BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

TS. LƯƠNG THẾ DŨNG

KS. CAO MINH TUẤN

GIÁO TRÌNH

QUẢN TRỊ AN TOÀN HỆ THỐNG

HÀ NỘI, 2013

BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

TS. LƯƠNG THẾ DŨNG

KS. CAO MINH TUẤN

GIÁO TRÌNH

QUẢN TRỊ AN TOÀN HỆ THỐNG

HÀ NỘI, 2013

MỤC LỤC

DANH MỤC VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
ACE	Access Control Entry	Danh sách kiểm soát đầu vào
ACL	Access Control List	Danh sách kiểm soát truy cập
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ
DAC	Discretionary Access Control	Kiểm soát truy cập tùy ý
DDoS	Distributed Denial Of Service	Tấn công từ chối dịch vụ phân tán
DoS	Denial of Service	Tấn công từ chối dịch vụ
DRDoS	Distributed Reflection Denial of Service	Tấn công từ chối dịch vụ bằng phương pháp phản xạ nhiều vùng
EAP	Extensible Authentication Protocol	Giao thức xác thực mở rộng
GLBA	Gramm Leach Bliley Act	Quy tắc bảo bệ bí mật thông tin cá nhân về tài chính
HIPAA	Health Insurance Portability and Accountability Act	Quy tắc bảo vệ thông tin người dùng cá nhân
L2TP	Layer 2 Tunneling Protocol	Giao thức mã hóa đường hầm lớp 2
MAC	Media Access Control	Địa chỉ vật lý của giao diện mạng
MAC	Mandatory Access Control	Kiểm soát truy cập bắt buộc
MIC	Message Integrity Check	Kiểm tra toàn vẹn thông điệp
MTA	Mail Tranfer Agent	Trạm trung chuyển thư
NFS	Network File System	Hệ thống tệp tin mạng
OASIS	Organization for the Advancement of Structured	Tổ chức tiêu chuẩn về nâng

	Information Standards	cao thông tin có cấu trúc
OSI	Open Systems Interconnection	Mô hình tham chiếu kết nối các hệ thống mở
RBAC	Role-based Access Control	Kiểm soát truy cập dựa vào vai trò
SAN	Storage Area Network	Mạng lưu trữ
SMB	Server Message Block	Khối tin báo của máy chủ
SOAP	Simple Object Access Protocol	Giao thức truy cập đối tượng đơn giản
SSID	Service Set Identifier	Định danh dịch vụ
UCE	Unsolicited Comercial Email	Thư thương mại không được yêu cầu
URL	Uniform Resource Locator	Địa chỉ tham chiếu tài nguyên Internet
VPN	Virtual Private Network	Mạng riêng ảo
WAP	Wireless Application Protocol	Giao thức ứng dụng không dây
WLAN	Wireless local area network	Mạng cục bộ không dây
WSDL	Web Services Description Language	Ngôn ngữ miêu tả dịch vụ Web
WSPA	WS-Policy Attachment	Chính sách đính kèm dịch vụ Web
XACML	eXtensible Access Control Markup Language	Ngôn ngữ đánh dấu điều khiển truy cập mở rộng
XKMS	XML Key Management Specification	Quản lý khóa đặc biệt XML
XSLT	Extensible Stylesheet Language Transformations	Ngôn ngữ chuyển đổi mở rộng XML

DANH MỤC BẢNG

DANH MỤC CÁC HÌNH VẼ

LỜI NÓI ĐẦU

Ngày nay, công nghệ thông tin (CNTT) đang phát triển với nhịp độ nhanh, loại hình ngày càng phức tạp và xu hướng toàn cầu hoá rất rõ nét kéo theo các vấn đề ứng dụng rất đa dạng và đi sâu vào mọi hoạt động của con người. Các hệ thống công nghệ thông tin của mọi ngành nghề của mỗi quốc gia đã hình thành và kết nối lại tạo ra hạ tầng công nghệ thông tin toàn cầu thống nhất và rộng khắp trong mọi hoạt động tin học hoá.

Tuy nhiên, cùng với sự phát triển nhanh và mạnh của CNTT trong năm qua đã phát sinh nhiều lỗ hổng trong công tác an ninh bảo mật. Các nguy cơ và hình thức mất an toàn thông tin ngày một đa dạng, phức tạp. Mức độ nguy hiểm ngày một gia tăng. Bởi vậy nhu cầu đảm bảo an toàn thông tin trong các hoạt động trên mạng CNTT ngày càng trở nên cấp thiết.

An toàn hệ thống là một quá trình liên tục gắn liền với các hoạt động hàng ngày của các cán bộ chuyên trách, các hoạt động này là một quá trình được lặp đi lặp lại và được quản lý nhằm giảm thiểu các nguy cơ và nâng cao hiệu quả sử dụng của hệ thống. Quá trình này bao gồm bốn giai đoạn: đảm bảo an ninh, giám sát, đánh giá và cải tiến. Giáo trình "Quản trị an toàn hệ thống" cung cấp các kiến thức và kỹ năng để thực hiện cả bốn giai đoạn trên, nội dung của giáo trình bao gồm:

Chương 1: Tổng quan về quản trị an toàn hệ thống

Nội dung của chương này giới thiệu chung về các nguy cơ gây mất an toàn đối với hệ thống mạng, và trình bày các loại hình tấn công chính lên hệ thống. Từ đó nêu tổng quan về quản trị an toàn cho hệ thống mạng.

Chương 2: Thiết lập an toàn cho hệ thống mạng

Nội dung của chương này trình bày về các phương pháp cần phải thực hiện đối với hệ thống mạng như: phân vùng an toàn, thiết lập an toàn cho hệ điều hành mạng, thiết lập các nền tảng xác thực an toàn.

Chương 3: Thiết lập an toàn cho các dịch vụ mạng

Nội dung của chương này trình bày chi tiết về cách thức thiết lập, cấu hình an toàn cho các dịch vụ mạng như: dịch vụ web, cơ sở dữ liệu, thư tín điện tử.

Chương 4: Thiết lập an toàn cho mạng không dây

Chương này trình bày các phương thức thiết lập sử dụng mã hóa và xác thực đảm bảo an toàn cho mạng không dây, xây dựng chính sách an toàn cho mạng không dây. Tìm và loại bỏ các mạng không dây giả mạo.

