BỘ CÔNG THƯƠNG

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

MÔN HỌC: NGUYÊN LÝ HỆ ĐIỀU HÀNH

ĐỀ TÀI: NGHIÊN CỨU VÀ TÌM HIỂU VỀ HỆ THỐNG BẢO VỆ TRONG HỆ ĐIỀU HÀNH WINDOWS

Giáo viên hướng dẫn: TS. Nguyễn Bá Nghiễn

Nhóm số: Nhóm 3

Lớp: 20212IT6025004 – K15

Hà Nội,, năm 2022

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP LỚN : NGUYÊN LÝ HỆ ĐIỀU HÀNH

ĐỀ TÀI: NGHIÊN CỨU VÀ TÌM HIỂU VỀ HỆ THỐNG BẢO VỆ TRONG HỆ ĐIỀU HÀNH WINDOWS

Giáo viên: TS. Nguyễn Bá Nghiễn

Sinh viên thực hiện : Mai Xuân Hải

Ngô Kim Đông

Nguyễn Văn Hoàng

Phạm Ngọc An

Nguyễn Tất Đạt

Lớp: 20212IT6025004 – K15

MỤC LỤC HÌNH ẢNH

LỜI NÓI ĐẦU

Trong bối cảnh tiến trình hội nhập, vấn đề an ninh mạng và bảo mật dữ liệu đang trở nên rất được quan tâm. Trong khi cơ sở hạ tầng và các công nghệ mạng đã đáp ứng tốt các yêu cầu về băng thông, chất lượng dịch vụ, thì thực trạng tấn công trên mạng lại ngày một gia tăng. Vì vậy, vấn đề bảo mật càng cần phải được chú trọng hơn. Đó là môt vấn đề cấp bách không chỉ với các nhà cung cấp dịch vụ Internet, các cơ quan chính phủ mà còn cả với các tổ chức doanh nghiệp, họ cũng ngày càng có ý thức hơn về an toàn thông tin.

Để các bạn có cái nhìn tổng quan hơn về các phương pháp bảo vệ hệ thống trong windows. Trong tài liệu này chúng tôi xin cùng các bạn tìm hiểu về các phương thức bảo vệ hệ thống trong windows.

CHƯƠNG I: AN NINH MẠNG.

1.1. Bảo mật

Trong bối cảnh tiến trình hội nhập, vấn đề an ninh mạng và bảo mật dữ liệu đang trở nên rất được quan tâm. Khi cơ sở hạ tầng và các công nghệ mạng đã đáp ứng tốt các yêu cầu về băng thông, chất lượng dịch vụ, đồng thời thực trạng tấn công trên mạng đang ngày một gia tăng thì vấn đề bảo mật càng được chú trọng hơn. Không chỉ các nhà cung cấp dịch vụ Internet, các cơ quan chính phủ mà các doanh nghiệp, tổ chức cũng có ý thức hơn về an toàn thông tin.

1.2.Các hình thức tấn công trên mạng

1.2.1. Tấn công trực tiếp.

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm được quyền truy nhập hệ thống mạng bên trong.

1.2.2. Nghe trộm trên mạng.

Thông tin gửi đi trên mạng thường được luân chuyển từ máy tính này qua hàng loạt các máy tính khác mới đến được đích. Điều đó, khiến cho thông tin của ta có thể bị kẻ khác nghe trộm. Tồi tệ hơn thế, những kẻ nghe trộm này còn thay thế thông tin của chúng ta bằng thông tin do họ tự tạo ra và tiếp tục gửi nó đi. Việc nghe trộm thường được tiến hành sau khi các hacker đã chiếm được quyền truy nhập hệ thống hoặc kiểm soát đường truyền. May mắn thay, chúng ta vẫn còn có một số cách để bảo vệ được nguồn thông tin cá nhân của mình trên mạng bằng cách mã hóa nguồn thông tin trước khi gửi đi qua mạng Internet. Bằng cách này, nếu như có ai đón được thông tin của mình thì đó cũng chỉ là những thông tin vô nghĩa.

1.2.3. Giả mạo địa chỉ.

Giả mạo địa chỉ có thể được thực hiện thông qua sử dụng khả năng dẫn

đường trực tiếp. Với cách tấn công này kẻ tấn công gửi các gói tin tới mạng khác với một địa chỉ giả mạo, đồng thời chỉ rõ đường dẫn mà các gói tin phải đi. Thí dụ người nào đó có thể giả mạo địa chỉ của bạn để gửi đi những thông tin có thể làm ảnh hưởng xấu tới bạn.

1.2.4. Vô hiệu hóa chức năng của hệ thống.

Đây là kiểu tấn công làm tê liệt hệ thống, làm mất khả năng cung cấp dịch vụ (Denial of Service- DoS) không cho hệ thống thực hiện được các chức năng mà nó được thiết kế. Kiểu tấn công này rất khó ngăn chặn bởi chính những phương tiện dùng để tổ chức tấn công lại chính là những phương tiện dùng để làm việc và truy cập thông tin trên mạng. Một thí dụ về trường hợp có thể xảy ra là một người trên mạng sử dụng chương trình đẩy ra những gói tin yêu cầu về một trạm nào đó. Khi nhận được gói tin, trạm luôn luôn phải xử lý và tiếp tục thu các gói tin đến sau cho đến khi bộ đệm đầy, dẫn tới tình trạng những nhu cầu cung cấp dịch vụ của các máy khác đến trạm không được phục vụ.

1.2.5. Tấn công vào yếu tố con người.

Đây là một hình thức tấn công nguy hiểm nhất nó có thể dẫn tới những tổn thất hết sức khó lường. Kẻ tấn công có thể liên lạc với người quản trị hệ thống thay đổi một số thông tin nhằm tạo điều kiện cho các phương thức tấn công khác.

1.2.6. Một số kiểu tấn công khác.

Ngoài các hình thức tấn công kể trên, các hacker còn sử dụng một số kiểu tấn công khác như tạo ra các virus đặt nằm tiềm ẩn trên các file khi người sử dụng do vô tình trao đổi thông tin qua mạng mà người sử dụng đã tự cài đặt nó lên trên máy của mình. Ngoài ra hiện nay còn rất nhiều kiểu tấn công khác mà chúng ta còn chưa biết tới và chúng được đưa ra bởi những hacker.

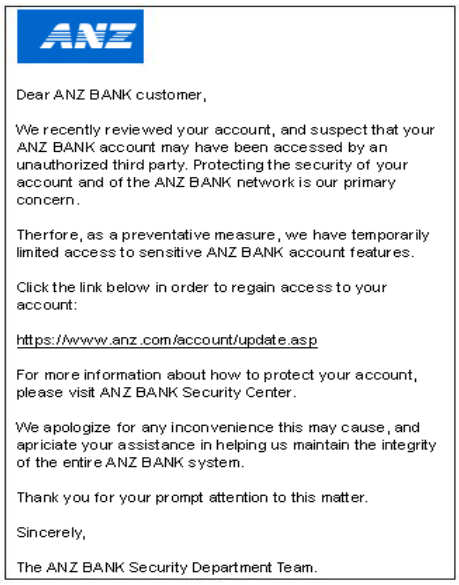
CHƯƠNG II: CÁC MỐI ĐE DỌA.

2.1. Phishing.

Phishing là một thủ đoạn của hacker nhằm lấy thông tin cá nhân của khách hàng bằng cách dùng email giả danh các tổ chức tài chính. Cách này rất hay được những tên trộm ảo sử dụng.

Các email tự xưng là các ngân hàng hoặc tổ chức hợp pháp thường được gởi số lượng lớn. Nó yêu cầu người nhận cung cấp các thông tin khá nhạy cảm như tên truy cập, mật khẩu, mã đăng ký hoặc số PIN bằng cách dẫn đến một đường link tới một website nhìn có vẻ hợp pháp, điều đó giúp cho tên trộm có thể thu thập được những thông tin của quý khách để tiến hành các giao dịch bất hợp pháp sau đó.

