiện được trong các hệ thống sử dụng cụm mật khẩu.

Cuộc tấn công này được áp dụng trong hai tình huống:

* Trong phân tích mật mã, để khám phá khóa giải mã để lấy bản rõ từ bản mã
* Trong bảo mật máy tính, để vượt qua xác thực và truy cập vào cơ chế kiểm soát của máy tính bằng cách đoán mật khẩu

Các phương pháp để cải thiện sự thành công của một cuộc tấn công từ điển:

* Sử dụng một số từ điển khác nhau, chẳng hạn như từ điển kỹ thuật và nước ngoài, làm tăng số lượng khả năng
* Sử dụng thao tác chuỗi cùng với từ điển (ví dụ: nếu từ điển chứa từ "hệ thống", thao tác chuỗi sẽ tạo đảo chữ cái như "metsys" trong số những từ khác)

Tấn công vét cạn

Trong một cuộc tấn công vét cạn, những kẻ tấn công thử mọi tổ hợp ký tự cho đến khi mật khẩu bị phá vỡ. Các thuật toán mật mã phải đủ mạnh để ngăn chặn tấn công vét cạn, được RSA định nghĩa như sau: "Tìm kiếm khóa toàn diện, hay tìm kiếm vét cạn, là kỹ thuật cơ bản để lần lượt thử mọi khóa có thể cho đến khi tìm được khóa chính xác". được xác định."

Một cuộc tấn công vét cạn là khi ai đó cố gắng tạo ra mọi khóa mã hóa duy nhất cho dữ liệu để phát hiện thông tin cần thiết. Thậm chí ngày nay, chỉ những người có đủ sức mạnh xử lý mới có thể thực hiện thành công kiểu tấn công này.

Phân tích mật mã là một cuộc tấn công vét cạn vào mã hóa sử dụng tìm kiếm không gian khóa. Nói cách khác, kiểm tra tất cả các khóa có thể là một trong những nỗ lực khôi phục bản rõ được sử dụng để tạo ra một bản mã cụ thể. Việc phát hiện một khóa hoặc bản rõ nhanh hơn một cuộc tấn công vét cạn là một cách để phá vỡ mật mã. Một mật mã được bảo mật nếu không có phương pháp nào để phá vỡ nó ngoài một cuộc tấn công vét cạn. Nói chung, tất cả các mật mã đều thiếu bằng chứng toán học về tính bảo mật. Nếu người dùng chọn các khóa một cách ngẫu nhiên hoặc tìm kiếm ngẫu nhiên, trung bình bản rõ sẽ có sẵn sau khi hệ thống đã thử một nửa số khóa có thể.

Một số cân nhắc cho các cuộc tấn công vét cạn như sau:

* Đó là một quá trình tốn nhiều thời gian
* Tất cả mật khẩu cuối cùng sẽ được tìm thấy

Tấn công dựa trên quy tắc

Những kẻ tấn công sử dụng kiểu tấn công này khi chúng lấy được một số thông tin về mật khẩu. Đây là một cuộc tấn công mạnh hơn so với các cuộc tấn công từ điển và brute-force vì cracker biết loại mật khẩu. Ví dụ: nếu kẻ tấn công biết rằng mật khẩu chứa số có hai hoặc ba chữ số, kẻ đó có thể sử dụng một số kỹ thuật cụ thể để trích xuất mật khẩu một cách nhanh chóng.

Bằng cách lấy thông tin hữu ích, chẳng hạn như phương pháp sử dụng số và/hoặc ký tự đặc biệt và độ dài mật khẩu, kẻ tấn công có thể giảm thiểu thời gian cần thiết để bẻ khóa mật khẩu và do đó nâng cao công cụ bẻ khóa. Kỹ thuật này liên quan đến vũ lực, từ điển và các cuộc tấn công âm tiết.

Đối với các cuộc tấn công bẻ khóa mật khẩu trực tuyến, đôi khi kẻ tấn công sẽ sử dụng kết hợp cả vũ lực và từ điển. Sự kết hợp này thuộc loại tấn công bẻ khóa mật khẩu hỗn hợp và âm tiết.

* Tấn công âm tiết

Tin tặc sử dụng kỹ thuật bẻ khóa này khi mật khẩu không phải là từ đã biết. Những kẻ tấn công sử dụng từ điển và các phương pháp khác để bẻ khóa chúng, cũng như tất cả các kết hợp có thể có của chúng.

* Tấn công hỗn hợp

Loại tấn công này phụ thuộc vào tấn công từ điển. Thông thường, mọi người thay đổi mật khẩu của họ chỉ bằng cách thêm một số số vào mật khẩu cũ của họ. Trong trường hợp này, chương trình sẽ thêm một số số và ký hiệu vào các từ trong từ điển để cố gắng bẻ khóa mật khẩu. Ví dụ: nếu mật khẩu cũ là "system", thì có khả năng người đó sẽ đổi nó thành "system1" hoặc "system2".

Đoán mật khẩu

Đoán mật khẩu là một kỹ thuật bẻ khóa mật khẩu liên quan đến việc cố gắng đăng nhập vào hệ thống đích bằng các mật khẩu khác nhau theo cách thủ công. Đoán là yếu tố chính của việc bẻ khóa mật khẩu thủ công. Kẻ tấn công tạo danh sách tất cả các mật khẩu có thể có từ thông tin được thu thập thông qua kỹ thuật xã hội hoặc bất kỳ phương pháp nào khác và thử chúng theo cách thủ công trên máy của nạn nhân để bẻ khóa mật khẩu.

Sau đây là các bước liên quan đến đoán mật khẩu:

* Tìm người dùng hợp lệ
* Tạo một danh sách các mật khẩu có thể
* Xếp hạng mật khẩu từ xác suất cao đến thấp
* Nhập từng mật khẩu, cho đến khi tìm được mật khẩu đúng

Tin tặc có thể bẻ khóa mật khẩu theo cách thủ công hoặc bằng cách sử dụng các công cụ, phương pháp và thuật toán tự động. Họ cũng có thể tự động bẻ khóa mật khẩu bằng vòng lặp FOR đơn giản hoặc tạo tệp tập lệnh thử từng mật khẩu trong danh sách. Những kỹ thuật này vẫn được coi là bẻ khóa thủ công. Tỷ lệ thất bại của kiểu tấn công này là cao.

Thuật toán bẻ khóa mật khẩu thủ công

Ở dạng đơn giản nhất, thuật toán này có thể tự động đoán mật khẩu bằng vòng lặp FOR đơn giản. Trong ví dụ sau, kẻ tấn công tạo một tệp văn bản đơn giản có tên người dùng và mật khẩu rồi lặp lại chúng bằng vòng lặp FOR.

Vòng lặp FOR chính có thể trích xuất tên người dùng và mật khẩu từ tệp văn bản, đóng vai trò như một từ điển khi nó lặp qua từng dòng:

[file: credentials.txt] administrator ""

administrator password

[Vân vân.]

Nhập các lệnh sau để truy cập tệp văn bản từ một thư mục:

More? 2>>nul^

c:\>FOR /F "tokens=1,2\*" %i in (credentials.txt)^

More? do net use \\victim.com\IPC$ %j /u: victim.com\%i^

More? && echo time% %date% >> outfile.txt^

More? && echo \\victim.com acct: %i pass: %j >> outfile.txt

c:\>type outfile.txt

Tệp outfile.txt chứa tên người dùng và mật khẩu chính xác, nếu tên người dùng và mật khẩu trong credentials.txt là chính xác. Kẻ tấn công có thể thiết lập phiên mở với máy chủ nạn nhân bằng hệ thống của anh ta/cô ta.

Mật khẩu mặc định

Mật khẩu mặc định là mật khẩu do nhà sản xuất cung cấp cho thiết bị mới (ví dụ: bộ chuyển mạch, bộ tập trung, bộ định tuyến). Thông thường, mật khẩu mặc định do nhà sản xuất thiết bị bảo vệ bằng mật khẩu cung cấp cho phép người dùng truy cập thiết bị trong quá trình thiết lập ban đầu và sau đó thay đổi mật khẩu. Tuy nhiên, thường quản trị viên sẽ quên đặt mật khẩu mới hoặc bỏ qua đề xuất thay đổi mật khẩu và tiếp tục sử dụng mật khẩu ban đầu. Kẻ tấn công có thể khai thác lỗ hổng này và tìm mật khẩu mặc định cho thiết bị mục tiêu từ các trang web của nhà sản xuất hoặc sử dụng các công cụ trực tuyến hiển thị mật khẩu mặc định để truy cập thành công vào thiết bị mục tiêu. Những kẻ tấn công sử dụng mật khẩu mặc định trong danh sách từ hoặc từ điển mà chúng sử dụng để thực hiện các cuộc tấn công đoán mật khẩu.

Sau đây là một số công cụ trực tuyến để tìm kiếm mật khẩu mặc định:

http://open-sez.me

https://www.fortypoundhead.com

https://cirt.net

http://www.defaultpassword.us

http://defaultpasswords.in

https://www.routerpasswords.com

<https://default-password.info>

Trojan/Phần mềm gián điệp/Keylogger

Trojan là một chương trình tự ngụy trang dưới dạng một ứng dụng lành tính. Phần mềm ban đầu dường như thực hiện một chức năng mong muốn hoặc lành tính, nhưng thay vào đó lại đánh cắp thông tin hoặc gây hại cho hệ thống. Với một Trojan, kẻ tấn công có thể truy cập từ xa và thực hiện nhiều hoạt động khác nhau bị giới hạn bởi đặc quyền của người dùng trên máy tính mục tiêu.

Phần mềm gián điệp là một loại phần mềm độc hại mà kẻ tấn công cài đặt trên máy tính để bí mật thu thập thông tin về người dùng mà họ không biết. Phần mềm gián điệp ẩn mình khỏi người dùng và có thể khó phát hiện.

Keylogger là một chương trình ghi lại tất cả các thao tác gõ phím của người dùng mà người dùng không hề hay biết. Keylogger gửi nhật ký thao tác bàn phím của người dùng đến máy của kẻ tấn công hoặc giấu nó trong máy của nạn nhân để truy xuất sau này. Kẻ tấn công sau đó xem xét kỹ lưỡng nhật ký để tìm mật khẩu hoặc thông tin hữu ích khác có thể xâm phạm hệ thống.

Kẻ tấn công cài đặt Trojan/phần mềm gián điệp/keylogger trên máy của nạn nhân để thu thập tên người dùng và mật khẩu của họ. Các chương trình này chạy trong nền và gửi lại tất cả thông tin đăng nhập của người dùng cho kẻ tấn công.

Ví dụ: trình ghi khóa trên máy tính của nạn nhân có thể tiết lộ nội dung của tất cả email của người dùng. Hình ảnh sau đây mô tả một tình huống mô tả cách kẻ tấn công giành được quyền truy cập mật khẩu bằng cách sử dụng Trojan/phần mềm gián điệp/keylogger.

Tấn công chèn mã băm/Truyền mã băm (PtH)

Kiểu tấn công này có thể xảy ra khi hệ thống đích sử dụng hàm băm như một phần của quy trình xác thực để xác thực người dùng của nó. Nói chung, hệ thống lưu trữ các giá trị băm của thông tin đăng nhập trong cơ sở dữ liệu/tệp SAM trên máy tính Windows. Trong những trường hợp như vậy, máy chủ sẽ tính toán giá trị băm của thông tin đăng nhập do người dùng gửi hoặc cho phép người dùng nhập trực tiếp giá trị băm. Sau đó, máy chủ sẽ kiểm tra nó với giá trị băm được lưu trữ để xác thực.

Những kẻ tấn công khai thác các cơ chế xác thực như vậy và trước tiên khai thác máy chủ mục tiêu để lấy các giá trị băm từ cơ sở dữ liệu SAM. Sau đó, họ nhập các giá trị băm thu được trực tiếp vào cơ chế xác thực để xác thực với các giá trị băm được tính toán trước bị đánh cắp của người dùng. Do đó, trong một cuộc tấn công tiêm băm/PtH, những kẻ tấn công đưa một hàm băm LanMan (LM) hoặc NTLM bị xâm nhập vào một phiên cục bộ và sau đó sử dụng hàm băm để xác thực tài nguyên mạng. Bất kỳ máy chủ hoặc dịch vụ nào (chạy trên Windows, UNIX hoặc bất kỳ HĐH nào khác) sử dụng xác thực NTLM hoặc LM đều dễ bị tấn công này. Cuộc tấn công này có thể được thực hiện trên bất kỳ hệ điều hành nào, nhưng Windows có thể dễ bị tổn thương hơn do tính năng Đăng nhập một lần (SSO) lưu trữ mật khẩu bên trong hệ thống và cho phép người dùng truy cập tất cả các tài nguyên bằng thông tin đăng nhập một lần.

Các kỹ thuật khác nhau được sử dụng để thực hiện tấn công băm/tấn công PtH:

Kẻ tấn công cố gắng xâm phạm các đặc quyền của quản trị viên để nắm bắt các giá trị bộ đệm ẩn của mật khẩu người dùng được băm từ cơ sở dữ liệu tài khoản người dùng cục bộ hoặc SAM. Tuy nhiên, quản trị viên mạng có thể hạn chế việc sử dụng ngoại tuyến các giá trị băm được lưu trong bộ nhớ cache này. Do đó, phương pháp này có thể không phải lúc nào cũng khả thi.

* Kẻ tấn công kết xuất các hàm băm mật khẩu từ cơ sở dữ liệu tài khoản người dùng cục bộ hoặc SAM để lấy các hàm băm mật khẩu của người dùng cục bộ và giành quyền truy cập vào tài khoản quản trị viên để xâm phạm các hệ thống được kết nối khác.
* Kẻ tấn công nắm bắt các thông báo phản hồi thách thức LM hoặc NTLM giữa máy khách và máy chủ để trích xuất các giá trị băm được mã hóa thông qua cưỡng bức vũ phu.
* Kẻ tấn công lấy thông tin đăng nhập của người dùng cục bộ cũng như những người thuộc miền bảo mật từ quy trình Windows Isass.exe.

Tin tặc thực hiện cuộc tấn công này bằng cách thực hiện năm bước sau:

* Tin tặc xâm phạm một máy trạm/máy chủ bằng cách khai thác cục bộ/từ xa.
* Tin tặc trích xuất các hàm băm được lưu trữ bằng các công cụ như pwdump7, Mimikatz, v.v. và tìm thấy một hàm băm tài khoản quản trị viên miền.
* Tin tặc sử dụng các công cụ như Mimikatz để đặt một trong các hàm băm đã truy xuất vào quy trình Isass.exe cục bộ của anh ta/cô ta và sau đó sử dụng hàm băm để đăng nhập vào bất kỳ hệ thống nào (bộ điều khiển miền) có cùng thông tin đăng nhập.
* Tin tặc trích xuất tất cả các giá trị băm từ cơ sở dữ liệu Active Directory và hiện có thể xâm phạm bất kỳ tài khoản nào trong miền.

Tấn công độc thoại nội bộ

Cuộc tấn công bằng độc thoại nội bộ tương tự như cuộc tấn công được thực hiện bằng Mimikatz, ngoại trừ vùng bộ nhớ của quy trình Dịch vụ Hệ thống con của Cơ quan Bảo mật Cục bộ (LSASS) không bị kết xuất, do đó tránh được Windows Credential Guard và phần mềm chống vi-rút. Mimikatz là một công cụ hậu khai thác, qua đó kẻ tấn công có thể trích xuất mật khẩu văn bản gốc, vé Kerberos và hàm băm NTLM từ bộ nhớ quy trình LSASS. Những kẻ tấn công sử dụng Mimikatz để truy xuất thông tin đăng nhập của người dùng từ bộ nhớ tiến trình LSASS và thông tin thu được sẽ giúp chúng thực hiện chuyển động ngang trong giai đoạn hậu khai thác.

Một cuộc tấn công độc thoại nội bộ thường được thực hiện trong một môi trường an toàn mà Mimikatz không thể thực hiện được. Trong cuộc tấn công này, bằng cách sử dụng Giao diện nhà cung cấp hỗ trợ bảo mật (SSPI) từ ứng dụng chế độ người dùng, lệnh gọi thủ tục cục bộ tới gói xác thực NTLM được gọi để tính toán phản hồi NetNTLM trong ngữ cảnh của người dùng đã đăng nhập.

Các bước thực hiện tấn công độc thoại nội bộ:

1. Kẻ tấn công vô hiệu hóa các biện pháp kiểm soát bảo mật của NetNTLMv1 bằng cách sửa đổi các giá trị của LMCompatibilityLevel, NTLMMinClientSec và RestrictSendingNTLMTraffic.
2. Kẻ tấn công trích xuất tất cả các mã thông báo đăng nhập không phải mạng từ tất cả các quy trình đang hoạt động để giả dạng người dùng hợp pháp.
3. Giờ đây, kẻ tấn công tương tác cục bộ với NTLM SSP để mỗi người dùng giả mạo nhận được phản hồi NetNTLMv1 đối với thách thức đã chọn trong ngữ cảnh bảo mật của người dùng đó.
4. Giờ đây, kẻ tấn công khôi phục LMCompatibilityLevel, NTLMMinClientSec và RestrictSendingNTLMTraffic về giá trị thực của chúng.
5. Kẻ tấn công sử dụng bảng cầu vồng để bẻ khóa hàm băm NTLM của các phản hồi đã chụp.
6. Cuối cùng, kẻ tấn công sử dụng các mã băm đã bẻ khóa để giành quyền truy cập cấp hệ thống.

Bẻ khóa mật khẩu Kerberos

Kerberos là giao thức xác thực được sử dụng phổ biến nhất cho các thực thể mạng. Do sự chấp nhận rộng rãi của nó, nó dễ bị tấn công khác nhau. Những kẻ tấn công đã phát triển nhiều cách khác nhau để xâm nhập vào Kerberos và khai thác các lỗ hổng của nó để bẻ khóa các mật khẩu yếu, chèn mã độc hại và lấy thông tin về cơ sở hạ tầng mạng cũng như các thực thể mạng khác nhau. Những kẻ tấn công nhắm mục tiêu giao thức xác thực Kerberos theo hai cách phổ biến: cụ thể là bẻ khóa TGS, được gọi là Kerberoasting và bẻ khóa TGT, được gọi là AS-REP Roasting.

* AS-REP Rang (Cracking TGT)

Trong cuộc tấn công này, những kẻ tấn công yêu cầu một vé xác thực (TGT) từ KDC dưới dạng gói AS-REQ. Nếu tài khoản người dùng tồn tại, KDC sẽ trả lời bằng TGT được mã hóa bằng thông tin xác thực của tài khoản. Điều này cho phép kẻ tấn công nhận được một vé được mã hóa, vé này sau đó có thể được lưu ngoại tuyến và bẻ khóa thêm để lấy mật khẩu. Những kẻ tấn công có thể thực hiện kiểu tấn công này cả chủ động và bị động. Trong kịch bản tích cực, kẻ tấn công tạo thông báo AS-REP cho người dùng, trong khi ở kịch bản thụ động, kẻ tấn công quan sát thông báo AS-REP.

Các bước sau đây liên quan đến AS-REP Roasting:

1. Kẻ tấn công xác định tài khoản người dùng đã tắt tùy chọn xác thực trước.
2. Thay mặt người dùng, kẻ tấn công yêu cầu một vé xác thực (TGT) từ bộ điều khiển miền hoặc KDC.
3. Bộ điều khiển miền xác minh tài khoản người dùng và trả lời bằng TGT được mã hóa với thông tin xác thực của tài khoản.
4. Kẻ tấn công lưu trữ TGT ngoại tuyến và bẻ khóa nó để trích xuất mật khẩu tài khoản người dùng và tiếp tục truy cập vào thực thể mạng (ở đây, máy chủ ứng dụng).

* Kerberoasting (Bẻ khóa TGS)

Trong cuộc tấn công này, những kẻ tấn công yêu cầu một TGS cho tên dịch vụ chính (SPN) của tài khoản dịch vụ đích. Yêu cầu này được gửi tới bộ điều khiển miền bằng cách sử dụng vé xác thực của người dùng miền hợp lệ (TGT). Bộ điều khiển miền không có bất kỳ bản ghi nào; nếu người dùng đã truy cập tài nguyên mạng, thì nó chỉ tìm kiếm SPN trong Active Directory và trả lời thêm bằng một vé được mã hóa bằng tài khoản dịch vụ được liên kết với SPN. Loại mã hóa được sử dụng cho phiếu dịch vụ được yêu cầu (ST) là RC4\_HMAC\_MD5, cho biết rằng để mã hóa ST, hàm băm mật khẩu NTLM được sử dụng. Để bẻ khóa ST, kẻ tấn công xuất các vé TGS từ bộ nhớ và lưu chúng ngoại tuyến vào hệ thống cục bộ. Hơn nữa, những kẻ tấn công sử dụng các hàm băm NTLM khác nhau để bẻ khóa ST và khi bẻ khóa thành công, mật khẩu tài khoản dịch vụ có thể bị phát hiện. Những kẻ tấn công sử dụng các công cụ như Kerberoast để thực hiện các cuộc tấn công Kerberoasting vào xác thực Kerberos.

Pass-the-Ticket tấn công

Pass-the-ticket là một kỹ thuật được sử dụng để xác thực người dùng với hệ thống đang sử dụng vé Kerberos mà không cần cung cấp mật khẩu của người dùng. Xác thực Kerberos cho phép người dùng truy cập các dịch vụ do máy chủ từ xa cung cấp mà không cần cung cấp mật khẩu cho mọi dịch vụ được yêu cầu. Để thực hiện cuộc tấn công này, kẻ tấn công kết xuất vé Kerberos của các tài khoản hợp pháp bằng cách sử dụng các công cụ kết xuất thông tin xác thực.

TGT hoặc ST có thể được nắm bắt dựa trên mức độ truy cập được phép đối với khách hàng. Ở đây, ST cho phép truy cập vào các tài nguyên cụ thể và TGT được sử dụng để gửi yêu cầu tới TGS để ST truy cập tất cả các dịch vụ mà máy khách đã được phép truy cập.

Vé bạc được nắm bắt cho các tài nguyên sử dụng Kerberos cho quy trình xác thực và có thể được sử dụng để tạo vé để gọi một dịch vụ cụ thể và truy cập hệ thống cung cấp dịch vụ.

Vé vàng được ghi lại cho miền với hàm băm KDS KRBTGT NTLM cho phép tạo TGT cho bất kỳ cấu hình nào trong Active Directory.

Những kẻ tấn công khởi động các cuộc tấn công qua vé bằng cách đánh cắp ST/TGT từ máy của người dùng cuối và sử dụng nó để cải trang thành người dùng hợp lệ hoặc bằng cách đánh cắp ST/TGT từ một AS bị xâm phạm. Sau khi có được một trong những vé này, kẻ tấn công có thể truy cập trái phép vào các dịch vụ mạng và tìm kiếm các quyền bổ sung cũng như dữ liệu quan trọng.

Những kẻ tấn công sử dụng các công cụ như Mimikatz, Rubeus, Windows Credentials Editor, v.v. để khởi chạy các cuộc tấn công qua vé:

* Mimikatz

Mimikatz cho phép kẻ tấn công chuyển Kerberos TGT sang các máy tính khác và đăng nhập bằng vé của nạn nhân. Công cụ này cũng giúp trích xuất mật khẩu văn bản gốc, hàm băm, mã PIN và vé Kerberos từ bộ nhớ. Đây là một công cụ mã nguồn mở cho phép mọi người xem và lưu trữ dữ liệu xác thực, chẳng hạn như vé Kerberos. Những kẻ tấn công có thể tận dụng điều này để leo thang đặc quyền và đánh cắp thông tin xác thực.

Các cuộc tấn công trực tuyến tích cực khác

Tấn công kết hợp

Trong một cuộc tấn công tổ hợp, những kẻ tấn công kết hợp các mục của từ điển đầu tiên với các từ điển thứ hai. Danh sách kết quả của các mục có thể được sử dụng để tạo tên đầy đủ và từ ghép. Những kẻ tấn công sử dụng danh sách từ này để bẻ khóa mật khẩu trên hệ thống đích và giành quyền truy cập trái phép vào các tệp hệ thống.

Các bước liên quan đến một cuộc tấn công tổ hợp:

* Tìm người dùng mục tiêu hợp lệ.
* Xây dựng hai từ điển của riêng bạn hoặc tải xuống hai từ điển danh sách từ khác nhau từ các nguồn trực tuyến.
* Tạo danh sách từ cuối cùng bằng cách hợp nhất các mục từ của hai từ điển riêng biệt. Ví dụ: nếu từ điển đầu tiên chứa 100 từ và từ điển thứ hai chứa 70 từ, thì từ điển được hợp nhất chứa 100 x 70 = 7000 từ.
* Sử dụng các công cụ tự động, chẳng hạn như hashcat, để bẻ khóa mật khẩu của người dùng mục tiêu.

Những kẻ tấn công thực hiện kiểu bẻ khóa mật khẩu này trong tình huống một cụm từ ngẫu nhiên được sử dụng làm thủ tục tạo mật khẩu mặc định.

Tấn công dấu vân tay

Trong một cuộc tấn công bằng dấu vân tay, cụm mật khẩu được chia nhỏ thành các dấu vân tay bao gồm các tổ hợp một và nhiều ký tự mà người dùng mục tiêu có thể chọn làm mật khẩu của mình. Ví dụ: đối với từ 'mật khẩu', kỹ thuật này sẽ tạo dấu vân tay "p", "a", "s", "s", "w", "o", "r", "d", "pa" , "ss", "wo", "rd", v.v. Những kẻ tấn công thường thực hiện cuộc tấn công này để bẻ khóa các mật khẩu phức tạp như "pass-10".

Để thực hiện cuộc tấn công này, những kẻ tấn công tạo một danh sách các hàm băm mật khẩu duy nhất từ cơ sở dữ liệu hàm băm mật khẩu bị rò rỉ, sau đó thực hiện một cuộc tấn công vũ phu để có được một danh sách từ và tiếp tục bắt đầu cuộc tấn công dấu vân tay.

PRINCE tấn công

Một cuộc tấn công PRObability INfinite Chained Elements (PRINCE) là phiên bản nâng cao của một cuộc tấn công tổ hợp, trong đó, thay vì lấy đầu vào từ hai từ điển khác nhau, kẻ tấn công sử dụng một từ điển đầu vào duy nhất để xây dựng chuỗi các từ kết hợp. Chuỗi này có thể có từ 1 đến n từ trong từ điển đầu vào được nối với nhau để tạo thành một chuỗi từ. Ví dụ: nếu độ dài của các ký tự được đoán là 5, thì các kết hợp sau được tạo từ từ điển đầu vào:

từ có 5 chữ cái

từ 3 chữ cái + từ 2 chữ cái

từ 2 chữ cái + từ 3 chữ cái

từ 1 chữ cái + từ 4 chữ cái

... vân vân.

Chuyển đổi trường hợp tấn công

Trong một cuộc tấn công chuyển đổi trường hợp, những kẻ tấn công thử tất cả các kết hợp chữ hoa và chữ thường có thể có của một từ có trong từ điển đầu vào. Ví dụ: nếu một từ trong từ điển đầu vào là "xyz", tập hợp các kết hợp sau đây sẽ được tạo:

Xyz

Xyz

XYZ

XYZ

xYz

... vân vân.

Tỷ lệ thành công của cuộc tấn công này thấp vì những lý do sau:

* Nếu người dùng sử dụng chữ in hoa thì họ sử dụng nó ở vị trí đầu tiên hoặc ở giữa từ
* Các trường hợp khác, người dùng sử dụng số lượng chữ in thường hoặc viết thường bằng nhau

Tấn công chuỗi Markov

Trong các cuộc tấn công chuỗi Markov, kẻ tấn công thu thập cơ sở dữ liệu mật khẩu và chia mỗi mục nhập mật khẩu thành các âm tiết gồm hai và ba ký tự (2 gam và 3 gam); bằng cách sử dụng các thành phần ký tự này, một bảng chữ cái mới được phát triển, sau đó được khớp với cơ sở dữ liệu mật khẩu hiện có.

Trong giai đoạn đầu của cuộc tấn công này, kẻ tấn công đặt tham số ngưỡng cho số lần xuất hiện của các phần tử và chỉ các chữ cái có trong bảng chữ cái mới xuất hiện ít nhất với số lần tối thiểu mới được chọn. Hơn nữa, kỹ thuật này kết hợp các chữ cái đã chọn thành các từ có độ dài tối đa là tám ký tự, sau đó một cuộc tấn công từ điển được thực hiện để bẻ khóa mật khẩu mục tiêu.

* Tấn công trực tuyến thụ động: Tấn công thụ động là một kiểu tấn công hệ thống không dẫn đến bất kỳ thay đổi nào trong hệ thống. Trong cuộc tấn công này, kẻ tấn công không phải giao tiếp với hệ thống mà theo dõi hoặc ghi lại dữ liệu truyền qua kênh giao tiếp đến và đi từ hệ thống một cách thụ động. Dữ liệu sau đó được sử dụng để đột nhập vào hệ thống. Các kỹ thuật được sử dụng để thực hiện các cuộc tấn công trực tuyến thụ động bao gồm nghe lén dây, tấn công trung gian, tấn công lặp lại, v.v.

Nghe lén dây

Nghe lén gói tin là một hình thức nghe trộm hoặc nghe lén trong đó tin tặc nghe lén thông tin đăng nhập trong quá trình truyền bằng cách bắt các gói Internet. Những kẻ tấn công hiếm khi sử dụng các trình thám thính để thực hiện kiểu tấn công này. Với tính năng nghe lén gói, kẻ tấn công có thể lấy được mật khẩu cho các ứng dụng như email, trang web, SMB, FTP, phiên đăng nhập rlogin hoặc SQL. Khi những kẻ nghe lén chạy trong nền, nạn nhân vẫn không biết về việc nghe lén.

Khi các trình thám thính thu thập các gói ở lớp liên kết dữ liệu, chúng có thể lấy tất cả các gói trên mạng LAN của máy chạy chương trình thám thính. Phương pháp này tương đối khó thực hiện và tính toán phức tạp. Điều này là do một mạng với một trung tâm thực hiện một phương tiện quảng bá mà tất cả các hệ thống chia sẻ trên mạng LAN. Mạng LAN gửi dữ liệu đến tất cả các máy được kết nối với nó. Nếu kẻ tấn công chạy chương trình nghe lén trên một hệ thống trong mạng LAN, kẻ đó có thể thu thập dữ liệu được gửi đến và từ bất kỳ hệ thống nào khác trong mạng LAN. Phần lớn các công cụ nghe trộm rất phù hợp để nghe lén dữ liệu trong môi trường trung tâm. Những công cụ này là những công cụ nghe lén thụ động, vì chúng chờ truyền dữ liệu một cách thụ động trước khi nắm bắt thông tin. Chúng hiệu quả trong việc thu thập dữ liệu từ mạng LAN một cách dễ nhận thấy. Dữ liệu bị bắt có thể bao gồm mật khẩu được gửi đến các hệ thống từ xa trong FTP, phiên rlogin và thư điện tử. Kẻ tấn công sử dụng các thông tin đăng nhập đã nghe lén này để có quyền truy cập trái phép vào hệ thống đích. Có rất nhiều công cụ có sẵn trên Internet để dò tìm dây điện thụ động.

Man-in-the-Middle và Replay Attacks

Khi hai bên đang liên lạc, một cuộc tấn công trung gian (MITM) có thể diễn ra, trong đó bên thứ ba chặn liên lạc giữa hai bên mà họ không hề hay biết. Bên thứ ba nghe trộm lưu lượng và sau đó chuyển nó đi. Để làm được điều này, “người ở giữa” phải nghe lén đồng thời từ cả hai phía của kết nối. Trong một cuộc tấn công MITM, kẻ tấn công giành được quyền truy cập vào các kênh liên lạc giữa nạn nhân và máy chủ để trích xuất thông tin. Kiểu tấn công này thường được sử dụng trong công nghệ telnet và không dây. Không dễ để thực hiện các cuộc tấn công như vậy do số thứ tự TCP và tốc độ truyền thông. Phương pháp này tương đối khó thực hiện và đôi khi có thể bị phá vỡ bằng cách vô hiệu hóa lưu lượng truy cập.

Trong một cuộc tấn công lặp lại, các gói và mã thông báo xác thực bị bắt bằng trình thám thính. Sau khi thông tin liên quan được trích xuất, mã thông báo sẽ được đặt lại trên mạng để có quyền truy cập. Kẻ tấn công sử dụng kiểu tấn công này để phát lại các giao dịch ngân hàng hoặc các kiểu truyền dữ liệu tương tự, với hy vọng sao chép và/hoặc thay đổi các hoạt động, chẳng hạn như gửi tiền hoặc chuyển khoản ngân hàng.

* Tấn công ngoại tuyến: Tấn công ngoại tuyến đề cập đến các cuộc tấn công mật khẩu trong đó kẻ tấn công cố gắng khôi phục mật khẩu văn bản rõ ràng từ kết xuất hàm băm mật khẩu. Các cuộc tấn công ngoại tuyến thường tốn thời gian nhưng có tỷ lệ thành công cao, vì mật khẩu băm có thể bị đảo ngược do không gian khóa nhỏ và độ dài ngắn. Những kẻ tấn công sử dụng các giá trị băm được tính toán trước từ các bảng cầu vồng để thực hiện các cuộc tấn công mạng phân tán và ngoại tuyến.

Tấn công ngoại tuyến

Các cuộc tấn công ngoại tuyến xảy ra khi kẻ xâm nhập kiểm tra tính hợp lệ của mật khẩu. Anh ấy / cô ấy quan sát cách mật khẩu được lưu trữ. Nếu tên người dùng và mật khẩu được lưu trữ trong một tệp có thể đọc được, kẻ tấn công sẽ dễ dàng giành được quyền truy cập vào hệ thống. Do đó, điều quan trọng là phải bảo vệ danh sách mật khẩu và giữ nó ở dạng không thể đọc được, tốt nhất là được mã hóa.

Các cuộc tấn công ngoại tuyến, mặc dù tốn thời gian, nhưng thành công do không gian khóa nhỏ và độ dài ngắn. Đáng chú ý là có nhiều kỹ thuật bẻ mật khẩu khác nhau trên Internet.

Hai ví dụ về các cuộc tấn công ngoại tuyến như sau:

1. Tấn công bàn cầu vồng

2. Tấn công mạng phân tán

Tấn công bảng cầu vồng

Một cuộc tấn công bảng cầu vồng sử dụng kỹ thuật đánh đổi bộ nhớ thời gian bằng mã hóa, đòi hỏi ít thời gian hơn các kỹ thuật khác. Nó sử dụng thông tin đã được tính toán sẵn được lưu trữ trong bộ nhớ để bẻ khóa mã hóa. Trong cuộc tấn công bảng cầu vồng, kẻ tấn công tạo trước một bảng gồm tất cả các mật khẩu có thể có và giá trị băm tương ứng của chúng, được gọi là bảng cầu vồng.

* Bảng cầu vồng: Bảng cầu vồng là một bảng được tính toán trước có chứa các danh sách từ như tệp từ điển và danh sách brute-force cũng như giá trị băm của chúng. Nó là một bảng tra cứu được sử dụng đặc biệt để khôi phục mật khẩu văn bản gốc từ bản mã. Kẻ tấn công sử dụng bảng này để tìm kiếm mật khẩu và cố gắng khôi phục nó từ các hàm băm mật khẩu.

So sánh các giá trị băm: Kẻ tấn công nắm bắt giá trị băm của mật khẩu và so sánh nó với bảng băm được tính toán trước. Nếu một trận đấu được tìm thấy, thì mật khẩu đã bị bẻ khóa. Thật dễ dàng để khôi phục mật khẩu bằng cách so sánh các giá trị băm mật khẩu đã chụp với các bảng được tính toán trước.

Công cụ tạo bảng cầu vồng: rtgen

RainbowCrack là một triển khai có mục đích chung, tận dụng kỹ thuật đánh đổi bộ nhớ thời gian để bẻ khóa các giá trị băm. Dự án này cho phép bạn bẻ khóa mật khẩu băm.

Những kẻ tấn công sử dụng công cụ rtgen của dự án này để tạo ra các bảng cầu vồng. Như được hiển thị trong ảnh chụp màn hình, chương trình rtgen cần một số tham số để tạo bảng cầu vồng.

Cú pháp của dòng lệnh là:

Cú pháp: rtgen hash\_algorithm bộ ký tự plaintext\_len\_min plaintext\_len\_max table\_index chain\_len chain\_num part\_index

* Tấn công mạng phân tán

Tấn công mạng phân tán (DNA) là một kỹ thuật được sử dụng để khôi phục các tệp được bảo vệ bằng mật khẩu sử dụng sức mạnh xử lý không được sử dụng của các máy trải rộng trên mạng để giải mã mật khẩu. Trong cuộc tấn công này, kẻ tấn công cài đặt trình quản lý DNA ở vị trí trung tâm nơi các máy chạy ứng dụng khách DNA có thể truy cập qua mạng. Trình quản lý DNA điều phối cuộc tấn công và chỉ định các phần nhỏ của quá trình tìm kiếm khóa cho các máy được phân phối trên toàn mạng. Ứng dụng khách DNA chạy trong nền, chỉ chiếm thời gian của bộ xử lý không được sử dụng. Chương trình kết hợp khả năng xử lý của tất cả các máy khách được kết nối với mạng và sử dụng nó để bẻ khóa mật khẩu. Những kẻ tấn công sử dụng Bộ công cụ khôi phục mật khẩu (PRTK), được trang bị các công cụ DNA, để thực hiện cuộc tấn công này.

Các đặc điểm của DNA như sau:

* Dễ dàng đọc số liệu thống kê và đồ thị
* Thêm từ điển người dùng để bẻ khóa mật khẩu
* Tối ưu hóa các cuộc tấn công mật khẩu cho các ngôn ngữ cụ thể
* Sửa đổi từ điển người dùng
* Bao gồm chức năng cài đặt máy khách tàng hình
* Tự động cập nhật máy khách trong khi cập nhật máy chủ DNA

DNA có thể được phân loại thành hai mô-đun:

* Giao diện máy chủ DNA

Giao diện máy chủ DNA cho phép người dùng quản lý DNA từ máy chủ. Mô-đun máy chủ DNA cung cấp cho người dùng trạng thái của tất cả các công việc mà máy chủ DNA đang thực hiện. Giao diện chứa các công việc sau:

* + Công việc hiện tại: Hàng công việc hiện tại bao gồm tất cả các công việc được thêm vào danh sách bởi bộ điều khiển. Danh sách công việc hiện tại có nhiều cột, chẳng hạn như số nhận dạng do DNA gán cho công việc, tên của tệp được mã hóa, mật khẩu của người dùng, mật khẩu khớp với khóa có thể mở khóa dữ liệu, trạng thái của công việc, và nhiều cột khác.
  + Công việc đã hoàn thành: Danh sách công việc đã hoàn thành cung cấp thông tin về các công việc giải mã, bao gồm cả mật khẩu. Nó cũng có nhiều cột tương tự như danh sách công việc hiện tại. Các cột này bao gồm số nhận dạng do DNA gán cho công việc, tên của tệp được mã hóa, đường dẫn được giải mã của tệp, khóa được sử dụng để mã hóa và giải mã tệp, ngày và giờ mà máy chủ DNA bắt đầu thực hiện công việc. , ngày và giờ máy chủ DNA hoàn thành công việc, thời gian đã trôi qua, v.v.
* Giao diện máy khách DNA

Người dùng có thể sử dụng giao diện máy khách DNA từ nhiều máy trạm. Giao diện giúp thống kê máy khách phối hợp dễ dàng và có sẵn trên các máy có cài đặt sẵn ứng dụng máy khách DNA. Có một số thành phần, chẳng hạn như tên của ứng dụng khách DNA, tên của nhóm mà ứng dụng khách DNA thuộc về và số liệu thống kê về công việc hiện tại.

Quản lý mạng

Hộp thoại Lưu lượng mạng hỗ trợ khám phá tốc độ mạng mà DNA sử dụng và mỗi độ dài đơn vị công việc của máy khách DNA. Sử dụng chiều dài đơn vị công việc, máy khách DNA có thể hoạt động mà không cần liên hệ với máy chủ DNA. Ứng dụng máy khách DNA có thể liên hệ với máy chủ DNA ở đầu và cuối chiều dài đơn vị công việc.

Người dùng có thể theo dõi hàng đợi trạng thái công việc và DNA. Sau khi thu thập dữ liệu từ hộp thoại Lưu lượng mạng, người dùng có thể sửa đổi công việc của khách hàng. Khi kích thước của chiều dài đơn vị công việc tăng lên, tốc độ của lưu lượng mạng sẽ giảm. Tốc độ lưu lượng truy cập giảm khiến khách hàng làm việc trong công việc mất nhiều thời gian hơn. Do đó, người dùng có thể thực hiện ít yêu cầu hơn đối với máy chủ do giảm băng thông của lưu lượng mạng.

* 1. Leo thang đặc quyền

Nâng cao đặc quyền

Nâng cao đặc quyền là giai đoạn thứ hai của hack hệ thống. Những kẻ tấn công sử dụng mật khẩu có được ở bước đầu tiên để có quyền truy cập vào hệ thống mục tiêu và sau đó cố gắng đạt được các đặc quyền cấp cao hơn trong hệ thống. Các công cụ và kỹ thuật khác nhau mà kẻ tấn công sử dụng để leo thang đặc quyền của chúng được mô tả như sau.

Nâng cấp đặc quyền

Đặc quyền là vai trò bảo mật được gán cho người dùng để sử dụng các chương trình, tính năng, OSS, chức năng, tệp hoặc mã cụ thể, v.v., để giới hạn quyền truy cập của họ theo các loại người dùng khác nhau. Nếu người dùng được chỉ định nhiều đặc quyền hơn, họ có thể sửa đổi hoặc tương tác với nhiều phần bị hạn chế hơn của hệ thống hoặc ứng dụng so với người dùng ít đặc quyền hơn. Ban đầu, những kẻ tấn công giành được quyền truy cập hệ thống với đặc quyền thấp và sau đó cố gắng giành được nhiều đặc quyền hơn để thực hiện các hoạt động bị hạn chế đối với những người dùng có ít đặc quyền hơn. Một cuộc tấn công leo thang đặc quyền là quá trình giành được nhiều đặc quyền hơn so với ban đầu.

Trong một cuộc tấn công leo thang đặc quyền, trước tiên những kẻ tấn công có quyền truy cập vào mạng bằng tài khoản người dùng không phải quản trị viên và sau đó cố gắng giành được các đặc quyền quản trị. Những kẻ tấn công sử dụng các lỗi thiết kế, lỗi lập trình, lỗi và sơ suất cấu hình trong hệ điều hành và ứng dụng phần mềm để giành quyền truy cập quản trị vào mạng và các ứng dụng liên quan.

Sau khi kẻ tấn công giành được quyền truy cập vào hệ thống từ xa bằng tên người dùng và mật khẩu hợp lệ, kẻ tấn công sẽ cố gắng nâng cấp tài khoản người dùng lên một tài khoản có đặc quyền cao hơn, chẳng hạn như quyền của quản trị viên, để thực hiện các hoạt động bị hạn chế. Những đặc quyền này cho phép kẻ tấn công xem thông tin quan trọng/nhạy cảm, xóa tệp hoặc cài đặt các chương trình độc hại như vi-rút, Trojan, sâu, v.v.

Các loại nâng cấp đặc quyền

Cần phải nâng cấp đặc quyền khi bạn muốn truy cập các tài nguyên hệ thống mà bạn không được phép truy cập. Leo thang đặc quyền diễn ra dưới hai hình thức: leo thang đặc quyền theo chiều dọc và leo thang đặc quyền theo chiều ngang.

* Leo thang đặc quyền theo chiều ngang: Trong leo thang đặc quyền theo chiều ngang, người dùng trái phép cố gắng truy cập các tài nguyên, chức năng và các đặc quyền khác thuộc về người dùng được ủy quyền có quyền truy cập tương tự. Chẳng hạn, người dùng ngân hàng trực tuyến A có thể dễ dàng truy cập vào tài khoản ngân hàng của người dùng B.
* Leo thang đặc quyền theo chiều dọc: Trong leo thang đặc quyền theo chiều dọc, người dùng trái phép cố gắng giành quyền truy cập vào các tài nguyên và chức năng của người dùng có đặc quyền cao hơn, chẳng hạn như ứng dụng hoặc quản trị viên trang web. Ví dụ: ai đó sử dụng ngân hàng trực tuyến có thể truy cập trang web bằng các chức năng quản trị.

Nâng cao đặc quyền bằng cách sử dụng DLL Hijacking

Hầu hết các ứng dụng Windows không sử dụng đường dẫn đủ điều kiện khi tải thư viện DLL bên ngoài; thay vào đó, trước tiên họ tìm kiếm thư mục mà chúng đã được tải từ đó. Lợi dụng điều này, nếu kẻ tấn công có thể đặt một tệp DLL độc hại vào thư mục ứng dụng, ứng dụng sẽ thực thi tệp DLL độc hại thay cho tệp DLL thực. Ví dụ: nếu một chương trình ứng dụng ".exe" cần thư viện.dll (thường nằm trong thư mục hệ thống Windows) để cài đặt ứng dụng và không chỉ định đường dẫn thư viện.dll, Windows sẽ tìm kiếm tệp DLL trong thư mục mà từ đó ứng dụng đã được đưa ra. Nếu kẻ tấn công đã đặt DLL trong cùng thư mục với program.exe, thì DLL độc hại đó sẽ tải thay vì DLL thực, cho phép kẻ tấn công có quyền truy cập từ xa vào hệ thống đích.

Những kẻ tấn công sử dụng các công cụ như Robber và PowerSploit để phát hiện các DLL có thể chiếm quyền điều khiển và thực hiện chiếm quyền điều khiển DLL trên hệ thống đích:

cướp

* Robber là một công cụ nguồn mở giúp kẻ tấn công tìm thấy các tệp thực thi dễ bị chiếm quyền điều khiển DLL. Kẻ tấn công sử dụng Robber để tìm ra DLL nào là yêu cầu thực thi mà không có đường dẫn tuyệt đối (kích hoạt quá trình tìm kiếm này); sau đó, những kẻ tấn công có thể đặt DLL độc hại của chúng lên trên đường dẫn tìm kiếm để nó được gọi trước DLL gốc.

Nâng cao đặc quyền bằng cách khai thác các lỗ hổng

Lỗ hổng bảo mật là sự tồn tại của một điểm yếu, lỗi thiết kế hoặc lỗi triển khai có thể dẫn đến một sự kiện không mong muốn ảnh hưởng đến tính bảo mật của hệ thống. Kẻ tấn công sử dụng các lỗ hổng này để thực hiện các cuộc tấn công khác nhau vào tính bảo mật, tính khả dụng hoặc tính toàn vẹn của hệ thống. Các lỗi thiết kế phần mềm và lỗi lập trình dẫn đến các lỗ hổng bảo mật. Những kẻ tấn công khai thác các lỗ hổng phần mềm này, chẳng hạn như lỗi lập trình trong một chương trình hoặc dịch vụ, hoặc trong phần mềm hoặc nhân hệ điều hành, để thực thi mã độc. Khai thác các lỗ hổng phần mềm cho phép kẻ tấn công thực thi một lệnh hoặc mã nhị phân trên máy mục tiêu để giành được các đặc quyền cao hơn các đặc quyền hiện có hoặc bỏ qua các cơ chế bảo mật. Những kẻ tấn công sử dụng các lỗ hổng này thậm chí có thể truy cập vào các tài khoản và thông tin xác thực của người dùng đặc quyền.

Có nhiều kho lưu trữ lỗ hổng công cộng có sẵn trực tuyến cho phép truy cập thông tin về các lỗ hổng phần mềm khác nhau. Những kẻ tấn công tìm kiếm các khai thác dựa trên các trang web khai thác ứng dụng phần mềm và hệ điều hành như SecurityFocus trên (https://www.securityfocus.com) hoặc Khai thác cơ sở dữ liệu (https://www.exploit-db.com) và sử dụng các khai thác này để đạt được những đặc quyền cao.

Nâng cao đặc quyền bằng cách sử dụng Dylib Hijacking

Tương tự như Windows, OS X cũng dễ bị tấn công thư viện động. OS X cung cấp một số phương pháp hợp pháp, chẳng hạn như đặt biến môi trường DYLD\_INSERT\_LIBRARIES, dành riêng cho người dùng. Các phương pháp này buộc trình tải tự động tải các thư viện độc hại vào một tiến trình đang chạy mục tiêu. OS X cho phép tải động các dylib yếu (thư viện động), từ đó cho phép kẻ tấn công đặt một dylib độc hại vào vị trí đã chỉ định. Trong nhiều trường hợp, trình tải tìm kiếm các thư viện động trong nhiều đường dẫn. Điều này giúp kẻ tấn công đưa một dylib độc hại vào một trong các thư mục chính và chỉ cần tải dylib độc hại khi chạy. Những kẻ tấn công có thể sử dụng các phương pháp như vậy để thực hiện các hoạt động độc hại khác nhau như lén lút kiên trì, chèn quy trình thời gian chạy, bỏ qua phần mềm bảo mật và bỏ qua Gatekeeper.