Chương 5: Triển khai công nghệ phòng thủ mạng

Nội dung chương này trình bày cách thức thiết lập, cấu hình các công nghệ bảo mật cho hệ thống mạng. Bao gồm các công nghệ tường lửa, công nghệ phát hiện và ngăn chặn xâm nhập. Các phương pháp quản lý mã độc hại.

Chương 6: Quản lý và vận hành an toàn hệ thống

Nội dung chương này trình bày về các vấn đề liên quan tới quản lý và xử lý khi có sự cố xảy ra đối với hệ thống mạng như: quản lý sự thay đổi đối với hệ thống, quản lý cập nhật các bản vá cho phần mềm hoạt động trong hệ thống, quản lý các sự cố an toàn thông tin.

Giáo trình này được biên soạn lần đầu và tài liệu tham khảo chính là "Hardening Network Security" của John Mallery và nhiều tài liệu khác. Mặc dù nhóm tác giả đã hết sức cố gắng nhưng chắc chắn giáo trình không thể tránh được những thiếu sót, vì vậy chúng tôi rất mong nhận được những ý kiến đóng góp của các đồng nghiệp và các bạn đọc quan tâm.

Hà Nội, tháng 9 năm 2013

Các tác giả

Chương 1.
TỔNG QUAN VỀ QUẢN TRỊ AN TOÀN HỆ THỐNG

1.1. KHÁI NIỆM VỀ AN TOÀN HỆ THỐNG

Thông tin được lưu trữ bởi các sản phẩm và hệ thống công nghệ thông tin là tài nguyên, tài sản quan trọng cho sự thành công của mỗi tổ chức. Các thông tin mang tính riêng tư của mỗi cá nhân hay tổ chức lưu trữ trong hệ thống thông tin cần được bảo vệ để giữ bí mật và không bị thay đổi khi không được phép. Trong khi các sản phẩm và hệ thống công nghệ thông tin thực hiện các chức năng của chúng, các thông tin cần được kiểm soát để đảm bảo chúng được bảo vệ chống lại các nguy cơ, ví dụ như việc phổ biến và thay đổi thông tin không mong muốn hoặc trái phép, nguy cơ mất mát thông tin.

An toàn hệ thống là các kỹ thuật nhằm đảm bảo cho các hoạt động của các cơ sở hạ tầng thông tin, trong đó bao gồm an toàn phần cứng và phần mềm theo các tiêu chuẩn kỹ thuật do nhà nước ban hành; duy trì các tính chất bí mật, toàn vẹn, chính xác, sẵn sàng phục vụ của thông tin trong lưu trữ, xử lý và truyền tải trên các hệ thống.

Tính bí mật: là tâm điểm chính của mọi giải pháp an toàn cho một sản phẩm/hệ thống Công nghệ thông tin. Một giải pháp an toàn là tập hợp các quy tắc xác định quyền được truy cập đến với thông tin đang tìm kiếm, đối với một số lượng người sử dụng thông tin nhất định và một số lượng thông tin là tài sản nhất định. Trong trường hợp kiểm soát truy cập cục bộ, nhóm người truy cập sẽ được kiểm soát xem là họ đã truy cập những số liệu nào. Tính bí mật là sự đảm bảo rằng các chức năng kiểm soát truy cập có hiệu lực. Đảm bảo tính bí mật là nhằm loại bỏ những sự truy cập không được phép vào các khu vực là độc quyền của các cá nhân, tổ chức.

Tính toàn vẹn (không bị sửa đổi): là đặc tính phức tạp nhất và dễ bị hiểu lầm của thông tin. Một định nghĩa khái quát hơn được sử dụng ở trong tài liệu này là vấn đề chất lượng của số liệu (thông tin), chứ không phải là con người được hoặc không được phép truy cập. Tính toàn vẹn được hiểu là chất lượng của thông tin được xác định căn cứ vào độ chính xác khi phản ánh thực tế. Số liệu càng gần với thực tế bao nhiêu thì chất lượng thông tin càng chuẩn

bấy nhiêu. Để đảm bảo tính toàn vẹn của thông tin là một loạt các biện pháp đồng bộ nhằm hỗ trợ và đảm bảo tính thời sự kịp thời và sự đầy đủ trọn vẹn, cũng như sự bảo mật hợp lý cho thông tin.

Tính sẵn sàng: Là một đặc tính quan trọng, không khác gì các đặc tính bí mật và toàn vẹn. Đó là khía cạnh sống còn của an toàn thông tin, đảm bảo cho thông tin đến đúng địa chỉ (người được phép sử dụng) khi có nhu cầu, hoặc được yêu cầu. Tính sẵn sàng đảm bảo độ ổn định đáng tin cậy của thông tin, cũng như đảm nhiệm chức năng là thước đo, xác định phạm vi tới hạn của an toàn một hệ thống thông tin.

1.2. CÁC NGUYÊN NHÂN GÂY MẤT AN TOÀN HỆ THỐNG

Mục tiêu hướng tới của người dùng là bảo vệ các tài sản thông tin của họ. Tuy nhiên, các sản phẩm và hệ thống thường luôn tồn tại những điểm yếu dẫn đến những rủi ro có thể xảy ra, làm tổn hại đến giá trị tài sản thông tin. Các đối tượng tấn công (tin tặc) có chủ tâm đánh cắp, lợi dụng hoặc phá hoại tài sản của các chủ sở hữu, tìm cách khai thác các điểm yếu để tấn công, tạo ra các nguy cơ và các rủi ro cho các hệ thống.

Tồn tại rất nhiều nguyên nhân ảnh hưởng tới an ninh, trong đó phải kể đến ba loại điểm yếu cơ bản ảnh hưởng trực tiếp đối với an ninh đó là:

- Điểm yếu công nghệ
- Điểm yếu chính sách
- Cấu hình yếu.

Rõ ràng ở đây có thể đưa thêm các điểm yếu về con người và một số loại điểm yếu khác, nhưng mục đích của giáo trình là tập trung vào những vấn đề liên quan đến các công nghệ và những vấn đề quản lý các công nghệ được triển khai trên hệ thống.