Dưới đây là một ví dụ về email lừa đảo:



Dear ANZ BANK customer,

We recently reviewed your account, and suspect that your ANZ BANK account may have been accessed by an unauthorized third party. Protecting the security of your account and of the ANZ BANK network is our primary concern.

Therfore, as a preventative measure, we have temporarily limited access to sensitive ANZ BANK account features.

Click the link below in order to regain access to your account:

https://www.anz.com/account/update.asp

For more information about how to protect your account, please visit ANZ BANK Security Center.

We apologize for any inconvenience this may cause, and apriciate your assistance in helping us maintain the integrity of the entire ANZ BANK system.

Thank you for your prompt attention to this matter.

Sincerely,

The ANZ BANK Security Department Team.

Hình 1: Một email lừa đảo.

Nếu nhận được email yêu cầu đăng ký hãy nhập lại các thông tin cá nhân, cần xóa chúng ngày và thông báo với bộ phận hỗ trợ Ngân hàng điện tử của ANZ nơi quý khách ở. Có thể hạn chế nguy cơ trở thành nạn nhân của email lừa đảo bằng cách:

- Tuyệt đối không truy cập vào Ngân hàng điện tử qua link lạ gửi qua mail.
- Thận trọng với các thông emails yêu cầu khai báo thông tin như tên truy cập, mật khẩu, mã pin. Email xác thực của ANZ không yêu cầu chi tiết cá nhân hay đăng nhập các thông tin.
- Ngay lập tức xóa bỏ các email không rõ nguồn gốc, cho dù cho dù nó có vô hại hay dùng lời mời chào hấp dẫn thế nào đi nữa.
- Thay đổi mật khẩu của Ngân hàng điện tử định kỳ.
- Liên tục cập nhật chương trình diệt virus và tường lửa cũng như quét máy tính của quý khách thường xuyên.

2.2. Virus và Worm.

Virus máy tính là phần mềm được đính kèm với các chương trình khác. Giống như một virus sinh học, nó phải tự bám vào các chương trình khác để sinh trưởng và phát triển. Không giống với Trojans hoạt động độc lập, virus chỉ có thể hoạt động nếu như chương trình chứa nó đang hoạt động. Trong quá trình hoạt động, virus tự sinh sôi và lan truyền sang các chương trình khác. Nó có thể tấn công các nguồn như ổ đĩa hoặc bộ nhớ hay bất kỳ khu vực nào trên máy tính.

Virus qua email là hình thức mới nhất của virus máy tính. Nó xâm nhập vào tất cả các thư, và thường xuyên nhân bản để phát tán virus đến tất cả những người trong danh bạ.

Worm cũng giống như virus. Nó lợi dụng những máy tính đang nối mạng để xâm nhập vào những lỗ hổng bảo mật. Khi đã tìm thấy lỗ hổng bảo mật, nó sẽ xâm nhập một cách nhanh chóng từ máy này sang máy khác. Nó có sức phá hủy tương đương với virus.

2.3. Trojan.

Trojan xuất hiện để thực thi mã độc ở lớp phía sau. Đây không phải là virus và có thể dễ dàng được download mà không nhận thấy chúng. Remote access

Trojan (RAT) là một loại trojan phổ biến điều khiển truy cập từ xa, ví dụ Back Orifice hoặc NetBus; khả năng của chúng cho phép kẻ tấn công có thể thực thi các quyền quản trị.

2.4. Spyware.

Spyware là một phần mềm độc hại có thể được download về hoặc được cài đặt chung với một phần mềm khác. Thông thường, loại malware này sẽ thu thập thông tin về người dùng. Nó có thể là một đoạn code ghi lại các website mà người dùng đã truy cập hoặc ghi lại những gì mà bạn đánh trên bàn phím, mặt khác nó có khả năng thay đổi cấu hình máy tính của bạn mà không cần bất kỳ tương tác nào của người dùng.

CHƯƠNG III: CƠ CHẾ XÁC THỰC: QUẢN LÝ QUYỀN TRUY CẬP VÀ QUẢN LÝ DANH TÍNH (CƠ CHẾ XÁC NHẬN NGƯỜI DÙNG)

3.1. Sự khác biệt giữa Authentication và Authorization

Xác thực là bất kỳ quá trình bạn xác minh rằng một ai đó là người mà họ tuyên bố họ có quyền. Điều này thường liên quan đến một tên người dùng và mật khẩu, nhưng có thể bao gồm bất kỳ phương thức khác như chứng minh nhân dân, thẻ thông minh, quét võng mạc, nhận dạng giọng nói, hoặc dấu vân tay. Xác thực là tương đương với giấy phép hiển thị các trình điều khiển của bạn tại quầy vé sân bay.

Ủy quyền là tìm hiểu xem người đó một khi đã xác định, được phép có các nguồn tài nguyên nào. Điều này thường được xác định bằng cách tìm hiểu xem người đó là một phần của một nhóm đặc biệt nào đó hay không. Ủy quyền tương đương với việc kiểm tra danh sách khách mời tại một bữa tiệc độc quyền, hoặc kiểm tra vé của bạn khi bạn đi đến sân bay.

Trên mạng, chứng thực thường được thực hiện bằng cách cung cấp một tên người dùng và mật khẩu. Tên người sử dụng nhận dạng và mật khẩu cung cấp cho hệ thống máy tính của một bảo đảm rằng bạn thực sự là người được phép đòi truy cập (claim). Sau khi bạn được chứng thực, máy tính đồng ý rằng bạn đúng là người có quyền đòi truy cập. Tuy nhiên, nó chưa biết liệu bạn được phép truy cập vào các tài nguyên bạn đang yêu cầu hay không. Để uỷ quyền cho người sử dụng, hệ thống máy tính thường kiểm tra một danh sách điều khiển truy cập (Access control list - ACL). Các ACL bao gồm người dùng và nhóm người sử dụng, người được phép truy cập vào một nguồn tài nguyên.

3.2. Network Authentication Systems.

Để xác thực một người dùng trong mạng và chắc chắn rằng người dùng là những người được phép, người sử dụng cần cung cấp hai mẩu thông tin: identification và proof of identity (bằng chứng nhận dạng danh tính). Trong hầu hết các mạng, người dùng được nhận diện với một tên người dùng hoặc một địa chỉ e-mail. Tuy nhiên, cách chứng minh danh tính của họ khác nhau.

Theo truyền thống, mật khẩu được sử dụng để chứng minh danh tính của người dùng. Mật khẩu là một hình thức bí mật được chia sẻ. Người dùng biết mật khẩu của mình, và máy chủ xác thực người sử dụng hoặc có mật khẩu được lưu trữ, hoặc có một số thông tin có thể được sử dụng để xác nhận mật khẩu.

Mật khẩu chứng minh nhận dạng danh tính của bạn, chúng là một cái gì đó bạn biết. Cách khác để chứng minh nhận dạng của bạn là với một cái gì đó bạn có (something you have) hay cái gì bạn đang có (something you are). Nhiều hệ thống máy tính hiện đại xác thực người dùng bằng cách đọc thông tin từ smart card. Lĩnh vực sinh học cũng có thể làm điều này bằng cách quét một phần duy nhất của cơ thể như vân tay, võng mạc, hoặc các tính năng trên khuôn mặt.

Mật khẩu có thể được đoán, và các thẻ thông minh có thể bị đánh cắp. Một hình thức xác thực không thể đáp ứng yêu cầu an ninh của tổ chức. Multifactor

authentication (đa chứng thực) kết hợp hai hay nhiều phương pháp xác thực, và làm giảm đáng kể khả năng bị tấn công. Ví dụ phổ biến nhất của MA là kết hợp một thẻ thông minh và mật khẩu. Thông thường, mật khẩu được yêu cầu để lấy một khóa được lưu trên smart card. Trước khi có thể xác thực với hệ thống như vậy, bạn phải cung cấp một mật khẩu (something you know) và một thẻ thông minh (something you have).