Dylib Hijack Scanner giúp kẻ tấn công phát hiện các dylib dễ bị tấn công. Sau khi xác định các dylib dễ bị tấn công, kẻ tấn công sử dụng các công cụ như Dylib Hijack để thực hiện việc chiếm quyền điều khiển dylib trên hệ thống đích.

Nâng cao đặc quyền bằng cách sử dụng các lỗ hổng Spectre và Meltdown

Spectre và Meltdown là các lỗ hổng CPU gần đây được tìm thấy trong thiết kế của bộ xử lý hiện đại, bao gồm cả chip của AMD, ARM và Intel, do quá trình tối ưu hóa hiệu suất trong các bộ xử lý này gây ra. Kẻ tấn công có thể khai thác các lỗ hổng này để giành quyền truy cập trái phép và lấy cắp thông tin hệ thống quan trọng như thông tin đăng nhập, khóa bí mật, tổ hợp phím, khóa mã hóa, v.v. được lưu trữ trong bộ nhớ của ứng dụng để leo thang đặc quyền. Các cuộc tấn công này có thể được thực hiện do việc xác minh thông thường các đặc quyền của người dùng bị gián đoạn thông qua sự tương tác của các tính năng như dự đoán nhánh, thực thi không theo thứ tự, lưu vào bộ nhớ đệm và thực thi suy đoán. Sử dụng các lỗ hổng này, kẻ tấn công có thể khai thác nhiều tài nguyên CNTT khác nhau, chẳng hạn như hầu hết các hệ điều hành, máy chủ, PC, hệ thống đám mây và thiết bị di động.

* Lỗ hổng bóng ma

Lỗ hổng Spectre được tìm thấy trong nhiều bộ xử lý hiện đại, bao gồm bộ xử lý Apple, AMD, ARM, Intel, Samsung và Qualcomm. Lỗ hổng này cho phép kẻ tấn công lừa bộ xử lý khai thác việc thực thi suy đoán để đọc dữ liệu bị hạn chế. Các bộ xử lý hiện đại triển khai thực thi suy đoán để dự đoán tương lai nhằm hoàn thành việc thực thi nhanh hơn. Ví dụ: nếu con chip xác định rằng một chương trình bao gồm nhiều câu lệnh có điều kiện, nó sẽ bắt đầu thực hiện và kết thúc tất cả các kết quả có thể xảy ra trước khi chương trình thực hiện. Kẻ tấn công có thể khai thác lỗ hổng này theo nhiều cách khác nhau:

* Bộ xử lý buộc phải thực hiện một thao tác đọc suy đoán trước khi thực hiện kiểm tra giới hạn. Do đó, kẻ tấn công có thể truy cập và đọc các vị trí bộ nhớ ngoài giới hạn.
* Khi thực hiện các câu lệnh có điều kiện, để xử lý nhanh hơn, bộ xử lý sử dụng dự đoán rẽ nhánh để chọn đường dẫn thực thi theo suy đoán. Những kẻ tấn công có thể khai thác tính năng này để buộc bộ xử lý đưa ra quyết định suy đoán không phù hợp và tiếp tục truy cập dữ liệu ngoài phạm vi.

Kẻ tấn công có thể sử dụng lỗ hổng này để đọc các vị trí bộ nhớ liền kề của một quy trình và truy cập thông tin mà họ không được phép. Lỗ hổng này giúp kẻ tấn công trích xuất thông tin bí mật, chẳng hạn như thông tin đăng nhập được lưu trữ trong trình duyệt, từ quá trình mục tiêu đó. Trong một số trường hợp nhất định, bằng cách sử dụng lỗ hổng này, kẻ tấn công thậm chí có thể đọc bộ nhớ kernel hoặc thực hiện một cuộc tấn công dựa trên web bằng JavaScript.

* Lỗ hổng Meltdown
* Lỗ hổng Meltdown được tìm thấy trong tất cả các bộ xử lý Intel và ARM do Apple triển khai. Lỗ hổng này cho phép kẻ tấn công lừa một quy trình truy cập vào bộ nhớ ngoài giới hạn bằng cách khai thác các cơ chế tối ưu hóa CPU chẳng hạn như thực thi suy đoán. Ví dụ, kẻ tấn công yêu cầu truy cập vào một vị trí bộ nhớ bất hợp pháp. Anh ấy/cô ấy gửi một yêu cầu thứ hai để đọc một vị trí bộ nhớ hợp lệ một cách có điều kiện. Trong trường hợp này, bộ xử lý sử dụng thực thi suy đoán sẽ hoàn thành việc đánh giá kết quả cho cả hai yêu cầu trước khi kiểm tra yêu cầu đầu tiên. Khi bộ xử lý kiểm tra rằng yêu cầu đầu tiên không hợp lệ, nó sẽ từ chối cả hai yêu cầu sau khi kiểm tra các đặc quyền. Mặc dù bộ xử lý từ chối cả hai yêu cầu, kết quả của cả hai yêu cầu vẫn còn trong bộ nhớ cache. Bây giờ kẻ tấn công gửi nhiều yêu cầu hợp lệ để truy cập các vị trí bộ nhớ ngoài giới hạn.
* Kẻ tấn công có thể sử dụng lỗ hổng này để leo thang đặc quyền bằng cách buộc một quá trình không có đặc quyền đọc các vị trí bộ nhớ liền kề khác, chẳng hạn như bộ nhớ nhân và bộ nhớ vật lý. Điều này dẫn đến thông tin hệ thống quan trọng như thông tin đăng nhập, khóa riêng tư, v.v. bị tiết lộ.

Nâng cao đặc quyền bằng cách sử dụng Mạo danh đường ống được đặt tên

Trong HĐH Windows, các đường dẫn có tên được sử dụng để cung cấp giao tiếp hợp pháp giữa các quy trình đang chạy. Trong kỹ thuật này, các thông báo được trao đổi giữa các quy trình bằng một tệp. Ví dụ: nếu quy trình A muốn gửi tin nhắn đến quy trình B khác, thì quy trình A sẽ ghi tin nhắn vào một tệp và quy trình B đọc tin nhắn từ tệp đó. Những kẻ tấn công thường khai thác kỹ thuật này để nâng cấp đặc quyền của chúng trên hệ thống nạn nhân lên tài khoản người dùng có đặc quyền truy cập cao hơn.

Trong bất kỳ hệ thống Windows nào, khi một quy trình tạo một đường ống, nó sẽ hoạt động như một máy chủ đường ống. Nếu bất kỳ quy trình nào khác muốn giao tiếp với quy trình này, nó sẽ kết nối với đường ống này và trở thành máy khách đường ống. Khi một máy khách kết nối với đường ống, máy chủ đường ống có thể sử dụng các đặc quyền truy cập và bối cảnh bảo mật của máy khách đường ống. Kẻ tấn công khai thác tính năng này bằng cách tạo một máy chủ ống có ít đặc quyền hơn và cố gắng kết nối với máy khách có đặc quyền cao hơn máy chủ.

Những kẻ tấn công sử dụng các công cụ như Metasploit để thực hiện mạo danh đường ống có tên trên máy chủ mục tiêu. Những kẻ tấn công khai thác các lỗ hổng tồn tại trong máy chủ từ xa mục tiêu để có được một phiên hoạt động và sử dụng các lệnh Metasploit chẳng hạn như getsystem để giành được các đặc quyền cấp quản trị và trích xuất các hàm băm mật khẩu của tài khoản quản trị viên/người dùng.

Nâng cao đặc quyền bằng cách khai thác các dịch vụ được định cấu hình sai

Những kẻ tấn công thường khai thác các lỗ hổng zero-day tồn tại trong các hệ thống mục tiêu để leo thang đặc quyền. Nếu những kẻ tấn công không thể tìm thấy những khai thác như vậy, chúng sẽ cố gắng leo thang đặc quyền bằng cách lạm dụng các dịch vụ được định cấu hình sai trong HĐH đích. Cấu hình dịch vụ hệ thống không an toàn hoặc không phù hợp cho phép kẻ tấn công nâng cao đặc quyền của chúng trong hệ thống đích. Ví dụ: kẻ tấn công khai thác các dịch vụ bị định cấu hình sai, chẳng hạn như đường dẫn dịch vụ không được trích dẫn, quyền đối tượng dịch vụ, cài đặt không giám sát, cấu hình và tự động chạy sổ đăng ký có thể sửa đổi, v.v. để nâng cao đặc quyền truy cập.

Những kẻ tấn công sử dụng các công cụ như Metasploit để có được phiên hoạt động với máy chủ mục tiêu. Sau khi thiết lập một phiên hoạt động, kẻ tấn công sử dụng các công cụ như PowerSploit để phát hiện các dịch vụ bị định cấu hình sai tồn tại trong hệ điều hành đích.

* Đường dẫn dịch vụ không được trích dẫn

Trong HĐH Windows, khi một dịch vụ bắt đầu chạy, hệ thống sẽ cố gắng tìm vị trí của tệp thực thi để khởi chạy dịch vụ thành công. Nói chung, đường dẫn thực thi được đặt trong dấu ngoặc kép "", để hệ thống có thể dễ dàng xác định vị trí tệp nhị phân của ứng dụng. Một số tệp thực thi có thể không bao gồm các đường dẫn được trích dẫn và bao gồm khoảng trắng ở giữa; trong trường hợp này, hệ thống sẽ cố gắng tìm tệp nhị phân của ứng dụng bằng cách tìm kiếm tất cả các thư mục tồn tại trong đường dẫn cho đến khi tìm thấy tệp thực thi. Những kẻ tấn công khai thác các dịch vụ có đường dẫn không được trích dẫn chạy dưới các đặc quyền của HỆ THỐNG để nâng cao các đặc quyền của chúng.

* Quyền đối tượng dịch vụ
* Quyền dịch vụ được định cấu hình sai có thể cho phép kẻ tấn công sửa đổi hoặc định cấu hình lại các thuộc tính được liên kết với dịch vụ đó. Điều này thậm chí có thể dẫn đến việc thay đổi vị trí của tệp nhị phân ứng dụng thành tệp thực thi độc hại do kẻ tấn công tạo ra. Bằng cách khai thác các dịch vụ như vậy, kẻ tấn công thậm chí có thể thêm người dùng mới vào nhóm quản trị viên cục bộ trong hệ thống. Sau đó, những kẻ tấn công chiếm quyền điều khiển tài khoản mới để nâng cao đặc quyền truy cập của chúng.
* Cài đặt không giám sát

Cài đặt không giám sát cho phép kẻ tấn công triển khai Windows OSS mà không cần sự can thiệp của quản trị viên. Quản trị viên cần dọn sạch thủ công các chi tiết cài đặt không giám sát được lưu trữ trong tệp Unattend.xml. Tệp XML này lưu trữ tất cả thông tin liên quan đến cài đặt cấu hình được đặt trong quá trình cài đặt và cũng có thể bao gồm thông tin nhạy cảm như cấu hình tài khoản cục bộ, tên người dùng và thậm chí cả mật khẩu đã giải mã.

Trong hệ thống Windows, tệp Unattend.xml được lưu trữ ở một trong các vị trí sau:

C:\Windows\Panther\

C:\Windows\Panther\Không giám sát\

C:\Windows\System32\

C:\Windows\System32\sysprep\

Nếu kẻ tấn công có thể truy cập vào tệp này, thì chúng có thể dễ dàng lấy được thông tin xác thực và cài đặt cấu hình được sử dụng trong quá trình cài đặt dịch vụ hoặc ứng dụng đó. Những kẻ tấn công sử dụng thông tin này để leo thang đặc quyền.

Các kỹ thuật leo thang đặc quyền khác

* Thao tác mã thông báo truy cập

Trong HĐH Windows, mã thông báo truy cập được sử dụng để xác định bối cảnh bảo mật của quy trình hoặc luồng. Các mã thông báo này bao gồm hồ sơ truy cập (danh tính và đặc quyền) của người dùng được liên kết với một quy trình. Sau khi người dùng được xác thực, hệ thống sẽ tạo mã thông báo truy cập. Mọi quy trình mà người dùng thực hiện đều sử dụng mã thông báo truy cập này. Hệ thống xác minh mã thông báo truy cập này khi một quy trình đang truy cập vào một đối tượng được bảo mật.

Bất kỳ người dùng Windows nào cũng có thể sửa đổi các mã thông báo truy cập này để quy trình có vẻ thuộc về một số người dùng khác chứ không phải người đã bắt đầu quy trình. Sau đó, quy trình có được bối cảnh bảo mật của mã thông báo mới. Ví dụ: quản trị viên Windows phải đăng nhập với tư cách là người dùng bình thường và cần chạy các công cụ của họ với quyền quản trị viên bằng cách sử dụng lệnh thao tác mã thông báo "runas". Những kẻ tấn công có thể khai thác điều này để truy cập mã thông báo của người dùng khác hoặc tạo mã thông báo giả mạo để leo thang đặc quyền và thực hiện các hoạt động độc hại trong khi trốn tránh bị phát hiện.

* Application Shimming
* Hệ điều hành Windows sử dụng Khung tương thích ứng dụng Windows được gọi là miếng chêm để cung cấp khả năng tương thích giữa các phiên bản Windows cũ hơn và mới hơn. Ví dụ: làm mờ ứng dụng cho phép các chương trình được tạo cho Windows XP tương thích với Windows 10. Miếng chêm cung cấp vùng đệm giữa chương trình và HĐH. Bộ đệm này được tham chiếu khi một chương trình được thực thi để xác minh xem chương trình có yêu cầu quyền truy cập vào cơ sở dữ liệu shim hay không. Khi một chương trình cần giao tiếp với HĐH, cơ sở dữ liệu shim sử dụng API hooking để chuyển hướng mã. Tất cả các miếng chêm được cài đặt bởi trình cài đặt Windows mặc định (sbinst.exe) được lưu trữ tại &WINDIR%\AppPatch\sysmain.sdb hklm\software\microsoft\windows nt\currentversion\appcompatflags\installsdb

Miếng chêm chạy ở chế độ người dùng và chúng không thể sửa đổi hạt nhân. Một số miếng chêm này có thể được sử dụng để bỏ qua UAC (RedirectEXE), tiêm DLL độc hại (InjectDLL), chiếm địa chỉ bộ nhớ (GetProcAddress), v.v. Kẻ tấn công có thể sử dụng các miếng chêm này để thực hiện các cuộc tấn công khác nhau bao gồm vô hiệu hóa Windows Defender, leo thang đặc quyền, cài đặt cửa hậu , vân vân.

* Điểm yếu của quyền hệ thống tập tin

Nhiều quy trình trong Windows OSS thực thi tự động các tệp nhị phân như một phần chức năng của chúng hoặc để thực hiện các hành động nhất định. Nếu quyền hệ thống tệp của các tệp nhị phân này không được đặt đúng cách thì tệp nhị phân đích có thể được thay thế bằng tệp độc hại và quy trình thực tế có thể thực thi nó. Nếu quy trình đang thực thi tệp nhị phân này có quyền cấp cao hơn, thì tệp nhị phân cũng thực thi theo quyền cấp cao hơn, có thể bao gồm HỆ THỐNG. Những kẻ tấn công có thể khai thác kỹ thuật này để thay thế các tệp nhị phân gốc bằng các tệp nhị phân độc hại để leo thang đặc quyền. Những kẻ tấn công sử dụng kỹ thuật này để thao túng các tệp nhị phân dịch vụ Windows và trình cài đặt tự giải nén.

* Đánh chặn đường dẫn

Chặn đường dẫn là một phương pháp đặt một tệp thực thi trong một đường dẫn cụ thể theo cách mà ứng dụng sẽ thực thi nó thay cho mục tiêu hợp pháp. Kẻ tấn công có thể khai thác một số lỗ hổng hoặc cấu hình sai để thực hiện chặn đường dẫn như đường dẫn không được trích dẫn (đường dẫn dịch vụ và đường dẫn tắt), cấu hình sai biến môi trường đường dẫn và chiếm đoạt thứ tự tìm kiếm. Chặn đường dẫn giúp kẻ tấn công duy trì sự bền bỉ trên hệ thống và leo thang đặc quyền.

* Nhiệm vụ theo lịch trình

Hệ điều hành Windows bao gồm các tiện ích như 'at' và 'schtasks.' Người dùng có quyền quản trị viên có thể sử dụng các tiện ích này cùng với Trình lập lịch tác vụ để lên lịch cho các chương trình hoặc tập lệnh có thể được thực thi vào một ngày và giờ cụ thể. Nếu người dùng cung cấp xác thực phù hợp, anh ấy/cô ấy cũng có thể lên lịch tác vụ từ hệ thống từ xa bằng cách sử dụng lệnh gọi thủ tục từ xa (RPC). Kẻ tấn công có thể sử dụng kỹ thuật này để thực thi các chương trình độc hại khi khởi động hệ thống, duy trì tính bền vững, thực hiện thực thi từ xa, leo thang đặc quyền, v.v.

* Khởi chạy Daemon
* Trong quá trình khởi động MacOS và OS X, launchd được thực thi để hoàn tất quá trình khởi tạo hệ thống. Các tham số cho mỗi trình nền cấp hệ thống khởi chạy theo yêu cầu được tìm thấy trong /System/Library/LaunchDaemons và /Library/LaunchDaemons được tải bằng launchd. Các trình nền này có các tệp danh sách thuộc tính (plist) được liên kết với các tệp thực thi chạy tại thời điểm khởi động. Kẻ tấn công có thể tạo và cài đặt một trình nền khởi chạy mới, có thể được định cấu hình để thực thi khi khởi động bằng cách sử dụng launchd hoặc launchctl để tải plist vào các thư mục có liên quan. Các cấu hình yếu cho phép kẻ tấn công thay đổi tệp thực thi của trình nền khởi chạy hiện có để duy trì tính bền vững hoặc leo thang đặc quyền.
* Sửa đổi Plist
* Trong MacOS và OS X, các tệp plist (danh sách thuộc tính) bao gồm tất cả thông tin cần thiết để định cấu hình ứng dụng và dịch vụ. Các tệp này mô tả thời điểm chương trình nên thực thi, đường dẫn tệp thực thi, tham số chương trình, quyền hệ điều hành cần thiết, v.v. Các tệp plist được lưu trữ tại các vị trí cụ thể như /Library/Preferences (thực thi với đặc quyền cấp cao) và ~/Library/Preferences (thực thi với đặc quyền của người dùng). Những kẻ tấn công có thể truy cập và thay đổi các tệp plist này để thực thi mã độc thay mặt cho người dùng hợp pháp, đồng thời sử dụng chúng như một cơ chế duy trì lâu dài và để leo thang đặc quyền.
* Setuid và Setgid

Trong Linux và MacOS, nếu một ứng dụng sử dụng setuid hoặc setgid, ứng dụng sẽ thực thi tương ứng với các đặc quyền của người dùng hoặc nhóm sở hữu. Nói chung, các ứng dụng chạy dưới quyền của người dùng hiện tại. Có một số trường hợp mà các chương trình phải được thực thi với các đặc quyền nâng cao nhưng người dùng đang chạy chương trình không cần các đặc quyền nâng cao. Trong trường hợp này, người ta có thể đặt cờ setuid hoặc setgid cho ứng dụng của họ. Kẻ tấn công có thể khai thác các ứng dụng có cờ setuid hoặc setgid để thực thi mã độc với các đặc quyền nâng cao.

* Web shell

Vỏ web là tập lệnh dựa trên web cho phép truy cập vào máy chủ web. Vỏ web có thể được tạo trong tất cả các OSS như Windows, Linux, MacOS và OS X. Những kẻ tấn công tạo vỏ web để đưa tập lệnh độc hại vào máy chủ web nhằm duy trì quyền truy cập liên tục và leo thang đặc quyền. Những kẻ tấn công sử dụng vỏ web làm cửa hậu để giành quyền truy cập và kiểm soát máy chủ từ xa. Nói chung, trình bao web chạy theo đặc quyền của người dùng hiện tại. Sử dụng vỏ web, kẻ tấn công có thể thực hiện leo thang đặc quyền bằng cách khai thác các lỗ hổng hệ thống cục bộ. Sau khi leo thang đặc quyền, kẻ tấn công có thể cài đặt phần mềm độc hại, thay đổi quyền của người dùng, thêm hoặc xóa người dùng, đánh cắp thông tin đăng nhập, đọc email, v.v.

* Lạm dụng quyền Sudo

Sudo (người dùng thay thế do) là một tiện ích hệ thống dựa trên UNIX và Linux cho phép người dùng chạy các lệnh với tư cách là siêu người dùng hoặc root bằng cách sử dụng các đặc quyền bảo mật của người dùng khác. Tệp /etc/sudoers bao gồm cấu hình quyền sudo. Tệp này chứa thông tin chi tiết về quyền truy cập, bao gồm các lệnh được phép chạy có hoặc không có mật khẩu cho mỗi người dùng hoặc nhóm.

Kẻ tấn công có thể lạm dụng sudo để leo thang đặc quyền của chúng để chạy các chương trình mà người dùng bình thường không được phép chạy. Ví dụ: nếu kẻ tấn công có quyền sudo để chạy lệnh cp thì kẻ đó có thể ghi đè tệp /etc/sudoers hoặc /etc/shadow bằng tệp độc hại của chính kẻ đó. Bằng cách ghi đè nội dung của tệp sudoers, anh ấy/cô ấy có thể chỉnh sửa các quyền để chạy các lệnh hoặc chương trình bị hạn chế khác nhau nhằm khởi động các cuộc tấn công tiếp theo vào hệ thống.

* Lạm dụng quyền SUID và SGID

Đặt Nhận dạng Người dùng (SUID) và Đặt Nhận dạng Nhóm (SGID) là các quyền truy cập được cấp cho một tệp chương trình trong các hệ thống dựa trên UNIX. Các quyền này thường cho phép người dùng trên hệ thống chạy chương trình có đặc quyền nâng cao tạm thời hoặc đặc quyền gốc để thực thi một tác vụ cụ thể. Các tệp có quyền SUID và SGID chạy với đặc quyền cao hơn.

Trong Linux, có một số lệnh và tệp nhị phân có thể được thực thi bởi những kẻ tấn công để nâng cao đặc quyền của chúng từ người dùng không phải root lên người dùng root, nếu các cờ của quyền SUID và SGID được đặt. Một số lệnh thực thi mà kẻ tấn công có thể sử dụng để tạo shell và leo thang đặc quyền là Nmap, vim, less, more, Bash, Cat, Cp, echo, find, Nano, v.v.

Kẻ tấn công có thể sử dụng các lệnh sau để tìm các tệp SUID và SGID trong hệ thống đích:

# Find SUID

find/-perm -u-s -type f 2>/dev/null

# Find GUID

find -perm -g-s -type f 2>/dev/null

* Khai thác hạt nhân

Khai thác kernel đề cập đến các chương trình có thể khai thác các lỗ hổng có trong kernel để thực thi các lệnh hoặc mã tùy ý với các đặc quyền cao hơn. Bằng cách khai thác thành công các lỗ hổng hạt nhân, kẻ tấn công có thể đạt được quyền truy cập cấp siêu người dùng hoặc cấp gốc vào hệ thống đích. Để chạy khai thác kernel, kẻ tấn công phải có chi tiết cấu hình của hệ thống đích.

Những kẻ tấn công sử dụng các lệnh sau để lấy thông tin chi tiết như hệ điều hành, phiên bản kernel và kiến trúc của hệ thống đích:

# OS

uname -a

# Kernel version

cat /etc/issue

# Architecture

cat /proc/version

Những kẻ tấn công tìm kiếm https://www.exploit-db.com và thực thi các tập lệnh Python chẳng hạn như linprivchecker.py để phát hiện các hoạt động khai thác nhân để tăng đặc quyền.

* 1. Thực thi ứng dụng

Duy trì quyền truy cập

Sau khi giành được quyền truy cập và leo thang đặc quyền trên hệ thống mục tiêu, giờ đây, những kẻ tấn công cố gắng duy trì quyền truy cập của chúng để khai thác thêm hệ thống mục tiêu hoặc biến hệ thống bị xâm phạm thành bệ phóng để từ đó tấn công các hệ thống khác trong mạng. Những kẻ tấn công thực thi từ xa các ứng dụng độc hại như keylogger, phần mềm gián điệp và các chương trình độc hại khác để duy trì quyền truy cập của chúng vào hệ thống đích và đánh cắp thông tin quan trọng như tên người dùng và mật khẩu. Những kẻ tấn công che giấu các chương trình hoặc tệp độc hại của chúng bằng cách sử dụng rootkit, steganography, luồng dữ liệu NTFS, v.v. để duy trì quyền truy cập của chúng vào hệ thống đích.

Thực hiện các ứng dụng

Sau khi những kẻ tấn công giành được các đặc quyền cao hơn trong hệ thống đích bằng cách thử các nỗ lực leo thang đặc quyền khác nhau, chúng có thể cố gắng thực thi một ứng dụng độc hại bằng cách khai thác lỗ hổng để thực thi mã tùy ý. Bằng cách thực thi các ứng dụng độc hại, kẻ tấn công có thể đánh cắp thông tin cá nhân, truy cập trái phép vào tài nguyên hệ thống, bẻ khóa mật khẩu, chụp ảnh màn hình, cài đặt cửa hậu để duy trì quyền truy cập dễ dàng, v.v.

Những kẻ tấn công thực thi các ứng dụng độc hại ở giai đoạn này trong một quy trình được gọi là "sở hữu" hệ thống. Khi họ có được đặc quyền quản trị, họ sẽ thực thi các ứng dụng. Những kẻ tấn công thậm chí có thể cố gắng làm như vậy từ xa trên máy của nạn nhân để thu thập thông tin tương tự như trên.

Các chương trình độc hại mà kẻ tấn công thực thi trên hệ thống đích có thể là:

* Cửa hậu: Chương trình được thiết kế để từ chối hoặc làm gián đoạn hoạt động, thu thập thông tin dẫn đến khai thác hoặc mất quyền riêng tư hoặc giành quyền truy cập trái phép vào tài nguyên hệ thống.
* Phần mềm bẻ khóa: Các thành phần của phần mềm hoặc chương trình được thiết kế để bẻ khóa mã hoặc mật khẩu.
* Keylogger: Đây có thể là phần cứng hoặc phần mềm. Trong cả hai trường hợp, mục tiêu là ghi lại từng lần nhấn phím được thực hiện trên bàn phím máy tính.
* Phần mềm gián điệp: Phần mềm gián điệp có thể chụp ảnh màn hình và gửi chúng đến một vị trí cụ thể do tin tặc xác định. Với mục đích này, những kẻ tấn công phải duy trì quyền truy cập vào máy tính của nạn nhân. Sau khi lấy được tất cả thông tin cần thiết từ máy tính của nạn nhân, kẻ tấn công sẽ cài đặt một số cửa hậu để duy trì quyền truy cập dễ dàng vào nó trong tương lai.

Kỹ thuật thực thi mã từ xa

Kỹ thuật thực thi mã từ xa là các chiến thuật khác nhau mà kẻ tấn công có thể sử dụng để thực thi mã độc hại trên hệ thống từ xa. Những kỹ thuật này thường được thực hiện sau khi thỏa hiệp hệ thống ban đầu và tiếp tục mở rộng quyền truy cập vào các hệ thống từ xa có trên mạng đích.

Một số ví dụ về kỹ thuật thực thi mã từ xa như sau:

* Khai thác để Thực thi Client
* Thực hành viết mã không an toàn trong phần mềm có thể khiến phần mềm dễ bị tấn công. Những kẻ tấn công có thể khai thác các lỗ hổng cơ bản này trong phần mềm thông qua các hoạt động khai thác tập trung và có mục tiêu với mục tiêu thực thi mã tùy ý để duy trì quyền truy cập vào hệ thống từ xa mục tiêu.
* Các loại khai thác khác nhau để thực thi ứng dụng khách như sau:
* Khai thác dựa trên trình duyệt web

Những kẻ tấn công nhắm mục tiêu vào các trình duyệt web thông qua các liên kết lừa đảo và thỏa hiệp theo từng ổ đĩa. Các hệ thống từ xa có thể bị xâm phạm thông qua trình duyệt web thông thường hoặc thông qua một số người dùng là nạn nhân của các liên kết lừa đảo trực tuyến đến các trang web do kẻ tấn công kiểm soát được sử dụng để khai thác trình duyệt web. Loại khai thác này không cần sự can thiệp của người dùng để thực hiện.

* Khai thác dựa trên ứng dụng Office

Những kẻ tấn công khai thác dựa trên ứng dụng Office nhắm mục tiêu vào các ứng dụng văn phòng phổ biến như Microsoft Office thông qua các biến thể lừa đảo khác nhau. Email chứa liên kết đến tệp độc hại được gửi trực tiếp đến người dùng cuối để tải xuống. Để chạy khai thác, người dùng cuối được yêu cầu mở một tài liệu hoặc tệp độc hại.

* Khai thác dựa trên ứng dụng của bên thứ ba

Những kẻ tấn công cũng có thể khai thác các ứng dụng của bên thứ ba thường được sử dụng được triển khai như một phần của phần mềm. Các ứng dụng như Adobe Reader, Flash, v.v. thường là mục tiêu của những kẻ tấn công để giành quyền truy cập vào các hệ thống từ xa.

* Nhiệm vụ theo lịch trình

Các tác vụ đã lên lịch cho phép người dùng tự động thực hiện các tác vụ thông thường được chọn cho máy tính. Có hai tiện ích, at và schtasks, có thể được sử dụng cùng với Bộ lập lịch tác vụ của Windows để thực thi mã hoặc tập lệnh cụ thể vào một ngày và giờ đã lên lịch. Sử dụng lập lịch tác vụ, kẻ tấn công có thể thực thi các chương trình độc hại khi khởi động hệ thống hoặc lên lịch cho một ngày và giờ cụ thể để duy trì quyền truy cập vào hệ thống đích và tiếp tục thực hiện mã từ xa để có được các đặc quyền cấp quản trị viên đối với hệ thống từ xa.

* Thực hiện dịch vụ

Dịch vụ hệ thống là các chương trình chạy và hoạt động ở phần phụ trợ của HĐH. Những kẻ tấn công chạy các tệp nhị phân hoặc các lệnh có thể giao tiếp với các dịch vụ hệ thống Windows, chẳng hạn như Trình quản lý điều khiển dịch vụ. Kỹ thuật thực thi mã này được thực hiện bằng cách tạo một dịch vụ mới hoặc bằng cách sửa đổi một dịch vụ hiện có tại thời điểm leo thang đặc quyền hoặc duy trì quyền truy cập.

* Công cụ quản lý Windows (WMI)

WMI là một tính năng trong quản trị Windows, quản lý dữ liệu và hoạt động trên HĐH Windows, đồng thời cung cấp nền tảng để truy cập tài nguyên hệ thống Windows cục bộ và từ xa. Kẻ tấn công có thể sử dụng tính năng WMI để tương tác với hệ thống mục tiêu từ xa và sử dụng nó để thực hiện thu thập thông tin về tài nguyên hệ thống và tiếp tục thực thi mã để duy trì quyền truy cập vào hệ thống mục tiêu.

Quản lý từ xa Windows (WinRM)

WinRM là một giao thức dựa trên Windows được thiết kế để cho phép người dùng chạy tệp thực thi để sửa đổi các dịch vụ hệ thống và sổ đăng ký trên một hệ thống từ xa. Kẻ tấn công có thể sử dụng lệnh winrm để tương tác với WinRM và thực hiện tải trọng trên hệ thống từ xa như một phần của chuyển động ngang.

Keylogger

Keylogger là chương trình phần mềm hoặc thiết bị phần cứng ghi lại các phím được gõ trên bàn phím máy tính (còn gọi là ghi nhật ký tổ hợp phím) của một người dùng máy tính cá nhân hoặc một mạng máy tính. Bạn có thể xem tất cả các lần nhấn phím trên máy tính của nạn nhân bất kỳ lúc nào trong hệ thống của mình bằng cách cài đặt thiết bị phần cứng hoặc chương trình này. Nó ghi lại gần như tất cả các lần nhấn phím trên bàn phím của người dùng và lưu thông tin đã ghi trong một tệp văn bản. Khi keylogger ẩn các quy trình và giao diện của chúng, mục tiêu không biết về keylogger. Các văn phòng và ngành công nghiệp sử dụng keylogger để giám sát các hoạt động trên máy tính của nhân viên và chúng cũng có thể được sử dụng trong môi trường gia đình để cha mẹ giám sát các hoạt động trên Internet của trẻ em.

Keylogger, khi được liên kết với phần mềm gián điệp, sẽ giúp truyền thông tin của người dùng cho bên thứ ba không xác định. Những kẻ tấn công sử dụng nó một cách bất hợp pháp cho các mục đích xấu, chẳng hạn như đánh cắp thông tin nhạy cảm và bí mật về nạn nhân. Thông tin nhạy cảm này bao gồm ID email, mật khẩu, chi tiết ngân hàng, hoạt động của phòng trò chuyện, trò chuyện chuyển tiếp qua Internet (IRC), tin nhắn tức thời, số ngân hàng và số thẻ tín dụng. Dữ liệu được truyền qua kết nối Internet được mã hóa cũng dễ bị keylogging vì keylogger theo dõi các lần nhấn phím trước khi mã hóa.

Chương trình keylogger được cài đặt vào hệ thống của người dùng một cách vô hình thông qua tệp đính kèm email hoặc tải xuống "lái xe" khi người dùng truy cập một số trang web nhất định. Bộ ghi thao tác gõ phím vật lý "ngồi" giữa phần cứng bàn phím và HĐH, để chúng có thể không bị phát hiện và ghi lại mọi thao tác gõ phím.

Keylogger có thể:

* Ghi lại mọi lần nhấn phím được gõ trên bàn phím của người dùng
* Chụp ảnh màn hình theo định kỳ, hiển thị hoạt động của người dùng như các ký tự đã nhập hoặc nút chuột được nhấp
* Theo dõi các hoạt động của người dùng bằng cách ghi lại tiêu đề Cửa sổ, tên của các ứng dụng đã khởi chạy và các thông tin khác
* Giám sát hoạt động trực tuyến của người dùng bằng cách ghi lại địa chỉ của các trang web đã truy cập và với các từ khóa đã nhập
* Ghi lại tất cả tên đăng nhập, số ngân hàng và số thẻ tín dụng cũng như mật khẩu, bao gồm mật khẩu ẩn hoặc dữ liệu được hiển thị trong dấu hoa thị hoặc khoảng trống
* Ghi lại các cuộc hội thoại trò chuyện trực tuyến
* Tạo các bản sao trái phép của cả email gửi đi và gửi đến

Các loại keylogger:

* Hardware keystroke loggers
  + PC/BIOS nhúng
  + Keylogger bàn phím
  + Keylogger bên ngoài
* Software Keystroke Loggers
  + Phần mềm kelooger
  + Keylogger Kernel/Rootkit/Device Driver
  + Keylogger dựa trên Hypervisor
  + Keylogger dựa trên biểu mẫu
  + Keylogger dựa trên JavaScript
  + Keylogger dựa trên bộ nhớ

Phần mềm gián điệp

Phần mềm gián điệp là phần mềm giám sát máy tính lén lút cho phép bạn bí mật ghi lại tất cả các hoạt động của người dùng trên máy tính mục tiêu. Nó tự động gửi nhật ký cho kẻ tấn công từ xa bằng Internet (qua email, FTP, lệnh và kiểm soát thông qua lưu lượng được mã hóa, HTTP, DNS, v.v.). Nhật ký gửi bao gồm thông tin về tất cả các khu vực của hệ thống, chẳng hạn như email đã gửi, trang web đã truy cập, mọi thao tác gõ phím (bao gồm thông tin đăng nhập/mật khẩu cho Gmail, Facebook, Twitter, LinkedIn, v.v.), hoạt động của tệp và các cuộc trò chuyện trực tuyến. Nó cũng chụp ảnh màn hình theo các khoảng thời gian đã đặt, giống như một camera giám sát nhắm vào màn hình máy tính. Phần mềm gián điệp tương tự như một con ngựa thành Troia, thường được đóng gói dưới dạng một thành phần ẩn của phần mềm miễn phí hoặc phần mềm được tải xuống từ Internet. Nó ẩn quy trình, tệp và các đối tượng khác để tránh bị phát hiện và xóa. Điều này cho phép kẻ tấn công thu thập thông tin về nạn nhân hoặc tổ chức, chẳng hạn như địa chỉ email, thông tin đăng nhập của người dùng, mật khẩu, số thẻ tín dụng, thông tin đăng nhập ngân hàng, v.v.

* Tuyên truyền phần mềm gián điệp

Đúng như tên gọi của nó, phần mềm gián điệp được cài đặt mà người dùng không biết hoặc không đồng ý và điều này có thể được thực hiện bằng cách "cõng" phần mềm gián điệp vào các ứng dụng khác. Điều này có thể xảy ra vì phần mềm gián điệp sử dụng cookie quảng cáo, đây là một trong các lớp con của phần mềm gián điệp. Phần mềm gián điệp cũng có thể ảnh hưởng đến hệ thống của bạn khi bạn truy cập trang web phân phối phần mềm gián điệp. Bởi vì nó tự cài đặt khi bạn truy cập và nhấp vào nội dung nào đó trên một trang web, quá trình này được gọi là "tải xuống theo ổ đĩa". Do các hoạt động tải xuống hoặc lướt web thông thường, hệ thống có thể vô tình bị nhiễm phần mềm gián điệp. Nó thậm chí có thể giả dạng là phần mềm chống phần mềm gián điệp và chạy trên máy tính của người dùng mà không có bất kỳ thông báo nào, bất cứ khi nào người dùng tải xuống và cài đặt các chương trình đi kèm với phần mềm gián điệp.

* Phần mềm gián điệp làm gì?

Chúng ta đã thảo luận về phần mềm gián điệp và chức năng chính của nó là theo dõi các hoạt động của người dùng trên máy tính mục tiêu. Chúng tôi cũng biết rằng một khi kẻ tấn công thành công trong việc cài đặt phần mềm gián điệp trên máy tính của nạn nhân bằng cách sử dụng các kỹ thuật lan truyền đã thảo luận trước đó, chúng có thể thực hiện một số hành động tấn công máy tính của nạn nhân. Do đó, bây giờ chúng ta hãy tìm hiểu thêm về khả năng của phần mềm gián điệp, vì chúng ta đã biết khả năng giám sát các hoạt động của người dùng của phần mềm này.

Phần mềm gián điệp được cài đặt cũng có thể giúp kẻ tấn công thực hiện các thao tác sau trên máy tính mục tiêu:

* Đánh cắp thông tin cá nhân của người dùng và gửi thông tin đó đến máy chủ từ xa hoặc tin tặc
* Giám sát hoạt động trực tuyến của người dùng
* Hiển thị cửa sổ bật lên gây phiền nhiễu
* Chuyển hướng trình duyệt web đến các trang web quảng cáo
* Thay đổi cài đặt mặc định của trình duyệt và ngăn người dùng khôi phục cài đặt đó
* Thêm một số dấu trang vào danh sách yêu thích của trình duyệt
* Giảm mức độ bảo mật hệ thống tổng thể
* Giảm hiệu năng hệ thống và gây mất ổn định phần mềm
* Kết nối với các trang web khiêu dâm từ xa
* Đặt lối tắt trên màn hình tới các trang web phần mềm gián điệp độc hại
* Đánh cắp mật khẩu của bạn
* Gửi cho bạn email được nhắm mục tiêu
* Thay đổi trang chủ và ngăn người dùng khôi phục nó
* Sửa đổi các thư viện được liên kết động (DLL) và làm chậm trình duyệt o Thay đổi cài đặt tường lửa
* Theo dõi và báo cáo các trang web bạn truy cập
* Các loại phần mềm gián điệp

Ngày nay, các chương trình phần mềm gián điệp khác nhau tham gia vào nhiều nhiệm vụ tấn công khác nhau, chẳng hạn như thay đổi cài đặt trình duyệt, hiển thị quảng cáo, thu thập dữ liệu, v.v. ăn cắp thông tin về người dùng và các hoạt động của họ, tất cả mà họ không biết hoặc không đồng ý.

* Phần mềm gián điệp trên máy tính để bàn

Phần mềm gián điệp trên máy tính để bàn là phần mềm cho phép kẻ tấn công lấy thông tin về hoạt động hoặc thông tin cá nhân của người dùng, gửi thông tin đó qua Internet cho bên thứ ba mà người dùng không biết hoặc không đồng ý. Nó cung cấp thông tin liên quan đến những gì người dùng mạng đã làm trên máy tính để bàn của họ, cách thức và thời điểm.

Phần mềm gián điệp trên máy tính cho phép kẻ tấn công thực hiện những việc sau:

* Ghi âm trực tiếp máy tính để bàn từ xa
* Ghi lại và giám sát các hoạt động trên Internet • Ghi lại thời gian và việc sử dụng phần mềm
* Ghi nhật ký hoạt động và lưu trữ tại một địa điểm tập trung
* Ghi lại các lần gõ phím của người dùng
* Phần mềm gián điệp thư điện tử

Phần mềm gián điệp email là một chương trình theo dõi, ghi lại và chuyển tiếp tất cả các email đến và đi. Sau khi được cài đặt trên máy tính mà bạn muốn theo dõi, loại phần mềm gián điệp này ghi lại các bản sao của tất cả các email đến và đi và gửi chúng cho bạn thông qua một địa chỉ email được chỉ định hoặc lưu thông tin trên thư mục đĩa cục bộ của máy tính bị theo dõi. Điều này hoạt động ở chế độ tàng hình; người dùng sẽ không nhận thức được sự hiện diện của phần mềm gián điệp email trên máy tính của họ. Nó cũng có khả năng ghi lại các tin nhắn tức thời (ví dụ: AIM, MSN, Yahoo, Myspace, Facebook).

* Phần mềm gián điệp Internet

Phần mềm gián điệp Internet là một công cụ cho phép bạn giám sát tất cả các trang web được truy cập bởi người dùng trên máy tính của bạn khi bạn vắng mặt. Nó tạo ra một bản ghi thời gian của tất cả các URL đã truy cập. Điều này tự động tải khi khởi động hệ thống và chạy ở chế độ ẩn, có nghĩa là nó chạy trong nền không bị phát hiện. Công cụ ghi lại tất cả các lượt truy cập URL vào một tệp nhật ký và gửi nó đến một địa chỉ email được chỉ định. Nó cung cấp một bản tóm tắt báo cáo về việc sử dụng web tổng thể, chẳng hạn như các trang web đã truy cập và thời gian dành cho mỗi trang web, cũng như tất cả các ứng dụng được mở cùng với ngày/giờ truy cập. Nó cũng cho phép bạn chặn quyền truy cập vào một trang web cụ thể hoặc toàn bộ trang web bằng cách chỉ định các URL hoặc từ khóa mà bạn muốn chặn.

* Phần mềm gián điệp giám sát trẻ em

Phần mềm gián điệp theo dõi trẻ em cho phép bạn theo dõi và giám sát những gì trẻ em đang làm trên máy tính, cả trực tuyến và ngoại tuyến. Thay vì nhìn qua vai đứa trẻ, người ta có thể sử dụng phần mềm gián điệp giám sát trẻ em, hoạt động ở chế độ ẩn; con bạn sẽ không nhận thức được sự giám sát của bạn. Phần mềm gián điệp ghi nhật ký tất cả các chương trình được sử dụng và các trang web đã truy cập, đếm số lần nhấn phím và số lần nhấp chuột cũng như chụp ảnh màn hình hoạt động. Tất cả dữ liệu đã ghi đều có thể truy cập được thông qua giao diện web được bảo vệ bằng mật khẩu dưới dạng tệp được mã hóa, ẩn hoặc có thể được gửi đến một địa chỉ email được chỉ định.

Điều này cũng cho phép bạn bảo vệ trẻ em truy cập nội dung web không phù hợp bằng cách đặt các từ khóa cụ thể mà bạn muốn chặn. Nó sẽ gửi một cảnh báo theo thời gian thực cho bạn bất cứ khi nào nó bắt gặp các từ khóa cụ thể trên máy tính của bạn hoặc bất cứ khi nào con bạn muốn truy cập nội dung không phù hợp.

* Phần mềm gián điệp chụp màn hình

Phần mềm gián điệp chụp màn hình là một chương trình cho phép bạn giám sát các hoạt động của máy tính bằng cách chụp ảnh nhanh hoặc ảnh chụp màn hình của máy tính có cài đặt chương trình. Những ảnh chụp nhanh này được thực hiện cục bộ hoặc từ xa theo các khoảng thời gian đã chỉ định và được lưu trong một tệp ẩn trên đĩa cục bộ hoặc được gửi đến địa chỉ email hoặc trang FTP do kẻ tấn công xác định trước.

Phần mềm gián điệp chụp màn hình không chỉ có khả năng chụp ảnh màn hình mà còn ghi lại các thao tác gõ phím, hoạt động của chuột, URL trang web đã truy cập và hoạt động của máy in trong thời gian thực. Người dùng có thể cài đặt chương trình hoặc phần mềm này trên các máy tính nối mạng để theo dõi hoạt động của tất cả các máy tính trong mạng theo thời gian thực bằng cách chụp ảnh màn hình. Điều này hoạt động trong suốt ở chế độ ẩn để bạn có thể theo dõi các hoạt động của máy tính mà người dùng không hề hay biết.

* Phần mềm gián điệp USB

Phần mềm gián điệp USB là một chương trình được thiết kế để theo dõi máy tính, sao chép các tệp phần mềm gián điệp từ thiết bị USB vào đĩa cứng mà không có bất kỳ yêu cầu hoặc thông báo nào. Nó chạy ở chế độ ẩn, vì vậy người dùng sẽ không biết về phần mềm gián điệp hoặc giám sát.

Phần mềm gián điệp USB cung cấp một giải pháp nhiều mặt trong lĩnh vực giao tiếp USB, vì nó có thể giám sát hoạt động của thiết bị USB mà không cần tạo thêm bộ lọc, thiết bị, v.v. có thể làm hỏng cấu trúc của trình điều khiển hệ thống.

Phần mềm gián điệp USB cho phép bạn chụp, hiển thị, ghi và phân tích dữ liệu được truyền giữa bất kỳ thiết bị USB nào với PC được kết nối và các ứng dụng của nó. Điều này cho phép nó hoạt động trên trình điều khiển thiết bị hoặc phát triển phần cứng, do đó cung cấp một nền tảng mạnh mẽ để viết mã, thử nghiệm và tối ưu hóa hiệu quả, đồng thời biến nó thành một công cụ tuyệt vời để gỡ lỗi phần mềm.

Nó ghi lại tất cả các giao tiếp giữa thiết bị USB và máy chủ của nó và lưu nó vào một tệp ẩn để xem lại sau. Nhật ký chi tiết trình bày bản tóm tắt của từng giao dịch dữ liệu, cùng với thông tin hỗ trợ của nó. Phần mềm gián điệp USB sử dụng mức tài nguyên hệ thống thấp của máy tính chủ. Nó hoạt động với dấu thời gian riêng để ghi nhật ký tất cả các hoạt động trong chuỗi giao tiếp. Phần mềm gián điệp USB không chứa bất kỳ phần mềm quảng cáo hoặc phần mềm gián điệp nào khác. Nó hoạt động với các biến thể mới nhất của Windows.

* Phần mềm gián điệp USB sao chép các tệp từ thiết bị USB vào đĩa cứng của bạn ở chế độ ẩn mà không cần bất kỳ yêu cầu nào
* Nó tạo một tập tin/thư mục ẩn với ngày hiện tại và bắt đầu quá trình sao chép nền
* Nó cho phép bạn chụp, hiển thị, ghi và phân tích dữ liệu được truyền giữa bất kỳ thiết bị USB nào với PC và ứng dụng được kết nối
* Phần mềm gián điệp âm thanh

Phần mềm gián điệp âm thanh là một chương trình giám sát âm thanh được thiết kế để ghi lại âm thanh vào máy tính. Kẻ tấn công có thể âm thầm cài đặt phần mềm gián điệp trên máy tính mà không cần sự cho phép của người dùng máy tính và không gửi cho họ bất kỳ thông báo nào. Phần mềm gián điệp âm thanh chạy trong nền để ghi lại một cách kín đáo. Sử dụng phần mềm gián điệp âm thanh không yêu cầu bất kỳ đặc quyền quản trị nào.

Phần mềm gián điệp âm thanh theo dõi và ghi lại nhiều loại âm thanh trên máy tính, lưu chúng vào một tệp ẩn trên đĩa cục bộ để truy xuất sau này. Do đó, những kẻ tấn công hoặc người dùng có ác ý sử dụng phần mềm gián điệp âm thanh này để theo dõi và theo dõi các bản ghi hội nghị, cuộc gọi điện thoại và chương trình phát thanh có thể chứa thông tin bí mật.

Nó có thể ghi lại và theo dõi các tin nhắn trò chuyện bằng giọng nói trong các trình nhắn tin tức thời phổ biến khác nhau. Với phần mềm gián điệp âm thanh này, mọi người có thể theo dõi nhân viên hoặc con cái của họ và tìm ra người mà họ đang liên lạc.

Nó giúp giám sát các thiết bị âm thanh kỹ thuật số như nhiều trình nhắn tin, micrô và điện thoại di động. Nó có thể ghi lại các cuộc hội thoại âm thanh bằng cách nghe trộm và giám sát tất cả các cuộc gọi đến và đi, tin nhắn văn bản, v.v. Nó cho phép giám sát cuộc gọi trực tiếp, giám sát âm thanh, theo dõi SMS, ghi nhật ký cuộc gọi và theo dõi GPRS.