1.2.1. Điểm yếu công nghệ

Mỗi công nghệ thường tồn tại các điểm yếu (lỗ hổng bảo mật) đã được phát hiện hoặc chưa được phát hiện. Các điểm yếu thường là nhân tố không mong muốn trong các mã phần mềm hoặc hệ thống, sẽ tạo điều kiện cho kẻ

tấn công có khả năng khai thác theo phương thức truy cập trái phép hoặc thực hiện các hành vi phá hoại như virus, worm, trojan và nhiều phương thức khác, các phương thức này được gọi chung là khai thác lỗ hổng bảo mật. Có nhiều loại lỗ hổng bảo mật như do lỗi logic trong lập trình phần mềm, mật khẩu yếu, phần mềm đã bị nhiễm một loại virus máy tính hoặc tiêm mã kịch bản...

- **Điểm yếu trong TCP/IP:**

TCP/IP là một bộ các giao thức được phát triển để cho phép các máy tính truyền thông, chia sẻ tài nguyên qua mạng. Các giao thức trong TCP/IP được sử dụng rất rộng rãi ngày nay, tuy nhiên tồn tại một lượng lớn các lỗ hổng bảo mật cố hữu có thể dẫn đến nhiều phương thức tấn công thông qua các giao thức của TCP/IP như: chặn bắt gói tin, từ chối dịch vụ, giả mạo địa chỉ IP, chiếm quyền điều khiển, chuyển hướng giáo thức TCP, …

- **Trong máy tính và hệ điều hành mạng:**

Một hệ điều hành mạng là một tập hợp các phần mềm quản lý tài nguyên phần cứng máy tính và cung cấp dịch vụ chung cho các chương trình máy tính. Vì vậy, bất cứ một hệ điều hành nào cũng có những lỗ hổng bảo mật cần được khắc phục thông qua các bản vá, các bản nâng cấp, mỗi lần nâng cấp thì tùy vào mức độ nâng cấp sẽ làm thay đổi hệ điều hành nhằm loại bỏ các lỗ hổng đã biết. Tuy nhiên, trong khi các nhà sản xuất đều cố gắng cung cấp một sản phẩm an toàn cho người dùng thì việc bổ sung các tiêu chuẩn mới, tính năng mới thậm chí nâng cấp phần cứng có thể dẫn đến các điểm yếu mới mà nhà sản xuất không thể lường trước.

- **Các điểm yếu trong thiết bị mạng:**

Hầu hết các thiết bị mạng đều tồn tại các lỗ hổng bảo mật có thể bị khai thác. Một số chương trình phần mềm được tích hợp sẵn trong các thiết bị có thể an toàn trong một thời gian dài trước khi một người nào đó vô tình kích hoạt các điểm yếu tồn tại và gây ảnh hưởng đến an ninh cho hệ thống. Khi các bản vá lỗi của hệ thống được phát hành, hệ thống được nâng cấp ở mức tốt nhất có thể làm giảm thiểu hoặc loại bỏ các nguy cơ do các lỗ hổng gây ra.

1.2.2. Điểm yếu trong chính sách

Chính sách an toàn thông tin của công ty được lập ra để đảm bảo an toàn cho hệ thống, song nó cũng có những điểm yếu, lỗ hổng. Chính sách có thể xuất hiện điểm yếu sau một quá trình sử dụng hoặc sau một quá trình nâng cấp hệ thống. Các ví dụ sau minh họa cho các vấn đề có thể ảnh hướng xấu đến an toàn của hệ thống trong công ty:

- ✓ Không có các văn bản chính sách an toàn thông tin: việc thiếu một tài liệu chuyên môn có nghĩa là không có một kế hoạch cụ thể để chống lại các nguy cơ có thể xảy ra đối với hệ thống.
- ✓ Thiếu kế hoạch khôi phục sau thảm họa: Nếu không có một kế hoạch chi tiết, thì những nỗ lực chống lại cuộc tấn công hay trong những trường hợp khẩn cấp như bão lụt, hỏa hoạn sẽ để lại những hậu quả nghiêm trọng, việc có những kế hoạch cụ thể sẽ đem lại một lợi thế khi thảm họa xảy ra.
- ✓ Không có chính sách cho phần mềm, phần cứng khi có sự thay đổi bổ sung. Cho dù với nguyên nhân nào thì việc bổ sung các ứng dụng, các phần mềm hay việc thay thế, nâng cấp phần cứng có thể xảy ra bất cứ khi nào. Việc thay đổi này có thể dẫn tới các nguy cơ an toàn, an ninh thông tin. Khi đó nếu chính sách không theo kịp việc thay đổi này sẽ tạo cơ hội cho các kẻ tấn công thực hiện tấn công gây hại cho hệ thống.
- ✓ Thiếu kế hoạch giám sát an ninh: Một hệ thống mạng dù an toàn tới đâu cũng luôn luôn cần được theo dõi một cách thường xuyên, quá trình theo dõi này sẽ phát hiện ra các lỗ hổng mới, các phương thức tấn công mới khi chúng chưa được khai thác để gây ra những tổn thất nghiêm trọng cho hệ thống.
- ✓ Chính sách với con người, hệ thống nhân viên luôn thay đổi, chất lượng cũng không đồng nhất do đó chính sách đối với các nhân viên làm việc trong hệ thống luôn cần thiết, để đảm bảo an toàn cho chính những nhân viên này cũng như hệ thống.

Chính sách nội bộ là quy định về cách xử lý đối với các trường hợp vi phạm, tạo ra các quy tắc, các chuẩn đối với mỗi cá nhân trong hệ thống giúp

họ vượt qua, các sơ suất, cám dỗ và các vấn đề cạnh tranh nội bộ không lành mạnh hay việc mâu thuẫn nội bộ có thể gây ra các lỗ hổng khó lường trước.