3.3. Lưu trữ giấy chứng nhận người dùng (Storing User Credentials)

Các máy chủ xác thực người dùng phải có khả năng xác định các thông tin có giá trị. Để làm điều này, máy chủ phải lưu trữ thông tin có thể được sử dụng để xác minh các thông tin với người dùng. Làm thế nào và ở đâu thông tin này được lưu giữ là quyết định quan trọng để thực hiện khi thiết kế một mô hình chứng thực.

Lưu trữ giấy chứng thực của người dùng (user credentials) có thể gặp khó khăn là làm thế nào cho một kẻ tấn công không thể đánh cấp thông tin user và password, cho dù những thông tin quan trọng có thể được bị rò rỉ ra bên ngoài. Thay vì chỉ đơn giản là lưu trữ một danh sách các mật khẩu user trên một máy chủ, và trực tiếp so sánh các mật khẩu được cung cấp bởi user, nó thường lưu trữ một phiên bản được mã hóa hoặc Hash của mật khẩu người dùng. Nếu kẻ tấn công truy cập máy chủ để đánh cấp các thông tin này hắn ta vẫn cần để giải mã nội dung đó.

Xác định nơi lưu trữ các thông tin người dùng có hai mô hình chứng thực là tập trung và phân cấp.

Các mô hình chứng thực phân cấp đòi hỏi tài nguyên mạng để duy trì một danh sách user và các thông tin của user. Qua đó người dùng có thể xác thực việc sử dụng các tài nguyên mạng, nó sẽ trở thành không thể quản lý trên mạng với hơn một máy chủ. Trong các mạng Windows, mỗi máy chủ duy trì một danh sách những người dùng địa phương (local users) mà có thể được sử dụng để thực hiện một mô hình chứng thực phân cấp.

Mô hình chứng thực tập trung cho phép quản lý đơn giản đáng kể trong các mạng lớn hơn, tiện hơn cho Help desk quản lý mật khẩu. Trong mô hình tập trung, tài nguyên mạng dựa vào một cơ quan trung tâm để xác thực user. Chứng thực tập trung là cần thiết trong môi trường mà người dùng truy cập vào tất cả các tài nguyên mạng với một bộ các thông tin, một tình hình lý tưởng được gọi là single sign-on. Trong các mạng Windows, chứng thực tập trung được cung cấp bởi Active Directory. Các mạng lớn hơn có thể sử dụng nhiều domain, với viêc trusts để user trong domain này truy cập tài nguyên trong domain khác.

3.4. Authentication Features of Windows Server 2003.

Windows Server 2003 cung cấp phương pháp xác thực mạnh mẽ và linh hoạt có thể được cấu hình để đáp ứng nhu cầu của các tổ chức từ doanh nghiệp nhỏ cho đến doanh nghiệp tầm cở. Tính năng xác thực chính của Windows Server 2003 bao gồm:

- Trung tâm quản lý các tài khoản người dùng**:** (Central administration of user accounts) Các dịch vụ Active Directory cho phép người dùng đăng nhập vào máy tính trong một môi trường multidomain, multiforest bằng cách sử dụng một yếu tố xác thực (single-factor authentication) hoặc các loại đa chứng thực (multifactor authentication).
- Môi trường đăng nhập một lần**:** (Single sign-on environmentn) Khi người dùng được chứng thực torng một domain, các thông tin của người dùng được sử dụng để truy cập tài nguyên trong domain đó, qua đó loại bỏ sự xác thực không cần thiết khi người dùng truy cập tài nguyên khác nhau. Khi công nghệ này được sử dụng với người dùng là Windows XP, người dùng có thể truy cập tài nguyên trong các lĩnh vực khác bằng cách cung cấp mật khẩu một lần và lưu trữ các mật khẩu như một phần của tài khoản người dùng trong domain.

- Máy tính và các tài khoản dịch vụ (Computer and service accounts): Ngoài cho người dùng, máy tính và các tài khoản dịch vụ cũng được xác thực với hệ thống.
- Đa hỗ trợ (Multifactor support): Windows Server 2003 natively hỗ trợ thẻ thông minh và một loạt các cơ chế đa xác thực khác.
- Kiểm toán (Auditing): Windows Server 2003 cung cấp khả năng kiểm soát việc đăng nhập và truy cập vào tài nguyên của các user.
- Giao thức (Protocols): Windows Server 2003 sử dụng một loạt các giao thức xác thực, bao gồm cả LM, NTLM, NTLMv2, và Kerberos.

3.5. Giao thức xác thực NTLM và Kerberos.

Windows Server 2003 cung cấp khả năng xác thực một loạt các hệ điều hành máy khách. Windows Server 2003 hỗ trợ hai giao thức xác thực chính: NTLM và Kerberos.

3.5.1. Giao thức xác thực NTLM.

Giao thức xác thực NTLM sử dụng một cơ chế thách thức- đáp ứng (challenge-response) để xác thức xác thực trong Windows Server 2003**.**

Xác thực người dùng và máy tính chạy Windows Me hoặc hệ điều hành trước đó, hoặc máy tính chạy Windows 2000 hoặc sau đó mà không phải là một phần của domain. Một người dùng được thách thức (challenge) để được cung cấp một số phần thông tin cá nhân duy nhất cho người sử dụng (response). Windows Server 2003 hỗ trợ ba phương pháp xác thực theo kiểu challenge- response sau đây:

- LAN Manager (LM): Được phát triển bởi IBM và Microsoft để sử dụng trong OS2 và Windows cho Workgroups (Windows 95, Windows 98 và Windows Me). Đây là hình thức kém an toàn của xác thực challenge-response vì nó là dễ bị kẽ tấn công nghe trộm, và máy chủ chứng thực người dùng phải lưu trữ các thông tin trong LMHash.

- NTLM version 1: Một hình thức an toàn hơn so với kiểu LM. Nó được sử dụng để kết nối với máy chủ chạy Windows NT với Service Pack 3 hoặc sớm hơn. NTLMv1 sử dụng giao thức mã hóa 56-bit. Máy chủ xác thực người dùng với bất kỳ phiên bản của NTLM nào, việc xác thực phải lưu trữ các thông tin trong một Hash NT.
- NTLM version 2: Hình thức an toàn nhất có sẵn trong chứng thực challenge-response. Phiên bản này bao gồm một kênh an toàn để bảo vệ quá trình xác thực. Nó được sử dụng để kết nối với máy chủ chạy Windows 2000, Windows XP, và Windows NT với Service Pack 4 hoặc cao hơn. NTLMv2 sử dụng mã hóa 128-bit để đảm bảo các giao thức an toàn.

3.5.2. Giao thức xác thực Kerberos

Kerberos là một giao thức xác thực mặc định cho Windows Server 2003, Windows 2000 và Windows XP Professional. Kerberos được thiết kế để được an toàn hơn và khả năng mở rộng hơn so với NTLM trên mạng lớn. Kerberos cung cấp thêm các lợi ích sau đây:

- Hiệu quả (Efficiency): Khi một máy chủ cần xác thực một client, máy chủ Kerberos có thể xác nhận các thông tin của client mà không cần phải liên hệ với domain controller.
- Tự chứng thực (Mutual authentication): Ngoài việc chứng thực client đến server, Kerberos cho phép máy chủ xác thực lẫn nhau.
- Ủy quyền chứng thực (Delegated authentication)**:** Cho phép các dịch vụ để đóng vai client khi truy cập vào tài nguyên.
- Đơn giản hóa quản lý (Trust Kerberos)**:** có thể sử dụng trust giữa các domain trong cùng một forest và các domain kết nối với một forest.
- Khả năng cộng tác (Interoperability)**:** Kerberos được dựa trên tiêu chuẩn Internet Engineering Task Force (IETF) và do đó tương thích với IETF khác tuân theo lõi Kerberos.

3.6. LM Authentication.

LM Authentication cung cấp khả năng tương thích với hệ điều hành trước đó, bao gồm Windows 95, Windows 98 và Windows NT 4.0 Service Pack 3 hoặc sớm hơn. Ngoài ra còn có các ứng dụng trước đó mà có thể dựa vào cơ chế xác thực này. Tuy nhiên, giao thức LM là yếu nhất, và dễ dàng nhất để tấn công. Không sử dụng chứng thực LM trong một môi trường Windows Server 2003. Nâng cấp các máy tính dựa trên giao thức LM để loại bỏ lỗ hổng bảo mật này.