* Phần mềm gián điệp video

Phần mềm gián điệp video là phần mềm giám sát bằng video được cài đặt trên máy tính mục tiêu mà người dùng không hề hay biết. Tất cả hoạt động video có thể được ghi lại theo lịch trình đã lập trình. Phần mềm gián điệp video chạy ngầm trong suốt và bí mật theo dõi cũng như ghi lại chuyển đổi webcam và IM video. Tính năng truy cập từ xa của phần mềm gián điệp video cho phép kẻ tấn công kết nối với điều khiển từ xa hoặc hệ thống đích để kích hoạt cảnh báo và thiết bị điện, đồng thời xem hình ảnh đã ghi trong kho lưu trữ video hoặc thậm chí chụp ảnh trực tiếp từ tất cả các camera được kết nối với hệ thống bằng trình duyệt web chẳng hạn như Internet Explorer.

* In phần mềm gián điệp

Những kẻ tấn công có thể giám sát việc sử dụng máy in của tổ chức mục tiêu từ xa bằng cách sử dụng phần mềm gián điệp in. Phần mềm gián điệp in là phần mềm giám sát việc sử dụng máy in giám sát các máy in trong tổ chức. Nó cung cấp thông tin chính xác về các hoạt động in cho máy in văn phòng hoặc cục bộ, giúp tối ưu hóa việc in ấn, tiết kiệm chi phí, v.v. Nó ghi lại tất cả thông tin liên quan đến hoạt động của máy in, lưu thông tin trong nhật ký được mã hóa và gửi tệp nhật ký đến một địa chỉ được chỉ định. địa chỉ thư điện tử qua Internet. Báo cáo nhật ký bao gồm các thuộc tính công việc in chính xác, chẳng hạn như số trang đã in, số bản sao, nội dung được in và ngày giờ thực hiện hành động in.

Phần mềm gián điệp in ghi lại các báo cáo nhật ký ở các định dạng khác nhau cho các mục đích khác nhau, chẳng hạn như ở định dạng web để gửi báo cáo tới email qua Internet hoặc ở định dạng được mã hóa ẩn để lưu trữ trên đĩa cục bộ. Các báo cáo nhật ký được tạo sẽ phần mềm cũng cho phép giới hạn quyền truy cập vào máy in. Báo cáo nhật ký này giúp kẻ tấn công tìm ra thông tin về các tài liệu nhạy cảm và bí mật được in.

* Phần mềm gián điệp điện thoại/điện thoại di động

Phần mềm gián điệp điện thoại/điện thoại di động là một công cụ phần mềm cung cấp cho bạn toàn quyền truy cập để theo dõi điện thoại hoặc điện thoại di động của nạn nhân. Nó sẽ ẩn hoàn toàn khỏi người dùng điện thoại. Nó sẽ ghi lại và ghi nhật ký mọi hoạt động trên điện thoại, chẳng hạn như sử dụng Internet, tin nhắn văn bản và cuộc gọi điện thoại. Sau đó, bạn có thể truy cập thông tin đã ghi qua trang web chính của phần mềm hoặc bạn cũng có thể nhận thông tin theo dõi qua SMS hoặc email. Thông thường, phần mềm gián điệp này giúp giám sát và theo dõi việc sử dụng điện thoại của nhân viên. Tuy nhiên, những kẻ tấn công đang sử dụng nó để theo dõi thông tin từ điện thoại/điện thoại di động của người hoặc tổ chức mục tiêu của chúng. Sử dụng phần mềm gián điệp này không yêu cầu bất kỳ đặc quyền được ủy quyền nào.

Các tính năng phổ biến nhất của phần mềm gián điệp điện thoại/điện thoại di động bao gồm:

* Lịch sử cuộc gọi: Cho phép bạn xem toàn bộ lịch sử cuộc gọi của máy (cả cuộc gọi đến và cuộc gọi đi).
* Xem tin nhắn văn bản: Cho phép bạn xem tất cả các tin nhắn văn bản đến và đi. Nó thậm chí còn hiển thị các tin nhắn đã xóa trong báo cáo nhật ký.
* Lịch sử trang web: Ghi lại toàn bộ lịch sử của tất cả các trang web đã truy cập qua điện thoại trong tệp báo cáo nhật ký.
* Theo dõi GPS: Hiển thị cho bạn vị trí của điện thoại trong thời gian thực. Ngoài ra còn có nhật ký về vị trí của điện thoại di động để bạn có thể biết điện thoại đã ở đâu.
* Nó hoạt động như được mô tả trong sơ đồ sau.
* Phần mềm gián điệp GPS

Phần mềm gián điệp GPS là một thiết bị hoặc ứng dụng phần mềm sử dụng Hệ thống định vị toàn cầu (GPS) để xác định vị trí của một phương tiện, người hoặc tài sản được gắn hoặc cài đặt khác. Kẻ tấn công có thể sử dụng phần mềm này để theo dõi người mục tiêu.

**Ẩn tập tin**

Sau khi kẻ tấn công đã thực hiện các hoạt động độc hại (tức là đã thực thi các ứng dụng độc hại) trên hệ thống mục tiêu để giành được các đặc quyền leo thang, kẻ tấn công sẽ nhúng và ẩn các chương trình độc hại của mình. Kẻ tấn công có thể thực hiện việc này bằng cách sử dụng rootkit, NTFS stream và kỹ thuật Steganography, v.v. để ngăn chương trình độc hại khỏi các ứng dụng bảo vệ như ứng dụng chống vi-rút, chống phần mềm độc hại và chống phần mềm gián điệp được cài đặt trên hệ thống đích. Một tệp độc hại ẩn như vậy cho phép kẻ tấn công duy trì quyền truy cập trực tiếp vào hệ thống, ngay cả trong tương lai mà không cần sự đồng ý của nạn nhân. Phần này mô tả các kỹ thuật khác nhau được kẻ tấn công sử dụng để ẩn các tệp độc hại của chúng.

**Rootkit**

Rootkit là các chương trình phần mềm được thiết kế để truy cập vào máy tính mà không bị phát hiện. Chúng là phần mềm độc hại giúp kẻ tấn công có quyền truy cập trái phép vào hệ thống từ xa và thực hiện các hoạt động độc hại. Mục tiêu của rootkit là giành được quyền root đối với hệ thống. Bằng cách đăng nhập với tư cách là người dùng root của hệ thống, kẻ tấn công có thể thực hiện nhiều tác vụ khác nhau như cài đặt phần mềm hoặc xóa tệp. Nó hoạt động bằng cách khai thác các lỗ hổng trong HĐH và các ứng dụng của nó. Nó xây dựng một quy trình đăng nhập cửa sau trong HĐH mà qua đó kẻ tấn công có thể trốn tránh quy trình đăng nhập tiêu chuẩn.

Sau khi người dùng kích hoạt quyền truy cập root, rootkit có thể cố gắng che giấu dấu vết truy cập trái phép bằng cách sửa đổi trình điều khiển hoặc mô-đun hạt nhân và loại bỏ các quy trình đang hoạt động. Rootkit thay thế các lệnh gọi và tiện ích hệ điều hành nhất định bằng các phiên bản đã sửa đổi của riêng chúng đối với các quy trình đó, từ đó làm suy yếu tính bảo mật của hệ thống đích bằng cách thực thi các chức năng độc hại. Một rootkit điển hình bao gồm các chương trình cửa hậu, chương trình DDoS, trình nghe lén gói tin, tiện ích xóa nhật ký, bot IRC và các chương trình khác.

Tất cả các tệp chứa một tập hợp các thuộc tính. Có các trường khác nhau trong thuộc tính tệp. Trường đầu tiên xác định định dạng của tệp nếu đó là tệp ẩn, lưu trữ hoặc chỉ đọc. Trường khác mô tả thời gian tạo tệp, quyền truy cập và độ dài ban đầu của tệp. Các hàm GetFileAttributesExA() và GetFileInformationByHandle() được sử dụng cho các mục đích nói trên. ATTRIB.exe hiển thị hoặc thay đổi thuộc tính tệp. Kẻ tấn công có thể ẩn hoặc thậm chí thay đổi các thuộc tính của tệp nạn nhân để kẻ tấn công có thể truy cập chúng.

Kẻ tấn công đặt rootkit bằng cách

* Quét các máy tính và máy chủ có lỗ hổng trên web
* Gói rootkit trong một gói đặc biệt giống như một trò chơi
* Cài đặt nó trên máy tính công cộng hoặc doanh nghiệp thông qua kỹ thuật xã hội
* Khởi động một cuộc tấn công zero-day (leo thang đặc quyền, khai thác nhân Windows, v.v.)

Mục tiêu của rootkit:

* Để root hệ thống máy chủ và truy cập cửa hậu từ xa
* Để che giấu dấu vết của kẻ tấn công và sự hiện diện của các ứng dụng hoặc quy trình độc hại
* Để thu thập dữ liệu nhạy cảm, lưu lượng truy cập mạng, v.v. từ hệ thống mà kẻ tấn công có thể bị hạn chế hoặc không có quyền truy cập
* Để lưu trữ các chương trình độc hại khác trên hệ thống và đóng vai trò là tài nguyên máy chủ để cập nhật bot

**Kỹ thuật giấu tin**

**Phân tích mật**

* 1. Xóa dấu vết

Che dấu vết là một trong những giai đoạn chính trong quá trình hack hệ thống. Trong giai đoạn này, kẻ tấn công cố gắng che giấu và tránh bị phát hiện hoặc "truy tìm" bằng cách che tất cả "dấu vết" hoặc nhật ký được tạo trong khi truy cập mạng hoặc máy tính mục tiêu. Bây giờ chúng ta xem xét cách kẻ tấn công xóa dấu vết của một cuộc tấn công trên máy tính mục tiêu.

Xóa bằng chứng là điều bắt buộc đối với bất kỳ kẻ tấn công nào muốn giữ bí mật. Nó là một phương pháp được sử dụng để trốn tránh truy nguyên. Nó bắt đầu bằng việc xóa các bản ghi bị ô nhiễm và các thông báo lỗi có thể được tạo ra trong quá trình tấn công. Kẻ tấn công thực hiện các thay đổi đối với cấu hình hệ thống để không ghi nhật ký các hoạt động trong tương lai. Bằng cách thao túng và chỉnh sửa nhật ký sự kiện, kẻ tấn công đánh lừa quản trị viên hệ thống tin rằng không có hoạt động độc hại nào trong hệ thống và không có sự xâm nhập hoặc thỏa hiệp nào xảy ra.

Bởi vì điều đầu tiên mà quản trị viên hệ thống thực hiện khi giám sát hoạt động bất thường là kiểm tra các tệp nhật ký hệ thống nên những kẻ xâm nhập thường sử dụng một công cụ để sửa đổi các nhật ký này. Trong một số trường hợp, rootkit có thể vô hiệu hóa và loại bỏ tất cả nhật ký hiện có. Những kẻ tấn công chỉ xóa những phần nhật ký có thể tiết lộ sự hiện diện của chúng nếu chúng có ý định sử dụng hệ thống trong một thời gian dài làm cơ sở khởi chạy cho các hoạt động khai thác trong tương lai.

Những kẻ tấn công phải làm cho hệ thống xuất hiện như trước khi có được quyền truy cập và một cửa hậu được thiết lập. Điều này cho phép họ thay đổi bất kỳ thuộc tính tệp nào về trạng thái ban đầu. Thông tin được liệt kê, chẳng hạn như kích thước và ngày của tệp, chỉ là thông tin thuộc tính có trong tệp.

Việc bảo vệ chống lại những kẻ tấn công đang cố gắng che đậy dấu vết của chúng bằng cách thay đổi thông tin tệp có thể khó khăn. Tuy nhiên, có thể phát hiện xem kẻ tấn công có làm như vậy hay không bằng cách tính hàm băm mật mã của tệp. Loại băm này là phép tính của toàn bộ tệp trước khi mã hóa.

Những kẻ tấn công có thể không muốn xóa toàn bộ nhật ký để che dấu vết của chúng, vì làm như vậy có thể yêu cầu đặc quyền của quản trị viên. Nếu kẻ tấn công chỉ có thể xóa nhật ký sự kiện tấn công, chúng vẫn có thể thoát khỏi sự phát hiện.

Kẻ tấn công có thể thao tác các tệp nhật ký với sự trợ giúp của

* SECEVENT.EVT (bảo mật): đăng nhập không thành công, truy cập tệp không có đặc quyền
* SYSEVENT.EVT (hệ thống): lỗi trình điều khiển, mọi thứ hoạt động không chính xác
* APPEVENT.EVT (ứng dụng)

**Các kỹ thuật được sử dụng để che dấu vết**

Các hoạt động chính mà kẻ tấn công thực hiện để xóa dấu vết của mình trên máy tính như sau:

* Vô hiệu hóa Kiểm tra: Kẻ tấn công vô hiệu hóa các tính năng kiểm tra của hệ thống đích.
* Xóa nhật ký: Kẻ tấn công xóa/xóa các mục nhập nhật ký hệ thống tương ứng với các hoạt động của mình.
* Thao túng nhật ký: Kẻ tấn công thao túng nhật ký theo cách mà anh ta/cô ta sẽ không
* bị bắt trong hành động pháp lý.
* Che dấu vết trên mạng: Kẻ tấn công sử dụng các kỹ thuật như trình bao HTTP ngược, đường hầm ICMP ngược, đường hầm DNS và tham số TCP để che dấu vết trên mạng.
* Che dấu vết trên hệ điều hành: Kẻ tấn công sử dụng các luồng NTFS để che giấu phần mềm độc hại
* tập tin trong hệ thống đích.
* Xóa tệp: Kẻ tấn công sử dụng công cụ dòng lệnh như Cipher.exe để xóa dữ liệu và ngăn chặn việc khôi phục dữ liệu đó trong tương lai.
* Vô hiệu hóa chức năng của Windows: Kẻ tấn công vô hiệu hóa chức năng của Windows như dấu thời gian truy cập lần cuối, chế độ ngủ đông, bộ nhớ ảo, điểm khôi phục hệ thống, v.v. để che dấu vết.

Do đó, công việc hoàn chỉnh của kẻ tấn công không chỉ liên quan đến việc xâm phạm thành công hệ thống mà còn vô hiệu hóa việc ghi nhật ký, xóa các tệp nhật ký, loại bỏ bằng chứng, cài đặt các công cụ bổ sung và che dấu vết của anh ta/cô ta.

* 1. Giải pháp phòng chống
     1. Phòng chống cracking passowrd

Các thực tiễn tốt nhất để bảo vệ chống bẻ khóa mật khẩu được liệt kê như sau:

* Cho phép kiểm tra bảo mật thông tin để giám sát và theo dõi các cuộc tấn công mật khẩu.
* Không sử dụng cùng một mật khẩu trong quá trình thay đổi mật khẩu.
* Không chia sẻ mật khẩu.
* Không sử dụng mật khẩu có thể tìm thấy trong từ điển.
* Không sử dụng các giao thức văn bản rõ ràng hoặc các giao thức có mã hóa yếu.
* Đặt chính sách thay đổi mật khẩu thành 30 ngày.
* Tránh lưu trữ mật khẩu ở một vị trí không an toàn.
* Làm cho mật khẩu khó đoán bằng cách sử dụng 8-12 ký tự chữ và số, với sự kết hợp của chữ hoa và chữ thường, số và ký hiệu. Điều này là do mật khẩu mạnh rất khó đoán. Do đó, mật khẩu càng phức tạp thì càng ít bị tấn công.
* Đảm bảo rằng các ứng dụng không lưu trữ mật khẩu vào bộ nhớ cũng như không ghi chúng vào đĩa ở dạng văn bản rõ ràng. Mật khẩu luôn dễ bị đánh cắp nếu chúng được lưu trong bộ nhớ. Sau khi biết mật khẩu, kẻ tấn công sẽ cực kỳ dễ dàng leo thang quyền của họ trong ứng dụng.
* Sử dụng một chuỗi ngẫu nhiên (muối) làm tiền tố hoặc hậu tố mật khẩu trước khi thực hiện mã hóa. Điều này vô hiệu hóa tính toán trước và ghi nhớ. Bởi vì muối thường khác nhau đối với mỗi cá nhân, nên kẻ tấn công sẽ không thể xây dựng các bảng với một phiên bản được mã hóa duy nhất của mỗi mật khẩu ứng cử viên. Các hệ thống UNIX thường sử dụng bộ 12 bit.
* Bật SYSKEY bằng mật khẩu mạnh để mã hóa và bảo vệ cơ sở dữ liệu SAM. Thông thường, thông tin mật khẩu của tài khoản người dùng được lưu trữ trong cơ sở dữ liệu SAM. Phần mềm bẻ khóa mật khẩu rất dễ nhắm mục tiêu cơ sở dữ liệu SAM để truy cập mật khẩu. SYSKEY bảo vệ thông tin mật khẩu được lưu trữ trong dữ liệu SAM khỏi phần mềm bẻ khóa mật khẩu thông qua các kỹ thuật mã hóa mạnh. Việc bẻ khóa mật khẩu được mã hóa khó hơn mật khẩu không được mã hóa.
* Không bao giờ sử dụng thông tin cá nhân (ví dụ: ngày sinh hoặc tên của vợ/chồng, con cái hoặc tên thú cưng) để tạo mật khẩu. Mặt khác, những người thân thiết với bạn sẽ dễ dàng bẻ khóa mật khẩu của bạn.
* Theo dõi nhật ký của máy chủ để phát hiện các cuộc tấn công vũ phu vào tài khoản người dùng. Mặc dù rất khó ngăn chặn các cuộc tấn công brute-force nhưng chúng có thể dễ dàng bị phát hiện nếu nhật ký máy chủ web được theo dõi. Đối với mỗi lần đăng nhập không thành công, mã trạng thái HTTP 401 được ghi lại trong nhật ký máy chủ web.
* Khóa những tài khoản bị đoán sai mật khẩu quá nhiều. Điều này cung cấp sự bảo vệ chống lại các cuộc tấn công brute-force và đoán.
* Nhiều trình dò tìm mật khẩu có thể thành công nếu sử dụng trình quản lý mạng LAN và xác thực NTLM. Chỉ tắt trình quản lý mạng LAN và giao thức xác thực NTLM sau khi đảm bảo rằng nó không ảnh hưởng đến mạng.
* Thực hiện kiểm tra mật khẩu định kỳ trong tổ chức.
* Kiểm tra bất kỳ ứng dụng đáng ngờ nào lưu trữ mật khẩu trong bộ nhớ hoặc ghi chúng vào đĩa.
* Các hệ thống chưa được vá lỗi có thể đặt lại mật khẩu trong quá trình tràn bộ đệm hoặc tấn công từ chối dịch vụ. Đảm bảo cập nhật hệ thống.
* Kiểm tra xem tài khoản đang được sử dụng, bị xóa hay bị vô hiệu hóa. Vô hiệu hóa tài khoản người dùng nếu phát hiện nhiều lần đăng nhập không thành công.
* Cho phép khóa tài khoản với số lần thử, thời gian truy cập và thời lượng khóa nhất định.
* Một trong những cách hiệu quả nhất để quản lý mật khẩu trong các tổ chức là thiết lập đặt lại mật khẩu tự động.
* Bảo vệ mật khẩu BIOS của hệ thống, đặc biệt trên các thiết bị dễ bị đe dọa vật lý, chẳng hạn như máy chủ và máy tính xách tay.
* Đào tạo nhân viên để ngăn chặn các chiến thuật kỹ thuật xã hội, chẳng hạn như lướt vai và lặn trong thùng rác, được sử dụng để đánh cắp thông tin đăng nhập của người dùng.
* Định cấu hình chính sách mật khẩu trong đối tượng Chính sách nhóm trong HĐH Windows.
* Thực hiện sàng lọc mật khẩu khi mật khẩu mới được tạo để tránh sử dụng mật khẩu thường được sử dụng.
* Sử dụng xác thực hai yếu tố hoặc đa yếu tố, ví dụ: sử dụng CAPTCHA để ngăn chặn các cuộc tấn công tự động vào các hệ thống thông tin quan trọng.
* Bảo mật và kiểm soát quyền truy cập vật lý vào hệ thống để ngăn chặn các cuộc tấn công mật khẩu ngoại tuyến.
* Đảm bảo các tệp cơ sở dữ liệu mật khẩu được mã hóa và chỉ quản trị viên hệ thống mới có thể truy cập được.
* Che dấu mật khẩu hiển thị trên màn hình để tránh các cuộc tấn công lướt vai.
  + 1. Phòng chống leo thang đặc quyền

Biện pháp đối phó tốt nhất chống leo thang đặc quyền là đảm bảo rằng người dùng có đặc quyền thấp nhất có thể nhưng vẫn đủ để sử dụng hệ thống của họ một cách hiệu quả. Trong trường hợp này, ngay cả khi kẻ tấn công thành công trong việc giành quyền truy cập vào tài khoản có đặc quyền thấp, kẻ đó sẽ không thể giành được quyền truy cập cấp quản trị. Thông thường, các lỗi trong mã lập trình cho phép leo thang các đặc quyền như vậy trên hệ thống đích. Như đã nêu trước đó, kẻ tấn công có thể truy cập vào mạng bằng tài khoản không phải quản trị viên và sau đó có được đặc quyền cao hơn của quản trị viên.

Sau đây là các biện pháp đối phó tốt nhất để chống lại sự leo thang đặc quyền:

* Hạn chế đặc quyền đăng nhập tương tác
* Chạy người dùng và ứng dụng với đặc quyền thấp nhất
* Triển khai xác thực và ủy quyền đa yếu tố
* Chạy dịch vụ dưới dạng tài khoản không có đặc quyền
* Triển khai phương pháp phân tách đặc quyền để hạn chế phạm vi lỗi và lỗi lập trình
* Sử dụng kỹ thuật mã hóa để bảo vệ dữ liệu nhạy cảm
* Giảm số lượng mã chạy với một đặc quyền cụ thể
* Thực hiện gỡ lỗi bằng cách sử dụng trình kiểm tra giới hạn và kiểm tra căng thẳng
* Kiểm tra kỹ lưỡng hệ thống để tìm lỗi mã hóa ứng dụng và lỗi
* Thường xuyên vá và cập nhật kernel
* Thay đổi cài đặt UAC thành "Luôn thông báo" để tăng khả năng hiển thị của người dùng khi yêu cầu nâng cao UAC
* Hạn chế người dùng ghi tệp vào đường dẫn tìm kiếm cho ứng dụng
* Giám sát liên tục các quyền của hệ thống tệp bằng cách sử dụng các công cụ kiểm tra Giảm các đặc quyền của tài khoản người dùng và nhóm để chỉ quản trị viên hợp pháp mới có thể thực hiện thay đổi dịch vụ
* Sử dụng các công cụ danh sách trắng để xác định và chặn phần mềm độc hại thay đổi quyền của tệp, thư mục hoặc dịch vụ
* Sử dụng các đường dẫn đủ điều kiện trong tất cả các ứng dụng Windows
* Đảm bảo rằng tất cả các tệp thực thi được đặt trong các thư mục chống ghi
* Trong Mac OS, ngăn không cho người dùng thay đổi các tệp plist bằng cách đặt chúng ở chế độ chỉ đọc
* Chặn các tiện ích hoặc phần mềm hệ thống không mong muốn có thể được sử dụng để lên lịch tác vụ
* Thường xuyên vá và cập nhật máy chủ web
* Vô hiệu hóa tài khoản quản trị viên cục bộ mặc định
* Phát hiện, sửa chữa và khắc phục mọi sai sót hoặc lỗi đang chạy trong các dịch vụ hệ thống
* Bảo vệ chống lạm dụng quyền sudo:
* Triển khai chính sách mật khẩu mạnh cho người dùng sudo
* Tắt bộ nhớ đệm mật khẩu bằng cách đặt timestamp\_timeout thành 0, để mỗi khi sudo được thực thi, người dùng phải nhập mật khẩu của họ
* Tách tài khoản quản trị cấp sudo khỏi tài khoản thông thường của quản trị viên để ngăn chặn việc đánh cắp mật khẩu nhạy cảm
* Cập nhật quyền và tài khoản của người dùng theo định kỳ Kiểm tra người dùng sudo có quyền truy cập vào các chương trình chứa tham số để thực thi mã tùy ý
  + 1. Cách phòng chống keylogger

Cách phòng chống Keylogger

Các biện pháp đối phó khác nhau để chống lại keylogger được liệt kê như sau:

• Sử dụng trình chặn cửa sổ bật lên và tránh mở các email rác.

■ Cài đặt các chương trình chống phần mềm gián điệp/chống vi-rút và luôn cập nhật các chữ ký.

Cài đặt phần mềm tường lửa chuyên nghiệp và phần mềm chống keylogging.

Nhận biết các email lừa đảo và xóa chúng.

Thường xuyên cập nhật và vá lỗi phần mềm hệ thống.

Không nhấp vào các liên kết trong các email không mong muốn hoặc đáng ngờ có thể hướng bạn đến các trang web độc hại.

Sử dụng phần mềm can thiệp gõ phím chèn các ký tự ngẫu nhiên vào mỗi lần gõ phím.

Phần mềm chống vi-rút và chống phần mềm gián điệp có thể phát hiện bất kỳ phần mềm nào đã cài đặt, nhưng tốt hơn là phát hiện các chương trình này trước khi cài đặt. Quét kỹ các tệp trước khi cài đặt chúng vào máy tính và sử dụng trình chỉnh sửa sổ đăng ký hoặc trình khám phá quy trình để kiểm tra trình ghi nhật ký thao tác gõ phím.

Sử dụng tiện ích trợ năng bàn phím trên màn hình của Windows để nhập mật khẩu hoặc bất kỳ

thông tin bí mật khác. Sử dụng chuột để nhập bất kỳ thông tin nào như

mật khẩu và số thẻ tín dụng vào các trường, bằng cách sử dụng chuột thay vì

gõ mật khẩu bằng bàn phím. Điều này sẽ đảm bảo rằng thông tin của bạn được

bảo mật.

Sử dụng trình quản lý mật khẩu điền biểu mẫu tự động hoặc bàn phím ảo để nhập tên người dùng và mật khẩu, vì điều này sẽ tránh bị lộ thông qua keylogger. Trình quản lý mật khẩu điền biểu mẫu tự động này sẽ loại bỏ nhu cầu nhập các chi tiết cá nhân, tài chính hoặc bí mật của bạn như số thẻ tín dụng và mật khẩu qua bàn phím.

Giữ an toàn cho hệ thống phần cứng của bạn trong môi trường bị khóa và thường xuyên kiểm tra cáp bàn phím để biết các đầu nối đi kèm, cổng USB và trò chơi máy tính như PS2 có thể đã được sử dụng để cài đặt phần mềm keylogger.

Sử dụng phần mềm thường xuyên quét và theo dõi các thay đổi trong hệ thống hoặc mạng của bạn. Cài đặt IDS dựa trên máy chủ, có thể giám sát hệ thống của bạn và tắt cài đặt keylogger.

Sử dụng mật khẩu một lần (OTP) hoặc các cơ chế xác thực khác như xác minh hai bước hoặc nhiều bước để xác thực người dùng.

Bật danh sách trắng ứng dụng để chặn tải xuống hoặc cài đặt phần mềm không mong muốn, chẳng hạn như keylogger.

• Sử dụng các công cụ giám sát quy trình để phát hiện các quy trình và hoạt động hệ thống đáng ngờ.

• Thường xuyên vá lỗi và cập nhật phần mềm và hệ điều hành.

Các biện pháp đối phó với Keylogger phần cứng

• Hạn chế truy cập vật lý vào các hệ thống máy tính nhạy cảm.

• Kiểm tra định kỳ giao diện bàn phím của bạn để đảm bảo rằng không có bộ phận bổ sung nào được cắm vào đầu nối cáp bàn phím.

Sử dụng mã hóa giữa bàn phím và trình điều khiển của bàn phím.

• Sử dụng chương trình chống keylogger phát hiện sự hiện diện của keylogger phần cứng chẳng hạn như KeyGrabber.

Sử dụng bàn phím trên màn hình và nhấp vào nó bằng chuột.

Định kỳ kiểm tra cáp màn hình video để phát hiện sự hiện diện của keylogger phần cứng.

Thiết lập video giám sát xung quanh bàn máy tính để phát hiện việc cắm phần cứng độc hại.

Tắt cổng USB hoặc thiết lập cơ chế xác thực BIOS nâng cao để bật cổng USB.

* + 1. Cách phòng chống phần mềm gián điệp

Phần mềm gián điệp là bất kỳ chương trình độc hại nào được cài đặt trên hệ thống của người dùng mà họ không biết. Nó thu thập thông tin bí mật như dữ liệu cá nhân và nhật ký truy cập. Phần mềm gián điệp có thể bắt nguồn từ ba nguồn cơ bản: phần mềm được tải xuống miễn phí, tệp đính kèm email và các trang web tự động cài đặt phần mềm gián điệp khi bạn duyệt qua chúng.

Các cách khác nhau để bảo vệ chống lại phần mềm gián điệp như sau:

• Cố gắng tránh sử dụng bất kỳ hệ thống máy tính nào mà bạn không có toàn quyền kiểm soát.

Không bao giờ điều chỉnh mức cài đặt bảo mật Internet của bạn quá thấp vì nó tạo ra nhiều cơ hội cho phần mềm gián điệp được cài đặt trên máy tính của bạn. Do đó, hãy luôn đặt cài đặt bảo mật trình duyệt Internet của bạn ở mức cao hoặc trung bình để bảo vệ máy tính của bạn khỏi phần mềm gián điệp.

• Không mở các email và tệp đính kèm đáng ngờ nhận được từ những người gửi không xác định. Có khả năng cao là bạn sẽ cho phép vi-rút, phần mềm miễn phí hoặc phần mềm gián điệp xâm nhập vào máy tính. Không mở các trang web không xác định được liên kết trong thư rác, được công cụ tìm kiếm truy xuất hoặc hiển thị trong cửa sổ bật lên vì chúng có thể khiến bạn nhầm lẫn tải xuống phần mềm gián điệp.

• Bật tường lửa để nâng cao mức độ bảo mật cho máy tính của bạn.

• Thường xuyên cập nhật phần mềm và sử dụng tường lửa có tính năng bảo vệ bên ngoài.

Thường xuyên kiểm tra báo cáo Trình quản lý tác vụ và Trình quản lý cấu hình MS.

Thường xuyên cập nhật các tệp định nghĩa vi-rút và quét hệ thống để tìm phần mềm gián điệp.

Cài đặt phần mềm chống phần mềm gián điệp. Chống phần mềm gián điệp là tuyến phòng thủ đầu tiên chống lại phần mềm gián điệp. Phần mềm này ngăn phần mềm gián điệp cài đặt trên hệ thống của bạn. Nó định kỳ quét và bảo vệ hệ thống của bạn khỏi phần mềm gián điệp.

Luôn cập nhật hệ điều hành của bạn.

o Người dùng Windows nên thực hiện cập nhật Windows hoặc Microsoft định kỳ.

o Đối với người dùng PMNM hoặc các sản phẩm phần mềm khác, hãy tham khảo thông tin do nhà cung cấp HĐH cung cấp và thực hiện các bước cần thiết để chống lại bất kỳ lỗ hổng nào được xác định.

• Thực hiện lướt web một cách an toàn và tải xuống một cách thận trọng.

* + 1. Cách phòng chống Rootkit

Một đặc điểm chung của các rootkit này là kẻ tấn công yêu cầu quyền truy cập của quản trị viên vào hệ thống đích. Cuộc tấn công ban đầu dẫn đến quyền truy cập này thường ồn ào. Do đó, người ta nên theo dõi lưu lượng mạng dư thừa phát sinh khi đối mặt với một khai thác mới. Rõ ràng là phân tích nhật ký là một thành phần quan trọng của quản lý rủi ro. Kẻ tấn công có thể có các tập lệnh shell hoặc công cụ có thể giúp anh ta/cô ta che đậy dấu vết của mình, nhưng gần như chắc chắn sẽ có những dấu hiệu nhận biết khác có thể dẫn đến các biện pháp đối phó chủ động, chứ không chỉ là những biện pháp phản ứng.

Một biện pháp đối phó phản ứng là sao lưu tất cả dữ liệu quan trọng, ngoại trừ các tệp nhị phân và thực hiện cài đặt mới, sạch từ một nguồn đáng tin cậy. Người ta có thể thực hiện kiểm tra mã như một biện pháp bảo vệ tốt trước các công cụ như rootkit. MD5sum.exe có thể lấy dấu vân tay của tệp và lưu ý các vi phạm tính toàn vẹn khi có thay đổi. Để chống lại rootkit, nên sử dụng các chương trình kiểm tra tính toàn vẹn cho các tệp hệ thống quan trọng.

Sau đây là một số kỹ thuật được áp dụng để chống lại rootkit.

• Cài đặt lại hệ điều hành/ứng dụng từ một nguồn đáng tin cậy sau khi sao lưu dữ liệu quan trọng

• Duy trì các quy trình cài đặt tự động được ghi chép đầy đủ

• Thực hiện phân tích kết xuất bộ nhớ nhân để xác định sự hiện diện của rootkit

■ Tăng cường sức mạnh cho máy trạm hoặc máy chủ trước cuộc tấn công

• Hướng dẫn nhân viên không tải xuống bất kỳ tệp/chương trình nào từ các nguồn không đáng tin cậy

■ Cài đặt tường lửa dựa trên mạng và máy chủ và thường xuyên kiểm tra các bản cập nhật

• Đảm bảo có sẵn phương tiện khôi phục đáng tin cậy

• Cập nhật và vá lỗi hệ điều hành, ứng dụng và chương trình cơ sở

• Thường xuyên xác minh tính toàn vẹn của các tệp hệ thống bằng công nghệ dấu vân tay kỹ thuật số mạnh về mật mã

• Thường xuyên cập nhật phần mềm diệt virus và phần mềm gián điệp

• Luôn cập nhật chữ ký chống phần mềm độc hại

• Tránh đăng nhập vào tài khoản có quyền quản trị

• Tuân thủ nguyên tắc đặc quyền tối thiểu

• Đảm bảo rằng phần mềm chống vi-rút được chọn sở hữu tính năng bảo vệ rootkit

• Không cài đặt các ứng dụng không cần thiết và tắt các tính năng và dịch vụ không sử dụng

• Không tham gia vào các hoạt động nguy hiểm trên Internet

• Đóng mọi cổng không sử dụng

• Định kỳ quét hệ thống cục bộ bằng máy quét bảo mật dựa trên máy chủ

• Tăng tính bảo mật của hệ thống bằng xác thực hai bước hoặc nhiều bước, do đó kẻ tấn công sẽ không giành được quyền truy cập root vào hệ thống để cài đặt rootkit

• Không bao giờ đọc email, duyệt trang web hoặc mở tài liệu trong khi xử lý phiên hoạt động với máy chủ từ xa

• Sử dụng các công cụ quản lý cấu hình và quét lỗ hổng để xác minh việc triển khai hiệu quả các bản cập nhật

* + 1. Bảo vệ chống lại dấu vết che phủ

Các biện pháp đối phó khác nhau đối với việc che dấu vết được liệt kê như sau:

* Kích hoạt chức năng ghi nhật ký trên tất cả các hệ thống quan trọng
* Tiến hành kiểm toán định kỳ trên các hệ thống CNTT để đảm bảo chức năng ghi nhật ký phù hợp với chính sách bảo mật
* Đảm bảo các sự kiện mới không ghi đè lên các mục cũ trong tệp nhật ký khi vượt quá giới hạn lưu trữ
* Định cấu hình các quyền thích hợp và tối thiểu cần thiết để đọc và ghi các tệp nhật ký được lưu trữ trên các hệ thống quan trọng
* Duy trì một máy chủ ghi nhật ký riêng trên DMZ, để tất cả các máy chủ quan trọng, chẳng hạn như máy chủ DNS, máy chủ thư, máy chủ web, v.v., chuyển tiếp và lưu trữ nhật ký của chúng trên máy chủ đó
* Thường xuyên cập nhật và vá lỗi hệ điều hành, ứng dụng và chương trình cơ sở
* Đóng tất cả các cổng và dịch vụ đang mở không sử dụng
* Mã hóa các tệp nhật ký được lưu trữ trên hệ thống, do đó không thể thay đổi chúng nếu không có khóa giải mã thích hợp
* Đặt các tệp nhật ký thành chế độ "chỉ nối thêm" để ngăn việc xóa trái phép các mục nhật ký
* Định kỳ sao lưu các tệp nhật ký vào phương tiện không thể thay đổi

Câu hỏi và bài tập

1. Nghe lén và chặn bắt thông tin
   1. Khái niệm cơ bản
   2. Phần này mô tả việc dò tìm mạng và các mối đe dọa, cách thức hoạt động của phần mềm dò tìm, hoạt động dò tìm chủ động và thụ động, cách kẻ tấn công xâm nhập mạng bằng cách sử dụng phần mềm dò tìm, các giao thức dễ bị dò tìm, dò tìm trong lớp liên kết dữ liệu của mô hình Kết nối hệ thống mở (OSI), giao thức phần cứng máy phân tích, cổng Switched Port Analyzer (SPAN), nghe lén và chặn hợp pháp.
   3. Đánh hơi mạng
   4. Đánh hơi gói là quá trình giám sát và nắm bắt tất cả các gói dữ liệu đi qua một mạng nhất định bằng ứng dụng phần mềm hoặc thiết bị phần cứng. Sniffing rất đơn giản trong các mạng dựa trên trung tâm, vì lưu lượng trên một phân khúc đi qua tất cả các máy chủ được liên kết với phân khúc đó. Tuy nhiên, hầu hết các mạng ngày nay hoạt động trên các thiết bị chuyển mạch. Switch là một thiết bị mạng máy tính tiên tiến. Sự khác biệt chính giữa một trung tâm và một bộ chuyển mạch là một trung tâm truyền dữ liệu dòng đến từng cổng trên máy và không có ánh xạ dòng, trong khi một bộ chuyển mạch nhìn vào địa chỉ Điều khiển truy cập phương tiện (MAC) được liên kết với từng khung đi qua nó và gửi dữ liệu đến cổng yêu cầu. Địa chỉ MAC là địa chỉ phần cứng xác định duy nhất từng nút của mạng.
   5. Kẻ tấn công cần thao tác chức năng của công tắc để xem tất cả lưu lượng đi qua nó. Một chương trình đánh hơi gói (còn được gọi là trình nghe lén) chỉ có thể bắt các gói dữ liệu từ bên trong một mạng con nhất định, điều đó có nghĩa là nó không thể đánh hơi các gói từ một mạng khác. Thông thường, bất kỳ máy tính xách tay nào cũng có thể cắm vào mạng và có quyền truy cập vào mạng đó. Nhiều cổng chuyển đổi của doanh nghiệp được mở. Do đó, một trình nghe lén gói được đặt trên mạng ở chế độ hỗn hợp có thể nắm bắt và phân tích tất cả lưu lượng mạng. Các chương trình đánh hơi tắt bộ lọc được sử dụng bởi thẻ giao diện mạng Ethernet (NICS) để ngăn máy chủ nhìn thấy lưu lượng của các trạm khác. Do đó, các chương trình đánh hơi có thể giám sát tất cả lưu lượng.
   6. Mặc dù hầu hết các mạng ngày nay đều sử dụng công nghệ chuyển mạch, nhưng việc dò tìm gói vẫn hữu ích. Điều này là do việc cài đặt các chương trình dò tìm từ xa trên các thành phần mạng có lưu lượng truy cập lớn như máy chủ và bộ định tuyến là tương đối dễ dàng. Nó cho phép kẻ tấn công quan sát và truy cập toàn bộ lưu lượng mạng từ một điểm. Trình thám thính gói có thể nắm bắt các gói dữ liệu chứa thông tin nhạy cảm như mật khẩu, thông tin tài khoản, lưu lượng nhật ký hệ thống, cấu hình bộ định tuyến, lưu lượng DNS, lưu lượng email, lưu lượng truy cập web, phiên trò chuyện và mật khẩu FTP. Điều này cho phép kẻ tấn công đọc mật khẩu ở dạng văn bản rõ ràng, email thực tế, số thẻ tín dụng, giao dịch tài chính, v.v. Nó cũng cho phép kẻ tấn công đánh hơi lưu lượng SMTP, POP, IMAP, IMAP, HTTP Basic, xác thực telnet, cơ sở dữ liệu SQL, SMB, Lưu lượng NFS và FTP. Kẻ tấn công có thể thu được một lượng thông tin đáng kể bằng cách đọc các gói dữ liệu bị bắt; sau đó, kẻ tấn công có thể sử dụng thông tin đó để đột nhập vào mạng. Kẻ tấn công thực hiện các cuộc tấn công hiệu quả hơn bằng cách kết hợp các kỹ thuật này với đường truyền tích cực.
   7. Làm thế nào một Sniffer Works
   8. Cách phổ biến nhất của mạng máy tính là thông qua kết nối Ethernet. Một máy tính được kết nối với mạng cục bộ (LAN) có hai địa chỉ: địa chỉ MAC và địa chỉ Giao thức Internet (IP). Địa chỉ MAC xác định duy nhất từng nút trong mạng và được lưu trữ trên chính NIC. Giao thức Ethernet sử dụng địa chỉ MAC để truyền dữ liệu đến và đi từ hệ thống trong khi xây dựng khung dữ liệu. Lớp liên kết dữ liệu của mô hình OSI sử dụng tiêu đề Ethernet với địa chỉ MAC của máy đích thay vì địa chỉ IP. Lớp mạng chịu trách nhiệm ánh xạ địa chỉ mạng IP sang địa chỉ MAC theo yêu cầu của giao thức liên kết dữ liệu. Ban đầu, nó tìm kiếm địa chỉ MAC của máy đích trong một bảng, thường được gọi là bộ đệm Giao thức phân giải địa chỉ (ARP). Nếu không có mục nào cho địa chỉ IP, một quảng bá ARP của gói yêu cầu sẽ được gửi đến tất cả các máy trên mạng con cục bộ. Máy có địa chỉ cụ thể đó phản hồi máy nguồn bằng địa chỉ MAC của nó. Bộ đệm ARP của máy nguồn thêm địa chỉ MAC này vào bảng. Máy nguồn, trong tất cả các giao tiếp của nó với máy đích, sau đó sử dụng địa chỉ MAC này.
   9. Có hai loại môi trường Ethernet cơ bản và các trình thám thính hoạt động khác nhau trong mỗi loại. Hai loại này là:
   10. ■ Ethernet chia sẻ
   11. Trong môi trường Ethernet được chia sẻ, một bus duy nhất kết nối tất cả các máy chủ cạnh tranh băng thông. Trong môi trường này, tất cả các máy khác đều nhận được các gói dành cho một máy. Do đó, khi máy 1 muốn nói chuyện với máy 2, nó sẽ gửi một gói ra mạng với địa chỉ MAC đích của máy 2, cùng với địa chỉ MAC nguồn của chính nó. Các máy khác trong Ethernet dùng chung (máy 3 và 4) so sánh địa chỉ MAC đích của khung với địa chỉ MAC của chính chúng và loại bỏ khung chưa khớp. Tuy nhiên, một máy chạy trình thám thính bỏ qua quy tắc này và chấp nhận tất cả các khung. Sniffing trong môi trường Ethernet dùng chung là thụ động và do đó khó bị phát hiện.

■ Ethernet chuyển mạch

Trong môi trường Ethernet chuyển mạch, các máy chủ kết nối với một bộ chuyển mạch thay vì một trung tâm. Công tắc duy trì một bảng theo dõi địa chỉ MAC của từng máy tính và cổng vật lý mà địa chỉ MAC đó được kết nối, sau đó phân phối các gói dành cho một máy cụ thể. Công tắc là một thiết bị chỉ gửi các gói đến máy tính đích; hơn nữa, nó không phát chúng đến tất cả các máy tính trên mạng. Điều này dẫn đến việc sử dụng tốt hơn băng thông có sẵn và bảo mật được cải thiện. Do đó, quá trình đặt NIC của máy vào chế độ hỗn hợp để thu thập các gói không hoạt động. Kết quả là, nhiều người nghĩ rằng các mạng chuyển mạch là an toàn và không bị nghe lén. Tuy nhiên, điều này là không đúng sự thật.

Mặc dù một bộ chuyển mạch an toàn hơn một trung tâm, nhưng có thể đánh hơi mạng bằng các phương pháp sau:

■ Giả mạo ARP

ARP là không trạng thái. Một máy có thể gửi trả lời ARP ngay cả khi không yêu cầu; hơn nữa, nó có thể chấp nhận một câu trả lời như vậy. Khi một máy muốn đánh hơi lưu lượng bắt nguồn từ một hệ thống khác, nó có thể ARP giả mạo cổng của mạng. Bộ đệm ẩn ARP của máy mục tiêu sẽ có một mục không chính xác cho cổng. Do đó, tất cả lưu lượng truy cập định đi qua cổng bây giờ sẽ đi qua máy đã giả mạo địa chỉ MAC của cổng.

■ Ngập MAC

Công tắc duy trì một bảng dịch ánh xạ các địa chỉ MAC khác nhau tới các cổng vật lý trên công tắc. Kết quả là, chúng có thể định tuyến các gói tin từ máy chủ này sang máy chủ khác một cách thông minh. Tuy nhiên, công tắc có bộ nhớ hạn chế. Trào ngập MAC sử dụng giới hạn này để bắn phá các thiết bị chuyển mạch bằng địa chỉ MAC giả cho đến khi các thiết bị chuyển mạch không thể theo kịp nữa. Khi điều này xảy ra với một công tắc, nó sẽ chuyển sang chế độ mở không thành công, trong đó nó bắt đầu hoạt động như một trung tâm bằng cách phát các gói tin tới tất cả các cổng trên công tắc. Khi điều đó xảy ra, việc đánh hơi trở nên dễ dàng. macof là một tiện ích đi kèm với bộ dsniff và giúp kẻ tấn công thực hiện tràn ngập MAC.

Khi một công tắc biến thành một trung tâm, nó sẽ bắt đầu phát tất cả các gói mà nó nhận được tới tất cả các máy tính trong mạng. Theo mặc định, chế độ hỗn tạp bị tắt trong các máy mạng; do đó, NICS chỉ chấp nhận những gói được gửi đến máy của người dùng và loại bỏ các gói được gửi đến các máy khác. Một trình thám thính chuyển NIC của một hệ thống sang chế độ hỗn hợp để nó lắng nghe tất cả dữ liệu được truyền trên phân đoạn của nó. Một trình thám thính có thể liên tục theo dõi tất cả lưu lượng mạng đến một máy tính thông qua NIC bằng cách giải mã thông tin được gói gọn trong các gói dữ liệu. Những kẻ tấn công định cấu hình NIC trong máy của chúng chạy ở chế độ hỗn hợp để thẻ bắt đầu chấp nhận tất cả các gói. Như vậy, kẻ tấn công có thể xem tất cả các gói tin đang được truyền trong mạng.

* 1. Phương pháp nghe lén

Các kiểu đánh hơi

Những kẻ tấn công chạy trình thám thính để chuyển đổi NIC của hệ thống máy chủ sang chế độ hỗn tạp. Như đã thảo luận

trước đó, NIC ở chế độ hỗn hợp sau đó có thể bắt các gói được gửi đến địa chỉ cụ thể

mạng.

Có hai kiểu đánh hơi. Mỗi cái được sử dụng cho các loại mạng khác nhau. Hai loại là:

■ Đánh hơi thụ động

■ Hoạt động đánh hơi

Đánh hơi thụ động

Đánh hơi thụ động liên quan đến việc không gửi gói. Nó chỉ đơn giản là nắm bắt và giám sát các gói đang chảy trong mạng. Chỉ riêng trình thám thính gói không được ưu tiên cho một cuộc tấn công vì nó chỉ hoạt động trong một miền xung đột chung. Miền xung đột phổ biến là khu vực của mạng không được chuyển mạch hoặc bắc cầu (nghĩa là được kết nối thông qua một trung tâm). Các miền xung đột phổ biến có mặt trong môi trường trung tâm. Một mạng sử dụng các trung tâm để kết nối các hệ thống sử dụng phương pháp đánh hơi thụ động. Trong các mạng như vậy, tất cả các máy chủ trong mạng có thể thấy tất cả lưu lượng. Do đó, thật dễ dàng để nắm bắt lưu lượng truy cập qua trung tâm bằng cách sử dụng đánh hơi thụ động.

Những kẻ tấn công sử dụng các phương pháp đánh hơi thụ động sau đây để giành quyền kiểm soát mạng mục tiêu:

• Xâm phạm bảo mật vật lý: Kẻ tấn công thành công trong việc xâm phạm bảo mật vật lý của tổ chức mục tiêu có thể xâm nhập vào tổ chức bằng máy tính xách tay và cố gắng cắm vào mạng và lấy thông tin nhạy cảm về tổ chức.

⚫ Sử dụng ngựa thành Troia: Hầu hết các Trojan đều có khả năng đánh hơi tích hợp. Kẻ tấn công có thể cài đặt những thứ này trên máy của nạn nhân để xâm phạm nó. Sau khi xâm nhập vào máy nạn nhân, kẻ tấn công có thể cài đặt gói nghe trộm và thực hiện đánh hơi.