1.2.3. Cấu hình yếu

Nhiều thiết bị mạng được sử dụng theo nhu cầu về hiệu suất mà không quan tâm đến các vấn đề an ninh hoặc do việc thiết lập an ninh trên các thiết bị này yếu về mặt an ninh, dẫn đến nhiều vấn đề an ninh khác nhau như:

- ✓ Danh sách kiểm soát truy nhập không hiệu quả để ngăn chặn truy cập trái phép.
- ✓ Mật khẩu dùng trong hệ thống không mạnh, sử dụng mật khẩu mặc định, mật khẩu cũ, mật khẩu thuộc từ điển.
- ✓ Cổng dịch vụ mở khi không cần thiết.
- ✓ Tài khoản người dùng và mật khẩu được trao đổi khi không được mã hóa hoặc được lưu trữ khi không được bảo vệ.
- ✓ Các dịch vụ an ninh cho việc truy cập từ xa thông qua Internet không đủ mạnh.

1.3. CÁC HIỂM HỌA CHÍNH ĐỐI VỚI AN TOÀN HỆ THỐNG

Phân loại các hiểm họa vừa làm hiểu rõ hơn về các hiểm họa vừa tìm ra các biện pháp ngăn chặn chúng, dưới đây là 4 loại hiểm họa mà ta thường gặp:

- Hiểm họa không có cấu trúc
- Hiểm họa có cấu trúc
- Hiểm họa từ bên trong
- Hiểm họa từ bên ngoài

1.3.1. Các hiểm họa không có cấu trúc

Loại này thường liên quan đến các cuộc tấn công có tính chất tự phát, xảy ra với tất cả các hệ thống mạng, thường do các cá nhân có kĩ năng hạn chế hoặc tò mò thử nghiệm. Những hệ thống bị tấn công và xâm nhập thường

không biết thủ phạm là ai. Kẻ tấn công có thể không có mục đích xấu, nhưng họ lại hoàn toàn thờ ơ với những thiệt hại do mình gây ra.

Để thực hiện các tấn công, kẻ tấn công thường có thể tìm hiểu các tài liệu và thu thập các công cụ tấn công được phổ biến trên nhiều trang web trên Internet, hầu hết các công cụ là những đoạn mã nhỏ và thường do một cá nhân viết ra và chia sẻ cho cộng đồng, ví dụ như virus, worm hay Trojan horse, dưới đây là một số thuật ngữ phổ biến:

- ✓ Virus: Virus là một loại mã độc hại có khả năng tự nhân bản và lây nhiễm chính nó vào các file, chương trình hoặc máy tính. Virus phải luôn bám vào vật chủ (có thể là file dữ liệu hoặc file ứng dụng) để thực hiện lây lan.
- ✓ Worm: Là một dạng của mã độc lây lan bằng cách tạo ra các bản sao của chính nó trên ổ đĩa, hệ thống hay thông qua mạng. Ví dụ: Worm hoạt động với một hệ thống thư điện tử có thể gửi những bản sao của nó tới tất cả địa chỉ thư điện tử ở trong danh sách. Code Red và Nimda là những loại worm tiêu biểu gây ra nhiều thiệt hại đáng kể trong những năm trở lại đây.
- ✓ Trojan horse: Là một chương trình máy tính thường được thể hiện như một chương trình giải trí hoặc đem lại lợi ích rõ ràng, có thể là một trò chơi hoặc chương trình bảo vệ màn hình, nhưng phía sau nó lại có thể thực hiện những tác vụ khác như là xóa hoặc thay đổi dữ liệu, chụp lại mật khẩu hay các tổ hợp phím để gửi các thông tin này qua mạng. Về mặt kỹ thuật, Trojan horse không phải là một loại virus bởi vì nó không có khả năng tự nhân bản.

Những kẻ phát động một cuộc tấn công không có cấu trúc thường được gọi là script kiddy vì chúng thường thiếu những kỹ năng để tự phát triển chương trình của riêng mình. Email là một phương tiện chính để thực hiện việc phát tán loại tấn công này.

Những tấn công không có cấu trúc chứa đoạn mã tự tái tạo lại chính nó và gửi một bản sao tới tất cả mọi người có trong danh sách thư điện tử mà có thể dễ dàng phát tán rộng rãi chỉ trong vài giờ, gây ra những vấn đề cho hệ

thống mạng và các tổ chức trên toàn thế giới. Ban đầu, cuộc tấn công được thực hiện không hẳn với mục đích gây hại, nhưng kết quả có thể làm mất sự truy cập của người dùng hợp pháp, mất uy tín vào công ty khi mà tin tức về cuộc tấn công bị lọt ra ngoài, hoặc cũng có thể là sự mất quyền tự do của người dùng khi áp đặt các chính sách mới chặt chẽ hơn với mục đích triển khai để bảo vệ hệ thống khỏi những cuộc tấn công khác. Ngoài ra đối với mạng của các tổ chức bị tấn công có thể làm ngưng hoạt động kinh doanh của họ, dẫn đến hậu quả của các cuộc tấn công gây ra có thể quy ra giá trị được tính bằng tiền bị mất trong khoảng thời gian ngừng hoạt động.

1.3.2. Các hiểm họa có cấu trúc

Các mối đe dọa có cấu trúc tập trung hơn bởi một hoặc nhiều cá nhân có những kỹ năng cao cấp tích cực làm việc để gây tổn hại cho hệ thống. Hệ thống mục tiêu có thể bị phát hiện thông qua một vài quá trình tìm kiếm ngẫu nhiên, hoặc có thể đã được lựa chọn một cách đặc biệt. Những kẻ tấn công thường có kiến thức về thiết kế mạng, an toàn mạng, các quy trình truy cập, các công cụ tấn công và họ có khả năng tạo ra các kịch bản hoặc ứng dụng để phá hoại mục tiêu sâu hơn.

Các cuộc tấn công có cấu trúc thường không phải vì mục đích tò mò hay vì muốn khoe khoang với người nào đó. Sự tham lam, mục đích chính trị, phân biệt chủng tộc hoặc bất kì sự cực đoan nào đều có thể là động cơ đằng sau những hành động của tin tặc. Các loại tội phạm có động cơ tấn công không nhằm mục đích thu lợi trực tiếp mà chỉ ăn cắp các thông tin cho các mục đích khác như đánh cắp danh tính hoặc trộm cắp thông tin thẻ tín dụng.