3.6.1. LM passwords.

Lý do chính không sử dụng giao thức LM là khi mật khẩu được tạo ra bởi người sử dụng và được lưu trữ để sử dụng, mật khẩu được chuyển đổi để LMHash một lần. LMHash chứa tên người dùng và hash của mật khẩu tương ứng. Hash là một hình thức mã hóa một chiều. Khi một khách hàng cố gắng để xác thực với chứng thực LM các hash của mật khẩu được truyền trên mạng. Máy chủ chỉ có thể để xác thực người sử dụng nếu máy chủ có lưu trữ LMHash .

LMHash có một vài điểm yếu mà làm cho nó dễ bị tấn công hơn Hash NT. Các LMHash được lưu trữ là các chữ hoa, được giới hạn trong 14 ký tự. Nếu có hiểu biết, kẻ tấn công có được quyền truy cập vào LMHashes lấy được một số lượng lớn người sử dụng, có khả năng là kẻ tấn công sẽ giải mã được mật khẩu.

lemon	E783A3AE2A4557DBA5E1FA0269CBC58D
laoalagv	A766F44DDEA5CACC3323CE3E7D73AE82
unknowplayer12	V521E8FC82C39D47F02B1F4526E2804A
somebody	3T48E8FC82C39D47F02B1F4526E280EE

Bảng 1cho thấy ví dụ về mật khẩu và các LMHashes tương ứng mà có thể được lưu trữ.

Chú ý rằng với hash của mật khẩu luôn có 14 ký tự, nếu chưa đủ thì ký tự E (mã 16) được thêm vào sau cùng. Trong quá trình tính toán các hash, mật khẩu ban đầu được chia thành hai bộ bảy ký tự. Nếu mật khẩu là bảy ký tự hoặc ít hơn, tập

thứ hai của bảy ký tự là null. Điều này dẫn đến các ký E cuối cùng là một giá trị giúp cho kẻ tấn công biết các mật khẩu ban đầu là ít hơn tám ký tự. Điều này giúp kẽ tấn công giảm bớt thời gian dò tìm mã.

3.6.2. Vô hiệu hóa mật khẩu LM.

Windows Server 2003 cho phép bạn vô hiệu hóa các LMHash để loại bỏ các lỗ hổng được trình bày ở trên. Tuy nhiên, nếu bạn có client đang chạy Windows 3.1 hoặc bản phát hành ban đầu của Windows 95 kết nối với một máy tính chạy Windows Server 2003, thì bạn không vô hiệu hóa các LMHash. Tuy nhiên, bạn vẫn có thể vô hiệu hóa việc sử dụng LMHash trên cơ sở account-by-account bằng cách làm một trong những điều sau đây:

- Sử dụng mật khẩu với 15 ký tự hoặc dài hơn.
- Kích hoạt các giá trị registry NoLMHash cục bộ trên một máy tính hoặc bằng cách sử dụng chính sách an ninh.
- Sử dụng các ký tự ALT trong mật khẩu. Ký tự ALT được đưa vào một mật khẩu bằng cách giữ phím ALT, gõ các phím số, và sau đó thả phím ALT.

3.6.3. NTLM Authentication.

NTLM bao gồm ba phương pháp xác thực challenge-response: LM, NTLMv1, và NTLMv2. Quá trình xác thực cho tất cả các phương pháp là như nhau, nhưng chúng khác nhau ở mức độ mã hóa.

3.7. Quá trình xác thực

Các bước sau đây chứng tỏ quá trình của một sự kiện xác thực xảy ra khi một client xác nhận đến domain controller bằng cách sử dụng bất kỳ các giao thức NTLM:

- Các client và server thương lượng một giao thức xác thực. Điều này được thực hiện thông qua việc thương lượng nhà cung cấp dịch vụ hỗ trợ bảo mật của Microsoft (Security Support Provider).
- Client gửi tên người dùng và tên miền tới domain controller.
- Domain controller chọn ngẫu nhiên 16 byte để tạo ra một chuỗi ký tự được gọi là nonce
- Client mã hóa nonce này với một hash của mật khẩu và gửi nó trở lại domain controller.
- Domain controller trả lời hash của mật khẩu từ cơ sở dữ liệu tài khoản bảo mật.
- Domain controller sử dụng các giá trị băm lấy từ cơ sở dữ liệu tài khoản bảo mật để mã hóa nonce. Giá trị này được so sánh với giá trị nhận được từ client Nếu các giá trị phù hợp, client được chứng thực.

37.1. Các quy trình xác thực Kerberos.

Giao thức Kerberos lấy ý tưởng từ các con chó ba đầu trong thần thoại Hy Lạp. Ba thành phần của Kerberos là:

- Các client yêu cầu dịch vụ hoặc chứng thực.
- Các server lưu trữ các dịch vụ theo yêu cầu của client.
- Một máy tính có nghĩa là đáng tin cậy của khách hàng và máy chủ (trong trường hợp này, Windows Server 2003 domain controller chạy dịch vụ Kerberos Key Distribution Center).

Xác thực Kerberos được dựa trên các gói dữ liệu định dạng đặc biệt được gọi là ticket. Trong Kerberos, các ticket đi qua mạng thay vì mật khẩu. Truyền ticket thay vì mật khẩu làm cho quá trình xác thực tăng khả năng chống tấn công.

3.7.1.1. Kerberos Key Distribution Center.

Key Distribution Center(KDC) duy trì một cơ sở dữ liệu các thông tin tài khoản cho tất cả các hiệu trưởng an ninh (security principals) trong miền. Các KDC lưu trữ một khoá mật mã chỉ có các security principals được biết đến. Khóa này được sử dụng để giao tiếp giữa security principals và KDC, và được biết đến như một chìa khóa dài hạn. Chìa khóa dài hạn được bắt nguồn từ mật khẩu đăng nhập của người dùng.

3.7.1.2. Quá trình xác thực Kerberos.

Sau đây là mô tả một phiên giao dịch (giản lược) của Kerberos. Trong đó: AS = Máy chủ chứng thực (authentication server), TGS = Máy chủ cấp vé (ticket granting server), SS = Máy chủ dịch vụ (service server).

1. Người sử dụng nhập tên và mật khẩu tại máy tính của mình (máy khách).
2. Phần mềm máy khách thực hiện hàm băm một chiều trên mật khẩu nhận được. Kết quả sẽ được dùng làm khóa bí mật của người sử dụng.
3. Phần mềm máy khách gửi một gói tin (không mật mã hóa) tới máy chủ dịch vụ AS để yêu cầu dịch vụ. Nội dung của gói tin đại ý: "người dùng XYZ muốn sử dụng dịch vụ". Cần chú ý là cả khóa bí mật lẫn mật khẩu đều không được gửi tới AS.
4. AS kiểm tra nhân danh của người yêu cầu có nằm trong cơ sở dữ liệu của mình không. Nếu có thì AS gửi 2 gói tin sau tới người sử dụng:

* Gói tin A: "Khóa phiên TGS/máy khách" được mật mã hóa với khóa bí mật của người sử dụng.

*Gói tin B: "Vé chấp thuận" (bao gồm chỉ danh người sử dụng (ID), địa chỉ mạng của người sử dụng, thời hạn của vé và "Khóa phiên TGS/máy khách") được mật mã hóa với khóa bí mật của TGS.

5. Khi nhận được 2 gói tin trên, phần mềm máy khách giải mã gói tin A để có khóa phiên với TGS. (Người sử dụng không thể giải mã được gói tin B vì nó được mã hóa với khóa bí mật của TGS). Tại thời điểm này, người dùng có thể nhận thực mình với TGS.

6. Khi yêu cầu dịch vụ, người sử dụng gửi 2 gói tin sau tới TGS:

* Gói tin C: Bao gồm "Vé chấp thuận" từ gói tin B và chỉ danh (ID) của yêu cầu dịch vụ.