Hầu hết các mạng hiện đại sử dụng thiết bị chuyển mạch thay vì trung tâm. Một công tắc loại bỏ nguy cơ bị động

đánh hơi. Tuy nhiên, một công tắc vẫn dễ bị đánh hơi tích cực.

Lưu ý: Đánh hơi thụ động mang lại lợi thế tàng hình đáng kể so với đánh hơi chủ động.

đánh hơi tích cực

Đánh hơi tích cực tìm kiếm lưu lượng truy cập trên mạng LAN đã chuyển đổi bằng cách tích cực đưa lưu lượng truy cập vào đó. Đánh hơi tích cực cũng đề cập đến đánh hơi thông qua một công tắc. Trong thăm dò tích cực, Ethernet đã chuyển mạch không truyền thông tin đến tất cả các hệ thống được kết nối thông qua mạng LAN như trong mạng dựa trên trung tâm. Vì lý do này, một trình nghe lén thụ động không thể đánh hơi dữ liệu trên mạng đã chuyển đổi. Rất dễ phát hiện các chương trình nghe lén này và rất khó thực hiện kiểu nghe trộm này.

Công tắc kiểm tra các gói dữ liệu để biết địa chỉ nguồn và đích, sau đó truyền chúng đến các đích thích hợp. Do đó, việc đánh hơi các công tắc rất cồng kềnh. Tuy nhiên, những kẻ tấn công có thể chủ động đưa lưu lượng ARP vào mạng LAN để đánh hơi xung quanh mạng đã chuyển đổi và nắm bắt lưu lượng. Các thiết bị chuyển mạch duy trì bộ đệm ARP của riêng chúng trong Bộ nhớ có thể định địa chỉ nội dung (CAM). CAM là một loại bộ nhớ đặc biệt duy trì bản ghi máy chủ nào được kết nối với cổng nào. Một trình thám thính ghi lại tất cả thông tin hiển thị trên mạng để xem xét trong tương lai. Kẻ tấn công có thể xem tất cả thông tin trong các gói, bao gồm cả dữ liệu nên được ẩn.

Để tóm tắt các loại đánh hơi: đánh hơi thụ động không gửi bất kỳ gói nào; nó chỉ giám sát các gói được gửi bởi những người khác. Đánh hơi tích cực liên quan đến việc gửi nhiều đầu dò mạng để xác định các điểm truy cập.

Sau đây là danh sách các kỹ thuật đánh hơi tích cực khác nhau:

■ tràn ngập MAC

• Ngộ độc DNS

■ Ngộ độc ARP

■Các cuộc tấn công DHCP

Chuyển đổi cổng ăn cắp

tấn công giả mạo

* 1. Tấn công giả mạo địa chỉ MAC

Giả mạo/Sao chép MAC

Sao chép MAC đề cập đến việc giả mạo địa chỉ MAC bằng địa chỉ MAC của người dùng hợp pháp trên mạng. Một cuộc tấn công sao chép MAC liên quan đến việc đánh hơi mạng để tìm địa chỉ MAC của các máy khách hợp pháp được kết nối với mạng. Trong cuộc tấn công này, trước tiên kẻ tấn công lấy địa chỉ MAC của các máy khách đang tích cực liên kết với cổng chuyển đổi. Sau đó, kẻ tấn công giả mạo địa chỉ MAC bằng địa chỉ MAC của máy khách hợp pháp. Nếu việc giả mạo thành công, thì kẻ tấn công có thể nhận được tất cả lưu lượng dành cho máy khách. Do đó, kẻ tấn công có thể truy cập vào mạng và chiếm lấy danh tính của ai đó trên mạng.

Kỹ thuật giả mạo MAC: Windows

Có hai phương pháp để giả mạo MAC trong HĐH Windows 10:

Phương pháp 1: Nếu card giao diện mạng hỗ trợ sao chép địa chỉ MAC, hãy làm theo các bước sau:

1. Nhấp vào Bắt đầu, tìm kiếm Bảng điều khiển và mở nó, sau đó điều hướng đến Mạng và

Internet → Trung tâm Mạng và Chia sẻ.

2. Bấm vào Ethernet rồi bấm vào Thuộc tính trong cửa sổ Trạng thái Ethernet.

3. Trong cửa sổ Thuộc tính Ethernet, nhấp vào nút Cấu hình và sau đó nhấp vào tab Nâng cao.

4. Trong phần "Thuộc tính", tìm Địa chỉ mạng và nhấp vào địa chỉ đó.

5. Ở phía bên tay phải, bên dưới "Giá trị", nhập địa chỉ MAC mới mà bạn muốn chỉ định và nhấp vào OK.

Lưu ý: Nhập số địa chỉ MAC không có dấu ":" ở giữa.

6. Nhập "ipconfig/all" hoặc "net config rdr" vào dấu nhắc lệnh để xác minh các thay đổi.

7. Nếu các thay đổi hiển thị, hãy khởi động lại hệ thống, nếu không, hãy thử phương pháp 2 (thay đổi địa chỉ MAC trong sổ đăng ký).

Cách 2: Các bước thay đổi địa chỉ MAC trong registry:

1. Nhấn Win + R để mở Run và nhập regedit32 để bắt đầu trình chỉnh sửa sổ đăng ký.

2. Lưu ý: Không gõ Regedit để khởi động trình chỉnh sửa sổ đăng ký. Truy cập "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325- 11ce-bfc1-08002be10318} và nhấp đúp vào nó để mở rộng cây.

3. Sẽ tìm thấy các khóa phụ gồm bốn chữ số đại diện cho bộ điều hợp mạng (bắt đầu bằng 0000, 0001, 0002, v.v.).

4. Tìm kiếm phím "DriverDesc" thích hợp để tìm giao diện mong muốn.

5. Nhấp chuột phải vào khóa phụ thích hợp và thêm giá trị chuỗi mới "NetworkAddress" (kiểu dữ liệu "REG\_SZ") để chứa địa chỉ MAC mới.

6. Nhấp chuột phải vào giá trị chuỗi "NetworkAddress" ở bên phải và chọn Sửa đổi...

7. Bây giờ, trong hộp thoại "Chỉnh sửa chuỗi", hãy nhập địa chỉ MAC mới vào trường "Dữ liệu giá trị" và nhấp vào "OK".

8. Tắt rồi bật lại giao diện mạng đã thay đổi hoặc khởi động lại hệ thống.

* 1. Tấn công giả mạo DHCP

Tấn công bỏ đói DHCP

Trong một cuộc tấn công bỏ đói DHCP, kẻ tấn công làm tràn ngập máy chủ DHCP bằng cách gửi nhiều yêu cầu DHCP và sử dụng tất cả các địa chỉ IP khả dụng mà máy chủ DHCP có thể cấp. Kết quả là máy chủ không thể cấp thêm bất kỳ địa chỉ IP nào, dẫn đến tấn công DoS. Do sự cố này, người dùng hợp lệ không thể lấy hoặc gia hạn địa chỉ IP của họ; do đó, họ không thể truy cập mạng của họ. Kẻ tấn công phát đi các yêu cầu DHCP với các địa chỉ MAC giả mạo với sự trợ giúp của các công cụ như Yersinia, Hyenae và Gobbler.

Tấn công máy chủ DHCP lừa đảo

Ngoài các cuộc tấn công bỏ đói DHCP, kẻ tấn công có thể thực hiện các cuộc tấn công MITM như đánh hơi. Kẻ tấn công thành công trong việc sử dụng hết không gian địa chỉ IP của máy chủ DHCP có thể thiết lập một máy chủ DHCP giả mạo trên mạng, máy chủ này không nằm dưới sự kiểm soát của quản trị viên mạng. Máy chủ DHCP lừa đảo mạo danh một máy chủ hợp pháp và cung cấp địa chỉ IP cũng như thông tin mạng khác cho các máy khách khác trong mạng, hoạt động như một cổng mặc định. Các máy khách được kết nối với mạng bằng các địa chỉ được chỉ định bởi máy chủ giả mạo giờ đây sẽ trở thành nạn nhân của MITM và các cuộc tấn công khác, theo đó các gói được chuyển tiếp từ máy của khách hàng sẽ đến máy chủ giả mạo trước.

Trong một cuộc tấn công máy chủ DHCP giả mạo, kẻ tấn công sẽ đưa một máy chủ giả mạo vào mạng. Máy chủ lừa đảo này có thể phản hồi các yêu cầu khám phá DHCP của khách hàng. Mặc dù cả máy chủ DHCP giả mạo và thực tế đều phản hồi yêu cầu, nhưng máy khách chấp nhận phản hồi đến trước. Trong trường hợp máy chủ giả mạo phản hồi sớm hơn máy chủ DHCP thực, máy khách sẽ nhận phản hồi của máy chủ giả mạo. Thông tin do máy chủ giả mạo này cung cấp cho khách hàng có thể làm gián đoạn truy cập mạng của họ, gây ra một cuộc tấn công DoS.

Phản hồi DHCP từ máy chủ DHCP giả mạo của kẻ tấn công có thể chỉ định địa chỉ IP đóng vai trò là cổng mặc định của máy khách. Do đó, địa chỉ IP của kẻ tấn công nhận được tất cả lưu lượng truy cập từ máy khách. Kẻ tấn công sau đó nắm bắt tất cả lưu lượng và chuyển tiếp nó đến cổng mặc định thích hợp. Khách hàng nghĩ rằng mọi thứ đang hoạt động bình thường. Kiểu tấn công này rất khó để khách hàng phát hiện trong thời gian dài.

Đôi khi, máy khách sử dụng máy chủ DHCP giả mạo thay vì tiêu chuẩn. Máy chủ giả mạo hướng dẫn khách hàng truy cập các trang web giả mạo nhằm lấy thông tin đăng nhập của họ.

Để giảm thiểu cuộc tấn công máy chủ DHCP giả mạo, hãy đặt kết nối giữa giao diện và máy chủ giả mạo là không đáng tin cậy. Hành động này sẽ chặn tất cả các tin nhắn máy chủ DHCP đến từ giao diện đó.

* 1. Đầu độc ARP và DNS

**Tấn công giả mạo ARP**

ARP phân giải địa chỉ IP thành địa chỉ MAC (phần cứng) của giao diện để gửi dữ liệu. Các gói ARP có thể được giả mạo để gửi dữ liệu đến máy của kẻ tấn công. Giả mạo ARP liên quan đến việc xây dựng một số lượng lớn các gói yêu cầu và trả lời ARP giả mạo để làm quá tải một công tắc. Khi một máy gửi yêu cầu ARP, nó giả định rằng phản hồi ARP sẽ đến từ đúng máy. ARP không cung cấp phương tiện xác minh tính xác thực của thiết bị phản hồi. Ngay cả những hệ thống chưa thực hiện yêu cầu ARP cũng có thể chấp nhận phản hồi ARP đến từ các thiết bị khác. Những kẻ tấn công sử dụng lỗ hổng này trong ARP để tạo các phản hồi ARP không đúng định dạng chứa địa chỉ IP và MAC giả mạo. Giả sử đó là phản hồi ARP hợp pháp, máy tính của nạn nhân chấp nhận mục nhập ARP một cách mù quáng vào bảng ARP của nó. Khi bảng ARP tràn ngập các phản hồi ARP giả mạo, công tắc được đặt ở chế độ chuyển tiếp và kẻ tấn công sẽ chặn tất cả dữ liệu truyền từ máy của nạn nhân mà nạn nhân không hề hay biết về cuộc tấn công. Những kẻ tấn công làm ngập bộ đệm ARP của máy tính mục tiêu với các mục nhập giả mạo, còn được gọi là đầu độc. Giả mạo ARP là trung gian để thực hiện các cuộc tấn công như DoS, MITM và chiếm quyền điều khiển phiên.

Giả mạo ARP hoạt động như thế nào?

Giả mạo ARP là một phương pháp tấn công mạng LAN Ethernet. Khi một người dùng hợp pháp bắt đầu một phiên với một người dùng khác trong cùng miền quảng bá lớp 2, bộ chuyển mạch sẽ phát một yêu cầu ARP bằng địa chỉ IP của người nhận, trong khi người gửi đợi người nhận phản hồi bằng địa chỉ MAC. Kẻ tấn công nghe lén miền quảng bá lớp 2 không được bảo vệ này có thể phản hồi yêu cầu ARP quảng bá và trả lời người gửi bằng cách giả mạo địa chỉ IP của người nhận dự định. Kẻ tấn công chạy trình thám thính và chuyển bộ điều hợp NIC của máy sang chế độ hỗn tạp.

Giả mạo ARP là một phương pháp tấn công mạng LAN Ethernet. Nó thành công bằng cách thay đổi địa chỉ IP của máy tính của kẻ tấn công thành địa chỉ IP của máy tính mục tiêu. Một gói yêu cầu và trả lời ARP giả mạo có thể tìm thấy một vị trí trong bộ đệm ARP đích trong quá trình này. Vì phản hồi ARP đã được giả mạo, máy tính đích (đích) sẽ gửi các khung đến máy tính của kẻ tấn công, nơi kẻ tấn công có thể sửa đổi các khung trước khi gửi chúng đến máy nguồn (Người dùng A) trong một cuộc tấn công MITM. Kẻ tấn công cũng có thể khởi động một cuộc tấn công DoS bằng cách liên kết một địa chỉ MAC không tồn tại với địa chỉ IP của cổng; cách khác, kẻ tấn công có thể đánh hơi lưu lượng một cách thụ động và sau đó chuyển tiếp nó đến đích đích.

Các mối đe dọa của ngộ độc ARP

Với sự trợ giúp của đầu độc ARP, kẻ tấn công có thể sử dụng thông báo ARP giả để chuyển hướng tất cả liên lạc giữa hai máy để tất cả lưu lượng truy cập chuyển hướng qua PC của kẻ tấn công.

Các mối đe dọa của ngộ độc ARP bao gồm:

⚫ Packet Sniffing: Đánh hơi lưu lượng trên một mạng hoặc một phần của mạng.

⚫ Chiếm quyền truy cập phiên: Đánh cắp thông tin phiên hợp lệ và sử dụng thông tin đó để truy cập trái phép vào một ứng dụng.

Khai thác cuộc gọi VoIP: Sử dụng phản chiếu cổng, cho phép thiết bị khai thác cuộc gọi VoIP giám sát tất cả lưu lượng mạng và chỉ chọn lưu lượng VoIP để ghi theo địa chỉ MAC.

Thao túng dữ liệu: Giả mạo ARP cho phép kẻ tấn công nắm bắt và sửa đổi dữ liệu hoặc dừng luồng lưu lượng.

Man-in-the-Middle Attack: Kẻ tấn công thực hiện một cuộc tấn công MITM nơi chúng cư trú giữa nạn nhân và máy chủ.

■ Chặn dữ liệu: Chặn địa chỉ IP, địa chỉ MAC và VLAN được kết nối với bộ chuyển mạch trong mạng.

Cướp kết nối: Trong một mạng, các địa chỉ phần cứng được coi là duy nhất và cố định, nhưng một máy chủ có thể di chuyển khi tên máy chủ của nó thay đổi và sử dụng một giao thức khác. Trong chiếm quyền điều khiển kết nối, kẻ tấn công có thể thao túng kết nối của khách hàng để kiểm soát hoàn toàn.

• Đặt lại kết nối: Thông tin định tuyến sai có thể được truyền đi do lỗi phần cứng/phần mềm. Trong những trường hợp như vậy, nếu một máy chủ không thể bắt đầu kết nối, thì máy chủ đó sẽ thông báo cho mô-đun Giải quyết Địa chỉ để xóa thông tin của nó. Việc nhận dữ liệu từ máy chủ đó sẽ đặt lại thời gian chờ kết nối trong mục ARP được sử dụng để truyền dữ liệu đến máy chủ đó. Mục nhập này trong mô-đun ARP sẽ bị xóa nếu máy chủ không gửi bất kỳ thông tin nào trong một khoảng thời gian nhất định.

• Đánh cắp mật khẩu: Kẻ tấn công sử dụng các phản hồi ARP giả mạo và đánh lừa các máy chủ mục tiêu gửi thông tin nhạy cảm như tên người dùng và mật khẩu.

Tấn công DoS: Liên kết nhiều địa chỉ IP với một địa chỉ MAC duy nhất của máy chủ mục tiêu dành cho các địa chỉ IP khác nhau, địa chỉ này sẽ bị quá tải với một lượng lớn lưu lượng truy cập.

Kỹ thuật đánh hơi: Đầu độc DNS

Phần này mô tả các kỹ thuật đầu độc DNS để đánh hơi lưu lượng DNS của mạng mục tiêu. Sử dụng kỹ thuật này, kẻ tấn công có thể lấy ID của yêu cầu DNS bằng cách đánh hơi và có thể gửi phản hồi độc hại tới người gửi trước khi máy chủ DNS thực tế phản hồi.

**Kỹ thuật đầu độc DNS**

DNS là giao thức dịch tên miền (ví dụ: www.eccouncil.org) thành địa chỉ IP (ví dụ: 208.66.172.56). Giao thức sử dụng các bảng DNS chứa tên miền và địa chỉ IP tương đương của nó được lưu trữ trong cơ sở dữ liệu lớn phân tán. Trong ngộ độc DNS, còn được gọi là giả mạo DNS, kẻ tấn công đánh lừa máy chủ DNS tin rằng nó đã nhận được thông tin xác thực trong khi trên thực tế, nó không nhận được bất kỳ thông tin nào. Kẻ tấn công cố gắng chuyển hướng nạn nhân đến một máy chủ độc hại thay vì máy chủ hợp pháp. Kẻ tấn công thực hiện điều này bằng cách thao túng các mục trong bảng DNS trong DNS. Điều này dẫn đến việc thay thế địa chỉ IP giả ở cấp DNS, nơi địa chỉ web được chuyển đổi thành địa chỉ IP số.

Khi nạn nhân cố gắng truy cập một trang web, kẻ tấn công sẽ thao tác các mục trong bảng DNS để hệ thống của nạn nhân chuyển hướng URL đến máy chủ của kẻ tấn công. Kẻ tấn công thay thế các mục nhập địa chỉ IP cho một trang đích trên một máy chủ DNS nhất định bằng địa chỉ IP của máy chủ (máy chủ độc hại) mà kẻ đó kiểm soát. Kẻ tấn công có thể tạo các mục DNS giả cho máy chủ (chứa nội dung độc hại) có cùng tên với tên của máy chủ mục tiêu. Do đó, nạn nhân kết nối với máy chủ của kẻ tấn công mà không nhận ra. Khi nạn nhân kết nối với máy chủ của kẻ tấn công, kẻ tấn công có thể xâm phạm hệ thống của nạn nhân và đánh cắp dữ liệu.

Có thể ngộ độc DNS bằng các kỹ thuật sau:

• Giả mạo DNS mạng nội bộ

■ Giả mạo DNS Internet

• Đầu độc DNS máy chủ proxy

• Ngộ độc bộ đệm DNS

Giả mạo DNS mạng nội bộ

Kẻ tấn công có thể thực hiện tấn công giả mạo DNS mạng nội bộ trên mạng LAN được chuyển đổi với sự trợ giúp của kỹ thuật đầu độc ARP. Để thực hiện cuộc tấn công này, kẻ tấn công phải được kết nối với mạng LAN và có thể đánh hơi lưu lượng hoặc gói tin. Kẻ tấn công thành công trong việc đánh hơi ID của yêu cầu DNS từ mạng nội bộ có thể gửi phản hồi độc hại cho người gửi trước máy chủ DNS thực tế.

Giả mạo DNS Internet

Ngộ độc DNS Internet còn được gọi là ngộ độc DNS từ xa. Những kẻ tấn công có thể thực hiện các cuộc tấn công giả mạo DNS trên một nạn nhân hoặc nhiều nạn nhân ở bất kỳ đâu trên thế giới. Để thực hiện cuộc tấn công này, kẻ tấn công thiết lập một máy chủ DNS giả mạo với một địa chỉ IP tĩnh.

Những kẻ tấn công thực hiện giả mạo Internet DNS với sự trợ giúp của Trojan khi hệ thống của nạn nhân kết nối với Internet. Đây là một cuộc tấn công MITM trong đó kẻ tấn công thay đổi các mục DNS chính của máy tính nạn nhân. Kẻ tấn công thay thế địa chỉ IP DNS của nạn nhân bằng một địa chỉ IP giả để phân giải cho hệ thống của kẻ tấn công. Do đó, lưu lượng truy cập của nạn nhân chuyển hướng đến hệ thống của kẻ tấn công. Tại thời điểm này, kẻ tấn công có thể dễ dàng đánh cắp thông tin bí mật của nạn nhân.

Đầu độc DNS máy chủ proxy

Trong kỹ thuật đầu độc DNS của máy chủ proxy, kẻ tấn công thiết lập một máy chủ proxy trên hệ thống của kẻ tấn công. Kẻ tấn công cũng định cấu hình DNS lừa đảo và đặt địa chỉ IP của nó làm mục nhập DNS chính trong máy chủ proxy. Kẻ tấn công thay đổi cài đặt máy chủ proxy của nạn nhân với sự trợ giúp của Trojan. Proxy đóng vai trò là DNS chính và chuyển hướng lưu lượng truy cập của nạn nhân đến trang web giả mạo, nơi kẻ tấn công có thể đánh hơi thông tin bí mật của nạn nhân rồi chuyển hướng yêu cầu đến trang web thực.

Ngộ độc bộ đệm DNS

Ngộ độc bộ đệm DNS đề cập đến việc thay đổi hoặc thêm các bản ghi DNS giả mạo trong bộ đệm của trình phân giải DNS để truy vấn DNS được chuyển hướng đến một trang web độc hại. Hệ thống DNS sử dụng bộ nhớ cache để giữ các tên miền được giải quyết gần đây. Kẻ tấn công điền vào đó các tên miền được sử dụng gần đây và các mục nhập địa chỉ IP tương ứng của chúng. Khi nhận được yêu cầu của người dùng, trình phân giải DNS trước tiên sẽ kiểm tra bộ đệm DNS; nếu hệ thống tìm thấy tên miền mà người dùng yêu cầu trong bộ đệm, trình phân giải sẽ nhanh chóng gửi địa chỉ IP tương ứng của nó. Do đó, nó làm giảm lưu lượng và thời gian phân giải DNS.

Những kẻ tấn công nhắm mục tiêu và thực hiện các thay đổi hoặc thêm các mục vào bộ đệm DNS này. Nếu trình phân giải DNS không thể xác thực rằng các phản hồi DNS đến từ một nguồn có thẩm quyền, thì nó sẽ lưu cục bộ các mục nhập không chính xác vào bộ đệm ẩn và phân phối chúng cho những người dùng thực hiện cùng một yêu cầu. Kẻ tấn công thay thế địa chỉ IP do người dùng yêu cầu bằng địa chỉ IP giả và khi người dùng yêu cầu tên miền đó, trình phân giải DNS sẽ kiểm tra mục nhập trong bộ đệm ẩn DNS và chọn mục nhập phù hợp (đã sẵn sàng). Sau đó, nó chuyển hướng nạn nhân đến máy chủ giả mạo của kẻ tấn công thay vì máy chủ dự định.

* 1. Giải pháp phòng chống
     1. Phòng chống tấn công địa chỉ MAC

Cách phòng chống giả mạo MAC

Thực hiện đánh giá bảo mật là mục tiêu chính của một hacker có đạo đức. Một hacker có đạo đức tấn công một mạng hoặc tổ chức mục tiêu bằng kiến thức và sự cho phép của ban quản lý, để tìm ra các lỗ hổng trong kiến trúc bảo mật. Tuy nhiên, công việc không kết thúc ở đó. Tìm ra những sơ hở đó là một nhiệm vụ nhỏ. Nhiệm vụ quan trọng nhất của hack đạo đức là áp dụng các biện pháp đối phó thích hợp với các lỗ hổng bảo mật để khắc phục chúng.

Khi bạn đã kiểm tra mạng để phát hiện các cuộc tấn công giả mạo MAC và thu thập các lỗ hổng bảo mật, bạn nên áp dụng các biện pháp đối phó để bảo vệ mạng khỏi bị giả mạo MAC hơn nữa. Nhiều biện pháp đối phó giả mạo MAC có thể được áp dụng cho các sơ hở và kiến trúc mạng cụ thể. Áp dụng các biện pháp đối phó thích hợp cho mạng của bạn.

Để phát hiện giả mạo MAC, cần phải biết tất cả các địa chỉ MAC trong mạng. Cách tốt nhất để chống giả mạo địa chỉ MAC là đặt máy chủ phía sau bộ định tuyến. Điều này là do các bộ định tuyến chỉ phụ thuộc vào địa chỉ IP, trong khi các bộ chuyển mạch phụ thuộc vào địa chỉ MAC để liên lạc trong mạng. Thay đổi cấu hình giao diện bảo mật cổng là một cách khác để ngăn chặn các cuộc tấn công giả mạo MAC. Khi bạn bật lệnh bảo mật cổng, lệnh này cho phép bạn chỉ định địa chỉ MAC của hệ thống được kết nối với cổng cụ thể. Nó cũng cho phép thực hiện hành động cụ thể nếu xảy ra vi phạm an ninh cổng.

Bạn cũng có thể thực hiện các kỹ thuật sau để chống lại các cuộc tấn công giả mạo địa chỉ MAC:

DHCP Snooping Binding Table: Quá trình DHCP snooping lọc các thông điệp DHCP không đáng tin cậy và giúp xây dựng và liên kết một bảng liên kết DHCP. Bảng này chứa địa chỉ MAC, địa chỉ IP, thời gian thuê, loại liên kết, số VLAN và thông tin giao diện để tương ứng với các giao diện không đáng tin cậy của một công tắc. Nó hoạt động như một tường lửa giữa các máy chủ không đáng tin cậy và máy chủ DHCP. Nó cũng giúp phân biệt giữa các giao diện đáng tin cậy và không đáng tin cậy.

Kiểm tra ARP động: Hệ thống kiểm tra liên kết địa chỉ IP-MAC cho từng gói ARP trong mạng. Trong khi thực hiện DAI, hệ thống sẽ tự động loại bỏ các liên kết địa chỉ IP-MAC không hợp lệ.

■IP Source Guard: IP Source Guard là một tính năng bảo mật trong các bộ chuyển mạch hạn chế lưu lượng IP trên các cổng lớp 2 không đáng tin cậy bằng cách lọc lưu lượng dựa trên cơ sở dữ liệu ràng buộc rình mò DHCP. Nó ngăn chặn các cuộc tấn công giả mạo khi kẻ tấn công cố gắng giả mạo hoặc sử dụng địa chỉ IP của máy chủ khác.

• Mã hóa: Mã hóa giao tiếp giữa điểm truy cập và máy tính để ngăn giả mạo MAC.

• Truy xuất địa chỉ MAC: Bạn phải luôn truy xuất trực tiếp địa chỉ MAC từ NIC thay vì truy xuất từ HĐH.

Triển khai IEEE 802.1X Suites: Đây là một loại giao thức mạng dành cho Kiểm soát truy cập mạng dựa trên cổng (PNAC) và mục đích chính của nó là thực thi kiểm soát truy cập tại điểm mà người dùng tham gia mạng.

■ AAA (Xác thực, Ủy quyền và Kế toán): Sử dụng cơ chế máy chủ AAA (Xác thực, Ủy quyền và Kế toán) để lọc địa chỉ MAC sau đó.

* + 1. Phòng chống tấn công DHCP
* Bảo vệ chống lại sự đói khát DHCP

Kích hoạt tính năng bảo mật cổng để chống lại cuộc tấn công bỏ đói DHCP. Bảo mật cổng giới hạn số lượng địa chỉ MAC tối đa trên cổng chuyển đổi. Khi vượt quá giới hạn, bộ chuyển mạch sẽ loại bỏ các yêu cầu (gói) địa chỉ MAC tiếp theo từ các nguồn bên ngoài, điều này bảo vệ máy chủ khỏi cuộc tấn công bỏ đói DHCP.

* Bảo vệ chống lại cuộc tấn công máy chủ lừa đảo

Tính năng rình mò DHCP khả dụng trên các bộ chuyển mạch có thể giảm thiểu các máy chủ DHCP giả mạo. Nó được cấu hình trên cổng mà máy chủ DHCP hợp lệ được kết nối. Sau khi được định cấu hình, DHCP snooping không cho phép các cổng khác trên bộ chuyển mạch phản hồi các gói DHCP Discover do khách hàng gửi. Do đó, ngay cả kẻ tấn công quản lý để xây dựng máy chủ DHCP giả mạo và kết nối với bộ chuyển mạch cũng không thể phản hồi các gói DHCP Discover.

* + 1. Cách phòng chống ngộ độc ARP

Triển khai Kiểm tra ARP động (DAI) ngăn chặn các cuộc tấn công đầu độc. DAI là một tính năng bảo mật xác thực các gói ARP trong mạng. Khi DAI kích hoạt trên Vlan, tất cả các cổng trên Vlan được coi là không đáng tin cậy theo mặc định. DAI xác thực các gói ARP bằng cách sử dụng bảng liên kết rình mò DHCP. Bảng ràng buộc DHCP snooping bao gồm địa chỉ MAC, địa chỉ IP và giao diện VLAN có được bằng cách lắng nghe trao đổi thông báo DHCP. Do đó, bạn phải bật DHCP snooping trước khi bật DAI. Mặt khác, không thể thiết lập kết nối giữa các thiết bị VLAN dựa trên ARP. Do đó, một DoS tự áp đặt có thể xảy ra trên bất kỳ thiết bị nào trong VLAN đó.

Để xác thực gói ARP, DAI thực hiện kiểm tra liên kết địa chỉ IP với địa chỉ MAC được lưu trữ trong cơ sở dữ liệu rình mò DHCP trước khi chuyển tiếp gói đến đích. Nếu bất kỳ địa chỉ IP không hợp lệ nào liên kết với địa chỉ MAC, DAI sẽ loại bỏ gói ARP. Điều này giúp loại bỏ nguy cơ bị tấn công MITM. DAI đảm bảo chỉ chuyển tiếp các yêu cầu và phản hồi ARP hợp lệ.

Nếu các hệ thống máy chủ trong mạng giữ địa chỉ IP tĩnh, thì DHCP snooping sẽ không thể thực hiện được hoặc các bộ chuyển mạch khác trong mạng không thể chạy kiểm tra ARP động. Trong những tình huống như vậy, bạn phải thực hiện ánh xạ tĩnh liên kết địa chỉ IP với địa chỉ MAC trên VLAN để ngăn chặn cuộc tấn công đầu độc ARP.

Có thể triển khai phần mềm chạy các tập lệnh tùy chỉnh để giám sát các bảng ARP. Tập lệnh này có thể so sánh bảng ARP hiện tại với danh sách địa chỉ MAC và IP đã biết. Nếu có sự không phù hợp trong danh sách các cặp MAC/IP hợp lệ, bộ chuyển mạch sẽ hủy gói. Các tập lệnh như vậy rất hữu ích trong việc bảo vệ chống lại các cuộc tấn công đầu độc ARP bằng cách giám sát các cặp MAC/IP trên các máy LAN quan trọng như máy chủ và cổng.

Việc triển khai các giao thức mật mã như HTTP Secure (HTTPS), Secure Shell (SSH), Transport Layer Security (TLS) và nhiều giao thức mật mã mạng khác ngăn chặn các cuộc tấn công giả mạo ARP bằng cách mã hóa dữ liệu trước khi truyền và xác thực dữ liệu sau khi nhận được.

* + 1. Cách phòng chống giả mạo DNS

Triển khai DNS chính đã báo cáo các cuộc tấn công sử dụng giả mạo DNS và lỗ hổng này

vẫn ảnh hưởng đến một số lượng lớn các tổ chức. Điều này là do thiếu thông tin khi

thực hiện các truy vấn DNS, cho phép kẻ tấn công giả mạo các phản hồi DNS. Bạn đã thấy làm thế nào một

kẻ tấn công thực hiện các loại tấn công giả mạo DNS khác nhau. Bây giờ chúng ta xem xét làm thế nào để bảo vệ một

mạng khỏi các kiểu tấn công này.

Các biện pháp đối phó giúp ngăn chặn các cuộc tấn công giả mạo DNS:

• Thực hiện phần mở rộng bảo mật hệ thống tên miền (DNSSEC)

• Sử dụng Lớp cổng bảo mật (SSL) để bảo mật lưu lượng

• Giải quyết tất cả các truy vấn DNS tới máy chủ DNS cục bộ

• Chặn các yêu cầu DNS được gửi đến các máy chủ bên ngoài

• Định cấu hình tường lửa để hạn chế tra cứu DNS bên ngoài

• Triển khai và triển khai hệ thống phát hiện xâm nhập (IDS) một cách chính xác

• Định cấu hình trình phân giải DNS để sử dụng cổng nguồn ngẫu nhiên mới cho mỗi truy vấn gửi đi

• Hạn chế dịch vụ tái sử dụng DNS, toàn bộ hoặc một phần, đối với người dùng được ủy quyền

Sử dụng giới hạn tỷ lệ miền không tồn tại DNS (NXDOMAIN)

• Bảo vệ máy nội bộ của bạn

• Sử dụng bảng ARP và IP tĩnh

• Sử dụng mã hóa SSH

• Không cho phép lưu lượng gửi đi sử dụng cổng UDP 53 làm cổng nguồn mặc định

• Kiểm tra máy chủ DNS thường xuyên để loại bỏ các lỗ hổng

• Sử dụng các công cụ phát hiện đánh hơi

• Không mở các tệp đáng ngờ

Luôn sử dụng các trang web proxy đáng tin cậy

■ Nếu một công ty xử lý trình giải quyết của riêng mình, thì nó phải được giữ kín và được bảo vệ tốt

• Ngẫu nhiên hóa địa chỉ IP nguồn và đích

• Ngẫu nhiên hóa ID truy vấn

• Trường hợp ngẫu nhiên trong các yêu cầu tên

• Sử dụng Cơ sở hạ tầng khóa công khai (PKI) để bảo vệ máy chủ

• Duy trì một dải địa chỉ IP duy nhất hoặc cụ thể để đăng nhập vào hệ thống

• Thực hiện lọc gói cho cả lưu lượng truy cập vào và ra

Hạn chế chuyển vùng DNS sang một nhóm địa chỉ IP giới hạn

Câu hỏi và bài tập

1. Tấn công máy chủ và ứng dụng Web
   1. Khái niệm cơ bản

Kẻ tấn công có thể sử dụng nhiều kỹ thuật để xâm phạm máy chủ web, chẳng hạn như DOS/DDOS, chiếm quyền điều khiển máy chủ Hệ thống tên miền (DNS), khuếch đại DNS, duyệt thư mục, man in the middle (MITM)/đánh hơi, lừa đảo, phá hoại trang web, máy chủ web cấu hình sai, phân tách phản hồi HTTP, nhiễm độc bộ đệm web, lực lượng vũ phu Secure Shell (SSH) và bẻ khóa mật khẩu máy chủ web. Phần này mô tả chi tiết các kỹ thuật tấn công này.

Tấn công DOS/DDoS

Một cuộc tấn công DOS/DDoS liên quan đến việc làm tràn ngập các mục tiêu với vô số yêu cầu giả mạo để mục tiêu ngừng hoạt động và không khả dụng đối với người dùng hợp pháp. Bằng cách sử dụng một cuộc tấn công DoS/DDoS của máy chủ web, kẻ tấn công cố gắng đánh sập máy chủ web hoặc làm cho nó không khả dụng đối với người dùng hợp pháp. Một cuộc tấn công DoS/DDoS máy chủ web thường nhắm vào các máy chủ web cấu hình cao như máy chủ ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí cả máy chủ định danh gốc.

Để đánh sập máy chủ web đang chạy ứng dụng, kẻ tấn công nhắm mục tiêu các dịch vụ sau để tiêu thụ tài nguyên của máy chủ web bằng các yêu cầu giả mạo:

■Băng thông mạng

■ Bộ nhớ máy chủ

■ Cơ chế xử lý ngoại lệ của ứng dụng

• Sử dụng CPU

■ Dung lượng đĩa cứng

■ Không gian cơ sở dữ liệu

Chiếm đoạt máy chủ DNS

Hệ thống tên miền (DNS) phân giải tên miền thành địa chỉ IP tương ứng. Người dùng truy vấn máy chủ DNS bằng một tên miền và máy chủ DNS phản hồi bằng địa chỉ IP tương ứng.

Trong chiếm quyền điều khiển máy chủ DNS, kẻ tấn công xâm phạm máy chủ DNS và thay đổi cài đặt ánh xạ của nó để chuyển hướng đến máy chủ DNS giả mạo sẽ chuyển hướng yêu cầu của người dùng đến máy chủ giả mạo của kẻ tấn công. Do đó, khi người dùng nhập một URL hợp pháp trong trình duyệt, cài đặt sẽ chuyển hướng đến trang web giả mạo của kẻ tấn công.

Tấn công khuếch đại DNS

Truy vấn DNS đệ quy là một phương pháp yêu cầu ánh xạ DNS. Truy vấn đi qua các máy chủ DNS theo cách đệ quy cho đến khi không tìm thấy tên miền được chỉ định để ánh xạ địa chỉ IP.

Tấn công duyệt thư mục

Kẻ tấn công có thể thực hiện tấn công duyệt thư mục do lỗ hổng trong mã của ứng dụng web. Ngoài ra, phần mềm máy chủ web được vá lỗi hoặc cấu hình kém có thể khiến máy chủ web dễ bị tấn công qua thư mục.

Thiết kế của các máy chủ web hạn chế truy cập công khai ở một mức độ nào đó. Truyền tải thư mục là việc khai thác HTTP mà qua đó kẻ tấn công có thể truy cập vào các thư mục bị hạn chế và thực thi các lệnh bên ngoài thư mục gốc của máy chủ web bằng cách thao tác với Bộ định vị tài nguyên thống nhất (URL). Trong các cuộc tấn công duyệt thư mục, kẻ tấn công sử dụng chuỗi dấu chấm-chấm-gạch chéo (../) để truy cập các thư mục bị hạn chế bên ngoài thư mục gốc của máy chủ web. Kẻ tấn công có thể sử dụng phương pháp thử và sai để điều hướng bên ngoài thư mục gốc và truy cập thông tin nhạy cảm trong hệ thống.

Kẻ tấn công khai thác phần mềm máy chủ web (chương trình máy chủ web) để thực hiện tấn công duyệt thư mục. Kẻ tấn công thường thực hiện cuộc tấn công này với sự trợ giúp của trình duyệt. Máy chủ web dễ bị tấn công nếu nó chấp nhận dữ liệu đầu vào từ trình duyệt mà không được xác thực hợp lệ.

Man-in-the-Middle/Sniffing Attack

Các cuộc tấn công Man-in-the-middle (MITM) cho phép kẻ tấn công truy cập thông tin nhạy cảm bằng cách chặn và thay đổi thông tin liên lạc giữa người dùng cuối và máy chủ web. Trong một cuộc tấn công MITM hoặc tấn công đánh hơi, kẻ xâm nhập sẽ chặn hoặc sửa đổi các thông báo được trao đổi giữa người dùng và máy chủ web bằng cách nghe lén hoặc xâm nhập vào một kết nối. Điều này cho phép kẻ tấn công lấy cắp thông tin nhạy cảm của người dùng, chẳng hạn như chi tiết ngân hàng trực tuyến, tên người dùng và mật khẩu, được chuyển qua Internet đến máy chủ web. Kẻ tấn công dụ nạn nhân kết nối với máy chủ web bằng cách giả làm proxy. Nếu nạn nhân tin tưởng và chấp nhận yêu cầu của kẻ tấn công, thì tất cả các giao tiếp giữa người dùng và máy chủ web sẽ thông qua kẻ tấn công. Bằng cách này, kẻ tấn công có thể đánh cắp thông tin nhạy cảm của người dùng.

Tấn công lừa đảo

Những kẻ tấn công thực hiện một cuộc tấn công lừa đảo bằng cách gửi email chứa liên kết độc hại và lừa người dùng nhấp vào liên kết đó. Nhấp vào liên kết sẽ chuyển hướng người dùng đến một trang web giả mạo trông giống như trang web hợp pháp. Những kẻ tấn công tạo các trang web như vậy bằng cách lưu trữ địa chỉ của chúng trên các máy chủ web. Khi nạn nhân nhấp vào liên kết độc hại trong khi tin rằng liên kết đó là địa chỉ trang web hợp pháp, nạn nhân sẽ được chuyển hướng đến trang web độc hại được lưu trữ trên máy chủ của kẻ tấn công. Trang web nhắc người dùng nhập thông tin nhạy cảm, chẳng hạn như tên người dùng, mật khẩu, chi tiết tài khoản ngân hàng và số an sinh xã hội, đồng thời tiết lộ dữ liệu cho kẻ tấn công. Sau đó, kẻ tấn công có thể thiết lập phiên với trang web hợp pháp bằng cách sử dụng thông tin đăng nhập bị đánh cắp của nạn nhân để thực hiện các hoạt động độc hại trên trang web hợp pháp mục tiêu.

Đánh lừa trang web

Thay đổi giao diện trang web đề cập đến những thay đổi trái phép được thực hiện đối với nội dung của một trang web hoặc toàn bộ trang web, dẫn đến những thay đổi về giao diện trực quan của trang web hoặc trang web đó. Tin tặc đột nhập vào máy chủ web và thay đổi trang web được lưu trữ bằng cách chèn mã để thêm hình ảnh, cửa sổ bật lên hoặc văn bản vào một trang theo cách mà giao diện trực quan của trang thay đổi. Trong một số trường hợp, kẻ tấn công có thể thay thế toàn bộ trang web thay vì chỉ thay đổi một trang.

Các trang bị xóa khiến khách truy cập tiếp xúc với thông tin tuyên truyền hoặc gây hiểu lầm cho đến khi những thay đổi trái phép được phát hiện và sửa chữa. Những kẻ tấn công sử dụng nhiều phương pháp khác nhau, chẳng hạn như MySQL injection, để truy cập vào một trang web nhằm deface nó. Ngoài việc thay đổi giao diện trực quan của trang web mục tiêu, những kẻ tấn công làm xấu trang web để lây nhiễm vào máy tính của khách truy cập bằng cách làm cho trang web dễ bị vi-rút tấn công. Do đó, việc thay đổi giao diện trang web không chỉ khiến tổ chức mục tiêu bối rối bằng cách thay đổi giao diện của trang web mà còn nhằm mục đích gây hại cho khách truy cập.

Cấu hình sai máy chủ web

Cấu hình sai máy chủ web đề cập đến các điểm yếu cấu hình trong cơ sở hạ tầng web có thể bị khai thác để khởi chạy các cuộc tấn công khác nhau vào máy chủ web, chẳng hạn như duyệt thư mục, xâm nhập máy chủ và đánh cắp dữ liệu. Sau đây là một số cấu hình sai của máy chủ web:

• Thông báo lỗi/gỡ lỗi chi tiết

• Người dùng/mật khẩu ẩn danh hoặc mặc định

■ Tệp cấu hình mẫu và tập lệnh • Chức năng quản trị từ xa

• Đã bật các dịch vụ không cần thiết

• Chứng chỉ SSL mặc định/được định cấu hình sai

Một ví dụ về cấu hình sai máy chủ web

"Giữ an toàn cho cấu hình máy chủ yêu cầu phải cảnh giác"-Open Web Application Security Project (OWASP)

Quản trị viên định cấu hình máy chủ web không đúng cách có thể để lại các lỗ hổng nghiêm trọng trong máy chủ web, do đó tạo cơ hội cho kẻ tấn công khai thác máy chủ web được định cấu hình sai để xâm phạm bảo mật và lấy thông tin nhạy cảm. Các lỗ hổng của máy chủ web được định cấu hình không đúng cách có thể liên quan đến cấu hình, ứng dụng, tệp, tập lệnh hoặc trang web. Kẻ tấn công tìm kiếm các máy chủ web dễ bị tổn thương như vậy để khởi động các cuộc tấn công. Cấu hình sai của máy chủ web cung cấp cho kẻ tấn công một đường dẫn để vào mạng mục tiêu của một tổ chức. Những sơ hở này trong máy chủ cũng có thể giúp kẻ tấn công bỏ qua xác thực người dùng. Sau khi được phát hiện, những sự cố này có thể dễ dàng bị khai thác và có thể dẫn đến sự xâm phạm toàn bộ trang web được lưu trữ trên máy chủ web mục tiêu.

Tấn công phân tách phản hồi HTTP

Tấn công phân tách phản hồi HTTP là một cuộc tấn công dựa trên web, trong đó kẻ tấn công đánh lừa máy chủ bằng cách đưa các dòng mới vào tiêu đề phản hồi, cùng với mã tùy ý. Nó liên quan đến việc thêm dữ liệu phản hồi tiêu đề vào trường đầu vào để máy chủ chia phản hồi thành hai phản hồi. Kiểu tấn công này khai thác các lỗ hổng trong xác thực đầu vào. Tập lệnh chéo trang (XSS), giả mạo yêu cầu giữa các trang (CSRF) và đưa vào Ngôn ngữ truy vấn có cấu trúc (SQL) là những ví dụ về kiểu tấn công này. Trong cuộc tấn công này, kẻ tấn công kiểm soát tham số đầu vào và khéo léo xây dựng một tiêu đề yêu cầu gợi ra hai phản hồi từ máy chủ. Kẻ tấn công thay đổi một yêu cầu để xuất hiện dưới dạng hai yêu cầu bằng cách thêm dữ liệu phản hồi tiêu đề vào trường đầu vào. Đến lượt mình, máy chủ web sẽ đáp ứng từng yêu cầu. Kẻ tấn công có thể chuyển dữ liệu độc hại đến ứng dụng dễ bị tổn thương và ứng dụng bao gồm dữ liệu trong tiêu đề phản hồi HTTP. Kẻ tấn công có thể kiểm soát phản hồi đầu tiên để chuyển hướng người dùng đến một trang web độc hại, trong khi trình duyệt web sẽ loại bỏ các phản hồi khác.

Tấn công nhiễm độc bộ đệm web

Ngộ độc bộ đệm web làm hỏng độ tin cậy của nguồn bộ đệm web trung gian. Trong cuộc tấn công này, kẻ tấn công tráo đổi nội dung được lưu trong bộ nhớ cache để lấy một URL ngẫu nhiên có nội dung bị nhiễm. Người dùng nguồn bộ đệm web có thể vô tình sử dụng nội dung bị nhiễm độc thay vì nội dung thực và được bảo mật khi yêu cầu URL được yêu cầu thông qua bộ đệm web.

Kẻ tấn công buộc bộ đệm của máy chủ web xóa nội dung bộ đệm thực tế của nó và gửi một yêu cầu được chế tạo đặc biệt để lưu trữ trong bộ đệm. Trong trường hợp này, tất cả người dùng của bộ nhớ cache của máy chủ web đó sẽ nhận được nội dung độc hại cho đến khi máy chủ xóa bộ nhớ cache của web. Các cuộc tấn công nhiễm độc bộ đệm web có thể xảy ra nếu máy chủ web và ứng dụng có lỗi phân tách phản hồi HTTP.

Tấn công vũ phu SSH

Những kẻ tấn công sử dụng các giao thức SSH để tạo một đường hầm SSH được mã hóa giữa hai máy chủ để truyền dữ liệu không được mã hóa qua một mạng không an toàn. Thông thường, SSH chạy trên cổng TCP 22. Để thực hiện tấn công SSH, kẻ tấn công quét toàn bộ máy chủ SSH bằng bot (thực hiện quét cổng trên cổng TCP 22) để xác định các lỗ hổng có thể xảy ra. Với sự trợ giúp của một cuộc tấn công vũ phu, kẻ tấn công có được thông tin đăng nhập để có quyền truy cập trái phép vào đường hầm SSH. Kẻ tấn công có được thông tin đăng nhập của SSH có thể sử dụng cùng một đường hầm SSH để truyền phần mềm độc hại và các phương tiện khai thác khác cho nạn nhân mà không bị phát hiện. Những kẻ tấn công sử dụng các công cụ như Nmap và Ncrack trên nền tảng Linux để thực hiện một cuộc tấn công vũ phu SSH.

Bẻ khóa mật khẩu máy chủ web

Kẻ tấn công cố gắng khai thác điểm yếu để hack mật khẩu được lựa chọn tốt. Các mật khẩu phổ biến nhất được tìm thấy là mật khẩu, root, quản trị viên, quản trị viên, demo, kiểm tra, khách, qwerty, tên thú cưng, v.v. Kẻ tấn công chủ yếu nhắm mục tiêu sau thông qua bẻ khóa mật khẩu máy chủ web:

• Máy chủ SMTP và FTP

• Chia sẻ web

■ Đường hầm SSH

Xác thực biểu mẫu web

Những kẻ tấn công sử dụng các phương pháp khác nhau như kỹ thuật xã hội, giả mạo, lừa đảo, ngựa thành Troy hoặc vi rút, nghe lén và ghi nhật ký thao tác bàn phím để thực hiện bẻ khóa mật khẩu máy chủ web. Trong nhiều nỗ lực tấn công, kẻ tấn công bắt đầu bằng việc bẻ khóa mật khẩu để chứng minh với máy chủ web rằng họ là người dùng hợp lệ.

Kỹ thuật bẻ khóa mật khẩu máy chủ web

Bẻ khóa mật khẩu là phương pháp phổ biến nhất để giành quyền truy cập trái phép vào máy chủ web bằng cách khai thác các cơ chế xác thực yếu và thiếu sót. Khi mật khẩu bị bẻ khóa, kẻ tấn công có thể sử dụng mật khẩu để khởi động các cuộc tấn công tiếp theo.