Các cuộc tấn công lên hệ thống máy tính của nước khác được tài trợ bởi các tổ chức khủng bố thế giới hoặc bởi chính phủ cũng xuất hiện ngày một nhiều. Các hệ thống bị tấn công thường liên quan đến các hạ tầng thông tin cho các dịch vụ công cộng như: hệ thống giao thông, hệ thống tài chính hoặc các hệ thống phòng thủ, tất cả đều được quản lý bởi hệ thống dữ liệu lớn – với nhiều lỗ hổng.

1.3.3. Các hiểm họa từ bên trong

Các hiểm họa từ bên trong xuất phát từ cá nhân có hoặc đã được phép truy cập vào mạng. Đây có thể là một nhân viên bất mãn, một kẻ cơ hội, hoặc một nhân viên không hài lòng với công ty từ trước mà vẫn có quyền truy cập. Trong trường hợp nhân viên đó là một nhân viên quản trị mạng, ngay cả khi tài khoản của họ đã bị xóa, họ có thể sử dụng một tài khoản bị xâm nhập hoặc các thiết lập trước khi nghỉ việc để phục vụ cho mục đích này.

Nhiều cuộc khảo sát và nghiên cứu cho thấy các cuộc tấn công từ bên trong có số lượng và cả sự mất mát rất lớn. Tương tự như một nhân viên không trung thực đánh cắp hàng hóa, tiền mặt hoặc thực hiện các kế hoạch kỹ lưỡng để ăn cắp công quỹ, họ có thể học cách sử dụng hệ thống máy tính để thực hiện dã tâm của mình. Với việc được phép truy cập vào hệ thống, một nhân viên đáng tin cậy có thể phá hoại tổ chức mà không gây ra sự nghi ngờ nào.

Tất cả các nhà tuyển dụng thường rất khó phát hiện để truy cứu những kẻ thực hiện các kiểu tấn công này. Rất nhiều lý do dẫn đến khó khăn này như việc lo ngại tấn công này sẽ được cộng đồng biết đến, các hệ thống không có cơ chế để phát hiện, để đưa ra bằng chứng thuyết phục hoặc để chứng minh rằng các nghiệp vụ xử lý là đúng đắn và hợp pháp.

1.3.4. Các hiểm họa từ bên ngoài

Các hiểm họa từ bên ngoài là mối đe dọa từ các cá nhân bên ngoài tổ chức, thường xuyên sử dụng Internet thực hiện các tấn công vào trong hệ thống, những kẻ tấn công này không có quyền truy cập vào hệ thống.

Việc phân loại một hiểm họa cụ thể cũng chỉ mang tính chất tương đối vì một hiểm họa có thể là một sự kết hợp của hai hoặc nhiều mối hiểm họa khác nhau. Các cuộc tấn công có thể được sắp đặt từ một nguồn bên ngoài, nhưng một hành động tội phạm nguy hiểm cũng có thể được gây ra từ một hoặc nhiều nhân viên bất mãn từ bên trong chủ động tấn công.

1.4. CÁC LOẠI TẤN CÔNG CHÍNH LÊN HỆ THỐNG

Mặc dù có nhiều dạng và tên thường khác nhau nhưng chủ yếu và phổ biến nhất gồm 4 loại tấn công mạng là:

- Tấn công theo kiểu thăm dò
- Tấn công theo kiểu truy cập
- Tấn công theo kiểu từ chối dịch vụ
- Tấn công thao tác dữ liệu

1.4.1. Tấn công theo kiểu thăm dò

Một cuộc tấn công theo kiểu thăm dò là những nỗ lực của một người sử dụng trái phép nào đó để đạt được càng nhiều thông tin về hệ thống càng tốt trước khi đưa ra các hành động tấn công khác nghiêm trọng hơn. Việc thực hiện các cuộc tấn công thăm dò cũng có thể thực hiện được bằng cách sử dụng thông tin có sẵn.

1.4.1.1 Thu thập thông tin công khai

Tên nhân viên và địa chỉ e-mail cung cấp một khởi đầu tốt trong việc đoán tài khoản của khách hàng. Thực tế là phần lớn khách hàng sử dụng họ và tên làm tài khoản máy tính của họ. Địa chỉ Email cũng là một tài khoản thông thường hay được sử dụng. Các công ty lớn thường dùng số điện thoại đã được cấp phép bằng một đầu số điện thoại nhất định bằng cách sử dụng thông tin này kẻ tấn công có thể quay số tất cả các số nằm trong đầu số xác định để tìm ra một máy chủ truy cập từ xa. Khi một máy chủ truy cập từ xa được tìm thấy, kẻ xâm nhập có thể bắt đầu đoán tên tài khoản dựa trên các thông tin công cộng của công ty cũng như các nhân viên hoặc địa chỉ email của họ. Tiếp đến sử dụng các công cụ phá khóa có sẵn trên Internet để thực hiện đoán mật khẩu. Một tên người dùng được đoán ra thì mật khẩu không sớm thì muộn cũng sẽ bị phá.

War dialer là một chương trình được sử dụng để quay số khối của các số điện thoại cho đến khi nó tìm thấy một máy tính ở đầu bên kia của đường dây. Khi máy tính được tìm thấy việc sử dụng war dialer ghi lại số lượng cuộc gọi cho sử dụng sau này bởi những kẻ xâm nhập.

Để sử dụng một tài khoản người dùng trên một máy chủ hoặc một hệ thống đầu tiên cần phải có tên người dùng và mật khẩu. Việc phát hiện tên người dùng là một quá trình khá đơn giản đã được mô tả ở trên. Kẻ tấn công

sử dụng nhiều cách khác nhau để dò mật khẩu như việc dò mật khẩu từ tài khoản người dùng. Một số cách dò mật khẩu bằng cách tìm các tập tin mã hóa mật khẩu trên máy chủ và giải mã chúng. Khi một kẻ tấn công không có khả năng lấy các thông tin mật khẩu, kỹ thuật vét cạn sẽ được sử dụng để dò mật khẩu. Quá trình vét cạn sẽ cố gắng để đăng nhập vào một tài khoản máy tính nhiều lần, sử dụng nhiều mật khẩu khác nhau. Trong khi một số phần mềm dò quét sử dụng những từ điển mật khẩu thì một số khác thì thử kết hợp của các phím trên bàn phím.