* Gói tin D: Phần nhận thực (bao gồm chỉ danh người sử dụng và thời điểm yêu cầu), mật mã hóa với "Khóa phiên TGS/máy khách".

7. Khi nhận được 2 gói tin C và D, TGS giải mã D rồi gửi 2 gói tin sau tới người sử dụng:

* Gói tin E: "Vé" (bao gồm chỉ danh người sử dụng, địa chỉ mạng người sử dụng, thời hạn sử dụng và "Khóa phiên máy chủ/máy khách") mật mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ.

* Gói tin F: "Khóa phiên máy chủ/máy khách" mật mã hóa với "Khóa phiên TGS/máy khách".

8. Khi nhận được 2 gói tin E và F, người sử dụng đã có đủ thông tin để nhận thực với máy chủ cung cấp dịch vụ SS. Máy khách gửi tới SS 2 gói tin:

* Gói tin E thu được từ bước trước (trong đó có "Khóa phiên máy chủ/máy khách" mật mã hóa với khóa bí mật của SS).

* Gói tin G: phần nhận thực mới, bao gồm chỉ danh người sử dụng, thời điểm yêu cầu và được mật mã hóa với "Khóa phiên máy chủ/máy khách".

9. SS giải mã "Vé" bằng khóa bí mật của mình và gửi gói tin sau tới người sử dụng để xác nhận định danh của mình và khẳng định sự đồng ý cung cấp dịch vụ:

* Gói tin H: Thời điểm trong gói tin yêu cầu dịch vụ cộng thêm 1, mật mã hóa với "Khóa phiên máy chủ/máy khách".

10. Máy khách giải mã gói tin xác nhận và kiểm tra thời gian có được cập nhật chính xác. Nếu đúng thì người sử dụng có thể tin tưởng vào máy chủ SS và bắt đầu gửi yêu cầu sử dụng dịch vụ.

11. Máy chủ cung cấp dịch vụ cho người sử dụng.

Nhược điểm:

Tồn tại một điểm yếu: Nếu máy chủ trung tâm ngừng hoạt động thì mọi hoạt động sẽ ngừng lại. Điểm yếu này có thể được hạn chế bằng cách sử dụng nhiều máy chủ Kerberos.

Giao thức đòi hỏi đồng hồ của tất cả những máy tính liên quan phải được đồng bộ. Nếu không đảm bảo điều này, cơ chế nhận thực giữa trên thời hạn sử dụng sẽ không hoạt động. Thiết lập mặc định đòi hỏi các đồng hồ không được sai lệch quá 10 phút.

Cơ chế thay đổi mật khẩu không được tiêu chuẩn hóa.

CHƯƠNG IV: TỔNG QUAN VỀ FIREWALL.

Hàng phòng vệ đầu tiên chống lại những kẻ hay đi xâm nhập trộm là Firewall: một tập hợp những thủ thuật chuyên môn có thể giúp ngăn chặn ý đồ xâm

nhập xấu vào máy tính và hạn chế những gì đi ra khỏi máy. Windows cũng bao gồm một Firewall riêng và router (giúp kết nối máy tính với Internet) cũng có router riêng.

4.1. Firewall là gì.

Một bức tường lửa kiểm soát truy cập giữa các mạng. Nó thường bao gồm các cổng và các bộ lọc khác nhau từ một trong những tường lửa khác. Tường lửa cũng có màn hình lưu lượng mạng và có thể để ngăn chặn lưu lượng truy cập đó là nguy hiểm. Tường lửa hoạt động như các máy chủ trung gian giữa các kết nối SMTP và HTTP.

Bất kì máy tính nào kết nối tới Internet cũng cần có firewall, giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng. Việc có một "người gác cổng" như vậy để giám sát mọi việc xảy ra rất quan trọng bởi 2 lý do:

Thứ nhất, bất kì máy tính kết nối mạng nào thường kết nối vĩnh viễn với Internet. Thứ 2, mỗi máy tính trực tuyến lại có một chữ ký điện tử riêng, được gọi là Internet Protocol address (hay còn gọi là địa chỉ IP): Nếu không có Firewall hỗ trợ, nó chẳng khác gì chuyện bạn bật tất cả đèn lên và mở rộng cửa.

Một Firewall được cấu hình chính xác sẽ ngăn chặn điều này xảy ra và giúp máy tính "ẩn" một cách hiệu quả, cho phép người dùng thoải mái thưởng thức những gì thế giới trực tuyến mang lại. Firewall không giống chương trình diệt virus. Thay vào đó, nó làm việc cùng với những công cụ này nhằm đảm bảo rằng máy tính được bảo vệ từ hầu hết các mối tấn công nguy hại phổ biến.

Windows XP, Vista và 7 bao gồm một Firewall, gọi là Windows Firewall, được kích hoạt theo mặc định.

4.2. Hoạt động của Firewall.

Một Firewall cần biết được sự khác biệt giữa lưu lượng hợp pháp như trên với những loại dữ liệu gây hại khác.

Firewall sử dụng rule hoặc ngoại lệ để làm việc với những kết nối tốt và loại bỏ những kết nối xấu. Nhìn chung, quá trình này được thực hiện ẩn, người dùng không thấy được hoặc không cần tương tác gì cả.

Để xem cách Windows XP thực hiện như thế nào, kích vào Start → Control Panel và kích đúp vào icon Windows Firewall. Khi có hộp thoại xuất hiện, kích vào thẻ Exceptions ở top trên cùng để xem những phần mềm được phép nhận kết nối tới – nó giống như bao gồm những thứ như phần mềm diệt virus và dịch vụ lưu trữ trực tuyến, ví như Dropbox.

Người dùng Windows Vista và Windows 7 sẽ phải kích vào Start → Control Panel → System and Security (hoặc Security trong Vista) → Windows Firewall. Khi có cửa sổ xuất hiện, kích vào đường link Allow a program or feature through Windows Firewall trong danh sách bên trái (Vista là Allow a program through Windows Firewall) để xem những phần mềm được phép giao tiếp qua Firewall.

Nhìn chung, Windows tự động theo dõi những rule và ngoại lệ này, nhưng đây chính là nơi bạn cần đến mỗi khi muốn thay đổi điều gì đó.

CHƯƠNG V: SỬ DỤNG FIREWALL

5.1. Internet Firewall

Là một thiết bị (phần cứng + phần mềm) giữa mạng của một tổ chức, một công ty, hay một quốc gia (Intranet) và Internet. Nó thực hiện vai trò bảo mật các thông tin Intranet từ thế giới Internet bên ngoài.

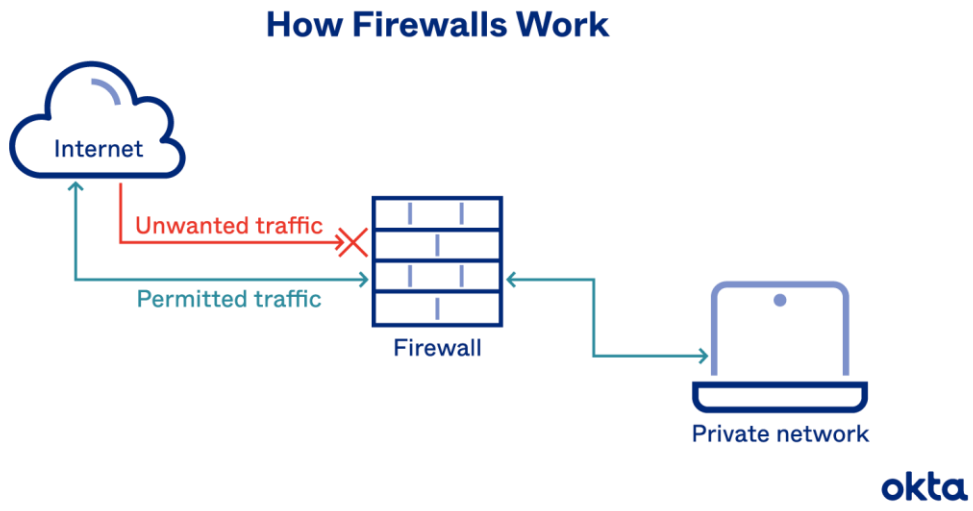
Chức Năng Của Firewall:

Internet Firewall (từ nay về sau gọi tắt là Firewall) là một thành phần đặt giữa Intranet và Internet để kiểm soát tất cả các việc lưu thông và truy cập giữa chúng với nhau bao gồm:

Firewall quyết định những dịch vụ nào từ bên trong được phép truy cập từ bên ngoài, những người nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong, và cả những dịch vụ nào bên ngoài được phép truy cập bởi những người bên trong.