Chúng tôi trình bày một số chi tiết về các công cụ và kỹ thuật khác nhau được những kẻ tấn công sử dụng để bẻ khóa mật khẩu. Kẻ tấn công có thể sử dụng các kỹ thuật bẻ khóa mật khẩu để trích xuất mật khẩu từ máy chủ web, máy chủ FTP, máy chủ SMTP, v.v. Họ có thể bẻ khóa mật khẩu theo cách thủ công hoặc bằng các công cụ tự động như THC Hydra, Ncrack và RainbowCrack.

Sau đây là một số kỹ thuật kẻ tấn công sử dụng để bẻ khóa mật khẩu:

Đoán: Đây là phương pháp bẻ khóa mật khẩu phổ biến nhất. Trong phương pháp này, kẻ tấn công đoán các mật khẩu có thể theo cách thủ công hoặc bằng cách sử dụng các công cụ tự động được cung cấp cùng với từ điển. Hầu hết mọi người có xu hướng sử dụng tên thú cưng, tên người thân, biển số xe, ngày sinh hoặc các mật khẩu yếu khác như "QWERTY", "mật khẩu", "quản trị viên", v.v. để họ có thể nhớ chúng dễ dàng. . Kẻ tấn công khai thác hành vi này của con người để bẻ khóa mật khẩu.

■ Tấn công từ điển: Tấn công từ điển sử dụng một tệp được xác định trước có chứa nhiều tổ hợp từ khác nhau và một chương trình tự động nhập từng từ một để kiểm tra xem có từ nào trong số chúng là mật khẩu hay không. Điều này có thể không hiệu quả nếu mật khẩu bao gồm các ký tự và ký hiệu đặc biệt. Nếu mật khẩu là một từ đơn giản, thì nó có thể được tìm thấy nhanh chóng. So với tấn công brute-force, tấn công từ điển tốn ít thời gian hơn.

■ Tấn công vũ phu: Trong phương pháp vũ phu, tất cả các tổ hợp ký tự có thể có đều được kiểm tra; ví dụ: bài kiểm tra có thể bao gồm tổ hợp các ký tự viết hoa từ A đến Z, các số từ 0 đến 9 và các ký tự viết thường từ a đến z. Phương pháp này rất hữu ích để xác định mật khẩu một từ hoặc hai từ. Nếu mật khẩu bao gồm chữ hoa và chữ thường cũng như các ký tự đặc biệt, có thể mất hàng tháng hoặc hàng năm để bẻ khóa mật khẩu bằng cách sử dụng một cuộc tấn công vũ phu.

■ Tấn công hỗn hợp: Tấn công hỗn hợp mạnh hơn các kỹ thuật trên vì nó sử dụng cả tấn công từ điển và tấn công vũ phu. Nó cũng sử dụng các ký hiệu và số. Bẻ khóa mật khẩu bằng phương pháp này dễ dàng hơn so với các phương pháp trên.

Tấn công giả mạo yêu cầu phía máy chủ (SSRF)

Những kẻ tấn công khai thác các lỗ hổng giả mạo yêu cầu phía máy chủ (SSRF), phát sinh từ việc sử dụng không an toàn các chức năng trong một ứng dụng, trong các máy chủ web công cộng để gửi các yêu cầu được tạo thủ công tới các máy chủ nội bộ hoặc máy chủ phụ trợ. Các máy chủ nội bộ thường được triển khai bằng tường lửa để ngăn mạng khỏi các luồng lưu lượng truy cập không mong muốn. Do đó, những kẻ tấn công tận dụng các lỗ hổng SSRF trong các máy chủ web kết nối Internet để giành quyền truy cập vào các máy chủ phụ trợ được bảo vệ bởi tường lửa. Máy chủ phụ trợ tin rằng yêu cầu được thực hiện bởi máy chủ web vì chúng nằm trên cùng một mạng và phản hồi bằng dữ liệu được lưu trữ trong đó.

Nói chung, các yêu cầu phía máy chủ được bắt đầu để lấy thông tin từ tài nguyên bên ngoài và đưa thông tin đó vào ứng dụng. Chẳng hạn, một nhà thiết kế có thể sử dụng một URL chẳng hạn như https://xyz.com/feed.php?url=externalsite.com/feed/to để lấy nguồn cấp dữ liệu từ xa. Nếu kẻ tấn công có thể thay đổi đầu vào URL thành máy chủ cục bộ, thì chúng có thể xem tất cả tài nguyên cục bộ trên máy chủ. Đây là cách các lỗ hổng SSRF phát triển.

Khi cuộc tấn công được thực hiện thành công, kẻ tấn công có thể thực hiện nhiều hoạt động khác nhau như quét cổng, quét mạng, khám phá địa chỉ IP, đọc tệp máy chủ web, bỏ qua xác thực dựa trên máy chủ, tương tác với các giao thức quan trọng và thực thi mã từ xa.

Tấn công ứng dụng web

Ngay cả khi máy chủ web được định cấu hình an toàn hoặc được bảo mật bằng các biện pháp bảo mật mạng chẳng hạn như tường lửa, ứng dụng web được mã hóa kém được triển khai trên máy chủ web có thể tạo đường dẫn cho kẻ tấn công xâm phạm bảo mật của máy chủ web. Nếu các nhà phát triển web không áp dụng các phương pháp mã hóa an toàn trong khi phát triển các ứng dụng web, thì những kẻ tấn công có thể khai thác các lỗ hổng và xâm phạm các ứng dụng web cũng như bảo mật máy chủ web. Kẻ tấn công có thể thực hiện các kiểu tấn công khác nhau vào các ứng dụng web dễ bị tổn thương để vi phạm bảo mật máy chủ web.

• Giả mạo tham số/biểu mẫu: Trong kiểu tấn công giả mạo này, kẻ tấn công thao túng các tham số được trao đổi giữa máy khách và máy chủ để sửa đổi dữ liệu ứng dụng, chẳng hạn như thông tin đăng nhập và quyền của người dùng cũng như giá cả và số lượng sản phẩm.

• Giả mạo cookie: Các cuộc tấn công giả mạo cookie xảy ra khi một cookie được gửi từ phía máy khách đến máy chủ. Các loại công cụ khác nhau giúp sửa đổi cookie liên tục và không liên tục.

■ Tấn công chèn tệp và đầu vào không hợp lệ: Các cuộc tấn công chèn tệp và đầu vào không hợp lệ được thực hiện bằng cách cung cấp đầu vào không hợp lệ hoặc bằng cách đưa tệp vào ứng dụng web.

• Cướp phiên: Cướp phiên là một cuộc tấn công trong đó kẻ tấn công khai thác, đánh cắp, dự đoán và thương lượng cơ chế kiểm soát phiên web hợp lệ thực sự để truy cập vào các phần được xác thực của ứng dụng web.

■ Tấn công SQL injection: SQL injection khai thác lỗ hổng bảo mật của cơ sở dữ liệu để tấn công. Kẻ tấn công đưa mã độc vào các chuỗi, mã này sau đó được chuyển đến máy chủ SQL để thực thi.

Truyền tải thư mục: Truyền tải thư mục là việc khai thác HTTP thông qua đó kẻ tấn công có thể truy cập các thư mục bị hạn chế và thực thi các lệnh bên ngoài thư mục gốc của máy chủ web bằng cách thao tác với một URL.

• Tấn công Từ chối Dịch vụ (DOS): Một cuộc tấn công DoS nhằm mục đích chấm dứt hoạt động của một trang web hoặc máy chủ khiến người dùng dự định không truy cập được.

• Tấn công Cross-Site Scripting (XSS): Trong phương pháp này, kẻ tấn công đưa các thẻ HTML hoặc tập lệnh vào một trang web mục tiêu.

• Tấn công tràn bộ đệm: Thiết kế của hầu hết các ứng dụng web giúp chúng duy trì một số lượng dữ liệu. Nếu dung lượng đó vượt quá dung lượng lưu trữ khả dụng, ứng dụng có thể gặp sự cố hoặc biểu hiện một số hành vi dễ bị tổn thương khác. Kẻ tấn công sử dụng lợi thế này và làm ngập ứng dụng với lượng dữ liệu dư thừa, gây ra một cuộc tấn công tràn bộ đệm.

• Tấn công giả mạo yêu cầu trên nhiều trang web (CSRF): Kẻ tấn công khai thác lòng tin của người dùng được xác thực để chuyển mã hoặc lệnh độc hại đến máy chủ web.

■Tấn công chèn lệnh: Trong kiểu tấn công này, tin tặc thay đổi nội dung của trang web bằng cách sử dụng mã HTML và bằng cách xác định các trường biểu mẫu thiếu các ràng buộc hợp lệ.

■ Tiết lộ mã nguồn: Tiết lộ mã nguồn là kết quả của lỗi đánh máy trong tập lệnh hoặc cấu hình sai, chẳng hạn như không cấp quyền thực thi cho tập lệnh hoặc thư mục. Tiết lộ mã nguồn đôi khi có thể cho phép kẻ tấn công truy cập thông tin nhạy cảm về thông tin đăng nhập cơ sở dữ liệu và khóa bí mật để xâm phạm máy chủ web.

* 1. Phương pháp tấn công máy chủ Web

Phương pháp tấn công máy chủ web

Phần trước đã mô tả các cuộc tấn công mà kẻ tấn công có thể thực hiện để xâm phạm bảo mật của máy chủ web. Phần này giải thích cách kẻ tấn công tiến tới thực hiện một cuộc tấn công thành công trên máy chủ web. Một cuộc tấn công máy chủ web thường liên quan đến các hoạt động được lên kế hoạch trước được gọi là phương pháp tấn công mà kẻ tấn công tuân theo để đạt được mục tiêu vi phạm bảo mật của máy chủ web mục tiêu.

Những kẻ tấn công hack một máy chủ web trong nhiều giai đoạn. Ở mỗi giai đoạn, kẻ tấn công cố gắng thu thập thông tin về các sơ hở và giành quyền truy cập trái phép vào máy chủ web. Sau đây là các giai đoạn khác nhau của phương pháp tấn công máy chủ web.

Thu thập thông tin

Mọi kẻ tấn công đều cố gắng thu thập càng nhiều thông tin càng tốt về máy chủ web mục tiêu. Kẻ tấn công thu thập thông tin và sau đó phân tích thông tin đó để tìm ra những sai sót trong cơ chế bảo mật hiện tại của máy chủ web.

Thu thập thông tin là bước đầu tiên và là một trong những bước quan trọng nhất để tấn công máy chủ web mục tiêu. Trong bước này, kẻ tấn công thu thập càng nhiều thông tin càng tốt về máy chủ mục tiêu bằng cách sử dụng các công cụ và kỹ thuật khác nhau. Thông tin thu được từ bước này giúp kẻ tấn công đánh giá tình trạng bảo mật của máy chủ web. Những kẻ tấn công có thể tìm kiếm trên Internet, các nhóm tin tức, bảng thông báo, v.v. để thu thập thông tin về tổ chức mục tiêu. Những kẻ tấn công có thể sử dụng các công cụ như Whois.net và Whois Lookup để trích xuất thông tin như tên miền, địa chỉ IP và số hệ thống tự trị của mục tiêu.

Thu thập thông tin từ tệp Robots.txt

Chủ sở hữu trang web tạo tệp robots.txt để liệt kê các tệp hoặc thư mục mà trình thu thập dữ liệu web sẽ lập chỉ mục để cung cấp kết quả tìm kiếm. Các tệp robots.txt được viết kém có thể gây ra việc lập chỉ mục hoàn chỉnh các tệp và thư mục của trang web. Nếu các tệp và thư mục bí mật được lập chỉ mục, kẻ tấn công có thể dễ dàng lấy được thông tin như mật khẩu, địa chỉ email, liên kết ẩn và khu vực thành viên.

Nếu chủ sở hữu của trang web mục tiêu viết tệp robots.txt mà không cho phép lập chỉ mục các trang bị hạn chế để cung cấp kết quả tìm kiếm, kẻ tấn công vẫn có thể xem tệp robots.txt của trang web để khám phá các tệp bị hạn chế và sau đó xem chúng để thu thập thông tin.

Kẻ tấn công nhập URL/robots.txt vào thanh địa chỉ của trình duyệt để xem tệp robots.txt của trang web mục tiêu. Kẻ tấn công cũng có thể tải xuống tệp robots.txt của trang web mục tiêu bằng công cụ Wget.

• Dấu chân Máy chủ Web

Mục đích của dấu chân là thu thập thông tin về các khía cạnh bảo mật của máy chủ web với sự trợ giúp của các công cụ hoặc kỹ thuật dấu chân. Thông qua dấu chân, kẻ tấn công có thể xác định khả năng truy cập từ xa của máy chủ web, các cổng và dịch vụ của nó cũng như các khía cạnh bảo mật khác của nó.

Bằng cách thực hiện dấu chân máy chủ web, kẻ tấn công có thể thu thập dữ liệu cấp hệ thống có giá trị như chi tiết tài khoản, hệ điều hành, phiên bản phần mềm, tên máy chủ và chi tiết lược đồ cơ sở dữ liệu. Tiện ích Telnet có thể được sử dụng để theo dõi máy chủ web và thu thập thông tin như tên máy chủ, loại máy chủ, OSS và các ứng dụng đang chạy. Hơn nữa, các công cụ đánh dấu dấu chân như Netcraft, ID Serve và httprecon có thể được sử dụng để thực hiện dấu chân máy chủ web. Các công cụ dấu chân này có thể trích xuất thông tin từ máy chủ mục tiêu. Ở đây, chúng tôi kiểm tra các tính năng và loại thông tin mà các công cụ này có thể thu thập từ máy chủ mục tiêu.

Phản chiếu trang web

Sao chép trang web là một phương pháp sao chép một trang web và nội dung của nó lên một máy chủ khác để duyệt ngoại tuyến. Với một trang web được nhân đôi, kẻ tấn công có thể xem cấu trúc chi tiết của trang web.

Sao chép trang web sao chép toàn bộ trang web và nội dung của nó vào một ổ đĩa cục bộ. Trang web được nhân đôi tiết lộ hồ sơ đầy đủ về cấu trúc thư mục, cấu trúc tệp, liên kết bên ngoài, hình ảnh, trang web, v.v. của trang web. Với một trang web mục tiêu được nhân đôi, kẻ tấn công có thể dễ dàng lập bản đồ các thư mục của trang web và thu được thông tin có giá trị. Kẻ tấn công sao chép trang web không cần phải trực tuyến để đi qua trang web mục tiêu. Hơn nữa, kẻ tấn công có thể thu được thông tin có giá trị bằng cách tìm kiếm các nhận xét và các mục khác trong mã nguồn HTML của các trang web đã tải xuống. Nhiều công cụ sao chép trang web có thể được sử dụng để sao chép trang web mục tiêu vào ổ đĩa cục bộ; các ví dụ bao gồm NCollector Studio, HTTrack Web Site Copier, WebCopier Pro và Website Ripper Copier.

Quản trị viên hoặc nhân viên bảo mật sử dụng giao diện quản trị để định cấu hình, quản lý và giám sát máy chủ ứng dụng web một cách an toàn. Nhiều giao diện quản trị máy chủ web có thể truy cập công khai và nằm trong thư mục gốc. Thông thường, các thông tin đăng nhập giao diện quản trị này không được định cấu hình đúng cách và vẫn được đặt thành mặc định. Những kẻ tấn công cố gắng xác định giao diện ứng dụng đang chạy của máy chủ web mục tiêu bằng cách thực hiện quét cổng. Khi giao diện quản trị đang chạy được xác định, kẻ tấn công sử dụng các kỹ thuật sau để xác định thông tin đăng nhập mặc định:

• Tham khảo tài liệu giao diện quản trị và xác định mật khẩu mặc định

• Sử dụng cơ sở dữ liệu có sẵn của Metasploit để quét máy chủ

Sử dụng các nguồn trực tuyến như Open Sez Me (http://open-sez.me) và cirt.net (https://cirt.net/passwords) để xác định mật khẩu mặc định

• Cố gắng đoán mật khẩu và tấn công vũ phu

Các thông tin đăng nhập mặc định này có thể cấp quyền truy cập vào giao diện quản trị, làm tổn hại máy chủ web và cho phép kẻ tấn công khai thác ứng dụng web chính.

Tìm nội dung mặc định của máy chủ web

Hầu hết các máy chủ của ứng dụng web đều có nội dung và chức năng mặc định cho phép kẻ tấn công khởi chạy các cuộc tấn công. Sau đây là một số chức năng và nội dung mặc định phổ biến mà kẻ tấn công cố gắng xác định trong máy chủ web.

• Quản trị viên gỡ lỗi và kiểm tra chức năng

Các chức năng được thiết kế cho quản trị viên để gỡ lỗi, chẩn đoán và kiểm tra các ứng dụng web cũng như máy chủ web chứa thông tin cấu hình hữu ích và trạng thái thời gian chạy của cả máy chủ và các ứng dụng đang chạy của nó. Do đó, các chức năng này là mục tiêu chính của những kẻ tấn công.

■ Chức năng mẫu để minh họa các tác vụ thông thường

Nhiều máy chủ chứa các tập lệnh và trang mẫu khác nhau được thiết kế để thể hiện các chức năng nhất định của máy chủ ứng dụng và giao diện lập trình ứng dụng (API). Thông thường, các máy chủ web không thể bảo mật các tập lệnh này khỏi những kẻ tấn công và các tập lệnh mẫu này chứa các lỗ hổng có thể bị kẻ tấn công khai thác hoặc triển khai các chức năng cho phép kẻ tấn công khai thác.

Các chức năng mạnh mẽ có thể truy cập công khai

Một số máy chủ web bao gồm các chức năng mạnh mẽ dành cho nhân viên hành chính và bị hạn chế sử dụng công khai. Tuy nhiên, những kẻ tấn công cố gắng khai thác các chức năng mạnh mẽ như vậy để xâm phạm máy chủ và giành quyền truy cập. Ví dụ: một số máy chủ ứng dụng cho phép triển khai kho lưu trữ web qua cùng một cổng HTTP như cổng được ứng dụng sử dụng. Kẻ tấn công có thể sử dụng các khung khai thác phổ biến như Metasploit để thực hiện quét nhằm xác định mật khẩu mặc định, tải lên các cửa hậu và giành quyền truy cập hệ vỏ lệnh vào máy chủ mục tiêu.

• Hướng dẫn cài đặt máy chủ

Kẻ tấn công cố gắng xác định hướng dẫn sử dụng máy chủ, có thể chứa thông tin hữu ích về cấu hình và cài đặt máy chủ. Truy cập thông tin này cho phép kẻ tấn công chuẩn bị một khung thích hợp để khai thác máy chủ web đã cài đặt.

Tìm danh sách thư mục của máy chủ web

Khi máy chủ web nhận được yêu cầu cho một thư mục, thay vì tệp, máy chủ web sẽ phản hồi yêu cầu theo các cách sau.

• Trả lại tài nguyên mặc định trong thư mục

Máy chủ có thể trả về tài nguyên mặc định trong thư mục, chẳng hạn như index.html.

■ Trả về Lỗi

Máy chủ có thể trả về lỗi, chẳng hạn như mã trạng thái HTTP 403, cho biết rằng yêu cầu không được phép.

• Trả về danh sách nội dung thư mục

Máy chủ có thể trả về một danh sách hiển thị nội dung của thư mục. Một danh sách thư mục mẫu được hiển thị trong ảnh chụp màn hình.

Mặc dù danh sách thư mục không có liên quan đáng kể từ góc độ bảo mật, nhưng đôi khi chúng có các lỗ hổng sau cho phép kẻ tấn công xâm phạm các ứng dụng web:

Kiểm soát truy cập không phù hợp

Vô tình truy cập vào thư mục gốc của máy chủ

Nói chung, sau khi phát hiện ra một thư mục trên máy chủ web, kẻ tấn công đưa ra yêu cầu cho thư mục đó và cố gắng truy cập vào danh sách thư mục. Những kẻ tấn công cũng cố gắng khai thác phần mềm máy chủ web dễ bị tổn thương cấp quyền truy cập vào danh sách thư mục.

• Quét lỗ hổng

Quét lỗ hổng là một phương pháp tìm lỗ hổng và cấu hình sai của máy chủ web. Những kẻ tấn công quét các lỗ hổng với sự trợ giúp của các công cụ tự động được gọi là máy quét lỗ hổng.

Quá trình quét lỗ hổng được thực hiện để xác định các lỗ hổng và cấu hình sai trong máy chủ web hoặc mạng mục tiêu. Quá trình quét lỗ hổng cho thấy các điểm yếu có thể có trong máy chủ mục tiêu để khai thác trong một cuộc tấn công máy chủ web. Trong giai đoạn quét lỗ hổng, kẻ tấn công sử dụng các kỹ thuật đánh hơi để lấy dữ liệu về lưu lượng mạng nhằm xác định các hệ thống, dịch vụ mạng và ứng dụng đang hoạt động. Các công cụ tự động như Acunetix Web Vulnerability Scanner được sử dụng để thực hiện quét lỗ hổng trên máy chủ mục tiêu và tìm máy chủ, dịch vụ cũng như lỗ hổng.

Tìm lỗ hổng có thể khai thác

Các sai sót và lỗi lập trình trong thiết kế phần mềm dẫn đến các lỗ hổng bảo mật. Những kẻ tấn công lợi dụng các lỗ hổng này để thực hiện các cuộc tấn công khác nhau vào tính bảo mật, tính khả dụng hoặc tính toàn vẹn của hệ thống. Các lỗ hổng phần mềm như lỗi lập trình trong chương trình, dịch vụ hoặc trong phần mềm hoặc nhân hệ điều hành có thể bị khai thác để thực thi mã độc.

Nhiều kho lưu trữ lỗ hổng công cộng có sẵn trực tuyến cho phép truy cập thông tin về các lỗ hổng phần mềm khác nhau. Những kẻ tấn công tìm kiếm trên các trang web khai thác như SecurityFocus (https://www.securityfocus.com) và Cơ sở dữ liệu khai thác (https://www.exploit-db.com) để tìm các lỗ hổng có thể khai thác của máy chủ web dựa trên hệ điều hành và ứng dụng phần mềm của nó. Những kẻ tấn công sử dụng thông tin được thu thập trong các giai đoạn trước để tìm các lỗ hổng liên quan bằng cách sử dụng Cơ sở dữ liệu khai thác.

Khai thác những lỗ hổng này cho phép kẻ tấn công thực thi lệnh hoặc mã nhị phân trên máy mục tiêu để có được các đặc quyền cao hơn các đặc quyền hiện có hoặc bỏ qua các cơ chế bảo mật. Những kẻ tấn công sử dụng các lỗ hổng này thậm chí có thể truy cập vào các tài khoản và thông tin xác thực của người dùng đặc quyền.

■ Cướp phiên

Kẻ tấn công có thể thực hiện chiếm quyền điều khiển phiên sau khi xác định được phiên hiện tại của máy khách. Kẻ tấn công kiểm soát hoàn toàn phiên người dùng thông qua chiếm quyền điều khiển phiên.

ID phiên hợp lệ có thể được đánh hơi để có quyền truy cập trái phép vào máy chủ web và rình mò dữ liệu của nó. Kẻ tấn công có thể chiếm quyền điều khiển hoặc đánh cắp nội dung phiên hợp lệ bằng nhiều kỹ thuật khác nhau như dự đoán mã thông báo phiên, phát lại phiên, cố định phiên, tấn công bên cạnh và XSS. Bằng cách sử dụng các kỹ thuật này, kẻ tấn công cố gắng nắm bắt ID và cookie phiên hợp lệ trong các phiên đã thiết lập. Kẻ tấn công sử dụng các công cụ như Burp Suite, Firesheep và JHijack để tự động chiếm quyền điều khiển phiên.

• Hack mật khẩu máy chủ web

Những kẻ tấn công sử dụng các phương pháp bẻ khóa mật khẩu như tấn công vũ phu, tấn công kết hợp và tấn công từ điển để bẻ khóa mật khẩu của máy chủ web.

Trong giai đoạn hack máy chủ web này, kẻ tấn công cố gắng bẻ khóa mật khẩu máy chủ web. Kẻ tấn công có thể sử dụng tất cả các kỹ thuật bẻ khóa mật khẩu có thể để trích xuất mật khẩu, bao gồm đoán mật khẩu, tấn công từ điển, tấn công vũ phu, tấn công kết hợp, băm được tính toán trước, tấn công dựa trên quy tắc, tấn công mạng phân tán và tấn công cầu vồng. Kẻ tấn công cần kiên nhẫn để bẻ khóa mật khẩu vì một số kỹ thuật này rất tẻ nhạt và tốn thời gian. Kẻ tấn công cũng có thể sử dụng các công cụ tự động như Hashcat, THC Hydra và Ncrack để bẻ khóa mật khẩu web và hàm băm.

* 1. Phương pháp tấn công ứng dụng Web

Những kẻ tấn công sử dụng phương pháp hack ứng dụng web để thu thập kiến thức về một ứng dụng web cụ thể để thỏa hiệp thành công. Phương pháp này cho phép họ lập kế hoạch chi tiết từng bước để tăng cơ hội hack thành công ứng dụng. Theo phương pháp này, họ làm như sau để thu thập thông tin chi tiết về các tài nguyên khác nhau cần thiết để chạy hoặc truy cập ứng dụng web:

• Footprint Web Infrastructure

Dấu chân là quá trình thu thập thông tin đầy đủ về một hệ thống và tất cả các thành phần liên quan của nó, cũng như cách chúng hoạt động. Cơ sở hạ tầng web của một ứng dụng web là sự sắp xếp để nó kết nối với các hệ thống, máy chủ khác, v.v. trong mạng. Dấu chân cơ sở hạ tầng web là bước đầu tiên trong việc hack ứng dụng web; nó giúp kẻ tấn công chọn nạn nhân và xác định các ứng dụng web dễ bị tấn công. Những kẻ tấn công dấu vết cơ sở hạ tầng web để biết cách ứng dụng web kết nối với các đồng nghiệp của nó và các công nghệ mà nó sử dụng, đồng thời tìm lỗ hổng trong các phần cụ thể của kiến trúc ứng dụng web. Những lỗ hổng này có thể giúp kẻ tấn công khai thác và giành quyền truy cập trái phép vào ứng dụng web.

Dấu chân cơ sở hạ tầng web cho phép kẻ tấn công tham gia vào các tác vụ sau:

■ Khám phá máy chủ: Những kẻ tấn công cố gắng khám phá các máy chủ vật lý lưu trữ các ứng dụng web, sử dụng các kỹ thuật như tra cứu Whois, thẩm vấn DNS, quét cổng, v.v.

■ Khám phá dịch vụ: Kẻ tấn công có thể khám phá các dịch vụ đang chạy trên máy chủ web để xác định xem chúng có thể sử dụng một số dịch vụ đó làm đường dẫn tấn công để hack ứng dụng web hay không. Quy trình này cũng cung cấp thông tin ứng dụng web chẳng hạn như vị trí lưu trữ, thông tin về các máy đang chạy dịch vụ cũng như việc sử dụng mạng và các giao thức liên quan. Những kẻ tấn công có thể sử dụng các công cụ như Nmap, NetScan Tools Pro và các công cụ khác để tìm các dịch vụ chạy trên các cổng mở và khai thác chúng.

• Nhận dạng máy chủ: Những kẻ tấn công sử dụng tính năng lấy biểu ngữ để lấy biểu ngữ máy chủ, giúp xác định nhãn hiệu và phiên bản của phần mềm máy chủ web. Các thông tin khác mà kỹ thuật này cung cấp bao gồm:

o Local Identity: thông tin như vị trí của máy chủ và Origin-Host.

o Địa chỉ Cục bộ: các địa chỉ IP cục bộ mà máy chủ sử dụng để gửi thông báo Trao đổi Khả năng Đường kính (tin nhắn CER/CEA), bao gồm nhận dạng máy chủ, khả năng và các thông tin khác như số phiên bản giao thức và các ứng dụng Đường kính được hỗ trợ.

Tên bản thân: trường này chỉ định tất cả các lĩnh vực mà máy chủ coi là cục bộ và coi tất cả các yêu cầu được gửi cho chúng là không có yêu cầu lĩnh vực nào.

■ Khám phá nội dung ẩn: Footprinting cũng cho phép kẻ tấn công trích xuất nội dung và

chức năng không được liên kết trực tiếp hoặc có thể truy cập được từ nội dung hiển thị chính.

• Phát hiện bộ cân bằng tải: Kẻ tấn công có thể phát hiện bộ cân bằng tải của tổ chức mục tiêu cùng với địa chỉ IP thực của chúng để xác định các máy chủ bị lộ qua Internet.

Khám phá máy chủ

Để theo dõi cơ sở hạ tầng web, trước tiên, bạn cần khám phá các máy chủ Internet đang hoạt động. Ba kỹ thuật, cụ thể là tra cứu Whois, thẩm vấn DNS và quét cổng, giúp khám phá các máy chủ đang hoạt động và thông tin liên quan của chúng.

• Tra cứu Whois

• Thẩm vấn DNS

• Quét cổng

Quét cổng là quá trình quét các cổng hệ thống để nhận ra các cổng đang mở. Nó cố gắng kết nối với một bộ cổng TCP hoặc UDP cụ thể để tìm ra dịch vụ tồn tại trên máy chủ. Nếu kẻ tấn công nhận ra một cổng mở không được sử dụng, chúng có thể khai thác cổng đó để xâm nhập vào hệ thống.

Khám phá dịch vụ

Dấu chân cơ sở hạ tầng web cung cấp dữ liệu về các dịch vụ được cung cấp, chẳng hạn như trao đổi và mã hóa dữ liệu, đường truyền và các giao thức được triển khai. Quét máy chủ web mục tiêu để xác định các cổng phổ biến mà nó sử dụng cho các dịch vụ khác nhau. Sau khi tìm thấy các dịch vụ này, kẻ tấn công có thể thỏa hiệp chúng để khai thác cơ sở hạ tầng web chạy ứng dụng. Các dịch vụ được xác định đóng vai trò là đường dẫn tấn công để hack ứng dụng web.

Nhận dạng máy chủ/Lấy biểu ngữ

Lấy biểu ngữ là một kỹ thuật dấu chân được tin tặc sử dụng để lấy thông tin nhạy cảm về mục tiêu. Kẻ tấn công thiết lập kết nối với mục tiêu và gửi yêu cầu giả tới mục tiêu. Sau đó, mục tiêu trả lời yêu cầu bằng một thông báo biểu ngữ chứa thông tin nhạy cảm mà kẻ tấn công yêu cầu để thâm nhập sâu hơn vào mục tiêu.

Thông qua việc lấy biểu ngữ, kẻ tấn công xác định tên và/hoặc phiên bản của máy chủ, hệ điều hành hoặc ứng dụng. Họ phân tích trường tiêu đề phản hồi của máy chủ để xác định kiểu dáng, mẫu mã và phiên bản của phần mềm máy chủ web. Thông tin này giúp họ chọn cách khai thác thích hợp từ cơ sở dữ liệu lỗ hổng để tấn công máy chủ web và các ứng dụng của nó.

Phát hiện tường lửa và proxy ứng dụng web trên trang đích

Trong khi theo dõi cơ sở hạ tầng web, kẻ tấn công phải khám phá tường lửa ứng dụng web và cài đặt proxy của trang đích để biết các biện pháp bảo mật được sử dụng.

Khám phá nội dung ẩn

Nội dung và chức năng ẩn không thể truy cập được từ nội dung hiển thị chính có thể được phát hiện để khai thác các đặc quyền của người dùng trong ứng dụng. Điều này cho phép kẻ tấn công khôi phục các bản sao lưu của tệp trực tiếp, tệp cấu hình và tệp nhật ký chứa dữ liệu nhạy cảm, kho lưu trữ sao lưu chứa ảnh chụp nhanh của tệp trong thư mục gốc của web, chức năng mới không được liên kết với ứng dụng chính, v.v.

Phát hiện cân bằng tải

Các tổ chức sử dụng bộ cân bằng tải để phân phối tải máy chủ web của họ trên nhiều máy chủ và do đó tăng năng suất và độ tin cậy của các ứng dụng web. Nói chung, có hai loại bộ cân bằng tải, đó là bộ cân bằng tải DNS (bộ cân bằng tải lớp 4) và bộ cân bằng tải HTTP (bộ cân bằng tải lớp 7). Những kẻ tấn công sử dụng nhiều công cụ khác nhau như đào, bộ phát hiện cân bằng tải (Ibd) và Halberd, để phát hiện bộ cân bằng tải của tổ chức đích cùng với địa chỉ IP thực của chúng. Ví dụ: nếu một máy chủ phân giải thành nhiều địa chỉ IP, thì kẻ tấn công có thể xác định rằng tổ chức đích đang sử dụng bộ cân bằng tải.

• Phân tích các ứng dụng web

Phân tích ứng dụng web

Khi những kẻ tấn công đã cố gắng thực hiện nhiều cuộc tấn công có thể xảy ra khác nhau trên một máy chủ web dễ bị tấn công, chúng có thể chuyển sự chú ý sang chính ứng dụng web đó. Để hack ứng dụng web, trước tiên, họ có thể cần phân tích nó để xác định các khu vực dễ bị tấn công. Ngay cả khi nó chỉ có một lỗ hổng duy nhất, những kẻ tấn công sẽ cố gắng xâm phạm tính bảo mật của nó bằng cách tung ra một cuộc tấn công thích hợp. Phần này mô tả cách kẻ tấn công tìm lỗ hổng trong ứng dụng web và khai thác chúng.

Những kẻ tấn công cần phân tích các ứng dụng web mục tiêu để xác định lỗ hổng của chúng. Làm như vậy giúp họ giảm bớt "bề mặt tấn công". Để phân tích một ứng dụng web, kẻ tấn công có được kiến thức cơ bản về ứng dụng web. Sau đó, họ có thể phân tích chức năng và công nghệ của ứng dụng đang hoạt động để xác định bất kỳ bề mặt tấn công nào bị lộ.

• Xác định điểm vào cho đầu vào của người dùng: Bước đầu tiên trong việc phân tích một ứng dụng web là kiểm tra điểm vào của ứng dụng, điểm này sau này có thể đóng vai trò là cửa ngõ cho các cuộc tấn công. Một trong những điểm vào bao gồm ứng dụng web giao diện người dùng chặn các yêu cầu HTTP. Các điểm nhập ứng dụng web khác là giao diện người dùng do các trang web cung cấp, giao diện dịch vụ do dịch vụ web cung cấp, các thành phần được dịch vụ và các thành phần .NET Remoting.

Những kẻ tấn công nên xem lại yêu cầu HTTP đã tạo để xác định các điểm nhập liệu của người dùng.

• Xác định công nghệ phía máy chủ: Công nghệ phía máy chủ hoặc hệ thống kịch bản phía máy chủ được sử dụng để tạo các trang web động do khách hàng yêu cầu và chúng được lưu trữ nội bộ trên máy chủ. Máy chủ cho phép chạy các trang web hoặc trang web tương tác trên trình duyệt web.

Các công nghệ phía máy chủ thường được sử dụng bao gồm Active Server Pages (ASP), ASP.NET, ColdFusion, JavaServer Pages (JSP), PHP, Python và Ruby on Rails.

Những kẻ tấn công có thể lấy dấu vân tay của các công nghệ đang hoạt động trên máy chủ bằng cách sử dụng các kỹ thuật dấu vân tay khác nhau, chẳng hạn như dấu vân tay HTTP.

• Xác định chức năng phía máy chủ: Chức năng phía máy chủ đề cập đến khả năng máy chủ thực thi các chương trình trên các trang web đầu ra. Yêu cầu của người dùng kích thích các tập lệnh nằm trên máy chủ web để hiển thị các trang web hoặc trang web tương tác. Máy chủ thực thi các tập lệnh phía máy chủ mà người dùng không nhìn thấy được.

Những kẻ tấn công nên đánh giá cấu trúc và chức năng phía máy chủ bằng

quan sát các ứng dụng được tiết lộ cho khách hàng.

• Xác định tệp và thư mục: Máy chủ web lưu trữ các ứng dụng web và cấu hình sai trong khi lưu trữ các ứng dụng web này có thể dẫn đến việc các tệp và thư mục quan trọng bị lộ trên Internet. Những kẻ tấn công xác định các tệp và thư mục của ứng dụng web mục tiêu được hiển thị trên Internet bằng các công cụ tự động khác nhau như Gobuster. Những thông tin như vậy tiếp tục giúp những kẻ tấn công thu thập thông tin nhạy cảm được lưu trữ trong các tệp và thư mục.

• Xác định các lỗ hổng của ứng dụng web: Các ứng dụng web được phát triển bằng nhiều công nghệ và nền tảng khác nhau. Việc không tuân thủ các thực hành mã hóa an toàn trong quá trình phát triển ứng dụng web có thể để lại các lỗ hổng có thể bị khai thác để thực hiện nhiều kiểu tấn công khác nhau.

• Lập bản đồ bề mặt tấn công: Những kẻ tấn công sau đó lập bản đồ bề mặt tấn công của ứng dụng web để nhắm mục tiêu vào các khu vực dễ bị tổn thương cụ thể. Chúng xác định các bề mặt tấn công khác nhau được phát hiện bởi các ứng dụng cũng như các lỗ hổng liên quan đến chúng.

Xác định điểm đầu vào cho đầu vào của người dùng

Các cổng đầu vào của ứng dụng web giúp kẻ tấn công khởi động nhiều kiểu tấn công tiêm chích vào ứng dụng. Nếu các cổng đầu vào như vậy dễ bị tấn công, thì việc truy cập vào ứng dụng rất dễ dàng. Do đó, trong quá trình phân tích ứng dụng web, kẻ tấn công cố gắng xác định các điểm đầu vào cho đầu vào của người dùng để chúng có thể hiểu cách ứng dụng web chấp nhận hoặc xử lý đầu vào của người dùng. Những kẻ tấn công kiểm tra URL, tiêu đề HTTP, tham số chuỗi truy vấn, dữ liệu POST và cookie để xác định tất cả các trường nhập của người dùng. Chúng cũng xác định các tham số tiêu đề HTTP có thể được ứng dụng xử lý làm đầu vào của người dùng, chẳng hạn như Tác nhân người dùng, Người giới thiệu, Chấp nhận, Ngôn ngữ chấp nhận và Máy chủ. Hơn nữa, chúng xác định các kỹ thuật mã hóa URL và các biện pháp mã hóa khác được triển khai để bảo mật lưu lượng truy cập web, chẳng hạn như SSL. Sau đó, họ có thể tìm thấy các lỗ hổng có trong cơ chế nhập liệu và khai thác chúng để giành quyền truy cập vào ứng dụng web.

Lập bản đồ bề mặt tấn công

Sau khi những kẻ tấn công phát hiện các điểm vào, công nghệ phía máy chủ và chức năng, chúng có thể tìm thấy các lỗ hổng tương ứng và lập bản đồ khu vực bề mặt tấn công của ứng dụng web mục tiêu. Do đó, phân tích ứng dụng web giúp kẻ tấn công giảm bề mặt tấn công của chúng.

■ Bỏ qua các điều khiển phía máy khách

Bỏ qua điều khiển phía máy khách

Ứng dụng web yêu cầu các điều khiển phía máy khách để hạn chế đầu vào của người dùng khi truyền dữ liệu qua các thành phần máy khách và triển khai các biện pháp để kiểm soát tương tác của người dùng với máy khách của chính họ. Nhà phát triển sử dụng các kỹ thuật như trường biểu mẫu HTML ẩn và tiện ích mở rộng trình duyệt để cho phép truyền dữ liệu đến máy chủ thông qua máy khách. Thông thường, các nhà phát triển web cho rằng dữ liệu được truyền từ máy khách đến máy chủ nằm trong tầm kiểm soát của người dùng và giả định này có thể khiến ứng dụng dễ bị tấn công.

Một số kỹ thuật để bỏ qua các điều khiển phía máy khách như sau:

• Tấn công các trường biểu mẫu ẩn: Xác định các trường biểu mẫu ẩn trên trang web và thao tác với các thẻ và trường để khai thác trang web trước khi truyền dữ liệu về máy chủ.

• Tấn công tiện ích mở rộng trình duyệt: Cố gắng chặn lưu lượng truy cập từ tiện ích mở rộng trình duyệt hoặc dịch ngược các tiện ích mở rộng trình duyệt để thu thập dữ liệu người dùng.

• Thực hiện đánh giá mã nguồn: Thực hiện đánh giá mã nguồn để xác định các lỗ hổng trong mã mà các công cụ quét lỗ hổng truyền thống không thể xác định được.

Né tránh bộ lọc XSS: Né tránh bộ lọc XSS bằng cách đưa các ký tự bất thường vào mã HTML.

Tấn công các trường biểu mẫu ẩn

Các ứng dụng web thương mại điện tử/bán lẻ sử dụng các trường biểu mẫu HTML ẩn để hạn chế người dùng xem/sửa đổi các trường dữ liệu như "sản phẩm" và "giá sản phẩm" và cho phép người dùng nhập một số trường nhất định như "số lượng", giả sử rằng người dùng nhập số lượng cần thiết trước khi gửi dữ liệu đến máy chủ. Nhà phát triển đánh dấu các trường này là ẩn để hạn chế người dùng sửa đổi chúng. Trong mỗi phiên khách hàng, nhà phát triển sử dụng các trường ẩn để lưu trữ thông tin khách hàng, bao gồm giá sản phẩm và tỷ lệ chiết khấu.

Thực hiện theo quy trình được mô tả bên dưới để tấn công các trường biểu mẫu ẩn:

• Xác định các ứng dụng web có lỗ hổng ■Lưu mã nguồn cho trang HTML

Xác định vị trí trường ẩn

■ Giả mạo giá trị giá bằng cách chỉnh sửa giá trị của trường giá

• Lưu tệp và tải lại nguồn vào trình duyệt

Nhấp vào nút Mua

Yêu cầu sẽ được truyền đến máy chủ với giá đã sửa đổi. Bạn cũng có thể sử dụng các công cụ proxy như Burp Suite để bẫy yêu cầu gửi biểu mẫu và sửa đổi trường giá thành bất kỳ giá trị nào. Ngoài ra, bạn có thể cố gắng nhập các giá trị giá âm để lừa ứng dụng bán lẻ hoàn lại số tiền thông qua giao dịch thẻ tín dụng.

Tấn công tiện ích mở rộng trình duyệt

Dữ liệu từ một ứng dụng web sử dụng các thành phần tiện ích mở rộng của trình duyệt có thể được thu thập bằng hai phương pháp:

• Chặn lưu lượng truy cập từ tiện ích mở rộng trình duyệt

Cố gắng chặn và sửa đổi yêu cầu và phản hồi của thành phần và máy chủ tương ứng. Bạn có thể sử dụng các công cụ như Burp Suite để thu thập dữ liệu. Phương pháp này có một số hạn chế nhất định như làm xáo trộn hoặc mã hóa dữ liệu và tuần tự hóa dữ liệu an toàn.

• Giải mã phần mở rộng trình duyệt

Sử dụng kỹ thuật này, bạn có thể thử dịch ngược mã byte của thành phần để xem nguồn chi tiết của nó, cho phép bạn xác định thông tin chi tiết về chức năng của thành phần. Ưu điểm chính của kỹ thuật này là nó cho phép bạn sửa đổi dữ liệu có trong các yêu cầu được gửi đến máy chủ, bất kể cơ chế che giấu hoặc mã hóa nào được sử dụng cho dữ liệu được truyền đi.

Bạn có thể sử dụng các công cụ proxy như Burp Suite để nắm bắt và sửa đổi các yêu cầu thành phần trang web. Trong trường hợp bỏ qua quy trình xác thực đầu vào phía máy khách được triển khai trong tiện ích mở rộng của trình duyệt, nếu thành phần gửi dữ liệu đã xác thực đến máy chủ một cách minh bạch, thì dữ liệu này có thể được sửa đổi bằng cách sử dụng proxy chặn giống như cách được mô tả cho dữ liệu biểu mẫu HTML .

Thực hiện đánh giá mã nguồn

Cố gắng lấy mã nguồn của ứng dụng web mục tiêu. Sau khi có được mã nguồn, hãy kiểm tra mã để hiểu các thành phần, khung, v.v., cũng như hoạt động của chúng để xác định mọi lỗ hổng hiện có trong mã. Quá trình kiểm tra này có thể cung cấp thông tin về các chức năng khác nhau, chẳng hạn như xóa xác thực đầu vào phía máy khách, gửi dữ liệu không chuẩn tới máy chủ, thao túng trạng thái hoặc sự kiện phía máy khách hoặc gọi trực tiếp chức năng có trong thành phần.

Thực hiện đánh giá mã nguồn để xác định các chức năng sau của thành phần đích:

■ Xác thực đầu vào phía máy khách hoặc các logic và sự kiện liên quan đến bảo mật khác

• Kỹ thuật che giấu hoặc mã hóa được áp dụng cho dữ liệu máy khách trước khi nó được truyền đến máy chủ

■ Các thành phần có thể sửa đổi với các chức năng ẩn phía máy khách • Tham chiếu tới các chức năng phía máy chủ

Né tránh bộ lọc XSS

Việc triển khai bộ lọc XSS được áp dụng cho các trình duyệt web để bảo vệ chúng khỏi các cuộc tấn công XSS sắp xảy ra; tuy nhiên, những kẻ tấn công có thể khiến chúng dễ bị tổn thương bằng cách đưa các ký tự bất thường vào mã HTML, qua đó chúng có thể trốn tránh việc triển khai bộ lọc.

Kẻ tấn công có thể nhúng JavaScript có hại vào ứng dụng web theo nhiều cách. Tuy nhiên, các trình duyệt mới nhất được triển khai với các biện pháp bảo mật mạnh mẽ; do đó, việc tiêm tập lệnh đôi khi không thành công. Do đó, những kẻ tấn công thường cố gắng không chỉ tận dụng các lỗi thiết kế ứng dụng mà còn bỏ qua các quy trình đánh giá đầu vào do máy chủ hoặc ứng dụng thực hiện để đánh lừa các bộ lọc phức tạp của trình duyệt.

Các cuộc tấn công XSS thường khai thác các cấu hình không phù hợp và triển khai bảo mật của trình duyệt, trong khi các phương pháp bỏ qua bộ lọc được thực hiện bằng cách tận dụng các lỗ hổng trong máy chủ hoặc bộ lọc phía trình duyệt, nhắm mục tiêu vào các phiên bản hoặc sản phẩm nhất định.

Phần lớn mã trình duyệt được viết bằng các biện pháp bảo mật phù hợp để xử lý HTML, JavaScript và CSS bất thường nhằm khắc phục chúng trước khi gửi tới người dùng cuối. Bỏ qua bộ lọc XSS tận dụng một thành phần phức tạp của thông số kỹ thuật, ngoại lệ, ngôn ngữ và các đặc điểm khác của trình duyệt để đưa tập lệnh qua bộ lọc mà không để lại dấu vết.

Các kỹ thuật tránh bộ lọc XSS khác nhau được thảo luận dưới đây:

Việc chèn thẻ <script> vào mã không được phép trong ngữ cảnh chung. Tuy nhiên, một số thẻ HTML khác có thể cho phép các nội dung tiêm bất thường này. Trình xử lý sự kiện được sử dụng để chạy các tập lệnh cụ thể tương ứng với các hành động của người dùng được ủy quyền. Nói chung, các trình xử lý sự kiện như <onfocus>, <onerror> và <onclick> có thể được khai thác để tránh các bộ lọc XSS.

• Cơ chế xác thực tấn công

Cơ chế xác thực tấn công

Nói chung, các ứng dụng web xác thực người dùng thông qua các cơ chế xác thực như chức năng đăng nhập. Trong quá trình phân tích ứng dụng web, kẻ tấn công cố gắng tìm các lỗ hổng xác thực như mật khẩu yếu (ví dụ: ngắn hoặc trống, từ hoặc tên phổ biến trong từ điển, tên người dùng, giá trị mặc định). Những kẻ tấn công khai thác các lỗ hổng này để giành quyền truy cập vào ứng dụng web bằng cách nghe trộm mạng, tấn công brute-force, tấn công từ điển, tấn công phát lại cookie, đánh cắp thông tin xác thực, v.v.

Hầu hết các cơ chế xác thực được sử dụng bởi các ứng dụng web đều có lỗi thiết kế. Những kẻ tấn công có thể xác định những lỗ hổng này và khai thác chúng để giành quyền truy cập trái phép vào ứng dụng web. Những lỗi thiết kế như vậy bao gồm việc không kiểm tra độ mạnh của mật khẩu, truyền thông tin xác thực qua Internet không an toàn, v.v. Các ứng dụng web thường xác thực ứng dụng khách hoặc người dùng của họ bằng sự kết hợp giữa tên người dùng và mật khẩu, có thể được xác định và khai thác.

■ Liệt kê tên người dùng

Những kẻ tấn công có thể liệt kê tên người dùng theo hai cách: thông báo lỗi dài dòng và tên người dùng có thể dự đoán được.