Dưới đây là một số công cụ thường được sử dụng để dò quét mật khẩu:

Microsoft Windows	**UNIX**
L0phtCrack 4	Qcrack by the Crypt Keeper
PWLVIEW	CrackerJack by Jackal
Pwlhack 4.10	John the Ripper by Solar Designer
PWL-Key	Crack by Alec Muffet

Thông tin địa chỉ IP được công bố công khai thông qua ARIN và nhiều cơ quan đăng ký internet khác. Từ www.arin.net, bất cứ ai cũng có thể bắt đầu tìm kiếm thông tin về các tổ chức bằng cách sử dụng địa chỉ IP duy nhất được biết. Việc tìm kiếm sẽ mang lại một khối hoàn chỉnh của địa chỉ IP thuộc các tổ chức. DNS là một hệ thống được công bố công khai có thể cung cấp nhiều thông tin liên quan đến địa chỉ IP và tên của hầu hết các tổ chức có kết nối với Internet.

Đối với một tổ chức có hệ thống thư điện tử riêng, web, ftp hay các dịch vụ khác trên Internet, đồng thời họ sẽ phải có máy chủ được liệt kê trong cơ sở hạ tầng DNS. Các máy chủ DNS liệt kê tên của các máy chủ của tổ chức, cùng với các địa chỉ IP có thể được sử dụng để truy cập các dịch vụ này. Để giảm thiểu rủi ro các công ty, tổ chức có thể đặt các máy chủ và dịch vụ trên mạng của nhà cung cấp dịch vụ Internet, các máy chủ cơ sở dữ liệu được đặt tại mạng riêng và kết nối mạng của các nhà cung cấp dịch vụ với các mạng của tổ chức thông qua một kênh riêng.

1.4.1.2 Tấn công thăm dò

Tấn công thăm dò là một quá trình mà kẻ tấn công sử dụng các công cụ để thực hiện các dò quét để tìm ra các hệ thống và tài nguyên trên mạng. Trừ khi kẻ tấn công đã có thông tin về mạng mục tiêu, đầu tiên nó sẽ phải tìm địa chỉ logic mà các nguồn tài nguyên của tổ chức được định vị trên mạng. Khi đã biết địa IP của tổ chức, kẻ tấn công sẽ thực hiện các thăm dò và quét mạng để phát hiện các máy chủ dễ bị tổn thương, các ứng dụng, hoặc các thiết bị cơ sở hạ tầng đang có trên mạng mục tiêu.

Quét mạng thường được thực hiện bằng cách sử dụng các tiện ích như ping để ping một loạt địa chỉ IP. Mục đích của việc quét này là để tìm ra các host hiện đang có trên mạng để xác định mục tiêu khả thi trên mạng đích. Một khi địa chỉ IP của máy chủ được biết kẻ tấn công có thể bắt đầu thăm dò các host để thu thập thêm thông tin, chẳng hạn như hệ điều hành hoặc các ứng dụng, dịch vụ gì đang chạy trên các máy chủ.

Các công cụ tấn công phổ biến và được sử dụng rộng rãi nhất là các công cụ thăm dò. Trong số những công cụ này nhiều công cụ đã được phát triển bởi tin tặc để hỗ trợ chung trong các hoạt động bất hợp pháp. Các công cụ khác được tin tặc sử dụng có thể có cùng công dụng tương tự như các công cụ khác được sử dụng bởi các kỹ sư mạng để kiểm tra các vấn đề của hệ thống mạng. Ngày càng có nhiều công cụ sử dụng cho việc dò tìm và xâm nhập trái phép. Tuy nhiên, sự phát triển của các hệ thống phát xâm nhập trái phép đã cho phép phát hiện được phần lớn các hành động của các cụ này. Vì vậy, tin tặc bắt đầu phát triển phần mềm mới để giấu đi các mục đích thực sự của nó. Dưới đây là một số công cụ được sử dụng phổ biến trong tấn công thăm dò:

NMAP	WHOIS
SATAN	Ping
Portscanner	Nslookup
Strobe	Trace

1.4.2. Tấn công truy cập

Tấn công truy cập là các loại tấn công thực hiện các hành động truy cập trái phép tài nguyên máy tính. Một cuộc tấn công truy cập có thể được thực hiện từ một hoặc một nhóm cá nhân bên ngoài có sử dụng các phương pháp khác nhau để xâm nhập vào hệ thống mạng của các tổ chức từ đó đánh cắp thông tin bí mật hoặc tham gia hủy hoại tài nguyên của hệ thống. Một cuộc tấn công truy cập cũng có thể xuất phát từ một người sử dụng bên trong truy cập vào các dữ liệu mà họ không được phép sử dụng, ý định của họ có thể do sự hiếu kỳ hoặc giống như ý định của các tin tặc bên ngoài. Dưới đây là một số kiểu tấn công truy cập:

- Tấn công dựa trên mật khẩu phổ biến (Password Attack)
- Tấn công khai thác sự tin cậy (Trust Exploitation)
- Tấn công chuyển hướng cổng (Port Redirection)
- Tấn công Man in the middle
- Tấn công tràn bộ đệm (Buffer overflow)

1.4.2.1 Tấn công mật khẩu

Tấn công mật khẩu được thể hiện bằng một loạt các đăng nhập không thành công trong khoảng thời gian ngắn bởi một kẻ tấn công. Những nỗ lực được lặp đi lặp lại này được gọi là tấn công từ điển (dictionary attack) hay tấn công brute-force.

Để tiến hành một cuộc tấn công từ điển, kẻ tấn công có thể sử dụng các công cụ để tự động lặp lại việc đăng nhập như một người dùng bằng cách sử dụng những từ trong từ điển. Tấn công từ điển thường thành công vì người dùng có xu hướng chọn những mật khẩu đơn giản.

Một phương pháp tấn công mật khẩu khác là sử dụng bảng mật khẩu. Bảng mật khẩu là hàng loạt các mật khẩu được tính toán trước, nó được xây dựng bằng cách tạo ra từ các chuỗi mật khẩu khác nhau. Mỗi một chuỗi được tạo ra bắt đầu bằng một dự đoán được lựa chọn ngẫu nhiên sau đó sẽ áp dụng các biến thể trên nó. Các phần mềm tấn công sẽ áp dụng các mật khẩu trong bảng này cho đến khi tìm được đúng mật khẩu phù hợp.