Để Firewall làm việc hiệu quả, tất cả trao đổi thông tin từ trong ra ngoài và ngược lại đều phải thực hiện thông qua Firewall.

Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ mới được quyền lưu thông qua Firewall.



Hình 2: Firewall

Firewall bao gồm:

Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.

Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

5.2. Các thành phần của Firewall và cơ chế hoạt động

- Một Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:
- Bộ lọc packet (packet-filtering router)
- Cổng ứng dụng (application-level gateway hay proxy server)
- Cổng mạch (circuit level gateway)

5.2.1. Bộ Lọc Gói Tin:

Nguyên lý:

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua Firewall thì điều đó có nghĩa rằng Firewall hoạt động chặt chẽ với giao thức liên mạng TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS...) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ để có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các packet và những con số địa chỉ của chúng.

Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (packet header), dùng để cho phép truyền các packet đó ở trên mạng. Đó là:

- Địa chỉ IP nơi xuất phát (IP Source address)
- Địa chỉ IP nơi nhận (IP Destination address)
- Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)
- Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)
- Cổng TCP/UDP nơi nhận (TCP/UDP destination port)
- Dạng thông báo ICMP (ICMP message type)
- Giao diện packet đến (incoming interface of packet)
- Giao diện packet đi (outcoming interface of packet)

Nếu luật lệ lọc packet được thoả mãn thì packet được chuyển qua Firewall. Nếu không packet sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) được phép mới chạy được trên hệ thống mạng cục bộ.

Ưu điểm

- Đa số các hệ thống Firewall đều sử dụng bộ lọc packet. Một trong những ưu điểm của phương pháp dùng bộ lọc packet là chi phí thấp vì cơ chế lọc packet đã được bao gồm trong mỗi phần mềm router.
- Ngoài ra, bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng, vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả.

Hạn chế:

- Việc định nghĩa các chế độ lọc packet là một việc khá phức tạp, nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ Internet, các dạng packet header, và các giá trị cụ thể mà họ có thể nhận trên mỗi trường.

Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển.

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

5.2.2Cổng ứng dụng (application-level gateway)

Nguyên lý

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service (dịch vụ đại diện). Proxy service là các bộ chương trình đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt chương trình proxy cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua Firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

Một cổng ứng dụng thường được coi như là một pháo đài (bastion host), bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đảm bảo an ninh của một bastion host là:

Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ thống (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào Operating System, cũng như là đảm bảo sự tích hợp Firewall.

Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể

bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.

Bastion host có thể yêu cầu nhiều mức độ xác thực khác nhau, ví dụ như user password hay smart card.

Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một sồ các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của giao thông qua nó, mỗi sự kết nối, khoảng thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.

Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ một proxy đang có vấn đề.

Ví dụ: Telnet Proxy

Ví dụ một người (gọi là outside client) muốn sử dụng dịch vụ TELNET để kết nối vào hệ thống mạng qua một bastion host có Telnet proxy. Quá trình xảy ra như sau:

Outside client telnets đến bastion host. Bastion host kiểm tra password, nếu hợp lệ thì outside client được phép vào giao diện của Telnet proxy. Telnet proxy cho phép một tập nhỏ những lệnh của Telnet, và quyết định những máy chủ nội bộ nào outside client được phép truy nhập.

Outside client chỉ ra máy chủ đích và Telnet proxy tạo một kết nối của riêng nó tới máy chủ bên trong, và chuyển các lệnh tới máy chủ dưới sự uỷ quyền của outside client. Outside client thì tin rằng Telnet proxy là máy chủ thật ở bên trong, trong khi máy chủ ở bên trong thì tin rằng Telnet proxy là client thật

Ưu điểm:

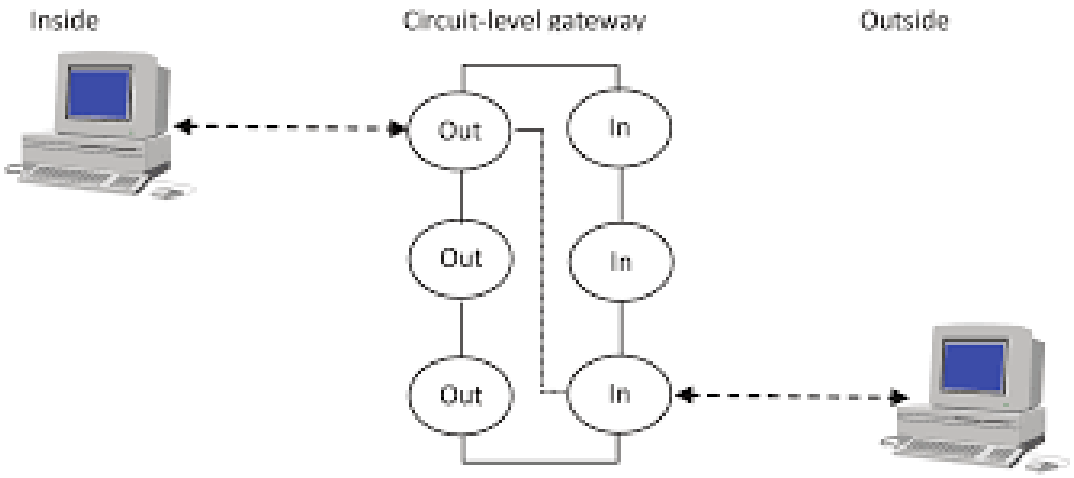
- Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.
- Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.
- Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.
- Luật lệ filtering (lọc) cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

Hạn chế:

Yêu cầu các users biến đổi (modify) thao tác, hoặc modify phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Ví dụ, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước đê nối với máy chủ chứ không phải là một bước thôi. Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet.

5.2.3 Cổng mạch (Circuit-Level Gateway*)*

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



Hình 3: Cổng vòng

Hình 3 minh hoạ một hành động sử dụng nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua Firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục Telnet nào. Cổng vòng làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên, vì sự kết nối này xuất hiện từ hệ thống Firewall, nó che dấu thông tin về mạng nội bộ.

Cổng vòng thường được sử dụng cho những kết nối ra ngoài, nơi mà các quản trị mạng thật sự tin tưởng những người dùng bên trong. Ưu điểm lớn nhất là một bastion host có thể được cấu hình như là một hỗn hợp cung cấp Cổng ứng dụng cho những kết nối đến, và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các dịch vụ Internet, trong khi vẫn cung cấp chức năng bức tường lửa để bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

5.3. Những hạn chế của Firewall

Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn

sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, nó không thể chống lại một cuộc tấn công từ một đường dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.

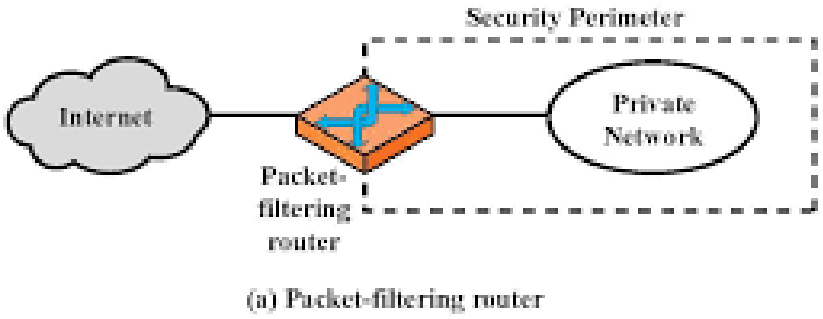
Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-driven attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua Firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.