。 Thông báo lỗi chi tiết

Trong một hệ thống đăng nhập điển hình, người dùng nhập hai trường, đó là tên người dùng và mật khẩu. Trong một số trường hợp, một ứng dụng sẽ yêu cầu thông tin bổ sung. Nếu người dùng đang cố đăng nhập và không thành công, điều đó có nghĩa là ít nhất một trường không chính xác. Điều này tạo cơ sở cho kẻ tấn công khai thác ứng dụng.

Ví dụ:

• Không tìm thấy tài khoản <tên người dùng>

• Mật khẩu được cung cấp không chính xác

• Tài khoản <tên người dùng> đã bị khóa

• Tên người dùng có thể đoán trước

Một số ứng dụng tự động tạo tên người dùng tài khoản theo một số trình tự có thể dự đoán được. Điều này giúp kẻ tấn công dễ dàng nhận ra trình tự cho một danh sách có khả năng đầy đủ tất cả các tên người dùng hợp lệ.

■ Tấn công mật khẩu

Tấn công mật khẩu là một quá trình thử các kỹ thuật bẻ khóa mật khẩu khác nhau để khám phá mật khẩu tài khoản người dùng mà nhờ đó kẻ tấn công có thể truy cập vào một ứng dụng.

Các phương pháp bẻ khóa mật khẩu bao gồm:

o Khai thác chức năng mật khẩu

o Đoán mật khẩu

o Tấn công vũ phu

o Tấn công từ điển

o Tấn công cơ chế reset mật khẩu

■ Phiên tấn công

Những kiểu tấn công phiên sau đây được kẻ tấn công sử dụng để chống lại các cơ chế xác thực:

o Dự đoán phiên: Nó tập trung vào việc dự đoán các giá trị ID phiên cho phép kẻ tấn công

để bỏ qua cơ chế xác thực của một ứng dụng. Bằng cách phân tích và

hiểu quy trình tạo ID phiên, kẻ tấn công có thể dự đoán giá trị ID phiên hợp lệ và giành quyền truy cập vào ứng dụng. o Session brute-forcing: Kẻ tấn công brute-force ID phiên của người dùng mục tiêu và

sử dụng nó để đăng nhập với tư cách là người dùng hợp pháp và có quyền truy cập vào ứng dụng.

o Đầu độc phiên: Nó cho phép kẻ tấn công đưa vào nội dung độc hại, sửa đổi trải nghiệm trực tuyến của người dùng và lấy thông tin trái phép.

■ Khai thác cookie

Các cuộc tấn công khai thác cookie có các loại sau:

o Ngộ độc cookie: Đây là một kiểu tấn công giả mạo tham số trong đó kẻ tấn công sửa đổi nội dung cookie để lấy thông tin trái phép về người dùng và do đó thực hiện hành vi trộm cắp danh tính.

Đánh hơi cookie: Đây là một kỹ thuật trong đó kẻ tấn công đánh hơi cookie chứa ID phiên của nạn nhân đã đăng nhập vào trang web mục tiêu và sử dụng cookie để bỏ qua quy trình xác thực và đăng nhập vào tài khoản của nạn nhân.

o Phát lại cookie: Đây là một kỹ thuật được sử dụng để mạo danh người dùng hợp pháp bằng cách phát lại phiên/cookie chứa ID phiên của người dùng đó (miễn là người đó vẫn đăng nhập). Cuộc tấn công này ngừng hoạt động sau khi người dùng đăng xuất khỏi phiên.

Bỏ qua xác thực

Bỏ qua SSO dựa trên SAML: Kẻ tấn công lợi dụng cấu hình sai chữ ký, thời gian chờ hết hạn của phiên, phát lại phiên, gửi sai thông báo SAML, v.v., để vượt qua xác thực SSO dựa trên SAML.

Lỗi thiết kế trong cơ chế xác thực

Các cơ chế xác thực dễ bị tấn công hơn so với các triển khai khác liên quan đến bảo mật ứng dụng web. Các ứng dụng thường xác thực người dùng thông qua thông tin đăng nhập của họ; ngay cả một điểm yếu nhỏ trong quá trình xác thực này cũng có thể dẫn đến hậu quả nghiêm trọng như cấp quyền truy cập cho người dùng bất hợp pháp.

Mật khẩu không hợp lệ: Bất kỳ ứng dụng nào cũng được thiết kế để có quyền kiểm soát tối thiểu đối với việc kiểm tra và xác thực thông tin đăng nhập của người dùng. Người dùng thường bắt gặp các ứng dụng chấp nhận mật khẩu như giá trị trống hoặc ngắn, tên thông thường, từ trong từ điển, cùng mật khẩu với tên người dùng và tham số mặc định. Những kẻ tấn công có thể dễ dàng đoán ra những mật khẩu như vậy, cho phép chúng truy cập vào tài nguyên ứng dụng.

• Đăng nhập Brute-Forcible: Tính năng đăng nhập của ứng dụng cho phép kẻ tấn công dự đoán thông tin đăng nhập của người dùng, qua đó kẻ tấn công có thể vào ứng dụng một cách bất hợp pháp. Nếu ứng dụng cho phép nhiều lần thử đăng nhập mà không có bất kỳ hạn chế nào, chẳng hạn như chặn tài khoản sau một số lần thử nhất định, kẻ tấn công có thể tiếp tục thử các mật khẩu khác nhau cho đến khi tìm được mật khẩu phù hợp. Do đó, ngay cả một hacker không chuyên nghiệp cũng có thể đăng nhập bằng cách nhập các tổ hợp mật khẩu khác nhau theo cách thủ công.

• Thông báo lỗi dài dòng: Bất kỳ biểu mẫu đăng nhập nào của ứng dụng đều yêu cầu người dùng cung cấp ít nhất hai trường, đó là tên người dùng và mật khẩu. Một số ứng dụng cũng có thể yêu cầu các tham số bổ sung như DOB, câu trả lời cho câu hỏi bảo mật và mã pin OTP để xác thực người dùng. Nếu nỗ lực đăng nhập không thành công, ứng dụng sẽ chỉ ra rằng thông tin được cung cấp không hợp lệ. Khi ứng dụng chỉ định trường nào không chính xác hoặc đưa ra lý do từ chối truy cập, kẻ tấn công có thể dễ dàng khai thác trường đó bằng cách thử một tập hợp lớn các tên hoặc từ tương tự để liệt kê dữ liệu hợp lệ cần thiết để truy cập ứng dụng. Danh sách dữ liệu được liệt kê cũng có thể được sử dụng sau này cho kỹ thuật xã hội.

Truyền thông tin xác thực không an toàn: Nếu một ứng dụng tạo kết nối HTTP không an toàn để truyền thông tin nhạy cảm, ứng dụng đó sẽ dễ bị tấn công MITM, qua đó kẻ tấn công có thể nghe trộm và cản trở việc truyền dữ liệu. Ngay cả khi kết nối HTTPS đã được tạo, kẻ tấn công vẫn có thể đánh cắp thông tin đăng nhập nếu ứng dụng xử lý thông tin đăng nhập theo cách không an toàn, chẳng hạn như chuyển thông tin dưới dạng tham số chuỗi truy vấn và lưu trữ thông tin đăng nhập trong cookie.

• Cơ chế đặt lại mật khẩu: Trong hầu hết các ứng dụng, cơ chế đặt lại mật khẩu là bắt buộc và được áp dụng định kỳ để giảm nguy cơ bị xâm phạm mật khẩu. Hơn nữa, khi người dùng nhận thấy thông tin đăng nhập của họ bị lạm dụng, họ có thể thay đổi mật khẩu ngay lập tức để ngăn chặn việc sử dụng bất hợp pháp. Đôi khi, tính năng đặt lại mật khẩu này cũng có thể bị khai thác. Các lỗ hổng bị bỏ qua trong chức năng đăng nhập chính có thể xuất hiện lại trong cơ chế đặt lại mật khẩu. Một số sai sót trong cơ chế đặt lại mật khẩu như sau:

o Tạo lỗi dài dòng, chỉ định nếu tên người dùng hợp lệ

o Cho phép đoán trường "Mật khẩu hiện tại" mà không có bất kỳ hạn chế nào

o Kiểm tra xem các trường "Mật khẩu mới" và "Xác nhận mật khẩu" chỉ bao gồm các giá trị giống nhau sau khi xác thực mật khẩu hiện có, do đó cho phép một cuộc tấn công thành công trong việc xác định rõ ràng mật khẩu hiện có

Cơ chế quên mật khẩu: Cũng như cơ chế thay đổi mật khẩu, các phương pháp khôi phục mật khẩu đã quên thường kéo theo các vấn đề thường bị bỏ qua trong chức năng đăng nhập chính, chẳng hạn như liệt kê tên người dùng. Ngoài ra, một số lỗi thiết kế trong cơ chế quên mật khẩu thường khiến nó dễ bị tấn công hơn, qua đó logic xác thực tổng thể của một ứng dụng được nhắm mục tiêu. Một số sai sót trong cơ chế quên mật khẩu như sau:

o Cung cấp thử thách phụ khi người dùng quên mật khẩu

o Các nhà phát triển thường bỏ qua khả năng ứng dụng bị cưỡng bức trong quá trình khôi phục mật khẩu. Nếu ứng dụng cho phép bất kỳ số lần thử khôi phục mật khẩu nào, thì rất có khả năng mật khẩu sẽ được khôi phục bằng cách đoán các câu trả lời ngẫu nhiên liên quan đến người dùng

Chức năng "Ghi nhớ tôi": Các ứng dụng cũng cung cấp chức năng "Ghi nhớ tôi" để thuận tiện tránh nhập lại tên người dùng và mật khẩu khi người dùng cố gắng đăng nhập nhiều lần vào một ứng dụng từ thiết bị của họ. Cơ chế này thường dễ bị tấn công vì người dùng có thể bị tấn công từ cả máy tính cục bộ và người dùng trên các máy khác. Các chức năng "Ghi nhớ tôi" được thực thi bằng một số cookie liên tục. Khi những cookie này được bắt đầu, ứng dụng sẽ tin tưởng chúng vì chúng đã được lưu trữ trong phiên trước đó và tạo một phiên mới mà không yêu cầu lại thông tin đăng nhập. Kẻ tấn công có thể thử danh sách các từ thông thường hoặc tên người dùng được liệt kê để có quyền truy cập đầy đủ vào ứng dụng mà không cần xác thực.

■ Mạo danh người dùng: Một số người dùng đặc quyền truy cập ứng dụng bằng thông tin đăng nhập của người dùng khác để hỗ trợ người dùng ban đầu thực hiện các thao tác của họ. Chẳng hạn, nếu kết nối Internet bị hỏng, người dùng sẽ liên hệ với nhà cung cấp dịch vụ để nhờ tư vấn. Sau đó, nhân viên chăm sóc khách hàng đăng nhập bằng dữ liệu người dùng vào hệ thống của họ và hỗ trợ người dùng giải quyết sự cố ngừng dịch vụ. Nếu một ứng dụng cho phép người dùng có đặc quyền mạo danh người khác, thì bất kỳ lỗi nào trong logic mạo danh đều có thể dẫn đến leo thang đặc quyền theo chiều dọc, mặc dù kẻ tấn công có thể có toàn quyền truy cập vào ứng dụng.

• Xác thực thông tin xác thực không đúng cách: Các ứng dụng được thiết kế với các cơ chế xác thực phù hợp như chấp nhận mật khẩu có độ dài tối thiểu và cho phép phân biệt chữ hoa chữ thường (chữ hoa và chữ thường), số và ký tự đặc biệt. Ngược lại, cơ chế xác thực của ứng dụng được thiết kế kém không chỉ bỏ qua việc triển khai bảo mật tốt mà còn không xem xét nỗ lực của người dùng để áp dụng các ký tự mật khẩu mạnh.

Chẳng hạn, một số ứng dụng rút ngắn mật khẩu và chỉ đánh giá một vài ký tự đầu tiên. Một vài ứng dụng kiểm tra mật khẩu không phân biệt chữ hoa chữ thường và những ứng dụng khác thực hiện tách ký tự bất thường trước khi kiểm tra mật khẩu. Những kẻ tấn công có thể thực hiện các cuộc tấn công đoán mật khẩu tự động trên các ứng dụng như vậy để loại bỏ các trường hợp thử nghiệm không mong muốn và rút ngắn số lượng yêu cầu cần thiết để xâm phạm tài khoản.

• Tên người dùng và mật khẩu có thể đoán trước: Một vài ứng dụng tự động tạo tên người dùng dựa trên một chuỗi có thể đoán trước. Những kẻ tấn công khai thác đặc điểm này của một ứng dụng và ngay lập tức có được danh sách tên người dùng hợp lệ, qua đó chúng có thể thực hiện các cuộc tấn công tiếp theo.

Đôi khi, danh sách người dùng được tạo cùng một lúc hoặc ở dạng nhóm và tất cả mật khẩu ban đầu của những người dùng này được phân phối qua một số nguồn. Các nguồn để tạo mật khẩu có thể cho phép kẻ tấn công đoán mật khẩu của người dùng. Các lỗ hổng như vậy thường được kích hoạt trong môi trường mạng nội bộ.

Phân phối thông tin xác thực không an toàn: Hầu hết các ứng dụng đều áp dụng quy trình trong đó thông tin xác thực đăng nhập được cung cấp qua SMS, email, bài đăng, v.v. code" để thay đổi mật khẩu do hệ thống tạo hoặc tạo ban đầu. Nếu một loạt các URL như vậy được gửi tới cùng một người dùng, kẻ tấn công có thể phát hiện ra hoạt động này bằng cách đăng ký nhiều tài khoản người dùng và suy ra mã kích hoạt được gửi qua URL tới người dùng mới đăng ký và chưa đăng ký.

Lỗ hổng triển khai trong cơ chế xác thực

Đôi khi, các cơ chế bảo mật ứng dụng được thiết kế cẩn thận sẽ mở ra cánh cổng cho các cuộc tấn công do một số lỗi trong quá trình thực thi. Những sai lầm này có thể dẫn đến rò rỉ thông tin, bỏ qua bảo mật đăng nhập hoặc giảm toàn bộ mô-đun bảo mật. Các lỗi triển khai trong xác thực nguy hiểm hơn vì chúng không thể được phát hiện bằng các phương pháp kiểm tra thông thường. Một số lỗi triển khai trong cơ chế xác thực như sau:

■ Cơ chế đăng nhập khi mở không thành công: Đây là lỗi logic dẫn đến hậu quả nghiêm trọng trong quá trình xác thực. Chẳng hạn, việc gọi db.getUser() có thể kích hoạt một số ngoại lệ, chẳng hạn như ngoại lệ con trỏ null, vì hàm được yêu cầu không có thông tin đăng nhập tên người dùng hoặc mật khẩu nhưng nó vẫn có thể đăng nhập. Phiên này có thể phụ thuộc vào danh tính người dùng cụ thể; do đó, ngay cả khi nó không hoạt động đầy đủ, nó vẫn có thể cho phép kẻ tấn công truy cập thông tin hoặc chức năng quan trọng.

Tên người dùng liệt kê

Nguồn: https://wordpress.com

Nếu lỗi đăng nhập cho biết tên người dùng hoặc mật khẩu nào không chính xác, trường đó có thể được đoán bằng phương pháp thử và sai.

Hãy xem xét ví dụ sau. Kẻ tấn công cố gắng liệt kê tên người dùng và mật khẩu của "Rini Matthews" trên wordpress.com. Trong lần thử đầu tiên, kẻ tấn công cố gắng đăng nhập với tên "rini.matthews", dẫn đến thông báo lỗi đăng nhập "email hoặc tên người dùng không hợp lệ".

Tấn công mật khẩu: Đoán mật khẩu

Đúng như tên gọi của nó, đoán mật khẩu là quá trình đoán các từ khóa có thể có của người dùng có thể tạo thành mật khẩu tài khoản cho đến khi tìm được mật khẩu chính xác. Để đoán mật khẩu, kẻ tấn công sử dụng các kỹ thuật như danh sách mật khẩu và từ điển mật khẩu.

Tấn công mật khẩu: Brute-force

Brute-forcing là một phương pháp khác được sử dụng để bẻ khóa mật khẩu. Việc đoán trở nên quan trọng khi mật khẩu dài hoặc chứa các chữ cái viết hoa và viết thường. Nếu số và ký hiệu được sử dụng, có thể mất vài năm để đoán mật khẩu, điều này là không thực tế.

Cố gắng bẻ khóa mật khẩu bằng cách thử tất cả các giá trị có thể có từ một tập hợp các ký tự chữ cái, số và ký tự đặc biệt. Sử dụng các công cụ bẻ khóa mật khẩu như Burp Suite để bẻ khóa mật khẩu.

Tấn công mật khẩu: Cơ chế thiết lập lại mật khẩu tấn công

Thực hành quản lý mật khẩu không an toàn dẫn đến các lỗ hổng bảo mật nghiêm trọng. Một lỗ hổng như vậy là đầu độc đặt lại mật khẩu được kẻ tấn công khai thác để tận dụng các tiêu đề như Máy chủ trong thông báo yêu cầu HTTP.

Đặt lại mật khẩu là chức năng thường được người dùng sử dụng khi quên mật khẩu và cần đặt lại mật khẩu. Người dùng nhận được liên kết quên mật khẩu qua email có chứa mã thông báo một lần và khi nhấp vào liên kết, máy chủ sẽ phản hồi bằng trang đặt lại mật khẩu.

Khai thác cookie: Đầu độc cookie

Cookie thường xuyên truyền thông tin xác thực nhạy cảm từ trình duyệt máy khách đến máy chủ.

Những kẻ tấn công có thể sửa đổi chúng một cách dễ dàng để giành quyền truy cập vào máy chủ hoặc giả định danh tính của

người dùng khác.

Trình duyệt máy khách sử dụng cookie để duy trì trạng thái phiên khi chúng sử dụng ID giao thức HTTP không trạng thái để liên lạc. Máy chủ liên kết các phiên duy nhất với cá nhân truy cập ứng dụng web. Việc đầu độc cookie và thông tin phiên có thể cho phép kẻ tấn công chèn nội dung độc hại hoặc sửa đổi trải nghiệm trực tuyến của người dùng và lấy thông tin trái phép.

Cookie có thể chứa dữ liệu phiên cụ thể như ID người dùng, mật khẩu, số tài khoản, liên kết đến nội dung giỏ hàng, thông tin cá nhân được cung cấp và ID phiên. Chúng tồn tại dưới dạng các tệp được lưu trữ trong bộ nhớ của máy tính khách hoặc trên đĩa cứng của nó. Bằng cách sửa đổi dữ liệu cookie, kẻ tấn công thường có thể giành được quyền truy cập cấp cao hoặc ảnh hưởng xấu đến phiên của người dùng. Nhiều trang web cung cấp tính năng "Nhớ tôi?" chức năng và lưu trữ thông tin người dùng trong cookie để người dùng không phải nhập lại dữ liệu sau mỗi lần truy cập trang web. Mọi thông tin cá nhân đã nhập sẽ được lưu trữ trong cookie. Để bảo vệ cookie, các nhà phát triển trang web thường mã hóa chúng. Cookie được mã hóa mang đến cho nhà phát triển cảm giác sai lầm về bảo mật cookie, vì quá trình mã hóa có thể dễ dàng bị đảo ngược bằng các phương pháp giải mã như Base64 và ROT13 (xoay vòng các chữ cái trong bảng chữ cái qua 13 ký tự).

Bỏ qua xác thực: Bỏ qua SSO dựa trên SAML

Sử dụng SAML Raider

• Kế hoạch ủy quyền tấn công

Kế hoạch ủy quyền tấn công

Tấn công ủy quyền

Tấn công ủy quyền: Giả mạo tham số cookie

■ Kiểm soát truy cập tấn công

Kiểm soát truy cập là một phần của cơ chế bảo mật của ứng dụng dựa trên logic xác thực và quản lý phiên. Kẻ tấn công đi qua một trang web để xác định các chi tiết kiểm soát truy cập sau đây của ứng dụng:

•Quyền truy cập cá nhân vào một tập hợp con cụ thể của dữ liệu

• Cấp độ tiếp cận trợ cấp (nhân viên, quản lý, giám sát viên, CEO, v.v.)

• Chức năng quản trị viên để cấu hình và giám sát

■Các chức năng cho phép tăng đặc quyền

• Cơ chế quản lý phiên tấn công

Quản lý phiên ứng dụng web liên quan đến việc trao đổi thông tin nhạy cảm giữa máy chủ và máy khách của nó bất cứ khi nào cần thiết. Nếu việc quản lý phiên như vậy không an toàn, kẻ tấn công có thể lợi dụng nó để tấn công ứng dụng web thông qua cơ chế quản lý phiên, đây là thành phần bảo mật chính trong hầu hết các ứng dụng web.

Ngày nay, hầu hết những kẻ tấn công nhắm mục tiêu quản lý phiên ứng dụng để khởi chạy các cuộc tấn công độc hại vào các ứng dụng web, cho phép chúng dễ dàng vượt qua các biện pháp kiểm soát xác thực mạnh mẽ và giả dạng người dùng khác mà không cần biết thông tin xác thực (tên người dùng, mật khẩu) của họ. Kẻ tấn công thậm chí có thể kiểm soát toàn bộ ứng dụng bằng cách xâm phạm tài khoản của quản trị viên hệ thống.

• Thực hiện các cuộc tấn công tiêm chích

Tấn công injection rất phổ biến trong các ứng dụng web. Chúng khai thác cơ chế xác thực đầu vào dễ bị tổn thương do ứng dụng web triển khai. Có nhiều kiểu tấn công tiêm chích, chẳng hạn như tiêm tập lệnh web, tiêm lệnh OS, tiêm SMTP, tiêm LDAP và tiêm XPath. Một cuộc tấn công thường xảy ra khác là tấn công SQL injection.

Quá trình chèn thường diễn ra khi trình duyệt gửi dữ liệu do người dùng cung cấp tới trình thông dịch như một phần của lệnh hoặc truy vấn. Để khởi động một cuộc tấn công tiêm chích, những kẻ tấn công cung cấp dữ liệu được tạo thủ công để đánh lừa trình thông dịch thực hiện các lệnh hoặc truy vấn ngoài ý muốn. Do những lỗi tiêm nhiễm này, kẻ tấn công có thể dễ dàng đọc, tạo, cập nhật và xóa bất kỳ dữ liệu tùy ý nào có sẵn cho ứng dụng. Trong một số trường hợp, kẻ tấn công thậm chí có thể bỏ qua môi trường tường lửa được lồng sâu và kiểm soát hoàn toàn ứng dụng cũng như hệ thống cơ bản của nó.

■ Tấn công các lỗi logic của ứng dụng

Trong tất cả các ứng dụng web, một lượng lớn logic được áp dụng ở mọi cấp độ. Việc thực hiện một số logic có thể dễ bị tấn công bởi các cuộc tấn công khác nhau sẽ không được chú ý. Hầu hết những kẻ tấn công chủ yếu tập trung vào các cuộc tấn công cấp cao như SQL Injection và XSS scripting vì chúng có chữ ký dễ nhận biết. Ngược lại, các lỗi logic ứng dụng không liên quan đến bất kỳ chữ ký chung nào, khiến các lỗi logic ứng dụng khó xác định hơn. Việc kiểm tra thủ công các trình quét lỗ hổng không thể xác định loại lỗ hổng này, điều này cho phép kẻ tấn công khai thác các lỗ hổng đó để gây ra thiệt hại nghiêm trọng cho các ứng dụng web.

Hầu hết các lỗi ứng dụng phát sinh từ sơ suất và giả định sai của các nhà phát triển. Các lỗi logic ứng dụng khác nhau giữa các loại ứng dụng web khác nhau và không bị giới hạn ở một lỗ hổng cụ thể. Thu thập kiến thức về các ứng dụng đã khai thác trước đó với các lỗi logic phổ biến có thể cung cấp thông tin thích hợp về cách tiếp cận khai thác các lỗ hổng trong logic ứng dụng.

■ Tấn công môi trường chia sẻ

Ngày nay, các tổ chức tận dụng các nhà cung cấp dịch vụ bên thứ ba để lưu trữ và duy trì các ứng dụng web cũng như cơ sở hạ tầng web có liên quan của họ. Các nhà cung cấp dịch vụ này cung cấp dịch vụ cho nhiều khách hàng và lưu trữ song song các ứng dụng web của họ bằng cách sử dụng cùng một cơ sở hạ tầng. Cách tiếp cận này dẫn đến nhiều mối đe dọa và tấn công vào các ứng dụng web. Ví dụ: ứng dụng khách độc hại của nhà cung cấp dịch vụ có thể cố gắng xâm phạm tính bảo mật của ứng dụng web của tổ chức khác hoặc ứng dụng khách có thể triển khai ứng dụng web dễ bị tổn thương mở đường cho việc xâm phạm ứng dụng web của các tổ chức khác.

■ Tấn công kết nối cơ sở dữ liệu

Chuỗi kết nối cơ sở dữ liệu được sử dụng để kết nối các ứng dụng với công cụ cơ sở dữ liệu. Trong các cuộc tấn công này, kẻ tấn công nhắm mục tiêu kết nối cơ sở dữ liệu tạo thành liên kết giữa máy chủ cơ sở dữ liệu và phần mềm máy khách của nó. Ứng dụng web thiết lập kết nối với cơ sở dữ liệu bằng cách cung cấp trình điều khiển với chuỗi kết nối chứa địa chỉ của cơ sở dữ liệu hoặc máy chủ cụ thể và cung cấp thông tin xác thực người dùng và phiên bản.

• Tấn công máy khách ứng dụng web

Các cuộc tấn công được thực hiện trên ứng dụng phía máy chủ sẽ lây nhiễm sang ứng dụng phía máy khách khi ứng dụng này tương tác với máy chủ độc hại hoặc xử lý dữ liệu độc hại. Tấn công phía máy khách xảy ra khi máy khách thiết lập kết nối với máy chủ. Nếu không có kết nối giữa máy khách và máy chủ thì sẽ không có rủi ro vì máy chủ không thể truyền dữ liệu độc hại cho máy khách.

Hãy xem xét một cuộc tấn công phía máy khách trong đó một trang web bị nhiễm nhắm vào một điểm yếu cụ thể của trình duyệt và khai thác thành công điểm yếu đó. Do đó, máy chủ độc hại giành quyền kiểm soát trái phép hệ thống máy khách. Những kẻ tấn công tương tác với các ứng dụng phía máy chủ theo những cách không mong muốn để thực hiện các hành động nguy hiểm đối với người dùng cuối và truy cập dữ liệu trái phép.

Tấn công các dịch vụ web

Các ứng dụng web thường sử dụng các dịch vụ web để thực hiện một chức năng cụ thể. Nếu các dịch vụ web được tích hợp trong các ứng dụng web dễ bị tấn công, thì bản thân các ứng dụng đó cũng trở nên dễ bị tổn thương, cho phép kẻ tấn công khai thác các ứng dụng đó thông qua các dịch vụ web dễ bị tấn công được tích hợp. Do đó, những kẻ tấn công dễ dàng nhắm mục tiêu các dịch vụ web. Do đó, các dịch vụ web bị xâm nhập là một mối đe dọa bảo mật nghiêm trọng.

Các dịch vụ web hoạt động trên các ứng dụng web cũ và bất kỳ cuộc tấn công nào vào dịch vụ web sẽ ngay lập tức làm lộ các lỗ hổng logic và nghiệp vụ của ứng dụng cơ bản cho các cuộc tấn công khác nhau. Những kẻ tấn công có thể nhắm mục tiêu các dịch vụ web bằng nhiều kỹ thuật khác nhau, vì các ứng dụng web cung cấp các dịch vụ này cho người dùng thông qua các cơ chế khác nhau. Do đó, khả năng lỗ hổng tăng lên. Những kẻ tấn công khai thác các lỗ hổng này để thỏa hiệp các dịch vụ web. Có nhiều lý do khiến kẻ tấn công nhắm mục tiêu vào các dịch vụ web. Những kẻ tấn công chọn một cuộc tấn công thích hợp tùy thuộc vào mục đích của cuộc tấn công. Nếu những kẻ tấn công chỉ muốn ngăn một dịch vụ web phục vụ những người dùng đã định, thì chúng có thể khởi động một cuộc tấn công DoS bằng cách gửi nhiều yêu cầu.

Nếu tin tặc không sử dụng quy trình này và cố gắng khai thác trực tiếp ứng dụng web, khả năng thất bại của chúng sẽ tăng lên. Các giai đoạn sau của mô-đun này sẽ cung cấp giải thích chi tiết về cách kẻ tấn công lấy thông tin về các tài nguyên này.

* 1. Giải pháp phòng chống
     1. Phòng chống tấn công máy chủ web

Biện pháp đối phó: Bản vá lỗi và cập nhật

Sau đây là các biện pháp đối phó khác nhau để quản lý bản vá và cập nhật an toàn cho máy chủ web.

• Quét các lỗ hổng hiện có; vá và cập nhật phần mềm máy chủ thường xuyên.

• Trước khi áp dụng bất kỳ gói dịch vụ, hotfix hoặc bản vá bảo mật nào, hãy đọc và xem xét ngang hàng tất cả các tài liệu liên quan.

■ Áp dụng tất cả các bản cập nhật, bất kể loại của chúng, trên cơ sở "khi cần thiết".

• Thử nghiệm các gói dịch vụ và hotfix trên môi trường phi sản xuất đại diện trước khi triển khai trong sản xuất.

Đảm bảo rằng các gói dịch vụ, hotfix và các mức độ vá lỗi bảo mật nhất quán trên tất cả các bộ điều khiển miền (DC).

Đảm bảo rằng việc ngừng hoạt động của máy chủ đã được lên lịch và có sẵn một bộ đầy đủ các băng sao lưu và đĩa sửa chữa khẩn cấp.

Giữ một kế hoạch dự phòng cho phép hệ thống và doanh nghiệp trở lại trạng thái ban đầu trước khi triển khai không thành công.

Lên lịch nâng cấp gói dịch vụ định kỳ như một phần của quá trình bảo trì vận hành và không bao giờ theo dõi quá hai gói dịch vụ.

• Tắt tất cả ánh xạ phần mở rộng tập lệnh không sử dụng.

• Tránh sử dụng các cấu hình mặc định mà máy chủ web được gửi kèm theo.

Sử dụng các bản vá ảo trong tổ chức vì chúng cung cấp khả năng nhận dạng/ghi nhật ký bổ sung.

• Thiết lập một kế hoạch khắc phục thảm họa để xử lý các lỗi quản lý bản vá.

Biện pháp đối phó: Giao thức và Tài khoản

Biện pháp đối phó: Giao thức

Sau đây là các biện pháp đối phó khác nhau để sử dụng các giao thức bảo mật trên máy chủ web.

Chặn tất cả các cổng không cần thiết, lưu lượng Giao thức thông báo điều khiển Internet (ICMP) và các giao thức không cần thiết như Hệ thống đầu vào/đầu ra cơ bản của mạng (NetBIOS) và SMB.

Củng cố ngăn xếp TCP/IP và liên tục áp dụng các bản vá và cập nhật phần mềm mới nhất cho phần mềm hệ thống.

Nếu các giao thức không an toàn như Telnet, POP3, SMTP và FTP được sử dụng, thì hãy thực hiện các biện pháp thích hợp để cung cấp xác thực và liên lạc an toàn, chẳng hạn như bằng cách sử dụng các chính sách Bảo mật IP (IPSec).

Nếu cần truy cập từ xa, hãy đảm bảo rằng các kết nối từ xa được bảo mật đúng cách bằng cách sử dụng các giao thức mã hóa và tạo đường hầm.

Vô hiệu hóa phiên bản và tác giả được phân phối trên web (WebDAV) nếu nó không được ứng dụng sử dụng hoặc giữ an toàn nếu được yêu cầu.

Sử dụng các giao thức bảo mật như Bảo mật tầng vận chuyển (TLS)/SSL để liên lạc với máy chủ web.

Đảm bảo rằng các máy chủ FTP không xác định hoạt động trong một phần vô thưởng vô phạt của cây thư mục khác với cây của máy chủ web.

Biện pháp đối phó: Tài khoản

Các biện pháp đối phó sau đây có thể được áp dụng để bảo mật tài khoản người dùng trên máy chủ web:

• Xóa tất cả các mô-đun và phần mở rộng ứng dụng không sử dụng.

• Vô hiệu hóa các tài khoản người dùng mặc định không sử dụng được tạo trong quá trình cài đặt HĐH.

• Khi tạo thư mục gốc web mới, hãy cấp quyền Hệ thống NT Fi (NTFS) thích hợp (ít nhất có thể) cho người dùng ẩn danh của máy chủ web IIS để truy cập nội dung của chúng tôi.

Loại bỏ những người dùng cơ sở dữ liệu không cần thiết và các thủ tục được lưu trữ, đồng thời tuân theo nguyên tắc đặc quyền tối thiểu đối với ứng dụng cơ sở dữ liệu để chống lại việc đầu độc truy vấn SQL.

• Sử dụng quyền truy cập web an toàn, quyền NTFS và cơ chế kiểm soát quyền truy cập .NET Framework bao gồm ủy quyền URL.

Làm chậm các cuộc tấn công từ điển và brute-force bằng các chính sách mật khẩu mạnh, đồng thời triển khai kiểm tra và cảnh báo khi đăng nhập thất bại.

Chạy các quy trình bằng tài khoản ít đặc quyền nhất cũng như dịch vụ ít đặc quyền nhất và tài khoản của chúng tôi

Giới hạn quyền truy cập của quản trị viên hoặc cấp gốc ở số lượng người dùng tối thiểu để duy trì một bản ghi giống nhau.

• Duy trì nhật ký của tất cả hoạt động của người dùng ở dạng mã hóa trên máy chủ web hoặc trong một máy riêng biệt trên mạng nội bộ.

• Vô hiệu hóa tất cả các tài khoản không tương tác nên tồn tại nhưng không yêu cầu đăng nhập tương tác.

Biện pháp đối phó: Tệp và Thư mục

Các biện pháp đối phó sau đây có thể được áp dụng để bảo mật các tệp và thư mục trên máy chủ web.

• Loại bỏ các tập tin không cần thiết trong các tập tin .jar.

• Loại bỏ thông tin cấu hình nhạy cảm trong mã byte.

■ Tránh ánh xạ các thư mục ảo giữa hai máy chủ khác nhau hoặc qua mạng.

• Thường xuyên theo dõi và kiểm tra tất cả nhật ký dịch vụ mạng, nhật ký truy cập trang web, nhật ký máy chủ cơ sở dữ liệu (ví dụ: Microsoft SQL Server, MySQL và Oracle) và nhật ký hệ điều hành.

■ Vô hiệu hóa việc cung cấp danh sách thư mục.

Loại bỏ các tệp không phải web như tệp lưu trữ, tệp sao lưu, tệp văn bản và tệp tiêu đề/bao gồm.

• Vô hiệu hóa việc cung cấp các loại tệp nhất định bằng cách tạo bản đồ tài nguyên.

• Đảm bảo rằng các ứng dụng web hoặc tệp trang web và tập lệnh được lưu trữ trong một phân vùng hoặc ổ đĩa tách biệt với phân vùng hoặc ổ đĩa của HĐH, nhật ký và bất kỳ tệp hệ thống nào khác.

■Chạy máy chủ web trong thư mục hộp cát để ngăn truy cập vào các tệp hệ thống.

■ Tránh tất cả các loại tệp không phải web được tham chiếu trong một URL.

Bảo vệ chống lại các cuộc tấn công máy chủ web bao gồm những điều sau đây.

• Ports

Giám sát tất cả các cổng trên máy chủ web thường xuyên để ngăn lưu lượng truy cập không cần thiết đến máy chủ web mục tiêu. Nếu lưu lượng truy cập không được giám sát, máy chủ web mục tiêu sẽ dễ bị phần mềm độc hại tấn công. Không cho phép truy cập công khai vào cổng 80 cho HTTP hoặc cổng 443 cho HTTPS; lưu lượng truy cập vào các cổng này nên được hạn chế. Nếu cổng 80 vẫn mở, máy chủ sẽ dễ bị tấn công DoS, làm tiêu tốn tài nguyên máy chủ. Lưu lượng mạng nội bộ phải được mã hóa hoặc hạn chế để bảo mật máy chủ web.

Những kẻ tấn công cố gắng che giấu danh tính của họ bằng cách giả mạo địa chỉ IP của người dùng hợp pháp. Bằng cách xử lý tệp nhật ký bảo mật, sử dụng quy tắc "từ chối địa chỉ IP này" trong tệp bộ quy tắc tường lửa hoặc bằng cách tạo lệnh "lỗ đen được định tuyến", hệ thống đích có thể chống lại các cuộc tấn công của máy chủ web.

■ Chứng chỉ máy chủ

Chứng chỉ máy chủ đảm bảo tính bảo mật và được ký bởi cơ quan đáng tin cậy. Tuy nhiên, kẻ tấn công có thể xâm phạm máy chủ được chứng nhận bằng cách sử dụng chứng chỉ giả mạo để chặn liên lạc an toàn bằng cách thực hiện các cuộc tấn công MITM. Có nhiều kỹ thuật khác nhau để tránh các cuộc tấn công MITM như vậy. Sau đây là một số trong số họ.

o Sử dụng xác thực trực tiếp các chứng chỉ.

o Sử dụng một giao thức mới không phụ thuộc vào bên thứ ba để xác thực chứng chỉ.

o Cho phép các miền kiểm tra trực tiếp và an toàn chứng chỉ của họ bằng cách sử dụng thông tin đăng nhập xác thực người dùng đã thiết lập trước đó.

o Sử dụng cấu trúc mật mã mạnh mẽ giúp tăng cường xác thực danh tính máy chủ và

giải quyết các hạn chế của các giải pháp của bên thứ ba.

o Đảm bảo rằng phạm vi dữ liệu chứng chỉ hợp lệ và chứng chỉ được sử dụng cho

mục đích dự định của họ.

o Đảm bảo rằng chứng chỉ chưa bị thu hồi và khóa công khai của chứng chỉ hợp lệ đối với cơ quan gốc đáng tin cậy.

• Machine.config

Tệp machine.config cung cấp cơ chế bảo mật thông tin bằng cách thay đổi cài đặt cấp độ máy. Nó ảnh hưởng đến tất cả các ứng dụng khác. Tệp machine.config bao gồm các cài đặt máy cho .Net framework, ảnh hưởng đến bảo mật. Có thể thực hiện các thao tác sau với tệp machine.config:

o Đảm bảo rằng các tài nguyên được bảo vệ được ánh xạ tới HttpForbiddenHandler và

HttpModules không sử dụng bị xóa

o Đảm bảo rằng tính năng theo dõi bị vô hiệu hóa <trace enable="false"/> và trình biên dịch gỡ lỗi bị tắt

o Xác minh rằng các lỗi ASP.NET không được hoàn nguyên về máy khách

o Xác minh cài đặt trạng thái phiên

• Bảo mật truy cập mã

Các biện pháp sau đây có thể được áp dụng để đảm bảo an ninh truy cập mã.

o Triển khai thực hành mã hóa an toàn để tránh tiết lộ mã nguồn và tấn công xác thực đầu vào.

o Hạn chế cài đặt chính sách bảo mật truy cập mã để đảm bảo rằng không có quyền thực thi mã được tải xuống từ Internet hoặc mạng nội bộ.

o Định cấu hình IIS để từ chối các URL có "../" để ngăn chặn việc truyền tải đường dẫn, khóa các lệnh và tiện ích của hệ thống với danh sách kiểm soát truy cập hạn chế (ACLS), đồng thời cài đặt các bản vá và cập nhật mới.

o Nếu các mục tiêu không triển khai bảo mật truy cập mã trong máy chủ web của họ, thì có khả năng thực thi mã độc hại.

anh ấy sau đây là một số biện pháp khác để bảo vệ chống lại các cuộc tấn công máy chủ web.

• Áp dụng ACLS bị hạn chế và chặn quản trị đăng ký từ xa.

• Bảo mật SAM (chỉ các máy chủ độc lập).

Đảm bảo rằng các cài đặt liên quan đến bảo mật được định cấu hình phù hợp và quyền truy cập vào tệp siêu dữ liệu bị hạn chế với các quyền NTES cứng

Xóa các bộ lọc Giao diện lập trình ứng dụng máy chủ Internet (ISAPI) không cần thiết khỏi máy chủ web.

• Xóa tất cả các chia sẻ tệp không cần thiết, bao gồm cả chia sẻ quản trị mặc định, nếu không cần thiết.

• Bảo mật các chia sẻ với các quyền NTFS bị hạn chế.

• Di chuyển các trang web và thư mục ảo sang các phân vùng không thuộc hệ thống và sử dụng quyền web IIS để hạn chế quyền truy cập. Xóa tất cả các ánh xạ tập lệnh IIS không cần thiết cho các phần mở rộng tệp tùy chọn để tránh

khai thác bất kỳ lỗi nào trong phần mở rộng ISAPI xử lý các loại tệp này.

• Kích hoạt mức kiểm tra tối thiểu trên máy chủ web và sử dụng quyền NTFS để bảo vệ các tệp nhật ký.

• Sử dụng máy chuyên dụng làm web server.

• Tạo ánh xạ URL tới các máy chủ nội bộ một cách thận trọng.

• Không cài đặt máy chủ IIS trên bộ điều khiển miền.

• Sử dụng theo dõi ID phiên phía máy chủ và khớp các kết nối với dấu thời gian, địa chỉ IP, v.v.

• Nếu một máy chủ cơ sở dữ liệu, chẳng hạn như Microsoft SQL Server, sẽ được sử dụng làm cơ sở dữ liệu phụ trợ, hãy cài đặt nó trên một máy chủ riêng biệt.

• Sử dụng các công cụ bảo mật được cung cấp cùng với phần mềm máy chủ web và máy quét để tự động hóa và

đơn giản hóa quá trình bảo mật máy chủ web.

■ Bảo vệ vật lý máy chủ web trong phòng máy an toàn.

• Không kết nối Máy chủ IIS với Internet cho đến khi nó được làm cứng hoàn toàn.

• Không cho phép bất kỳ ai đăng nhập cục bộ vào máy ngoại trừ quản trị viên.

■ Định cấu hình tài khoản người dùng ẩn danh riêng cho từng ứng dụng, nếu nhiều ứng dụng web được lưu trữ trên máy chủ.

• Giới hạn chức năng của máy chủ để chỉ hỗ trợ các công nghệ web được sử dụng.

■ Sàng lọc và lọc các yêu cầu lưu lượng đến.

Lưu trữ các tệp và tập lệnh trang web trên một phân vùng hoặc ổ đĩa riêng.

Câu hỏi và bài tập

1. Tấn công từ chối dịch vụ
   1. Khái niệm cơ bản

**Tấn công DoS là gì?**

Tấn công DoS là một cuộc tấn công vào máy tính hoặc mạng làm giảm, hạn chế hoặc ngăn chặn quyền truy cập vào tài nguyên hệ thống của người dùng hợp pháp. Trong một cuộc tấn công DoS, những kẻ tấn công làm tràn ngập hệ thống của nạn nhân với các yêu cầu dịch vụ hoặc lưu lượng truy cập không hợp pháp để làm quá tải tài nguyên của hệ thống và làm hệ thống ngừng hoạt động, dẫn đến việc trang web của nạn nhân không khả dụng hoặc ít nhất là làm giảm đáng kể hiệu suất mạng hoặc hệ thống của nạn nhân. Mục tiêu của một cuộc tấn công DoS là ngăn người dùng hợp pháp sử dụng hệ thống, thay vì giành quyền truy cập trái phép vào hệ thống hoặc làm hỏng dữ liệu.

Sau đây là những ví dụ về các kiểu tấn công DoS:

• Làm ngập hệ thống của nạn nhân với nhiều lưu lượng truy cập hơn mức có thể xử lý

• Làm ngập một dịch vụ (ví dụ: Trò chuyện chuyển tiếp qua Internet (IRC)) với nhiều sự kiện hơn mức nó có thể xử lý

• Làm hỏng ngăn xếp TCP/IP bằng cách gửi các gói bị hỏng

• Làm hỏng dịch vụ bằng cách tương tác với dịch vụ đó theo cách không mong muốn

Treo một hệ thống bằng cách đưa nó vào một vòng lặp vô hạn

Các cuộc tấn công DoS có nhiều hình thức khác nhau và nhắm mục tiêu vào các dịch vụ khác nhau. Các cuộc tấn công có thể gây ra những điều sau đây:

■Tiêu thụ tài nguyên

• Tiêu tốn băng thông, dung lượng ổ đĩa, thời gian CPU hoặc cấu trúc dữ liệu • Sự phá hủy hoặc thay đổi vật lý thực sự của các thành phần mạng

Phá hủy chương trình và tệp trong hệ thống máy tính

Nói chung, các cuộc tấn công DoS nhắm mục tiêu vào băng thông hoặc kết nối mạng. Các cuộc tấn công băng thông làm tràn mạng với lưu lượng truy cập lớn bằng cách sử dụng các tài nguyên mạng hiện có, do đó tước đi những tài nguyên này của người dùng hợp pháp. Các cuộc tấn công kết nối làm tràn hệ thống với số lượng lớn yêu cầu kết nối, tiêu tốn tất cả tài nguyên hệ điều hành có sẵn để ngăn hệ thống xử lý các yêu cầu hợp pháp của người dùng.

Hãy xem xét một công ty cung cấp thực phẩm tiến hành phần lớn hoạt động kinh doanh của mình qua điện thoại. Nếu một

kẻ tấn công muốn phá vỡ hoạt động kinh doanh này, họ cần tìm cách chặn điện thoại của công ty

dây chuyền, khiến cho công ty không thể kinh doanh được. Một cuộc tấn công DoS hoạt động

theo cùng một đường kẻ tấn công sử dụng tất cả các cách để kết nối với hệ thống của nạn nhân,

làm cho kinh doanh hợp pháp không thể.

Các cuộc tấn công DoS là một loại vi phạm an ninh thường không dẫn đến việc đánh cắp thông tin. Tuy nhiên, các cuộc tấn công này có thể gây tổn hại cho mục tiêu về thời gian và tài nguyên. Hơn nữa, lỗi bảo mật có thể gây mất dịch vụ như email. Trong trường hợp xấu nhất, một cuộc tấn công DoS có thể vô tình phá hủy các tệp và chương trình của hàng triệu người đã kết nối với hệ thống của nạn nhân tại thời điểm xảy ra cuộc tấn công.

**Tấn công DDoS là gì?**

Nguồn: http://searchsecurity.techtarget.com

Tấn công DDoS là một cuộc tấn công có phối hợp, quy mô lớn nhằm vào tính khả dụng của các dịch vụ trên hệ thống hoặc tài nguyên mạng của nạn nhân và được thực hiện gián tiếp thông qua nhiều máy tính bị xâm nhập (mạng botnet) trên Internet.

Theo định nghĩa trong Câu hỏi thường gặp về bảo mật World Wide Web, "Một cuộc tấn công từ chối dịch vụ (DDoS) phân tán sử dụng nhiều máy tính để khởi động một cuộc tấn công DoS có phối hợp nhằm vào một hoặc nhiều mục tiêu. Sử dụng công nghệ máy khách/máy chủ, thủ phạm có thể nhân rộng hiệu quả của việc từ chối dịch vụ một cách đáng kể bằng cách khai thác tài nguyên của nhiều máy tính đồng lõa vô tình, đóng vai trò là nền tảng tấn công." Lũ tin nhắn đến hệ thống đích về cơ bản buộc nó phải tắt, do đó từ chối dịch vụ cho người dùng hợp pháp.

Các dịch vụ bị tấn công thuộc về "nạn nhân chính", trong khi các hệ thống bị xâm nhập được sử dụng để khởi động cuộc tấn công được gọi là "nạn nhân phụ". Việc sử dụng các nạn nhân thứ cấp để thực hiện một cuộc tấn công DDoS cho phép kẻ tấn công thực hiện một cuộc tấn công lớn và gây rối trong khi gây khó khăn cho việc truy tìm kẻ tấn công ban đầu.

Mục tiêu chính của một cuộc tấn công DDoS trước tiên là giành quyền truy cập quản trị trên càng nhiều hệ thống càng tốt. Nói chung, những kẻ tấn công sử dụng tập lệnh tấn công tùy chỉnh để xác định các hệ thống dễ bị tấn công. Sau khi có quyền truy cập vào các hệ thống mục tiêu, kẻ tấn công tải lên và chạy phần mềm DDoS trên các hệ thống này vào thời điểm được chọn để khởi động cuộc tấn công.

Các cuộc tấn công DDoS đã trở nên phổ biến do khả năng tiếp cận dễ dàng của các kế hoạch khai thác và khối lượng công việc trí tuệ cần thiết để thực hiện chúng là không đáng kể. Các cuộc tấn công này có thể rất nguy hiểm vì chúng có thể nhanh chóng tiêu thụ các máy chủ lớn nhất trên Internet, khiến chúng trở nên vô dụng.

Các tác động của DDoS bao gồm mất thiện chí, mạng bị vô hiệu hóa, tổn thất tài chính và các tổ chức bị vô hiệu hóa.

Các cuộc tấn công DDoS hoạt động như thế nào?

Trong một cuộc tấn công DDoS, nhiều ứng dụng ngăn chặn trình duyệt hoặc mạng mục tiêu bằng các yêu cầu bên ngoài giả mạo khiến hệ thống, mạng, trình duyệt hoặc trang web trở nên chậm chạp, vô dụng và bị vô hiệu hóa hoặc không khả dụng.