Tấn công vét cạn là loại tấn công sử dụng kết hợp các bộ ký tự để tính toán tất cả các mật khẩu có thể được tạo nên từ các ký tự này. Tuy nhiên, để

thực hiện được tấn công này, có thể cần rất nhiều thời gian. Các mật khẩu đơn giản có thể được tìm ra một cách nhanh chóng, nhưng đối với các mật khẩu phức tạp thì có thể mất hàng ngày, hàng tuần hoặc thậm chí nhiều hơn để tìm ra.

Bảng dưới đây là một số công cụ tấn công mật khẩu phổ biến:

phtCrack 4	Qcrack by the Crypt Keeper
PWLVIEW	CrackerJack by Jackal
Pwlhack 4.10	John the Ripper by Solar Designer
PWL-Key	Crack by Alec Muffet
ntPassword	

1.4.2.2 Tấn công khai thác sự tin cậy

Việc tấn công khai thác thường được thực hiện dựa trên sự tin cậy lẫn nhau giữa các hệ thống. Ví dụ như hệ thống DNS được dùng phân giải tên miền cho các hệ thống trên mạng Internet, giả sử kẻ tấn công có được các quyền tối thiểu trên hệ thống DNS (bằng cách khai thác các lỗ hổng trên DNS), thì kẻ tấn công có thể thực hiện việc chuyển hướng phân giải về máy mình. Do đó, kẻ tấn công có thể thực hiện khai thác các lỗ hổng của các hệ thống sử dụng dịch vụ phân giải tên miền DNS.

1.4.2.3 Tấn công chuyển hướng cổng

Tấn công chuyển hướng cổng là một loại khác của tấn công khai thác sự tin cậy. Kẻ tấn công sử dụng hệ hống bị xâm nhập để truy cập qua firewall mà không bị chặn. Theo cách này, nếu kẻ tấn công chiếm được quyền của một hệ thống công khai (ví dụ máy chủ web), họ có thể cài đặt các phần mềm (Netcat) để chuyển hướng lưu lượng truy cập trực tiếp từ hệ thống bên ngoài đến các hệ thống bên trong. Mặc dù không vi phạm các luật của firewall, nhưng hệ thống bên ngoài đã kết nối được với hệ thông bên trong thông qua quá trình chuyển hướng cổng trên hệ thống công khai.

1.4.3. Tấn công từ chối dịch vụ (DoS)

Về cơ bản, tấn công từ chối dịch vụ DoS/DDoS chỉ là tên gọi chung của các loại tấn công làm cho một hệ thống nào đó bị quá tải không thể cung

cấp dịch vụ, hoặc phải ngưng hoạt động. Tấn công kiểu này chỉ làm gián đoạn hoạt động của hệ thống chứ rất ít có khả năng xâm nhập hay chiếm được thông tin dữ liệu của nó. Tùy theo phương thức thực hiện mà loại tấn công này được biết dưới nhiều tên gọi khác nhau. Ban đầu là lợi dụng sự yếu kém của giao thức TCP để thực hiện tấn công từ chối dịch vụ cổ điển DoS (Denial of Service), sau đó là tấn công từ chối dịch vụ phân tán DDoS (Distributed Denial of Service) và mới nhất là tấn công từ chối dịch vụ theo phương pháp phản xạ DRDoS (Distributed Reflection Denial of Service). Theo thời gian, đã xuất hiện nhiều biến thể khác nhau của tấn công DoS như: Broadcast Storms, SYN, Finger, Ping, Flooding,… với mục tiêu nhằm chiếm dụng các tài nguyên của hệ thống (máy chủ) như: chiếm dụng băng thông, bộ nhớ, ổ đĩa cứng, bộ vi xử lý, làm hoạt động của hệ thống bị quá tải dẫn đến không thể đáp ứng được các yêu cầu hợp lệ người dùng.

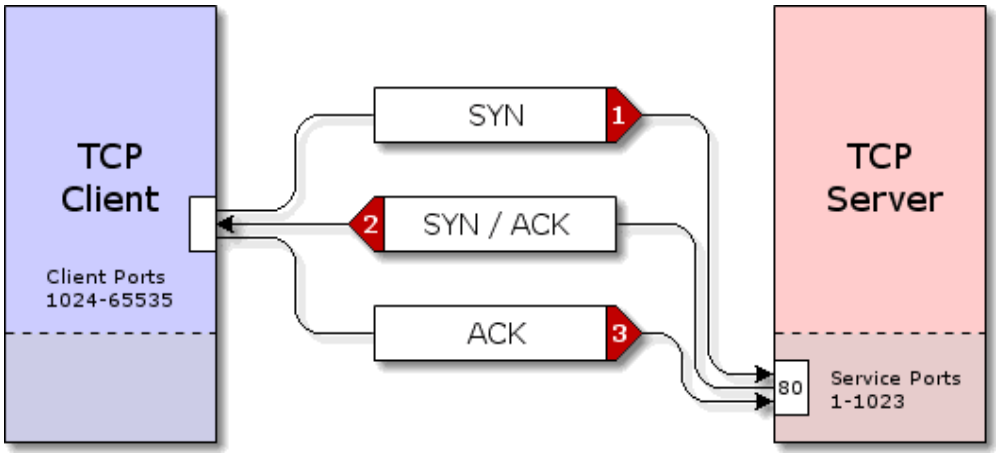
Tấn công DoS nói chung không cho phép kẻ tấn công chiếm quyền truy cập hệ thống hay có quyền thay đổi hệ thống. Tuy nhiên, nó lại gây thiệt hại khá lớn cho các tổ chức vì làm gián đoạn các hoạt động của họ. Đối với các hệ thống máy chủ được bảo vệ tốt, rất khó để xâm nhập vào thì tấn công từ chối dịch vụ được các kẻ tấn công sử dụng như là phương pháp hiệu quả để tấn công hệ thống.

1.4.3.1 Tấn công SYN

Được xem là một trong những kiểu tấn công DoS cổ điển: Lợi dụng sơ hở của thủ tục TCP khi "bắt tay ba bước", mỗi khi client muốn thực hiện kết nối với server thì nó thực hiện việc bắt tay ba bước thông qua các gói tin.