Một ví dụ là các virus máy tính. Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của Firewall.

5.4. Các ví dụ Firewall

5.4.1. Packet-Filtering Router (Bộ trung chuyển có lọc gói)

Hệ thống Internet Firewall phổ biến nhất chỉ bao gồm một packet-filtering router đặt giữa mạng nội bộ và Internet (Hình 2.4). Một packet-filtering router có hai chức năng: chuyển tiếp truyền thông giữa hai mạng và sử dụng các quy luật về lọc gói để cho phép hay từ chối truyền thông. Căn bản, các quy luật lọc được định nghĩa sao cho các host trên mạng nội bộ được quyền truy nhập trực tiếp tới Internet, trong khi các host trên Internet chỉ có một số giới hạn các truy nhập vào các máy tính trên mạng nội bộ. Tư tưởng của mô cấu trúc Firewall này là tất cả những gì không được chỉ ra rõ ràng là cho phép thì có nghĩa là bị từ chối.



(a) Packet-filtering router

Hình 4: Packet-filtering router

Ưu điểm:

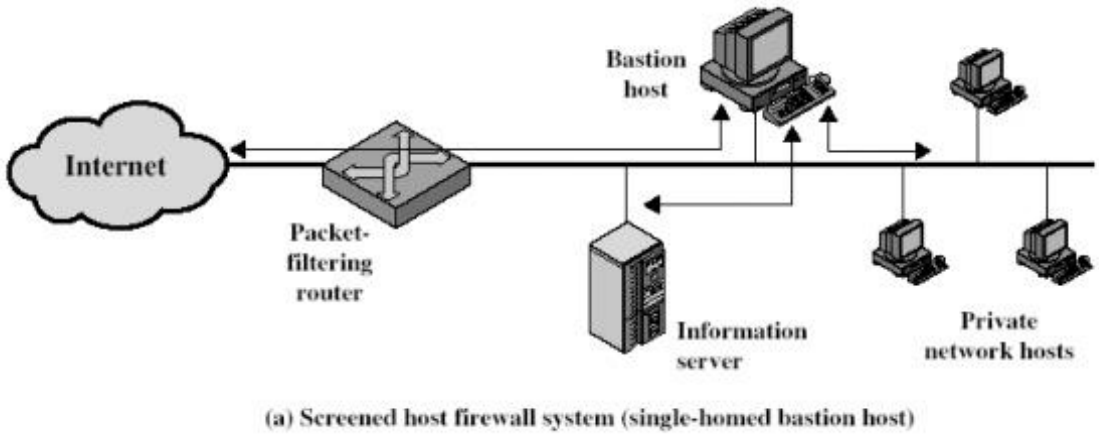
- Giá thành thấp (vì cấu hình đơn giản)
- Trong suốt đối với người sử dụng

Hạn chế:

- Có tất cả hạn chế của một packet-filtering router, như là dễ bị tấn công vào các bộ lọc mà cấu hình được đặt không hoàn hảo, hoặc là bị tấn công ngầm dưới những dịch vụ đã được phép.
- Bởi vì các packet được trao đổi trực tiếp giữa hai mạng thông qua router, nguy cơ bị tấn công quyết định bởi số lượng các host và dịch vụ được phép. Điều đó dẫn đến mỗi một host được phép truy nhập trực tiếp vào Internet cần phải được cung cấp một hệ thống xác thực phức tạp, và thường xuyên kiểm tra bởi người quản trị mạng xem có dấu hiệu của sự tấn công nào không.
- Nếu một packet-filtering router do một sự cố nào đó ngừng hoạt động, tất cả hệ thống trên mạng nội bộ có thể bị tấn công.

5.4.2. Screened Host Firewall

Hệ thống này bao gồm một packet-filtering router và một bastion host (hình 2.5). Hệ thống này cung cấp độ bảo mật cao hơn hệ thống trên, vì nó thực hiện cả bảo mật ở tầng network (packet-filtering) và ở tầng ứng dụng (application level). Đồng thời, kẻ tấn công phải phá vỡ cả hai tầng bảo mật để tấn công vào mạng nội bộ



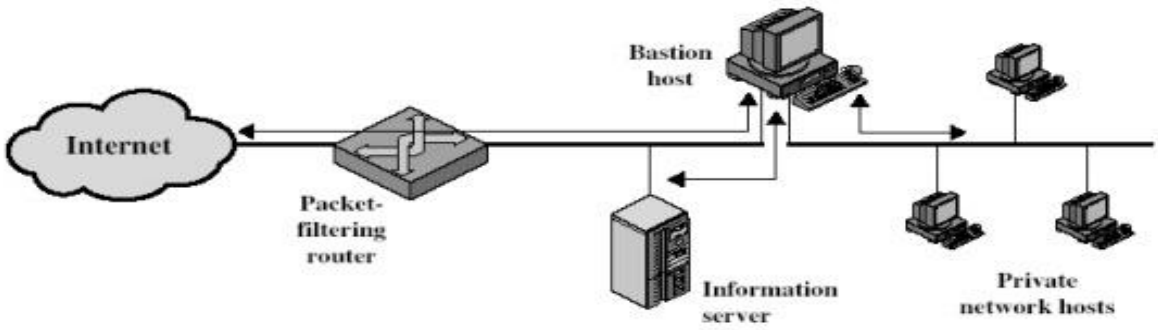
(a) Screened host firewall system (single-homed bastion host)

Hình 5: Screened host Firewall (Single- Homed Bastion Host)

Trong hệ thống này, bastion host được cấu hình ở trong mạng nội bộ. Qui luật filtering trên packet-filtering router được định nghĩa sao cho tất cả các hệ thống ở bên ngoài chỉ có thể truy nhập bastion host; Việc truyền thông tới tất cả các hệ thống bên trong đều bị khoá. Bởi vì các hệ thống nội bộ và bastion host ở trên cùng một mạng, chính sách bảo mật của một tổ chức sẽ quyết định xem các hệ thống nội bộ được phép truy nhập trực tiếp vào bastion Internet hay là chúng phải sử dụng dịch vụ proxy trên bastion host. Việc bắt buộc những user nội bộ được thực hiện bằng cách đặt cấu hình bộ lọc của router sao cho chỉ chấp nhận những truyền thông nội bộ xuất phát từ bastion host.

Ưu điểm:

- Máy chủ cung cấp các thông tin công cộng qua dịch vụ Web và FTP có thể đặt trên packet-filtering router và bastion. Trong trường hợp yêu cầu độ an toàn cao nhất, bastion host có thể chạy các dịch vụ proxy yêu cầu tất cả các user cả trong và ngoài truy nhập qua bastion host trước khi nối với máy chủ. Trường hợp không yêu cầu độ an toàn cao thì các máy nội bộ có thể nối thẳng với máy chủ.
- Nếu cần độ bảo mật cao hơn nữa thì có thể dùng hệ thống Firewall dual-home (hai chiều) bastion host (hình 2.6). Một hệ thống bastion host như vậy có 2 giao diện mạng (network interface), nhưng khi đó khả năng truyền thông trực tiếp giữa hai giao diện đó qua dịch vụ proxy là bị cấm.



(b) Screened host firewall system (dual-homed bastion host)

Hình 6: Screened host Firewall (Dual- Homed Bastion Host)

Bởi vì bastion host là hệ thống bên trong duy nhất có thể truy nhập được từ Internet, sự tấn công cũng chỉ giới hạn đến bastion host mà thôi. Tuy nhiên, nếu như người dùng truy nhập được vào bastion host thì họ có thể dễ dàng truy nhập toàn bộ mạng nội bộ. Vì vậy cần phải cấm không cho người dùng truy nhập vào bastion host.

5.4.3. Demilitarized Zone hay Screened-subnet Firewall

Hệ thống này bao gồm hai packet-filtering router và một bastion host (hình 2.7). Hệ thống Firewall này có độ an toàn cao nhất vì nó cung cấp cả mức bảo mật: network và application trong khi định nghĩa một mạng "phi quân sự". Mạng DMZ đóng vai trò như một mạng nhỏ, cô lập đặt giữa Internet và mạng nội bộ. Cơ bản, một DMZ được cấu hình sao cho các hệ thống trên Internet và mạng nội bộ chỉ có thể truy nhập được một số giới hạn các hệ thống trên mạng DMZ, và sự truyền trực tiếp qua mạng DMZ là không thể được.