Kẻ tấn công bắt đầu cuộc tấn công DDoS bằng cách gửi lệnh đến các tác nhân zombie, là các máy tính được kết nối Internet bị kẻ tấn công xâm nhập thông qua các chương trình phần mềm độc hại để thực hiện các hoạt động độc hại khác nhau thông qua máy chủ chỉ huy và kiểm soát (C&C). Các tác nhân zombie này gửi yêu cầu kết nối đến một số lượng lớn các hệ thống phản xạ với địa chỉ IP giả mạo của nạn nhân, điều này khiến các hệ thống phản xạ cho rằng các yêu cầu này bắt nguồn từ máy của nạn nhân thay vì các tác nhân zombie. Do đó, các hệ thống phản xạ gửi thông tin được yêu cầu (phản hồi yêu cầu kết nối) cho nạn nhân. Do đó, máy của nạn nhân tràn ngập các phản hồi không mong muốn từ một số máy tính phản xạ đồng thời, điều này có thể làm giảm hiệu suất hoặc khiến máy của nạn nhân tắt hoàn toàn.

* 1. Kỹ thuật tấn công từ chối dịch vụ

Kỹ thuật tấn công DOS/DDoS

Tiếp theo, các kỹ thuật tấn công DoS/DDoS sau đây sẽ được thảo luận:

■ Tấn công tràn ngập UDP

Trong một cuộc tấn công tràn ngập UDP, kẻ tấn công gửi các gói UDP giả mạo với tốc độ gói rất cao đến một máy chủ từ xa trên các cổng ngẫu nhiên của máy chủ đích bằng cách sử dụng dải IP nguồn lớn. Việc tràn ngập các gói UDP khiến máy chủ phải kiểm tra nhiều lần để tìm các ứng dụng không tồn tại tại các cổng. Do đó, hệ thống không thể truy cập các ứng dụng hợp pháp và mọi nỗ lực truy cập chúng đều trả về phản hồi lỗi với gói ICMP "Không thể truy cập đích". Cuộc tấn công này tiêu tốn tài nguyên mạng và băng thông có sẵn, làm cạn kiệt mạng cho đến khi nó ngoại tuyến.

• Tấn công lũ ICMP

Quản trị viên mạng sử dụng ICMP chủ yếu cho hoạt động IP, khắc phục sự cố và thông báo lỗi cho các gói không gửi được. Trong cuộc tấn công này, những kẻ tấn công gửi một lượng lớn các gói yêu cầu tiếng vang ICMP đến hệ thống của nạn nhân một cách trực tiếp hoặc thông qua các mạng phản xạ. Các gói này báo hiệu hệ thống của nạn nhân để trả lời và lưu lượng truy cập lớn sẽ làm bão hòa băng thông của kết nối mạng của nạn nhân, khiến nó bị quá tải và sau đó ngừng đáp ứng các yêu cầu TCP/IP hợp pháp.

Để bảo vệ chống lại các cuộc tấn công tràn ngập ICMP, cần phải đặt ngưỡng gọi tính năng chống tấn công tràn ngập ICMP khi vượt quá. Khi vượt quá ngưỡng ICMP (theo mặc định, giá trị ngưỡng là 1000 gói/giây), bộ định tuyến sẽ từ chối các yêu cầu tiếng vang ICMP tiếp theo từ tất cả các địa chỉ trong cùng một vùng bảo mật trong phần còn lại của giây hiện tại cũng như giây tiếp theo.

■ Tấn công PoD

Trong một cuộc tấn công Ping of Death (POD), kẻ tấn công cố gắng làm sập, làm mất ổn định hoặc đóng băng hệ thống hoặc dịch vụ đích bằng cách gửi các gói không đúng định dạng hoặc quá khổ bằng lệnh ping đơn giản. Giả sử kẻ tấn công gửi một gói có kích thước 65.538 byte đến máy chủ web mục tiêu. Kích thước này vượt quá giới hạn kích thước được quy định bởi RFC 791 IP, là 65.535 byte. Quá trình lắp ráp lại do hệ thống nhận thực hiện có thể khiến hệ thống gặp sự cố. Trong các cuộc tấn công như vậy, danh tính của kẻ tấn công có thể dễ dàng bị giả mạo và kẻ tấn công có thể không cần biết chi tiết về máy mục tiêu, ngoại trừ địa chỉ IP của nó.

• tấn công Smurf

Trong một cuộc tấn công Xì Trum, kẻ tấn công giả mạo địa chỉ IP nguồn bằng địa chỉ IP của nạn nhân và gửi một số lượng lớn các gói yêu cầu ICMP ECHO đến một mạng quảng bá IP. Điều này khiến tất cả các máy chủ trên mạng quảng bá phản hồi các yêu cầu ICMP ECHO đã nhận. Những phản hồi này được gửi đến máy của nạn nhân vì địa chỉ IP đã bị kẻ tấn công giả mạo, gây ra lưu lượng đáng kể cho máy của nạn nhân và cuối cùng khiến máy bị sập.

• Tấn công sóng xung

Các cuộc tấn công DDoS bằng sóng xung là loại tấn công DDoS mới nhất được các tác nhân đe dọa sử dụng để phá vỡ các hoạt động tiêu chuẩn của các mục tiêu. Nói chung, các kiểu tấn công DDoS là các luồng lưu lượng đến liên tục. Tuy nhiên, trong các cuộc tấn công DDoS bằng sóng xung, mô hình tấn công là định kỳ và cuộc tấn công có quy mô lớn, tiêu tốn toàn bộ băng thông của các mạng mục tiêu. Những kẻ tấn công gửi một chuỗi gói có tính lặp lại cao dưới dạng xung tới nạn nhân mục tiêu cứ sau 10 phút và phiên tấn công kéo dài khoảng một giờ hoặc vài ngày. Một xung đơn (300 Gbps trở lên) là quá đủ để làm đầy một đường ống mạng. Phục hồi từ các cuộc tấn công như vậy là rất khó khăn và đôi khi không thể.

• Tấn công Zero-day

Các cuộc tấn công DDoS Zero-day là các cuộc tấn công trong đó lỗ hổng DDoS không có bản vá hoặc cơ chế phòng thủ hiệu quả. Cho đến khi nạn nhân xác định được chiến lược tấn công của kẻ đe dọa và triển khai bản vá cho lỗ hổng DDoS bị khai thác, kẻ tấn công sẽ chủ động chặn tất cả tài nguyên của nạn nhân và đánh cắp dữ liệu của nạn nhân. Các cuộc tấn công này có thể gây thiệt hại nghiêm trọng cho cơ sở hạ tầng mạng và tài sản của nạn nhân. Hiện tại, không có cách tiếp cận linh hoạt nào để bảo vệ mạng khỏi kiểu tấn công này.

Tấn công lũ SYN

Trong một cuộc tấn công SYN, kẻ tấn công gửi một số lượng lớn các yêu cầu SYN đến máy chủ đích (nạn nhân) với các địa chỉ IP nguồn giả mạo. Cuộc tấn công tạo ra các kết nối TCP không hoàn chỉnh sử dụng hết tài nguyên mạng. Thông thường, khi máy khách muốn bắt đầu kết nối TCP với máy chủ, máy khách và máy chủ sẽ trao đổi một loạt thông báo sau:

• Một gói yêu cầu TCP SYN được gửi đến máy chủ.

• Máy chủ gửi SYN/ACK (xác nhận) để đáp ứng yêu cầu.

⚫ Máy khách gửi phản hồi ACK đến máy chủ để hoàn tất thiết lập phiên. Phương pháp này là một "bắt tay ba bước."

Trong một cuộc tấn công SYN, kẻ tấn công khai thác phương pháp bắt tay ba bước. Đầu tiên, kẻ tấn công gửi một yêu cầu TCP SYN giả mạo đến máy chủ mục tiêu. Sau khi máy chủ gửi SYN/ACK để phản hồi yêu cầu của máy khách (của kẻ tấn công), máy khách sẽ không bao giờ gửi phản hồi ACK. Điều này khiến máy chủ chờ hoàn tất kết nối.

Tràn ngập SYN tận dụng cách thức thiếu sót trong đó hầu hết các máy chủ thực hiện bắt tay ba bước TCP. Cuộc tấn công này xảy ra khi kẻ tấn công gửi các gói (yêu cầu) SYN không giới hạn đến hệ thống máy chủ. Quá trình truyền các gói như vậy nhanh hơn hệ thống có thể xử lý. Thông thường, một kết nối được thiết lập với quá trình bắt tay ba bước của TCP. Máy chủ theo dõi các kết nối mở một phần trong khi chờ các gói ACK phản hồi trong hàng đợi nghe.

Một máy chủ độc hại có thể khai thác một máy chủ khác, quản lý nhiều kết nối từng phần bằng cách gửi đồng thời nhiều yêu cầu SYN đến máy chủ mục tiêu. Khi hàng đợi đầy, hệ thống không thể mở các kết nối mới cho đến khi hệ thống loại bỏ một số mục từ hàng đợi kết nối thông qua thời gian chờ bắt tay. Khả năng duy trì mỗi kết nối không hoàn chỉnh trong 75 giây có thể bị khai thác tích lũy trong một cuộc tấn công DoS. Cuộc tấn công sử dụng địa chỉ IP giả, gây khó khăn cho việc truy tìm nguồn gốc. Kẻ tấn công có thể điền vào bảng kết nối ngay cả khi không giả mạo địa chỉ IP nguồn.

Ngoài các cuộc tấn công tràn ngập SYN, những kẻ tấn công cũng có thể sử dụng các cuộc tấn công tràn ngập SYN-ACK và ACK/PUSH ACK để phá vỡ các máy mục tiêu. Tất cả các cuộc tấn công này đều giống nhau về chức năng với các biến thể nhỏ.

Tấn công lũ SYN-ACK

Kiểu tấn công này tương tự như kiểu tấn công SYN lũ, ngoại trừ trong kiểu tấn công lũ này, kẻ tấn công khai thác giai đoạn thứ hai của bắt tay ba bước bằng cách gửi một số lượng lớn các gói SYN-ACK đến máy mục tiêu để làm cạn kiệt các gói tin SYN-ACK. tài nguyên.

Tấn công lũ ACK và PUSH ACK

Trong phiên TCP đang hoạt động, ACK và PUSH ACK là các cờ được sử dụng để truyền thông tin đến và đi từ máy chủ và máy khách cho đến khi phiên kết thúc. Trong một cuộc tấn công tràn ngập ACK và PUSH ACK, những kẻ tấn công gửi một lượng lớn các gói tin ACK và PUSH ACK giả mạo đến máy mục tiêu, khiến nó không hoạt động.

■ Tấn công phân mảnh

Các cuộc tấn công này phá hủy khả năng của nạn nhân trong việc tập hợp lại các gói bị phân mảnh bằng cách làm tràn ngập nó bằng các đoạn TCP hoặc UDP, dẫn đến giảm hiệu suất. Trong các cuộc tấn công phân mảnh, kẻ tấn công gửi một số lượng lớn các gói bị phân mảnh (hơn 1500 byte) đến máy chủ web mục tiêu với tốc độ gói tương đối nhỏ. Do giao thức cho phép phân mảnh nên các gói này thường không bị kiểm tra khi chúng đi qua thiết bị mạng như bộ định tuyến, tường lửa và hệ thống phát hiện xâm nhập (IDS)/hệ thống ngăn chặn xâm nhập (IPS). Việc lắp ráp lại và kiểm tra các gói bị phân mảnh lớn này tiêu tốn quá nhiều tài nguyên. Hơn nữa, nội dung trong các mảnh gói được kẻ tấn công ngẫu nhiên hóa, điều này khiến việc lắp ráp lại và kiểm tra tiêu tốn nhiều tài nguyên hơn và do đó, khiến hệ thống gặp sự cố.

⚫ACK tấn công lũ lụt

Trong kiểu tấn công này, kẻ tấn công tạo phiên TCP giả hoặc giả mạo bằng cách mang nhiều gói SYN, ACK và RST hoặc FIN. Những kẻ tấn công sử dụng cuộc tấn công này để vượt qua tường lửa và thực hiện các cuộc tấn công DDoS vào các mạng mục tiêu, làm cạn kiệt tài nguyên mạng của chúng.

Sau đây là các ví dụ về các cuộc tấn công lũ phiên giả mạo:

• Nhiều cuộc tấn công lũ phiên giả mạo SYN-ACK

Trong kiểu tấn công tràn ngập này, kẻ tấn công tạo một phiên giả với nhiều gói SYN và nhiều gói ACK, cùng với một hoặc nhiều gói RST hoặc FIN.

• Tấn công lũ phiên giả mạo nhiều ACK

Trong kiểu tấn công tràn ngập này, kẻ tấn công tạo phiên giả mạo bằng cách bỏ qua hoàn toàn các gói SYN và chỉ sử dụng nhiều gói ACK cùng với một hoặc nhiều gói RST hoặc FIN. Bởi vì các gói SYN không được sử dụng và tường lửa chủ yếu sử dụng bộ lọc gói SYN để phát hiện lưu lượng truy cập bất thường, tỷ lệ phát hiện DDOS của tường lửa là rất thấp đối với các loại tấn công này.

• Tấn công HTTPS GET/POST

Các cuộc tấn công HTTP là các cuộc tấn công lớp 7. Máy khách HTTP, chẳng hạn như trình duyệt web, kết nối với máy chủ web thông qua HTTP để gửi yêu cầu HTTP, có thể là HTTP GET hoặc HTTP POST. Những kẻ tấn công khai thác các yêu cầu này để thực hiện các cuộc tấn công DoS.

Trong một cuộc tấn công HTTP GET, kẻ tấn công sử dụng tiêu đề HTTP bị trì hoãn thời gian để giữ kết nối HTTP và làm cạn kiệt tài nguyên máy chủ web. Kẻ tấn công không bao giờ gửi yêu cầu đầy đủ đến máy chủ mục tiêu. Do đó, máy chủ giữ lại kết nối HTTP và chờ đợi, khiến người dùng hợp pháp không thể truy cập được. Trong các kiểu tấn công này, tất cả các tham số mạng có vẻ ổn định trong khi dịch vụ vẫn không khả dụng.

Trong một cuộc tấn công HTTP POST, kẻ tấn công gửi các yêu cầu HTTP có tiêu đề hoàn chỉnh nhưng nội dung thư không đầy đủ đến máy chủ hoặc ứng dụng web mục tiêu. Vì nội dung thư không đầy đủ nên máy chủ sẽ đợi phần còn lại của nội dung, khiến máy chủ web hoặc ứng dụng web không khả dụng cho người dùng hợp pháp.

Một cuộc tấn công HTTP GET/POST là một cuộc tấn công lớp 7 tinh vi không sử dụng các gói không đúng định dạng, giả mạo hoặc kỹ thuật phản chiếu. Kiểu tấn công này yêu cầu ít băng thông hơn các cuộc tấn công khác để đánh sập trang web hoặc máy chủ web được nhắm mục tiêu. Cuộc tấn công này nhằm mục đích buộc máy chủ phân bổ càng nhiều tài nguyên càng tốt để phục vụ cho cuộc tấn công, do đó từ chối quyền truy cập của người dùng hợp pháp vào tài nguyên của máy chủ.

Ngoài cuộc tấn công HTTP GET/POST đã nói ở trên, kẻ tấn công có thể sử dụng các cuộc tấn công HTTP sau đây để làm cạn kiệt băng thông của mạng mục tiêu:

■Tấn công lũ lụt HTTP một phiên

Trong kiểu tấn công tràn ngập này, kẻ tấn công khai thác các lỗ hổng trong HTTP 1.1 để bắn phá mục tiêu bằng nhiều yêu cầu trong một phiên HTTP.

■Tấn công HTTP theo yêu cầu đơn

Trong kiểu tấn công dồn dập này, kẻ tấn công thực hiện một số yêu cầu HTTP từ một phiên HTTP duy nhất bằng cách che dấu các yêu cầu này trong một gói HTTP. Kỹ thuật này cho phép kẻ tấn công ẩn danh và vô hình trong khi thực hiện các cuộc tấn công DDoS.

• HTTP đệ quy GET Lũ tấn công

Không bị phát hiện là chìa khóa cho những kẻ tấn công. Kẻ tấn công giả làm người dùng hợp pháp và thực hiện các hành động hợp pháp có thể lừa bất kỳ tường lửa nào tin rằng nguồn là hợp pháp trong khi thực tế không phải vậy. GET đệ quy thu thập danh sách các trang hoặc hình ảnh và dường như đang đi qua các trang hoặc hình ảnh này. Tuy nhiên, nó lén lút thực hiện các cuộc tấn công dồn dập vào mục tiêu. GET đệ quy kết hợp với một cuộc tấn công tràn ngập HTTP có thể gây ra thiệt hại cực lớn cho mục tiêu.

Đệ quy ngẫu nhiên GET Lũ tấn công

Kiểu tấn công này là một phiên bản tinh chỉnh của cuộc tấn công lũ GET đệ quy. Nó được thiết kế cho các diễn đàn, blog và các trang web khác có các trang theo trình tự. Tương tự như cuộc tấn công tràn ngập GET đệ quy, trong cuộc tấn công này, GET đệ quy giả vờ xem qua các trang. Vì mục tiêu là các diễn đàn, nhóm và các blog khác nên kẻ tấn công sử dụng các số ngẫu nhiên từ một phạm vi trang hợp lệ để giả làm người dùng hợp pháp và gửi yêu cầu GET mới mỗi lần. Trong cả hai cuộc tấn công tràn ngập GET đệ quy và GET đệ quy ngẫu nhiên, mục tiêu bị bắn phá với một số lượng lớn các yêu cầu GET, làm cạn kiệt tài nguyên của nó.

• Tấn công Slowloris

Slowloris là một công cụ tấn công DDoS được sử dụng để thực hiện các cuộc tấn công DDoS lớp 7 nhằm đánh sập cơ sở hạ tầng web. Nó khác hẳn với các công cụ khác ở chỗ nó sử dụng lưu lượng HTTP hoàn toàn hợp pháp để đánh sập máy chủ mục tiêu. Trong các cuộc tấn công Slowloris, kẻ tấn công gửi một phần yêu cầu HTTP đến máy chủ hoặc ứng dụng web mục tiêu. Khi nhận được một phần yêu cầu, máy chủ đích sẽ mở nhiều kết nối và đợi các yêu cầu hoàn tất. Tuy nhiên, các yêu cầu này vẫn chưa hoàn thành, khiến nhóm kết nối đồng thời tối đa của máy chủ mục tiêu bị lấp đầy và các nỗ lực kết nối bổ sung bị từ chối.

• Tấn công tràn ngập lớp ứng dụng UDP

Mặc dù các cuộc tấn công tràn ngập UDP được biết đến với bản chất tấn công theo khối lượng, nhưng một số giao thức lớp ứng dụng dựa trên UDP có thể được những kẻ tấn công sử dụng để thực hiện các cuộc tấn công dồn dập vào các mạng mục tiêu.

Sau đây là các ví dụ cho các giao thức lớp ứng dụng dựa trên UDP mà kẻ tấn công có thể sử dụng để làm ngập các mạng mục tiêu:

Giao thức tạo ký tự (CHARGEN)

Giao thức truyền tệp tầm thường (TFTP)

Hệ thống đầu vào/đầu ra cơ bản của mạng (NetBIOS)

Giao thức quản lý mạng đơn giản Phiên bản 2 (SNMPv2)

• NTP

• Trích dẫn trong ngày (QOTD)

• Giao thức mạng Quake

• Gọi thủ tục từ xa (RPC)

giao thức hơi nước

SSDP

Giao thức truy cập thư mục nhẹ ít kết nối (CLDAP)

• Thoại qua Giao thức Internet (VoIP)

• Tấn công đa vector

Trong các cuộc tấn công DDoS đa vectơ, kẻ tấn công sử dụng kết hợp các cuộc tấn công lớp thể tích, giao thức và lớp ứng dụng để đánh sập hệ thống hoặc dịch vụ đích. Kẻ tấn công nhanh chóng thay đổi từ một dạng tấn công DDoS (ví dụ: gói SYN) sang dạng khác (lớp 7). Các cuộc tấn công này được thực hiện thông qua một vectơ tại một thời điểm hoặc thông qua nhiều vectơ song song để gây nhầm lẫn cho bộ phận CNTT của công ty, khiến họ sử dụng tất cả tài nguyên và chuyển hướng tập trung một cách ác ý.

• Tấn công ngang hàng

Tấn công ngang hàng là một dạng tấn công DDoS trong đó kẻ tấn công khai thác một số lỗi trong máy chủ ngang hàng để bắt đầu một cuộc tấn công DDoS. Những kẻ tấn công khai thác các lỗ hổng được tìm thấy trong các mạng sử dụng giao thức Kết nối trực tiếp (DC++), cho phép trao đổi tệp giữa các máy khách nhắn tin tức thời. Loại tấn công này không sử dụng botnet. Không giống như một cuộc tấn công dựa trên botnet, một cuộc tấn công ngang hàng giúp những kẻ tấn công không cần phải giao tiếp với các máy khách mà chúng phá hoại. Tại đây, kẻ tấn công hướng dẫn khách hàng của các trung tâm chia sẻ tệp ngang hàng lớn ngắt kết nối khỏi mạng ngang hàng của họ và thay vào đó kết nối với trang web của nạn nhân. Do đó, hàng nghìn máy tính có thể cố gắng kết nối mạnh mẽ với một trang web mục tiêu, làm giảm hiệu suất của trang web mục tiêu. Thật dễ dàng để xác định các cuộc tấn công ngang hàng dựa trên chữ ký. Bằng cách sử dụng phương pháp này, kẻ tấn công khởi động các cuộc tấn công DoS lớn để xâm nhập các trang web.

Có thể giảm thiểu các cuộc tấn công DDoS ngang hàng bằng cách chỉ định các cổng cho giao tiếp ngang hàng. Ví dụ: chỉ định cổng 80 để không cho phép giao tiếp ngang hàng sẽ giảm thiểu khả năng bị tấn công vào các trang web.

• Tấn công DOS (PDOS) vĩnh viễn

Tấn công từ chối dịch vụ vĩnh viễn

Các cuộc tấn công DoS vĩnh viễn (PDOS), còn được gọi là tấn công lừa đảo, nhắm mục tiêu hoàn toàn vào phần cứng và gây ra thiệt hại không thể khắc phục cho phần cứng. Không giống như các kiểu tấn công DoS khác, nó phá hoại phần cứng hệ thống, yêu cầu nạn nhân phải thay thế hoặc cài đặt lại phần cứng. Cuộc tấn công PDoS khai thác các lỗi bảo mật trong thiết bị để cho phép quản trị từ xa trên giao diện quản lý của phần cứng nạn nhân, chẳng hạn như máy in, bộ định tuyến và các thiết bị mạng khác.

Kiểu tấn công này nhanh hơn và có sức tàn phá lớn hơn so với các cuộc tấn công DoS thông thường. Nó hoạt động với một lượng tài nguyên hạn chế, không giống như một cuộc tấn công DDoS, trong đó những kẻ tấn công giải phóng một nhóm thây ma vào mục tiêu. Những kẻ tấn công thực hiện các cuộc tấn công PDoS bằng cách sử dụng một phương pháp được gọi là "xếp gạch" hệ thống. Trong phương pháp này, kẻ tấn công gửi email, cuộc trò chuyện IRC, tweet hoặc video có nội dung lừa đảo để cập nhật phần cứng cho nạn nhân. Các bản cập nhật phần cứng được sửa đổi và bị hỏng với các lỗ hổng hoặc phần sụn bị lỗi. Khi nạn nhân nhấp vào một liên kết hoặc cửa sổ bật lên đề cập đến bản cập nhật phần cứng lừa đảo, nạn nhân sẽ cài đặt nó vào hệ thống của họ. Do đó, kẻ tấn công giành được quyền kiểm soát hoàn toàn đối với hệ thống của nạn nhân.

Tấn công DOS phản xạ phân tán (DRDOS)

Tấn công DOS phản ánh phân tán (DRDOS), còn được gọi là tấn công "giả mạo", liên quan đến việc sử dụng nhiều máy trung gian và máy thứ cấp góp phần vào một cuộc tấn công DDoS nhằm vào máy hoặc ứng dụng mục tiêu. Một cuộc tấn công DRDOS khai thác lỗ hổng bắt tay ba bước TCP.

Cuộc tấn công này liên quan đến máy tấn công, nạn nhân trung gian (thây ma), nạn nhân thứ cấp (máy phản xạ) và máy mục tiêu. Kẻ tấn công khởi động cuộc tấn công này bằng cách gửi yêu cầu đến các máy chủ trung gian, từ đó phản ánh lưu lượng tấn công đến mục tiêu.

Quá trình của một cuộc tấn công DRDOS như sau. Đầu tiên, kẻ tấn công ra lệnh cho nạn nhân trung gian (thây ma) gửi một luồng gói (TCP SYN) với địa chỉ IP của mục tiêu chính làm địa chỉ IP nguồn tới các máy không bị xâm phạm khác (nạn nhân thứ cấp hoặc máy phản xạ) để khuyến khích họ thiết lập kết nối với mục tiêu chính. Do đó, các thiết bị phản xạ gửi một lượng lớn lưu lượng (SYN/ACK) đến mục tiêu chính để thiết lập kết nối mới với nó vì chúng tin rằng máy chủ đã yêu cầu nó. Mục tiêu chính loại bỏ các gói SYN/ACK nhận được từ các bộ phản xạ vì chúng không gửi gói SYN. Trong khi đó, bộ phản xạ chờ phản hồi ACK từ mục tiêu chính. Giả sử rằng gói bị mất, các máy phản xạ sẽ gửi lại các gói SYN/ACK đến mục tiêu chính để thiết lập kết nối, cho đến khi hết thời gian chờ. Theo cách này, máy mục tiêu tràn ngập một lượng lớn lưu lượng truy cập từ các máy phản xạ. Băng thông kết hợp của các máy phản xạ này áp đảo máy mục tiêu.

Một cuộc tấn công DRDOS là một cuộc tấn công thông minh vì rất khó hoặc thậm chí không thể lần ra kẻ tấn công. Thay vì kẻ tấn công thực sự, nạn nhân thứ cấp (người phản xạ) dường như tấn công trực tiếp mục tiêu chính. Cuộc tấn công này hiệu quả hơn một cuộc tấn công DDoS điển hình vì nhiều nạn nhân trung gian và thứ cấp tạo ra băng thông tấn công lớn.

Biện pháp đối phó

o Tắt dịch vụ Character Generator Protocol (CHARGEN) để ngăn chặn phương thức tấn công này

o Tải xuống các bản cập nhật và bản vá lỗi mới nhất cho máy chủ

* 1. Botnet

Thuật ngữ "bot" là từ viết tắt của "robot" và dùng để chỉ các ứng dụng phần mềm chạy các tác vụ tự động qua Internet. Những kẻ tấn công sử dụng bot để lây nhiễm một số lượng lớn máy tính tạo thành mạng hoặc "botnet", cho phép chúng khởi chạy các cuộc tấn công DDoS, tạo thư rác, phát tán vi-rút và thực hiện các loại tội phạm khác.

Phần này đề cập đến các tập đoàn tội phạm mạng có tổ chức, sơ đồ tổ chức, mạng botnet và kỹ thuật lan truyền mạng botnet; hệ sinh thái botnet; phương pháp quét để tìm máy dễ bị tấn công; và sự lan truyền của mã độc hại.

Các bot được sử dụng cho các hoạt động thu thập dữ liệu hoặc khai thác dữ liệu lành tính, chẳng hạn như "dò tìm trên web" cũng như để điều phối các cuộc tấn công DoS. Mục đích chính của bot là thu thập dữ liệu. Có nhiều loại bot khác nhau, chẳng hạn như bot Internet, bot IRC và bot trò chuyện. Ví dụ về bot IRC là Supybot, Sopel, EnergyMech và Eggdrop.

Botnet (viết tắt của "mẠNG ROBOT") là một nhóm máy tính bị "lây nhiễm" bởi bot; tuy nhiên, botnet có thể được sử dụng cho cả mục đích tích cực và tiêu cực. Là một công cụ hack, botnet bao gồm một mạng lưới khổng lồ các hệ thống bị xâm nhập. Một mạng botnet tương đối nhỏ gồm 1.000 bot có băng thông kết hợp lớn hơn băng thông của hầu hết các hệ thống công ty.

Sự ra đời của botnet đã dẫn đến sự gia tăng mạnh mẽ của tội phạm mạng. Botnet tạo thành cốt lõi của trung tâm hoạt động tội phạm mạng liên kết và hợp nhất các phần khác nhau của thế giới tội phạm mạng. Các nhà cung cấp dịch vụ tội phạm mạng là một phần của mạng tội phạm mạng. Họ cung cấp các dịch vụ như phát triển mã độc, lưu trữ chống đạn, tạo khai thác trình duyệt, mã hóa và đóng gói.

Mã độc hại là công cụ chính được các tổ chức tội phạm sử dụng để thực hiện tội phạm mạng. Chủ sở hữu botnet ra lệnh cho cả bot và các chương trình độc hại khác như Trojan, vi rút, sâu, keylogger và các ứng dụng được chế tạo đặc biệt để tấn công các máy tính từ xa qua mạng. Các nhà phát triển cung cấp dịch vụ phần mềm độc hại trên các trang web công cộng hoặc tài nguyên Internet đã đóng.

Botnet là tác nhân mà kẻ xâm nhập có thể gửi đến hệ thống máy chủ để thực hiện một hoạt động bất hợp pháp. Botnet chạy các chương trình ẩn cho phép xác định các lỗ hổng hệ thống. Những kẻ tấn công có thể sử dụng botnet để thực hiện các nhiệm vụ tẻ nhạt liên quan đến việc thăm dò một hệ thống để tìm các lỗ hổng đã biết.

Kẻ tấn công có thể sử dụng botnet để thực hiện những việc sau:

• Tấn công DDoS: Botnet có thể tạo ra các cuộc tấn công DDoS, làm tiêu tốn băng thông của máy tính nạn nhân. Botnet cũng có thể làm hệ thống quá tải, lãng phí tài nguyên hệ thống máy chủ có giá trị và phá hủy kết nối mạng.

• Gửi thư rác: Những kẻ tấn công sử dụng proxy SOCKS để gửi thư rác. Họ thu thập địa chỉ email từ các trang web hoặc các nguồn khác. Sniffing traffic: Một packet sniffer quan sát lưu lượng dữ liệu đi vào một máy bị xâm nhập. Nó cho phép kẻ tấn công thu thập thông tin nhạy cảm như thẻ tín dụng

số và mật khẩu. Trình thám thính cũng cho phép kẻ tấn công đánh cắp thông tin từ

một botnet và sử dụng nó để chống lại một botnet khác. Nói cách khác, botnet có thể cướp một

nữa.

• Keylogging: Keylogging là phương pháp ghi lại các phím được gõ trên bàn phím và nó cung cấp thông tin nhạy cảm như mật khẩu hệ thống. Những kẻ tấn công sử dụng keylogging để thu thập thông tin đăng nhập tài khoản cho các dịch vụ như PayPal.

■ Phát tán phần mềm độc hại mới: Botnet có thể được sử dụng để phát tán các bot mới.

• Cài đặt tiện ích quảng cáo: Botnet có thể được sử dụng để thực hiện "gian lận nhấp chuột" bằng cách tự động nhấp chuột.

• Lạm dụng Google AdSense: Một số công ty cho phép hiển thị quảng cáo Google AdSense trên trang web của họ vì lợi ích kinh tế. Botnet cho phép kẻ xâm nhập tự động nhấp chuột vào quảng cáo, tạo ra phần trăm tăng trong hàng đợi nhấp chuột.

■ Tấn công vào mạng trò chuyện IRC: Còn được gọi là tấn công nhân bản, những cuộc tấn công này tương tự như tấn công DDoS. Một tác nhân chính hướng dẫn mỗi bot liên kết với hàng nghìn bản sao trong mạng IRC, có thể làm ngập mạng.

• Thao túng các cuộc thăm dò và trò chơi trực tuyến: Mỗi mạng botnet có một địa chỉ duy nhất, cho phép nó thao túng các cuộc thăm dò và trò chơi trực tuyến.

■ Đánh cắp danh tính hàng loạt: Botnet có thể gửi một số lượng lớn email trong khi mạo danh một tổ chức có uy tín như eBay. Kỹ thuật này cho phép kẻ tấn công đánh cắp thông tin để đánh cắp danh tính.

Hình bên dưới minh họa cách kẻ tấn công khởi động cuộc tấn công DoS dựa trên botnet vào máy chủ mục tiêu. Kẻ tấn công thiết lập một trung tâm bot C&C, sau đó chúng lây nhiễm vào một máy (bot) và xâm phạm nó. Sau đó, họ sử dụng bot này để lây nhiễm và xâm nhập các hệ thống dễ bị tổn thương khác có sẵn trong mạng, dẫn đến một mạng botnet. Các bot (còn được gọi là zombie) kết nối với trung tâm C&C và chờ hướng dẫn. Sau đó, kẻ tấn công gửi các lệnh độc hại đến các bot thông qua trung tâm C&C. Cuối cùng, theo hướng dẫn của kẻ tấn công, các bot khởi động một cuộc tấn công DoS trên máy chủ mục tiêu, khiến các dịch vụ của nó không khả dụng đối với người dùng hợp pháp trong mạng.

* 1. Phát hiện tấn công từ chối dịch vụ

Kỹ thuật phát hiện

Các kỹ thuật phát hiện sớm giúp ngăn chặn các cuộc tấn công DOS/DDoS. Phát hiện một cuộc tấn công DoS/DDoS là một nhiệm vụ khó khăn. Trình phát hiện lưu lượng tấn công DOS/DDoS cần phân biệt giữa gói dữ liệu thật và giả, điều này không phải lúc nào cũng có thể thực hiện được. Do đó, các kỹ thuật được sử dụng cho mục đích này là không hoàn hảo. Luôn có khả năng nhầm lẫn giữa lưu lượng được tạo bởi người dùng mạng hợp pháp và lưu lượng được tạo bởi một cuộc tấn công DoS/DDoS. Các kỹ thuật phát hiện dựa trên việc xác định và phân biệt sự gia tăng lưu lượng bất hợp pháp và các sự kiện chớp nhoáng từ lưu lượng gói hợp pháp.

Một vấn đề trong việc lọc lưu lượng không có thật từ lưu lượng hợp pháp là khối lượng lưu lượng. Không thể quét từng gói dữ liệu để đảm bảo an toàn trước cuộc tấn công DoS/DDoS.

Tất cả các kỹ thuật phát hiện được sử dụng ngày nay xác định một cuộc tấn công là một sai lệch bất thường và đáng chú ý trong các đặc điểm và số liệu thống kê lưu lượng mạng. Những kỹ thuật này liên quan đến phân tích thống kê về độ lệch để phân loại lưu lượng truy cập độc hại và chính hãng.

Sau đây là ba loại kỹ thuật phát hiện:

■ Lập hồ sơ hoạt động

Hồ sơ hoạt động được thực hiện dựa trên tốc độ gói trung bình cho lưu lượng mạng, bao gồm các gói liên tiếp có thông tin tiêu đề gói tương tự. Thông tin tiêu đề gói bao gồm địa chỉ IP của đích và người gửi, cổng và giao thức truyền tải được sử dụng. Một cuộc tấn công được chỉ định bởi

o Sự gia tăng mức độ hoạt động giữa các cụm lưu lượng mạng

o Tăng tổng số cụm riêng biệt (tấn công DDoS)

Đối với tốc độ gói trung bình cao hơn hoặc mức độ hoạt động của một luồng, thời gian giữa các gói phù hợp liên tiếp sẽ thấp hơn. Tính ngẫu nhiên trong tốc độ gói trung bình hoặc mức độ hoạt động có thể chỉ ra hoạt động đáng ngờ. Phương pháp tính toán entropy đo lường tính ngẫu nhiên trong các mức độ hoạt động. Nếu một mạng đang bị tấn công, entropy của các mức hoạt động của mạng sẽ tăng lên.

Một trong những rào cản lớn trong phương pháp lập hồ sơ hoạt động là khối lượng lớn lưu lượng truy cập. Vấn đề này có thể được khắc phục bằng cách phân cụm các luồng gói có đặc điểm tương tự. Bởi vì các cuộc tấn công DoS tạo ra một số lượng lớn các gói dữ liệu rất giống nhau, nên việc tăng tốc độ gói trung bình hoặc tăng tính đa dạng của các gói có thể chỉ ra một cuộc tấn công DoS.

Phát hiện điểm thay đổi tuần tự

Trong kỹ thuật phát hiện điểm thay đổi tuần tự, lưu lượng truy cập mạng được lọc theo địa chỉ IP, số cổng được nhắm mục tiêu và giao thức truyền thông được sử dụng và dữ liệu lưu lượng truy cập được lưu trữ trong biểu đồ hiển thị tốc độ lưu lượng truy cập theo thời gian. Các thuật toán phát hiện điểm thay đổi cô lập các thay đổi trong thống kê lưu lượng truy cập mạng và tốc độ lưu lượng truy cập do các cuộc tấn công gây ra. Nếu có sự thay đổi lớn về tốc độ lưu lượng truy cập, một cuộc tấn công DoS có thể xảy ra.

Kỹ thuật này sử dụng thuật toán tổng tích lũy (CUSUM) để xác định và định vị các cuộc tấn công DoS. Thuật toán tính toán độ lệch trong thực tế so với mức trung bình cục bộ dự kiến trong chuỗi thời gian lưu lượng truy cập. Kỹ thuật phát hiện điểm thay đổi tuần tự xác định các hoạt động quét điển hình của sâu mạng.

Phân tích tín hiệu dựa trên wavelet

Kỹ thuật phân tích wavelet phân tích lưu lượng mạng theo các thành phần quang phổ. Nó chia các tín hiệu đến thành các tần số khác nhau và phân tích các thành phần tần số khác nhau một cách riêng biệt. Phân tích năng lượng của từng cửa sổ quang phổ cho thấy sự hiện diện của dị thường. Các kỹ thuật này kiểm tra các thành phần tần số xuất hiện tại một thời điểm cụ thể và cung cấp mô tả về các thành phần đó. Sự hiện diện của một tần số lạ cho biết hoạt động mạng đáng ngờ.

Tín hiệu mạng bao gồm tín hiệu luồng gói dữ liệu được định vị theo thời gian và nhiễu nền. Phân tích tín hiệu dựa trên sóng con lọc các tín hiệu đầu vào của luồng lưu lượng truy cập bất thường khỏi nhiễu nền. Lưu lượng mạng thông thường nói chung là lưu lượng tần số thấp. Trong một cuộc tấn công, các thành phần tần số cao của tín hiệu tăng lên.

* 1. Giải pháp phòng chống
     1. Các biện pháp đối phó với các cuộc tấn công lũ SYN

Lọc gói thích hợp là một giải pháp khả thi đối với các cuộc tấn công lũ lụt SYN. Quản trị viên cũng có thể điều chỉnh ngăn xếp TCP/IP để giảm tác động của các cuộc tấn công SYN trong khi vẫn cho phép lưu lượng khách hàng hợp pháp

Một số cuộc tấn công SYN không cố gắng làm đảo lộn máy chủ; thay vào đó, chúng cố gắng sử dụng toàn bộ băng thông của kết nối Internet. Hai công cụ để chống lại cuộc tấn công này là SYN cookie và SynAttackProtect

Để đề phòng kẻ tấn công cố gắng sử dụng băng thông của kết nối Internet, quản trị viên có thể thực hiện một số biện pháp an toàn bổ sung; ví dụ: họ có thể giảm khoảng thời gian chờ trong đó kết nối đang chờ xử lý được duy trì ở trạng thái "SYN RECEIVED" trong hàng đợi. Thông thường, nếu máy khách không gửi phản hồi ACK, máy chủ sẽ truyền lại gói ACK đầu tiên. Có thể loại bỏ lỗ hổng này bằng cách giảm thời gian truyền lại gói đầu tiên, giảm số lần truyền lại gói hoặc tắt hoàn toàn việc truyền lại gói.

* + 1. Phòng chống DdoS

Chiến lược đối phó DoS/DDoS

• Hấp thụ cuộc tấn công: Trong chiến lược này, khả năng bổ sung được sử dụng để hấp thụ một cuộc tấn công, đòi hỏi phải lập kế hoạch trước. Nó cũng yêu cầu các nguồn lực bổ sung. Một bất lợi liên quan đến chiến lược này là chi phí tài nguyên bổ sung, phát sinh ngay cả khi không có cuộc tấn công nào đang diễn ra.

• Làm suy giảm dịch vụ: Nếu không thể giữ cho tất cả các dịch vụ hoạt động trong một cuộc tấn công, bạn nên giữ ít nhất các dịch vụ quan trọng hoạt động. Đối với điều này, các dịch vụ quan trọng được xác định đầu tiên, sau đó mạng, hệ thống và thiết kế ứng dụng được tùy chỉnh để cắt giảm các dịch vụ không quan trọng. Chiến lược này có thể giúp giữ cho các dịch vụ quan trọng hoạt động.

■ Tắt dịch vụ: Trong chiến lược này, tất cả các dịch vụ sẽ bị tắt cho đến khi cuộc tấn công lắng xuống. Mặc dù nó có thể không phải là sự lựa chọn lý tưởng, nhưng nó có thể là một phản ứng hợp lý trong một số trường hợp.

Các biện pháp đối phó tấn công DDoS

Nhiều giải pháp đã được đề xuất để giảm thiểu tác động của một cuộc tấn công DDoS. Tuy nhiên, không có giải pháp hoàn chỉnh duy nhất nào có thể bảo vệ tất cả các dạng tấn công DDoS đã biết. Hơn nữa, những kẻ tấn công liên tục nghĩ ra các phương pháp mới để thực hiện các cuộc tấn công DDoS nhằm vượt qua các giải pháp bảo mật được sử dụng.

Sau đây là các ví dụ về các biện pháp đối phó với cuộc tấn công DDoS:

• Bảo vệ nạn nhân thứ cấp

• Vô hiệu hóa các trình xử lý

• Làm chệch hướng các cuộc tấn công

• Giảm thiểu các cuộc tấn công

• Ngăn chặn các cuộc tấn công tiềm ẩn

pháp y sau cuộc tấn công

Câu hỏi và bài tập

1. Tấn công mạng không dây và thiết bị di động
   1. Khái niệm cơ bản
      1. Mạng ko dây

Mạng không dây sử dụng truyền sóng vô tuyến, thường xảy ra ở lớp vật lý của cấu trúc mạng. Với cuộc cách mạng truyền thông không dây toàn cầu, mạng dữ liệu và viễn thông đang thay đổi về cơ bản. Wi-Fi đề cập đến một mạng WLAN dựa trên tiêu chuẩn IEEE 802.11 và nó cho phép một thiết bị truy cập mạng từ bất kỳ đâu trong phạm vi của một AP. Wi-Fi là một công nghệ được sử dụng rộng rãi trong giao tiếp không dây qua kênh radio. Wi-Fi sử dụng nhiều kỹ thuật như DSSS, FHSS, hồng ngoại (IR) và OFDM để thiết lập kết nối giữa bộ phát và bộ thu. Các thiết bị như máy tính cá nhân, máy chơi trò chơi điện tử và điện thoại thông minh sử dụng Wi-Fi để kết nối với tài nguyên mạng như Internet thông qua mạng không dây AP.

Sau đây là một số ưu điểm và nhược điểm của mạng không dây:

■ Ưu điểm

o Lắp đặt nhanh chóng và dễ dàng không cần đi dây xuyên tường và trần nhà

o Dễ dàng cung cấp kết nối ở những khu vực khó đặt cáp

o Mạng có thể được truy cập từ mọi nơi trong phạm vi của một AP

o Các không gian công cộng như sân bay, thư viện, trường học và thậm chí cả quán cà phê cung cấp kết nối Internet liên tục thông qua mạng WLAN

■ Nhược điểm

o An ninh có thể không đáp ứng mong đợi

o Băng thông bị ảnh hưởng khi số lượng thiết bị trong mạng tăng lên

o Nâng cấp Wi-Fi có thể yêu cầu thẻ không dây và/hoặc AP mới

Một số thiết bị điện tử có thể can thiệp vào mạng Wi-Fi

Các loại mạng không dây

Các loại mạng không dây khác nhau được mô tả như sau.

• Mở rộng mạng có dây

Người dùng có thể mở rộng mạng có dây bằng cách đặt các AP giữa mạng có dây và các thiết bị không dây. Một mạng không dây cũng có thể được tạo bằng AP.

Các loại AP bao gồm:

o Phần mềm APS (SAPS): SAP có thể được kết nối với mạng có dây và chúng chạy trên máy tính được trang bị thẻ giao diện mạng không dây (NIC).

o APS phần cứng (HAPS): HAPS hỗ trợ hầu hết các tính năng không dây.

Trong loại mạng này, AP hoạt động như một bộ chuyển mạch, cung cấp kết nối cho các máy tính sử dụng NIC không dây. AP có thể kết nối các máy khách không dây với mạng LAN có dây, cho phép truy cập không dây vào các tài nguyên LAN như máy chủ tệp và kết nối Internet.

Nhiều điểm truy cập

Loại mạng này kết nối không dây các máy tính sử dụng nhiều AP. Nếu một AP duy nhất không thể bao phủ một khu vực, thì có thể thiết lập nhiều AP hoặc điểm mở rộng.

Khu vực không dây của mỗi AP phải chồng lên khu vực của hàng xóm. Điều này cung cấp cho người dùng khả năng di chuyển liền mạch bằng cách sử dụng một tính năng gọi là chuyển vùng. Một số nhà sản xuất phát triển các điểm mở rộng hoạt động như rơle không dây, mở rộng phạm vi của một AP. Nhiều điểm mở rộng có thể được xâu chuỗi lại với nhau để cung cấp khả năng truy cập không dây đến các địa điểm cách xa AP trung tâm.

• Mạng không dây LAN-to-LAN

AP cung cấp kết nối không dây cho các máy tính cục bộ và các máy tính cục bộ trên các mạng khác nhau có thể được kết nối với nhau. Tất cả các AP phần cứng đều có khả năng kết nối với các AP phần cứng khác. Tuy nhiên, kết nối mạng LAN qua kết nối không dây là một nhiệm vụ phức tạp.

Điểm truy cập 3G/4G

Điểm phát sóng 3G/4G là một loại mạng không dây cung cấp khả năng truy cập Wi-Fi cho các thiết bị hỗ trợ Wi-Fi, bao gồm máy nghe nhạc MP3, máy tính xách tay, máy tính bảng, máy ảnh, PDA, netbook, v.v.

* 1. Cơ chế an toàn mạng không dây

Mã hóa không dây là một quá trình bảo vệ mạng không dây khỏi những kẻ tấn công cố gắng thu thập thông tin nhạy cảm bằng cách vi phạm lưu lượng RF. Phần này cung cấp thông tin chi tiết về các tiêu chuẩn mã hóa không dây khác nhau, chẳng hạn như Quyền riêng tư tương đương có dây (WEP), Truy cập được bảo vệ bằng Wi-Fi (WPA), WPA2 và WPA3, ngoài các sự cố trong WEP, WPA và WPA2.

Các loại mã hóa không dây

Các cuộc tấn công vào mạng không dây đang gia tăng hàng ngày với việc sử dụng mạng không dây ngày càng nhiều.

Việc mã hóa thông tin trước khi truyền trên mạng không dây là

phương pháp phổ biến để bảo vệ mạng không dây chống lại những kẻ tấn công. Có một số loại

các thuật toán mã hóa không dây có thể bảo mật mạng không dây. Mỗi mã hóa không dây

thuật toán có ưu điểm và nhược điểm.

⚫ 802.11i: Đây là bản sửa đổi của IEEE chỉ định cơ chế bảo mật cho mạng không dây 802.11.

• WEP: WEP là thuật toán mã hóa cho mạng không dây IEEE 802.11. Nó là một tiêu chuẩn bảo mật không dây cũ và có thể bị bẻ khóa dễ dàng. EAP: Giao thức xác thực mở rộng (EAP) hỗ trợ nhiều xác thực

các phương thức, chẳng hạn như thẻ mã thông báo, Kerberos và chứng chỉ.

LEAP: EAP nhẹ (LEAP) là phiên bản độc quyền của EAP do Cisco phát triển.

WPA: Đây là một giao thức mã hóa không dây tiên tiến sử dụng TKIP và Kiểm tra tính toàn vẹn của tin nhắn (MIC) để cung cấp khả năng mã hóa và xác thực mạnh mẽ. Nó sử dụng vectơ khởi tạo 48 bit (IV), kiểm tra dự phòng theo chu kỳ 32 bit (CRC) và mã hóa TKIP để bảo mật không dây.

•TKIP: Đây là một giao thức bảo mật được sử dụng trong WPA để thay thế cho WEP.

• WPA2: Đây là bản nâng cấp lên WPA bằng cách sử dụng AES và Giao thức mã xác thực thông báo chuỗi khối mã hóa chế độ truy cập (CCMP) để mã hóa dữ liệu không dây.

• AES: Đây là mã hóa khóa đối xứng được sử dụng trong WPA2 để thay thế cho TKIP.

CCMP: Đây là một giao thức mã hóa được sử dụng trong WPA2 để mã hóa và xác thực mạnh mẽ.

• WPA2 Enterprise: Nó tích hợp các tiêu chuẩn EAP với mã hóa WPA2.