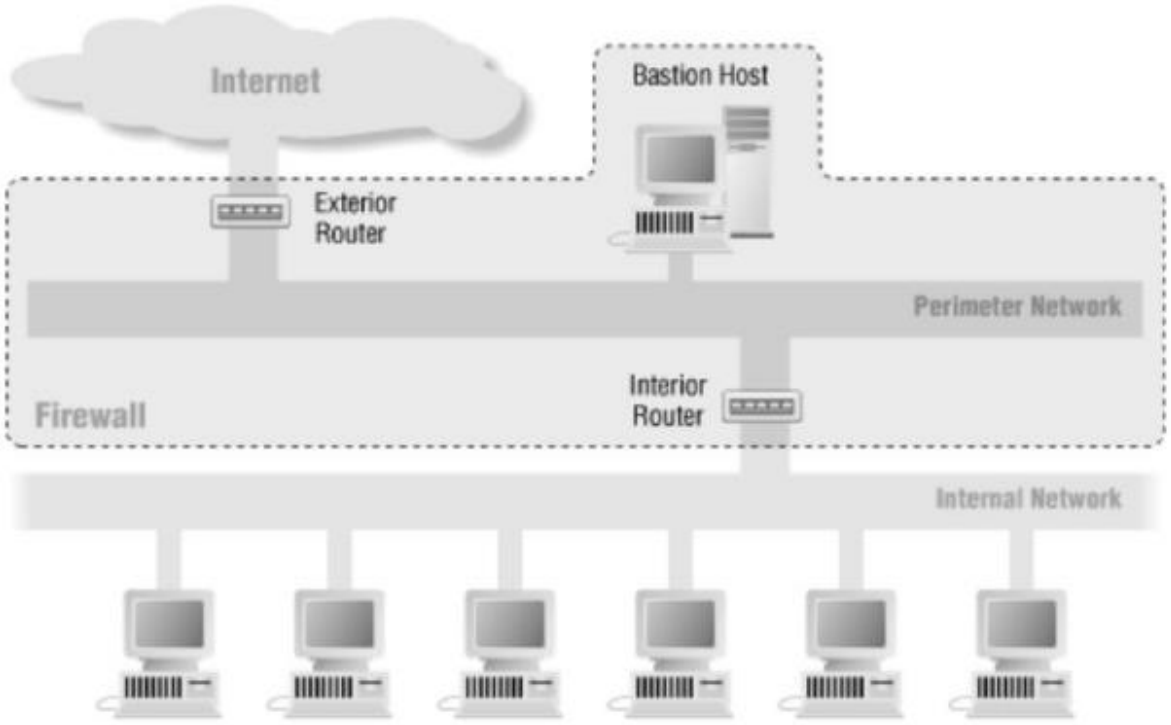
Với những thông tin đến, router ngoài chống lại những sự tấn công chuẩn (như giả mạo địa chỉ IP), và điều khiển truy nhập tới DMZ. Nó cho phép hệ thống bên ngoài truy nhập chỉ bastion host, và có thể cả information server. Router trong cung cấp sự bảo vệ thứ hai bằng cách điều khiển DMZ truy nhập mạng nội bộ chỉ với những truyền thông bắt đầu từ bastion host.

Với những thông tin đi, router trong điều khiển mạng nội bộ truy nhập tới DMZ. Nó chỉ cho phép các hệ thống bên trong truy nhập bastion host và có thể cả information server. Quy luật filtering trên router ngoài yêu cầu sử dung dịch vụ proxy bằng cách chỉ cho phép thông tin ra bắt nguồn từ bastion host.

Ưu điểm:

- Kẻ tấn công cần phá vỡ ba tầng bảo vệ: router ngoài, bastion host và router trong.
- Bởi vì router ngoài chỉ quảng cáo DMZ network tới Internet, hệ thống mạng nội bộ là không thể nhìn thấy (invisible). Chỉ có một số hệ thống đã được chọn ra trên DMZ là được biết đến bởi Internet qua routing table và DNS information exchange (Domain Name Server).
- Bởi vì router trong chỉ quảng cáo DMZ network tới mạng nội bộ, các hệ thống trong mạng nội bộ không thể truy nhập trực tiếp vào Internet. Điều

nay đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ proxy.



Hình 7: Screened-Subnet Firewall

5.4.4.ISA (Internet Security Access)

ISA là một trong những phần mềm phổ biến và tốt nhất về bảo mật hiện nay dùng cho HDH window

ISA Server 2004 được thiết kế để bảo vệ Mạng, chống các xâm nhập từ bên ngoài lẫn kiểm soát các truy cập từ bên trong Mạng nội bộ của một tổ chức. ISA Server 2004 Firewall làm điều này thông qua cơ chế điều khiển những gì có thể được phép qua Firewall và những gì sẽ bị ngăn chặn. Chúng ta hình dung đơn giản như sau: Có một quy tắc được áp đặt trên Firewall cho phép thông tin được truyền qua Firewall, sau đó những thông tin này sẽ được "Pass" qua, và ngược lại nếu không có bất kì quy tắc nào cho phép những thông tin ấy truyền qua, những thông tin này sẽ bị Firewall chặn lại.

ISA Server 2004 Firewall chứa nhiều tính năng mà các Security Admin có thể dùng để đảm bảo an toàn cho việc truy cập Internet, và cũng bảo đảm an ninh cho các tài nguyên trong Mạng nội bộ. Cuốn sách cung cấp cho các Security Admin hiểu được những khái niệm tổng quát và dùng những tính năng phổ biến, đặc thù nhất trên ISA SERVER 2004, thông qua những bước hướng dẫn cụ thể (Steps by Steps)

Firewalls không làm việc trong một môi trường không có gì, đơn giản là chúng ta triển khai Firewall để bảo vệ một cái gì đó, có thể là một PC, một Server hay cả một hệ thống Mạng với nhiều dịch vụ được triển khai như Web, Mail, Database….

Chúng ta sẽ có một hướng dẫn đầy đủ về việc triển khai các dịch vụ cần thiết cho hoạt động mạng của một tổ chức. Cách thức cài đặt và cấu hình những dịch vụ này như thế nào. Và điều tối quan trọng là Mạng và các dịch vụ phải được cấu hình đúng cách trước khi triển khai Firewall. Điều này giúp chúng ta tránh được những vấn đề phiền toái nảy sinh khi triển khai ISA SERVER 2004.

KẾT LUẬN.

Có thể nói, An ninh là một quá trình liên tục. Một khi bạn muốn hoàn thành cài đặt ban đầu hoặc triển khai đầy đủ, bạn phải tiếp tục cảnh giác. Kẻ gian liên tục cố gắng để đạt được quyền truy cập vào tài nguyên của bạn. Bạn phải thận trọng và liên tục đảm bảo an ninh mạnh mẽ được áp dụng và kiểm tra toàn bộ tổ chức của bạn để có một cơ hội tốt để bảo vệ tài sản của bạn.

Bài tiểu luận được tổng hợp từ nhiều nguồn tài liệu trong và ngoài nước được nhóm tìm hiểu và đúc kết lại. Việc dịch từ các nguồn tài liệu nước ngoài sẽ không tránh khỏi sai sót trong quá trình làm bài rất mong nhận được những góp ý và nhận xét từ thầy và các bạn đọc.

TÀI LIỆU THAM KHẢO

An toàn thông tin – Lê Văn Phùng

Giáo trình Cơ sở an toàn thông tin – Nguyễn Khanh Vân

Windows Server 2003 Security Guide (Microsoft Solutions forSecurity and Compliance)

Cryptography and Network Security - CS8792, CS6701

Building Internet Firewalls - D. Brent Chapman & Elizabeth D. Zwicky

----------Hết----------