RADIUS: Đây là một hệ thống quản lý ủy quyền và xác thực tập trung.

PEAP: Đây là một giao thức đóng gói EAP trong một đường hầm Bảo mật tầng vận chuyển (TLS) được mã hóa và xác thực.

WPA3: Đây là giao thức bảo mật Wi-Fi thế hệ thứ ba cung cấp các tính năng mới cho mục đích sử dụng cá nhân và doanh nghiệp. Nó sử dụng Galois/Counter Mode-256 (GCMP-256) để mã hóa và mã xác thực thông báo băm 384-bit với Thuật toán băm an toàn (HMAC-SHA-384) để xác thực.

* 1. Phương pháp tấn công mạng không dây

Để hack mạng không dây, kẻ tấn công tuân theo phương pháp hack bao gồm các bước có hệ thống để thực hiện một cuộc tấn công thành công vào mạng không dây mục tiêu. Phần này giải thích các bước của phương pháp hack không dây.

Phương pháp hack không dây giúp kẻ tấn công đạt được mục tiêu hack mạng không dây mục tiêu. Kẻ tấn công thường tuân theo một phương pháp tấn công để chắc chắn tìm thấy mọi điểm vào đơn lẻ để đột nhập vào mạng mục tiêu.

Mục tiêu của phương pháp hack không dây là xâm phạm mạng Wi-Fi để có quyền truy cập trái phép vào tài nguyên mạng. Những kẻ tấn công sử dụng các bước sau để thực hiện hack không dây:

• Phát hiện Wi-Fi

Bước đầu tiên là tìm mạng Wi-Fi hoặc thiết bị. Kẻ tấn công thực hiện khám phá Wi-Fi để xác định vị trí mạng không dây mục tiêu bằng cách sử dụng các công cụ như inSSIDer Plus, NetSurveyor, v.v. Các quy trình khám phá Wi-Fi bao gồm theo dõi mạng không dây và tìm mạng mục tiêu thích hợp nằm trong phạm vi để khởi chạy một cuộc tấn công.

Dấu chân mạng không dây

Một cuộc tấn công vào mạng không dây bắt đầu bằng việc phát hiện và theo dấu vết của nó. Dấu chân liên quan đến việc định vị và phân tích (hoặc hiểu) mạng. Để đánh dấu một mạng không dây, kẻ tấn công cần xác định BSS do AP cung cấp. Kẻ tấn công có thể xác định BSS hoặc BSS độc lập (IBSS) với sự trợ giúp của SSID của mạng không dây. Do đó, kẻ tấn công cần xác định SSID của mạng không dây mục tiêu, SSID này có thể được sử dụng để thiết lập liên kết với AP nhằm xâm phạm bảo mật của nó.

Tìm mạng Wi-Fi trong phạm vi để tấn công

Nhiệm vụ đầu tiên của kẻ tấn công khi tìm kiếm các mục tiêu Wi-Fi là kiểm tra các mạng tiềm năng trong phạm vi để tìm ra mạng tốt nhất để tấn công. Những kẻ tấn công sử dụng các kỹ thuật tạo phấn Wi-Fi khác nhau như WarWalking, WarChalking, WarFlying và WarDriving để tìm mạng Wi-Fi mục tiêu.

• Kỹ thuật đánh phấn Wi-Fi

o WarWalking: Kẻ tấn công đi vòng quanh với máy tính xách tay hỗ trợ Wi-Fi được cài đặt công cụ khám phá không dây để vạch ra các mạng không dây mở.

• WarChalking: Các biểu tượng được vẽ ở những nơi công cộng để quảng cáo các mạng Wi-Fi mở.

o WarFlying: Kẻ tấn công sử dụng máy bay không người lái để phát hiện các mạng không dây mở.

o WarDriving: Kẻ tấn công lái xe xung quanh với máy tính xách tay hỗ trợ Wi-Fi được cài đặt công cụ khám phá không dây để vạch ra các mạng không dây mở.

Tìm APS hỗ trợ WPS

Những kẻ tấn công sử dụng tiện ích dòng lệnh Wash để xác định các AP hỗ trợ WPS trong mạng không dây mục tiêu. Tiện ích này cũng giúp kẻ tấn công kiểm tra xem AP có ở trạng thái bị khóa hay không. Hầu hết các bộ định tuyến hỗ trợ WPS đều tự động bị khóa khi nhập thông tin xác thực không chính xác hơn 5 lần liên tiếp và chúng chỉ có thể được mở khóa trong giao diện quản trị viên của bộ định tuyến theo cách thủ công. Lệnh Wash hỗ trợ kênh 5 GHz và có thể được sử dụng bằng cách cài đặt gói Reaver.

■ Lập bản đồ GPS

Bước thứ hai trong phương pháp hack không dây là lập bản đồ GPS. Kẻ tấn công phát hiện ra mạng không dây mục tiêu có thể tiến hành tấn công mạng không dây bằng cách vẽ bản đồ của mạng. Trong bước này, kẻ tấn công có thể sử dụng nhiều công cụ tự động khác nhau để lập bản đồ mạng không dây mục tiêu.

Hệ thống Định vị Toàn cầu (GPS) là một hệ thống định vị vệ tinh trong không gian cung cấp vị trí của các thực thể vật lý trên Trái đất, cùng với thời gian chúng có mặt tại vị trí đó. Sử dụng tiện ích GPS, bất kỳ ai cũng có thể tìm thấy một vị trí cụ thể trên Trái đất và các đặc điểm địa lý của nó. Kẻ tấn công sử dụng tiện ích GPS này để định vị và lập bản đồ mạng không dây mục tiêu trong một khu vực địa lý cụ thể.

Máy thu GPS tính toán vị trí, thời gian và vận tốc bằng cách xử lý các tín hiệu vệ tinh được mã hóa cụ thể. Những kẻ tấn công biết rằng sự hiện diện của các mạng Wi-Fi miễn phí trong một khu vực có thể cho thấy sự tồn tại của một mạng không an toàn. Những kẻ tấn công thường tạo bản đồ của các mạng Wi-Fi được phát hiện và cơ sở dữ liệu với số liệu thống kê được thu thập bằng các công cụ phát hiện Wi-Fi như inSSIDer Office và NetSurveyor. GPS rất hữu ích trong việc theo dõi vị trí của các mạng Wi-Fi được phát hiện và tọa độ được tải lên các trang web như WIGLE. Những kẻ tấn công có thể chia sẻ thông tin đó với cộng đồng hack hoặc bán nó để kiếm lời.

• Phân tích lưu lượng không dây

Bước thứ ba trong phương pháp hack không dây là phân tích lưu lượng của mạng không dây được phát hiện. Kẻ tấn công thực hiện phân tích lưu lượng không dây trước khi tung ra các cuộc tấn công thực sự trên mạng không dây. Phân tích này giúp kẻ tấn công xác định các lỗ hổng và nạn nhân dễ mắc phải trong mạng mục tiêu cũng như chiến lược thích hợp để tấn công thành công. Kẻ tấn công sử dụng các công cụ và kỹ thuật khác nhau để phân tích lưu lượng của mạng không dây mục tiêu.

Các giao thức Wi-Fi là duy nhất cho Lớp 2 và lưu lượng truy cập qua mạng không được tuần tự hóa, điều này giúp dễ dàng đánh hơi và phân tích các gói không dây. Kẻ tấn công phân tích mạng không dây để xác định SSID được phát, sự hiện diện của nhiều AP, khả năng khôi phục SSID, phương thức xác thực được sử dụng, thuật toán mã hóa mạng WLAN, v.v.. Kẻ tấn công sử dụng các công cụ dò tìm gói Wi-Fi như AirMagnet WiFi Analyzer PRO, Wireshark, SteelCentral Packet Trình phân tích, Trình phân tích giao thức mạng OmniPeek và CommView cho Wi-Fi để nắm bắt và phân tích lưu lượng truy cập của mạng không dây mục tiêu.

• Khởi động các cuộc tấn công không dây

Sau khi hoàn thành việc phát hiện, lập bản đồ và phân tích mạng không dây của mạng không dây mục tiêu, kẻ tấn công sẽ có thể khởi động một cuộc tấn công vào mạng không dây mục tiêu. Kẻ tấn công có thể khởi chạy nhiều kiểu tấn công khác nhau như tấn công phân mảnh, tấn công giả mạo MAC, tấn công DoS và tấn công đầu độc Giao thức phân giải địa chỉ (ARP). Phần này mô tả các cuộc tấn công không dây và cách chúng được thực hiện.

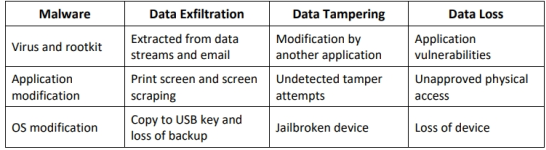
• Bẻ khóa mã hóa Wi-Fi

Sau khi kẻ tấn công thành công trong việc giành được quyền truy cập trái phép vào mạng mục tiêu thông qua các phương pháp như tấn công không dây, AP lừa đảo và cặp song sinh độc ác, kẻ tấn công phải bẻ khóa bảo mật do mạng không dây mục tiêu áp đặt. Nói chung, để bảo mật liên lạc không dây, mạng Wi-Fi sử dụng mã hóa WEP hoặc WPA/WPA2 mà kẻ tấn công phải bẻ khóa. Trong phần này, chúng ta xem xét cách kẻ tấn công có thể bẻ khóa các hệ thống mã hóa này để vi phạm an ninh mạng không dây.

• Mạng Wi-Fi bị ảnh hưởng

* 1. Tấn công thiết bị di động

Các thiết bị di động đã thu hút sự chú ý của những kẻ tấn công do chúng được sử dụng rộng rãi. Những thiết bị như vậy truy cập nhiều tài nguyên mà máy tính truyền thống sử dụng. Hơn nữa, các thiết bị này có một số tính năng độc đáo đã dẫn đến sự xuất hiện của các giao thức và vectơ tấn công mới. Các vectơ như vậy làm cho các nền tảng điện thoại di động dễ bị tấn công nguy hiểm cả từ mạng và khi bị xâm phạm vật lý. Đưa ra dưới đây là một số vectơ tấn công cho phép kẻ tấn công khai thác các lỗ hổng trong hệ điều hành di động, phần sụn thiết bị hoặc ứng dụng di động.



Phần mềm độc hại

Virus và rootkit

sửa đổi

ứng dụng

sửa đổi hệ điều hành

Lọc dữ liệu

Trích xuất từ ​​các

luồng dữ liệu và email

In màn hình và cạo

màn hình

Sao chép vào khóa USB và

mất bản sao lưu

Giả mạo dữ liệu

Sửa đổi bởi

ứng dụng khác

Nỗ lực giả mạo không bị

phát hiện

thiết bị đã bẻ khóa

Mất dữ liệu

lỗ hổng

ứng dụng

Truy cập vật lý không được

chấp thuận

Mất thiết bị

* 1. Giải pháp phòng chống
     1. Phòng chống ko dây

**Chống bẻ khóa WPA/WPA2/WPA3**

• Cụm mật khẩu

Cách duy nhất để bẻ khóa WPA là đánh hơi mật khẩu PMK được liên kết với quy trình xác thực "bắt tay". Nếu mật khẩu này cực kỳ phức tạp, nó sẽ gần như không thể bẻ khóa. Các biện pháp sau đây có thể được áp dụng để bảo mật mật khẩu.

o Chọn một cụm mật khẩu ngẫu nhiên không được tạo thành từ các từ trong từ điển.

o Chọn một cụm mật khẩu phức tạp có độ dài tối thiểu 20 ký tự và thay đổi cụm mật khẩu đó theo định kỳ.

o Sử dụng các từ diceware hoặc trình quản lý mật khẩu để bảo mật mật khẩu.

Cài đặt máy khách

o Chỉ sử dụng WPA2 với mã hóa AES/CCMP.

o Đặt cài đặt máy khách phù hợp (ví dụ: xác thực máy chủ, chỉ định địa chỉ máy chủ và không nhắc máy chủ mới).

o Tạo lại khóa cho mọi kết nối mới.

• Điều khiển bổ sung

o Đảm bảo cập nhật định kỳ chương trình cơ sở của thiết bị không dây.

o Sử dụng các công nghệ mạng riêng ảo (VPN) như VPN truy cập từ xa, VPN mạng bên ngoài và VPN mạng nội bộ.

o Triển khai các giao thức như IPSec và SSL/TLS để liên lạc an toàn

o Triển khai giải pháp kiểm soát truy cập mạng (NAC) hoặc bảo vệ truy cập mạng (NAP) để kiểm soát bổ sung đối với kết nối của người dùng cuối

o Triển khai giải pháp kiểm soát truy cập mạng (NAC) hoặc bảo vệ truy cập mạng (NAP) để kiểm soát bổ sung đối với kết nối của người dùng cuối

**Phòng thủ chống lại các cuộc tấn công KRACK**

Sau đây là một số biện pháp đối phó để ngăn chặn các cuộc tấn công KRACK.

• Cập nhật tất cả các bộ định tuyến và thiết bị Wi-Fi bằng các bản vá bảo mật mới nhất.

• Bật cập nhật tự động cho tất cả các thiết bị không dây và vá lỗi chương trình cơ sở của thiết bị.

• Tránh sử dụng mạng Wi-Fi công cộng.

• Chỉ duyệt các trang web được bảo mật và không truy cập các tài nguyên nhạy cảm khi thiết bị được kết nối với mạng không được bảo vệ.

• Nếu có thiết bị loT, hãy kiểm tra thiết bị và không kết nối với bộ định tuyến Wi-Fi không an toàn.

■ Luôn bật tiện ích mở rộng HTTPS Everywhere.

• Bật xác thực hai yếu tố.

• Sử dụng VPN để bảo mật thông tin khi truyền.

**Bảo vệ chống lại các cuộc tấn công THAY ĐỔI**

Phương pháp được đề xuất hàng đầu để bảo vệ mạng khỏi các cuộc tấn công của aLTEr là mã hóa các truy vấn DNS bằng các tiêu chuẩn bảo mật phù hợp. Để thực hiện biện pháp này, Cisco, phối hợp với Apple, đã phát triển một ứng dụng có tên "Cisco Security Connectors" ngăn khách hàng truy cập vào các trang web ngoài ý muốn. Ứng dụng này mã hóa các truy vấn DNS và tải chúng vào Cisco Umbrella (khối thông minh) để xác thực thêm. Nó bảo vệ mạng khỏi bị tấn công ở cấp độ IP cũng như cấp độ DNS. Các biện pháp đối phó sau đây có thể được áp dụng để chống lại các cuộc tấn công của aLTEr.

• Mã hóa các truy vấn DNS và chỉ sử dụng các trình phân giải DNS đáng tin cậy.

• Giải quyết các truy vấn DNS bằng giao thức HTTPS.

• Chỉ truy cập các trang web có kết nối HTTPS.

• Sử dụng DNS qua Bảo mật tầng vận chuyển (TLS) hoặc DNS qua datagram TLS (DTLS) để mã hóa lưu lượng DNS và để bảo vệ tính toàn vẹn.

• Triển khai RFC 7858/RFC 8310 để ngăn chặn các cuộc tấn công giả mạo DNS. Nó cũng có thể tăng các chính sách mã hóa và thông minh để phân giải tên.

• Thêm mã xác thực tin nhắn (MAC) vào các gói mặt phẳng người dùng.

• Sử dụng giao thức DNSCrypt để xác thực giao tiếp giữa máy khách DNS và trình phân giải DNS.

Sử dụng các công cụ dành cho thiết bị di động như Zimperium để phát hiện lừa đảo và các cuộc tấn công khác từ các trang web độc hại.

**Bảo vệ chống lại các cuộc tấn công không dây**

• Thực hành tốt nhất cho cấu hình

o Thay đổi SSID mặc định sau khi cấu hình mạng WLAN.

o Đặt mật khẩu truy cập bộ định tuyến và bật bảo vệ tường lửa.

o Tắt phát sóng SSID.

o Tắt đăng nhập bộ định tuyến từ xa và quản trị mạng không dây.

o Kích hoạt tính năng lọc địa chỉ MAC trên các AP hoặc bộ định tuyến.

o Kích hoạt mã hóa trên các AP và thay đổi cụm mật khẩu thường xuyên.

o Đóng tất cả các cổng không sử dụng để ngăn chặn các cuộc tấn công vào Aps.

Thực tiễn tốt nhất cho cài đặt SSID

o Sử dụng kỹ thuật che giấu SSID để ngăn một số tin nhắn không dây mặc định phát SSID cho mọi người.

Không sử dụng SSID, tên công ty, tên mạng hoặc bất kỳ chuỗi dễ đoán nào trong cụm mật khẩu. o Đặt tường lửa hoặc bộ lọc gói giữa AP và Mạng nội bộ của công ty.

o Giới hạn độ mạnh của mạng không dây để nó không thể bị phát hiện bên ngoài

giới hạn của tổ chức. o Thường xuyên kiểm tra các thiết bị không dây để biết các sự cố về cấu hình hoặc thiết lập.

o Thực hiện một kỹ thuật bổ sung để mã hóa lưu lượng, chẳng hạn như IPSec trên

không dây.

■ Thực hành tốt nhất để xác thực

o Chọn WPA2-Enterprise với xác thực 802.1x thay vì WPA hoặc WEP.

o Triển khai WPA2/WPA3-Enterprise bất cứ khi nào có thể.

o Tắt mạng khi không cần thiết.

o Đặt các AP không dây ở một vị trí an toàn.

o Luôn cập nhật trình điều khiển trên tất cả các thiết bị không dây. o Sử dụng máy chủ tập trung để xác thực.

o Cho phép xác minh máy chủ ở phía máy khách bằng cách sử dụng xác thực 802.1X để ngăn chặn các cuộc tấn công MITM.

o Kích hoạt xác thực hai yếu tố như một tuyến phòng thủ bổ sung.

o Triển khai hệ thống phát hiện/phát hiện rogue-AP hoặc hệ thống ngăn chặn/phát hiện xâm nhập không dây để ngăn chặn các cuộc tấn công không dây.

Câu hỏi và bài tập

1. Các dạng tấn công phổ biến khác
   1. Tấn công kỹ nghệ xã hội

**Kỹ thuật xã hội là gì?**

Trước khi thực hiện một cuộc tấn công kỹ thuật xã hội, kẻ tấn công thu thập thông tin về tổ chức mục tiêu từ nhiều nguồn khác nhau như:

Các trang web chính thức của tổ chức, nơi ID, tên và địa chỉ email của nhân viên được chia sẻ

Quảng cáo của tổ chức mục tiêu được truyền qua phương tiện truyền thông tiết lộ thông tin như sản phẩm và ưu đãi.

Blog, diễn đàn và các không gian trực tuyến khác nơi nhân viên chia sẻ thông tin cá nhân và tổ chức cơ bản.

Sau khi thu thập thông tin, kẻ tấn công thực hiện các cuộc tấn công kỹ thuật xã hội bằng nhiều cách tiếp cận khác nhau như mạo danh, cõng, điều chỉnh, kỹ thuật xã hội đảo ngược và các phương pháp khác.

Kỹ thuật xã hội là nghệ thuật thao túng mọi người để tiết lộ thông tin nhạy cảm để sử dụng nó để thực hiện một số hành động độc hại. Bất chấp các chính sách bảo mật, những kẻ tấn công có thể xâm phạm thông tin nhạy cảm của tổ chức bằng cách sử dụng kỹ thuật xã hội nhắm vào điểm yếu của con người. Thông thường, nhân viên thậm chí không nhận thức được lỗi bảo mật từ phía họ và vô tình tiết lộ thông tin quan trọng của tổ chức. Chẳng hạn, vô tình trả lời câu hỏi của người lạ hoặc trả lời thư rác.

Để thành công, những kẻ tấn công đặc biệt quan tâm đến việc phát triển các kỹ năng kỹ thuật xã hội và có thể thành thạo đến mức nạn nhân thậm chí có thể không nhận ra hành vi lừa đảo. Những kẻ tấn công luôn tìm kiếm những cách mới để truy cập thông tin. Họ cũng đảm bảo rằng họ biết phạm vi hoạt động của tổ chức và những người thuộc phạm vi hoạt động của tổ chức, chẳng hạn như nhân viên bảo vệ, nhân viên lễ tân và nhân viên bộ phận trợ giúp, để khai thác sự giám sát của con người. Mọi người đã tự rèn luyện bản thân để không quá nghi ngờ và họ liên kết các hành vi và ngoại hình cụ thể với các thực thể đã biết. Chẳng hạn, một người đàn ông mặc đồng phục mang một đống gói hàng đi giao sẽ được coi là người giao hàng. Với sự trợ giúp của các thủ thuật kỹ thuật xã hội, những kẻ tấn công thành công trong việc lấy thông tin bí mật, ủy quyền và truy cập thông tin chi tiết từ mọi người bằng cách đánh lừa và thao túng lỗ hổng của con người.

**Các giai đoạn của một cuộc tấn công kỹ thuật xã hội**

Những kẻ tấn công thực hiện các bước sau để thực hiện một cuộc tấn công kỹ thuật xã hội thành công:

• Nghiên cứu Công ty Mục tiêu

Trước khi tấn công mạng của tổ chức mục tiêu, kẻ tấn công thu thập đủ thông tin để xâm nhập vào hệ thống. Kỹ thuật xã hội là một kỹ thuật giúp trích xuất thông tin. Ban đầu, kẻ tấn công nghiên cứu thông tin cơ bản về tổ chức mục tiêu, chẳng hạn như bản chất của doanh nghiệp, vị trí, số lượng nhân viên và các sự kiện khác. Trong khi nghiên cứu, kẻ tấn công thực hiện các hoạt động như tìm kiếm thùng rác, duyệt trang web của công ty và tìm thông tin chi tiết về nhân viên.

• Chọn một Mục tiêu

Sau khi hoàn thành nghiên cứu, kẻ tấn công chọn mục tiêu để trích xuất thông tin nhạy cảm về tổ chức. Thông thường, những kẻ tấn công cố gắng tiếp cận những nhân viên bất mãn vì họ dễ thao túng hơn.

• Phát triển mối quan hệ

Khi mục tiêu được đặt ra, kẻ tấn công sẽ xây dựng mối quan hệ với nhân viên đó để hoàn thành nhiệm vụ của họ.

• Khai thác mối quan hệ

Kẻ tấn công khai thác mối quan hệ và trích xuất thông tin nhạy cảm về tài khoản, thông tin tài chính, công nghệ đang sử dụng và các kế hoạch sắp tới của tổ chức.

**Các loại kỹ thuật xã hội**

Trong một cuộc tấn công kỹ thuật xã hội, kẻ tấn công sử dụng các kỹ năng xã hội của họ để lừa nạn nhân

tiết lộ thông tin cá nhân như số thẻ tín dụng, số tài khoản ngân hàng và số điện thoại

số hoặc thông tin bí mật về tổ chức hoặc hệ thống máy tính của họ. kẻ tấn công

sử dụng dữ liệu này để khởi động một cuộc tấn công hoặc thực hiện hành vi gian lận. Các cuộc tấn công kỹ thuật xã hội là

được phân loại thành ba loại: dựa trên con người, dựa trên máy tính và dựa trên thiết bị di động.

• Kỹ thuật xã hội dựa trên con người

Kỹ thuật xã hội dựa trên con người liên quan đến sự tương tác của con người. Hành động như thể họ là một người hợp pháp, kẻ tấn công tương tác với nhân viên của tổ chức mục tiêu để thu thập thông tin nhạy cảm, chẳng hạn như kế hoạch kinh doanh và mạng, có thể giúp họ thực hiện cuộc tấn công. Ví dụ, mạo danh một kỹ thuật viên hỗ trợ CNTT, kẻ tấn công có thể dễ dàng truy cập vào phòng máy chủ.

Kẻ tấn công có thể thực hiện kỹ thuật xã hội dựa trên con người bằng cách sử dụng các kỹ thuật sau:

o Mạo danh

o Viếng thăm

o Nghe trộm

o Nối đuôi nhau

o Trộm cắp chuyển hướng

。 Lướt vai

o Lặn thùng rác

o Kỹ thuật xã hội đảo ngược

o Cõng

o Bẫy mật ong

o mồi nhử

。 Quid Pro Quo

o Khơi gợi

Kỹ thuật xã hội dựa trên máy tính

Kỹ thuật xã hội dựa trên máy tính dựa vào máy tính và hệ thống Internet để thực hiện hành động được nhắm mục tiêu.

Các kỹ thuật sau đây có thể được sử dụng cho kỹ thuật xã hội dựa trên máy tính:

o Lừa đảo

o Các cuộc tấn công cửa sổ bật lên

o Thư rác

o Đồ hù dọa

o Trình nhắn tin trò chuyện tức thì

Kỹ thuật xã hội dựa trên thiết bị di động

Những kẻ tấn công sử dụng các ứng dụng di động để thực hiện kỹ thuật xã hội dựa trên thiết bị di động. Những kẻ tấn công lừa người dùng bằng cách bắt chước các ứng dụng phổ biến và tạo các ứng dụng di động độc hại với các tính năng hấp dẫn và gửi chúng đến các cửa hàng ứng dụng lớn có cùng tên. Người dùng vô tình tải xuống ứng dụng độc hại, cho phép phần mềm độc hại lây nhiễm vào thiết bị của họ.

Dưới đây là một số kỹ thuật mà kẻ tấn công sử dụng để thực hiện kỹ thuật xã hội dựa trên thiết bị di động:

o Xuất bản ứng dụng độc hại

o Đóng gói lại các ứng dụng hợp pháp

。 Sử dụng các ứng dụng bảo mật giả mạo

。 SMishing (SMS Lừa đảo)

* 1. Tấn công điện toán đám mây

Điện toán đám mây là sự cung cấp các khả năng CNTT theo yêu cầu, trong đó cơ sở hạ tầng và ứng dụng CNTT được cung cấp cho người đăng ký dưới dạng dịch vụ đo lường qua mạng. Ví dụ về đám mây giải pháp bao gồm Gmail, Facebook. Dropbox và Salesforce.com.

**Hack đám mây là gì?**

Ngày nay, nhiều tổ chức đang di chuyển các quy trình kinh doanh và dữ liệu khách hàng của họ lên đám mây. Việc di chuyển ồ ạt dữ liệu cá nhân và công ty lên đám mây đã làm gia tăng các bề mặt tấn công và các mối đe dọa đối với cả tổ chức và cá nhân. Những kẻ tấn công khai thác các lỗ hổng hiện có trong công nghệ đám mây để thực hiện các cuộc tấn công cấu hình cao được nhắm mục tiêu khác nhau trên hệ thống lưu trữ đám mây, làm tổn hại dữ liệu của khách hàng và công ty. Mục tiêu chính của việc hack môi trường đám mây là giành quyền truy cập vào dữ liệu người dùng và chặn quyền truy cập vào các dịch vụ đám mây. Điều này có tác động tai hại đối với cả người dùng cuối và các công ty doanh nghiệp, phá vỡ niềm tin vào tính bảo mật của các dịch vụ đám mây. Do đó, các tổ chức cần đảm bảo an toàn và bảo mật cho các quy trình kinh doanh và thông tin khách hàng được lưu trữ trên đám mây.

Quét lỗ hổng Kubernetes bằng Sysdig

Quét lỗ hổng vùng chứa bằng Trivy

Liệt kê các nhóm S3

Xác định các nhóm S3 mở bằng S3Scanner

Liệt kê Kubernetes, v.v.

Liệt kê ID tài khoản AWS

Liệt kê vai trò IAM

Liệt kê các quyền nhóm bằng S3Inspector

Khai thác cơ sở hạ tầng đám mây của Amazon bằng Nimbostratus

Xâm phạm AWS IAM Trust

Chiếm vai trò IAM bị định cấu hình sai

Bẻ khóa khóa truy cập AWS bằng DumpsterDiver

Khai thác Docker Container trên AWS bằng Cloud Container Attack Tool (CCAT)

Khai thác Docker Remote API

Hack khối lượng container

CloudGoat AWS - Dễ bị tổn thương theo thiết kế

Giành quyền truy cập bằng cách khai thác lỗ hổng SSRF

Kỹ thuật nâng cấp đặc quyền AWS IAM

Nâng cao đặc quyền của Goo GCPBucketBrute

Backdooring Docker Images sử dụng dockerscan

Duy trì quyền truy cập và theo dõi trên môi trường đám mây AWS bằng cách điều khiển dịch vụ CloudTrial

* 1. Tấn công lên hệ thống IoT

**IoT là gì?**

Internet of Things (IoT), còn được gọi là Internet of Everything (loE), dùng để chỉ các thiết bị điện toán hỗ trợ web và có khả năng cảm nhận, thu thập và gửi dữ liệu bằng các cảm biến cũng như phần cứng và bộ xử lý giao tiếp mà được nhúng trong thiết bị. Trong IoT, một "thứ" dùng để chỉ một thiết bị được cấy vào một vật thể tự nhiên, nhân tạo hoặc máy móc và có chức năng giao tiếp qua mạng. LoT sử dụng công nghệ mới nổi hiện có để cảm biến, kết nối mạng và rô-bốt, do đó cho phép người dùng đạt được phân tích sâu hơn, tự động hóa và tích hợp trong một hệ thống.

Với sự gia tăng khả năng kết nối mạng của máy móc và thiết bị hàng ngày được sử dụng trong các lĩnh vực khác nhau như văn phòng, gia đình, công nghiệp, giao thông, tòa nhà và thiết bị đeo được, chúng mở ra một thế giới cơ hội để cải thiện doanh nghiệp và sự hài lòng của khách hàng. Một số tính năng chính của lô là kết nối, cảm biến, trí tuệ nhân tạo, thiết bị nhỏ và sự tham gia tích cực.

**Sau đây là các giai đoạn khác nhau trong việc hack một thiết bị IoT:**

Thu thập thông tin

Bước đầu tiên và quan trọng nhất trong hack thiết bị loT là trích xuất thông tin như địa chỉ IP, giao thức được sử dụng (Zigbee, BLE, 5G, IPv6LOWPAN, v.v.), cổng mở, loại thiết bị, vị trí địa lý của thiết bị, số sản xuất, và công ty sản xuất của một thiết bị. Trong bước này, kẻ tấn công cũng xác định thiết kế phần cứng, cơ sở hạ tầng của nó và các thành phần chính được nhúng trong thiết bị mục tiêu có mặt trực tuyến. Những kẻ tấn công sử dụng các công cụ như Shodan, Censys và Thingful để thực hiện thu thập hoặc do thám thông tin trên thiết bị mục tiêu. Các thiết bị không khả dụng trong mạng nhưng nằm trong khu vực giao tiếp cũng có thể được phát hiện bằng cách sử dụng các trình nghe trộm như Foren6, Suphacap, CloudShark và Wireshark.

Quét lỗ hổng

Sau khi những kẻ tấn công thu thập thông tin về thiết bị mục tiêu, chúng sẽ tìm kiếm các bề mặt tấn công của thiết bị (xác định các lỗ hổng) mà chúng có thể tấn công. Tính năng quét lỗ hổng cho phép kẻ tấn công tìm thấy tổng số lỗ hổng có trong phần sụn, cơ sở hạ tầng và các thành phần hệ thống của thiết bị loT có thể truy cập được. Sau khi xác định khu vực bề mặt tấn công, kẻ tấn công sẽ quét các lỗ hổng trong khu vực đó để xác định vectơ tấn công và thực hiện khai thác tiếp trên thiết bị.

Tính năng quét lỗ hổng giúp kẻ tấn công xác định các thiết bị loT có cấu hình yếu như khai thác ẩn, lỗi chương trình cơ sở, cài đặt và mật khẩu yếu cũng như thông tin liên lạc được mã hóa kém. Ngược lại, nó cũng hỗ trợ các chuyên gia bảo mật trong việc bảo mật các thiết bị loT trong mạng bằng cách xác định các lỗ hổng hoặc lỗ hổng bảo mật trong các cơ chế bảo mật hiện tại trước khi kẻ tấn công có thể khai thác chúng.

• Khởi động các cuộc tấn công

Trong giai đoạn quét lỗ hổng, kẻ tấn công cố gắng xác định các lỗ hổng có trong thiết bị mục tiêu. Các lỗ hổng được tìm thấy sau đó được khai thác thêm để khởi động các cuộc tấn công khác nhau như tấn công DDoS, tấn công mã cuộn, tấn công gây nhiễu tín hiệu, tấn công Sybil, tấn công MITM và tấn công đánh cắp dữ liệu và danh tính. Ví dụ: kẻ tấn công có thể sử dụng công cụ RFCrack để thực hiện tấn công mã cuộn, tấn công phát lại và tấn công gây nhiễu trên thiết bị. Tương tự, kẻ tấn công cũng có thể sử dụng các công cụ như KillerBee để tấn công mạng ZigBee và IEEE 802.15.4.

■Nhận quyền truy cập từ xa

Các lỗ hổng được xác định trong giai đoạn quét lỗ hổng cho phép kẻ tấn công giành quyền truy cập từ xa, ra lệnh và kiểm soát cuộc tấn công trong khi tránh bị các sản phẩm bảo mật khác nhau phát hiện. Dựa trên các lỗ hổng trong thiết bị loT, kẻ tấn công có thể biến thiết bị thành cửa hậu để giành quyền truy cập vào mạng của tổ chức mà không lây nhiễm bất kỳ hệ thống đầu cuối nào được bảo vệ bởi IDS/IPS, tường lửa, phần mềm chống vi-rút, v.v. Sau khi giành được quyền truy cập từ xa, kẻ tấn công sử dụng các thiết bị này làm nền tảng để khởi động các cuộc tấn công vào các thiết bị khác trong mạng.

• Duy trì quyền truy cập

Khi kẻ tấn công giành được quyền truy cập vào thiết bị, kẻ tấn công sẽ sử dụng các kỹ thuật khác nhau để duy trì quyền truy cập và thực hiện khai thác thêm. Những kẻ tấn công vẫn không bị phát hiện bằng cách xóa nhật ký, cập nhật chương trình cơ sở và sử dụng các chương trình độc hại như backdoor, trojan, v.v. để duy trì quyền truy cập. Những kẻ tấn công sử dụng các công cụ như Firmware Mod Kit, Firmwalker, Firmalyzer Enterprise và Firmware Analysis Toolkit để khai thác firmware.

* 1. Giải pháp phòng chống
     1. Biện pháp đối phó kỹ thuật xã hội

Những kẻ tấn công thực hiện các kỹ thuật tấn công xã hội để lừa mọi người tiết lộ thông tin bí mật của tổ chức. Họ sử dụng kỹ thuật xã hội để thực hiện gian lận, đánh cắp danh tính, gián điệp công nghiệp và các hành vi gây tai tiếng khác. Để bảo vệ chống lại các cuộc tấn công kỹ thuật xã hội, các tổ chức phải phát triển các chính sách và thủ tục hiệu quả; tuy nhiên, chỉ phát triển chúng thôi là chưa đủ.

Để thực sự hiệu quả, một tổ chức nên:

• Phổ biến chính sách cho nhân viên và cung cấp giáo dục và đào tạo phù hợp. Đào tạo chuyên biệt mang lại lợi ích cho nhân viên ở các vị trí có rủi ro cao hơn trước các mối đe dọa kỹ thuật xã hội.

Có được chữ ký của nhân viên trên một tuyên bố xác nhận rằng họ hiểu các chính sách của tổ chức.

• Xác định hậu quả của việc vi phạm chính sách.

Mục tiêu chính của các chiến lược phòng thủ kỹ thuật xã hội là tạo ra nhận thức của người dùng, kiểm soát mạng nội bộ mạnh mẽ và các chính sách, kế hoạch và quy trình bảo mật.

Các thủ tục và chính sách bảo mật chính thức giúp nhân viên hoặc người dùng thực hiện bảo mật phù hợp

các quyết định. Chúng nên bao gồm các biện pháp bảo vệ sau:

■ Chính sách mật khẩu

Chính sách mật khẩu nêu rõ các nguyên tắc sau giúp tăng cường bảo mật mật khẩu:

o Thay đổi mật khẩu thường xuyên.

o Tránh mật khẩu dễ đoán. Có thể đoán mật khẩu từ câu trả lời cho các câu hỏi kỹ thuật xã hội, chẳng hạn như "Bạn sinh ra ở đâu?" "Bộ phim yêu thích của bạn là gì?" hoặc "Tên thú cưng của bạn là gì?"

o Chặn tài khoản người dùng nếu người dùng vượt quá một số lần thử đoán mật khẩu không thành công.

o Chọn mật khẩu dài (tối thiểu 6 8 ký tự) và phức tạp (sử dụng nhiều chữ và số và ký tự đặc biệt).

o Không tiết lộ mật khẩu cho bất kỳ ai.

Chính sách bảo mật mật khẩu thường bao gồm lời khuyên về quản lý mật khẩu thích hợp, ví dụ:

o Tránh dùng chung tài khoản máy tính.

o Tránh sử dụng cùng một mật khẩu cho các tài khoản khác nhau.

o Tránh lưu trữ mật khẩu trên phương tiện hoặc viết chúng ra giấy ghi chú hoặc ghi chú dán.

o Tránh trao đổi mật khẩu qua điện thoại hoặc qua email hoặc tin nhắn SMS.

o Đảm bảo khóa hoặc tắt máy tính trước khi rời khỏi máy tính.

Chính sách bảo mật vật lý

Chính sách bảo mật vật lý giải quyết các lĩnh vực sau.

o Cấp thẻ nhận dạng (thẻ ID) và đồng phục cùng với các biện pháp kiểm soát ra vào khác cho nhân viên của tổ chức.

An ninh hoặc nhân viên văn phòng phải hộ tống khách đến phòng dành cho khách hoặc phòng chờ được chỉ định.

o Hạn chế quyền truy cập vào các khu vực nhất định của tổ chức để ngăn người dùng trái phép

từ việc xâm phạm tính bảo mật của dữ liệu nhạy cảm.

o Vứt bỏ các tài liệu cũ có chứa thông tin có giá trị bằng cách sử dụng các thiết bị như máy hủy giấy và thùng đốt. Điều này ngăn chặn việc thu thập thông tin của những kẻ tấn công bằng các kỹ thuật như Dumpster Dive.

o Sử dụng nhân viên an ninh trong một tổ chức để bảo vệ con người và tài sản, bổ sung nhân viên an ninh được đào tạo với hệ thống báo động, camera giám sát và các thiết bị khác.

Chiến lược phòng thủ

o Chiến dịch Kỹ thuật Xã hội: Một tổ chức nên tiến hành nhiều hoạt động kỹ thuật xã hội bằng cách sử dụng các kỹ thuật khác nhau trên một nhóm người khác nhau để kiểm tra cách nhân viên của mình có thể phản ứng với các cuộc tấn công kỹ thuật xã hội thực sự.

o Phân tích khoảng cách: Sử dụng thông tin thu được từ chiến dịch kỹ thuật xã hội, phân tích khoảng cách đánh giá tổ chức dựa trên các thông lệ hàng đầu trong ngành, các mối đe dọa mới nổi và chiến lược giảm thiểu.

o Chiến lược khắc phục: Tùy thuộc vào kết quả đánh giá trong phân tích lỗ hổng, các tổ chức xây dựng kế hoạch khắc phục chi tiết để giảm thiểu các điểm yếu hoặc sơ hở được tìm thấy trong bước trước đó. Kế hoạch tập trung chủ yếu vào việc giáo dục và nâng cao nhận thức của nhân viên dựa trên vai trò của họ, đồng thời xác định và giảm thiểu các mối đe dọa tiềm ẩn đối với tổ chức.

Một số biện pháp đối phó bổ sung chống lại kỹ thuật xã hội như sau:

■ Đào tạo các cá nhân về chính sách bảo mật: Một chương trình đào tạo hiệu quả bao gồm các khái niệm và kỹ thuật tấn công xã hội cơ bản, tất cả các chính sách bảo mật và các phương pháp để nâng cao nhận thức về tấn công mạng xã hội.

■ Triển khai Đặc quyền Truy cập Thích hợp: Cần có tài khoản quản trị viên, người dùng và khách với các cấp độ ủy quyền tương ứng.

■ Sự hiện diện của Thời gian Ứng phó Sự cố Thích hợp: Cần có các hướng dẫn thích hợp cho

phản ứng với một nỗ lực kỹ thuật xã hội.

■ Tài nguyên chỉ dành cho người dùng được ủy quyền: Đảm bảo thông tin nhạy cảm được bảo mật và tài nguyên chỉ được truy cập bởi người dùng được ủy quyền

■ Xem xét kỹ lưỡng thông tin: Phân loại thông tin là tuyệt mật, độc quyền, chỉ sử dụng nội bộ và sử dụng công khai hoặc sử dụng các danh mục khác.

■ Thực hiện Kiểm tra Lý lịch và Quy trình Chấm dứt Thích hợp: Người trong cuộc với tội phạm

lý lịch và nhân viên bị thôi việc là những mục tiêu dễ dàng để thu thập thông tin.

■ Bảo vệ chống vi-rút và chống lừa đảo: Sử dụng nhiều lớp bảo vệ chống vi-rút ở cấp độ người dùng cuối và cổng thư để giảm thiểu các cuộc tấn công kỹ thuật xã hội.

Triển khai xác thực hai yếu tố: Thay vì mật khẩu cố định, hãy sử dụng xác thực hai yếu tố cho các dịch vụ mạng có rủi ro cao như VPN và nhóm modem. Trong phương pháp xác thực hai yếu tố (TFA), người dùng phải xuất trình hai hình thức chứng minh danh tính khác nhau. Nếu kẻ tấn công đang cố xâm nhập vào tài khoản người dùng, thì họ cần phá vỡ cả hai dạng nhận dạng người dùng, điều này khó thực hiện hơn. Do đó, TFA là một cơ chế bảo mật chuyên sâu về phòng thủ và là một phần của họ xác thực đa yếu tố. Hai bằng chứng mà người dùng cung cấp có thể bao gồm một mã thông báo vật lý chẳng hạn như thẻ và thường là thứ mà người đó có thể nhớ mà không cần nỗ lực nhiều, chẳng hạn như mã bảo mật, mã PIN hoặc mật khẩu.

■ Áp dụng Quản lý Thay đổi được Lập thành Văn bản: Quy trình quản lý thay đổi được lập thành văn bản sẽ an toàn hơn quy trình đặc biệt.

■ Đảm bảo cập nhật phần mềm thường xuyên: Các tổ chức nên đảm bảo rằng hệ thống và phần mềm thường xuyên được vá lỗi và cập nhật khi những kẻ tấn công khai thác phần mềm chưa được vá lỗi và lỗi thời để lấy thông tin hữu ích nhằm khởi động một cuộc tấn công.

* + 1. Cách phòng chống hack IoT

• Vô hiệu hóa tài khoản người dùng "khách" và "thử nghiệm" nếu được bật

• Sử dụng tính năng "Khóa" để khóa tài khoản đối với những lần đăng nhập không hợp lệ quá mức

Triển khai cơ chế xác thực mạnh mẽ

• Xác định vị trí các mạng và thiết bị của hệ thống điều khiển phía sau tường lửa và cách ly chúng khỏi mạng doanh nghiệp

■ Triển khai IPS và IDS trong mạng

• Triển khai mã hóa đầu cuối và sử dụng cơ sở hạ tầng khóa công khai (PKI)

• Sử dụng kiến trúc VPN để liên lạc an toàn

•

Triển khai bảo mật như một hệ thống thống nhất, tích hợp

■ Chỉ cho phép các địa chỉ IP đáng tin cậy truy cập thiết bị từ Internet

• Tắt telnet (cổng 23)

• Vô hiệu hóa cổng UPnP trên bộ định tuyến

• Bảo vệ thiết bị chống giả mạo vật lý

■ Vá lỗ hổng và cập nhật firmware thiết bị thường xuyên

■ Giám sát lưu lượng truy cập trên cổng 48101, vì các thiết bị bị nhiễm cố gắng phát tán tệp độc hại bằng cổng 48101

• Vị trí của các nút di động phải được xác minh với mục đích chỉ một nút vật lý có một nhận dạng phương tiện, điều đó có nghĩa là một phương tiện không thể có hai hoặc nhiều nhận dạng

• Bảo mật dữ liệu nên được thực hiện; do đó, tài khoản hoặc danh tính của người dùng phải được bảo vệ và ẩn khỏi những người dùng khác

• Xác thực dữ liệu nên được thực hiện để xác nhận danh tính của nguồn ban đầu

nút

• Duy trì tính bảo mật của dữ liệu bằng cách sử dụng mã hóa khóa đối xứng Thực hiện chính sách mật khẩu mạnh yêu cầu mật khẩu dài ít nhất 8-10 ký tự

với sự kết hợp của các chữ cái, số và ký tự đặc biệt • Sử dụng CAPTCHA và các phương pháp chính sách khóa tài khoản để tránh các cuộc tấn công vũ phu

• Sử dụng các thiết bị do nhà sản xuất có thành tích về nhận thức bảo mật tạo ra

• Cách ly các thiết bị loT trên các mạng được bảo vệ

Triển khai tùy chọn khởi động an toàn sử dụng kỹ thuật ký mã mật mã và đảm bảo thiết bị thực thi mã do nhà sản xuất thiết bị gốc (OEM) của thiết bị tạo ra

■ Triển khai xác thực hai chiều bằng cách sử dụng thuật toán mật mã có thể sử dụng

cả khóa đối xứng sử dụng SHA với HMAC và khóa bất đối xứng sử dụng ECDSA Tạo kho lưu trữ nội dung để lập bản đồ mạng và khám phá tất cả các đường vào và lối ra để xác định xem mạng loT có cổng Internet riêng hay không

không tuân theo các chính sách bảo mật hoặc luật, quy định và hợp đồng hiện hành • Áp dụng các biện pháp kiểm soát truy cập giữa các thiết bị loT và tài nguyên CNTT bằng cách sử dụng tường lửa doanh nghiệp, IDS/IPS, UBA, IAM, v.v.

■ Luôn đọc chính sách bảo mật của ứng dụng trước khi cài đặt để kiểm tra thông tin mà ứng dụng có thể truy cập

• Sử dụng môi trường thực thi đáng tin cậy (TEE) hoặc yếu tố bảo mật (SE), TrustZone cho ARM, để bảo mật thông tin nhạy cảm

■ Triển khai che chắn hoặc che chắn tích cực để bảo vệ thiết bị khỏi các cuộc tấn công kênh bên • Xác thực mã ngay trước khi sử dụng để giảm nguy cơ tấn công từ kiểm tra đến thời gian sử dụng (TOCTOU)

• Bảo mật khóa mã hóa và thông tin xác thực bằng cách lưu trữ chúng trong Mô-đun truy cập an toàn (SAM), Mô-đun nền tảng đáng tin cậy (TPM), Mô-đun bảo mật phần cứng (HSM) hoặc kho lưu trữ khóa đáng tin cậy khác

• Ngăn tiết lộ địa chỉ IP bằng cách vô hiệu hóa WebRTC trong trình duyệt Sử dụng trình chặn quảng cáo và tiện ích mở rộng không thể theo dõi có sẵn trên trình duyệt để ngăn chặn các cuộc tấn công dựa trên web vào thiết bị loT

• Lọc các địa chỉ IP riêng khỏi các phản hồi DNS bằng dnswall để ngăn chặn các cuộc tấn công liên kết lại DNS

• Sử dụng giải pháp chống DDoS dựa trên đám mây để lọc hoặc chuyển hướng lưu lượng DDoS độc hại

Sử dụng các mạng phân phối nội dung (CDN) và các dịch vụ phân giải DNS thông minh để cung cấp thêm một lớp cơ sở hạ tầng mạng

Cách ngăn chặn các cuộc tấn công dựa trên SDR

Các cuộc tấn công vào các thiết bị loT có thể được thực hiện từ bất kỳ hướng nào với nỗ lực bền bỉ và kiến thức về một số công cụ có sẵn. Tuy nhiên, người ta phải chủ động ngăn chặn các cuộc tấn công như vậy trước khi thiết bị bị xâm nhập.

Các phương pháp sau đây có thể giúp bảo vệ các thiết bị IoT khỏi các cuộc tấn công dựa trên SDR:

⚫ Bảo mật tín hiệu

Một trong những biện pháp phòng ngừa quan trọng nhất để tránh các cuộc tấn công vô tuyến dựa trên phần mềm là bảo mật tín hiệu bằng các phương pháp mã hóa tiêu chuẩn.

• Tránh lặp lại lệnh bằng cách sử dụng kỹ thuật cuốn chiếu

Việc sử dụng thường xuyên các lệnh giống nhau có thể cho phép lặp lại các cuộc tấn công. Các lệnh nên được bắt đầu dựa trên sơ đồ cửa sổ cuộn; điều này có nghĩa là một lệnh được sử dụng trước đó sẽ không được bắt đầu lại. Lỗ hổng trong việc thực hiện này có thể cho phép các cuộc tấn công vũ phu.

■ Áp dụng đồng bộ hóa và phần mở đầu

Tách chuỗi lệnh bằng cách sử dụng các đoạn mở đầu và đồng bộ hóa, nếu không, các giao thức có thể bị ép buộc bằng cách sử dụng phương pháp rút gọn, chẳng hạn như chuỗi de Bruijn. Điều này có thể chồng lên các bit chung đàm phán số lượng bit cần thiết để phát lại nhiều chuỗi lệnh.