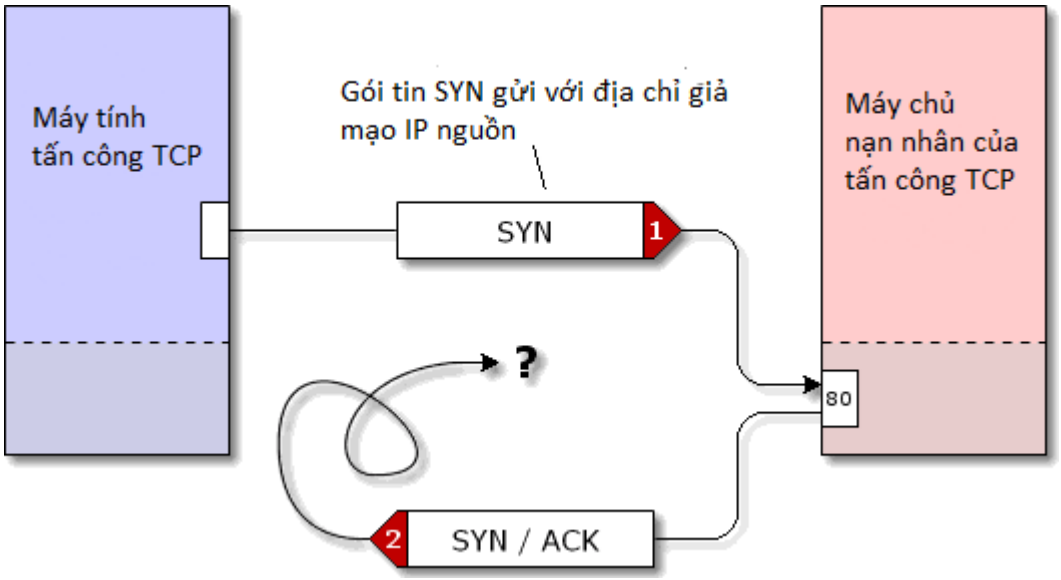
- Bước 1: Client sẽ gửi các gói tin (chứa SYN=1) đến server để yêu cầu kết nối.
- Bước 2: Khi nhận được gói tin này, server sẽ gửi lại gói tin SYN/ACK để thông báo cho client biết là nó đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Server sẽ dành một phần tài nguyên hệ thống như bộ nhớ đệm để nhận và truyền dữ liệu. Ngoài ra, các thông tin khác của client như địa chỉ IP và cổng cũng được ghi nhận.

- Bước 3: Cuối cùng, client hoàn tất việc bắt tay ba bước bằng cách hồi âm lại gói tin chứa ACK cho server và tiến hành kết nối.



Hình 1.1 – Quá trình bắt tay 3 bước TCP

Do TCP là giao thức truyền thông tin cậy nên trong lần bắt tay thứ hai, server gửi các gói tin SYN/ACK trả lời lại client mà không nhận lại được hồi âm của client để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lặp lại việc gửi gói tin SYN/ACK cho client đến khi nào nhận được hồi đáp của máy client.



Hình 1.2 – Quá trình tin tặc thực hiện tấn công

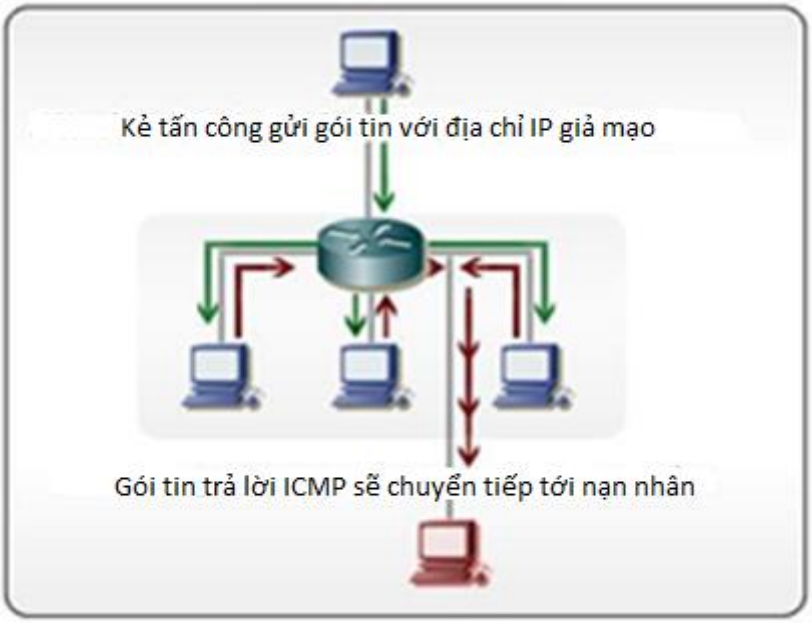
Nếu quá trình này kéo dài, server sẽ nhanh chóng trở nên quá tải, dẫn đến tình trạng treo nên các yêu cầu hợp lệ sẽ bị từ chối không thể đáp ứng

được. Quá trình này cũng giống như khi máy tính cá nhân hay bị treo khi mở cùng lúc quá nhiều chương trình phần mềm.

Thông thường, để giả địa chỉ IP trong gói tin, kẻ tấn công có thể dùng Raw Sockets (không phải gói tin TCP hay UDP) để làm giả mạo hay ghi đè lên IP gốc của gói tin. Khi một gói tin SYN với IP giả mạo được gửi đến server, nó cũng như các gói tin khác vẫn hợp lệ đối với server và server sẽ cấp tài nguyên cho kênh kết nối này, đồng thời ghi nhận toàn bộ thông tin và gửi gói SYN/ACK ngược lại cho client. Vì địa chỉ IP của client là giả mạo nên sẽ không có client nào nhận được SYN/ACK này để hồi đáp cho server. Sau một thời gian không nhận được gói tin ACK từ client, server sẽ cho rằng gói tin bị thất lạc nên lại tiếp tục gửi tiếp SYN/ACK, cứ như thế các kết nối tiếp tục mở.

Nếu như kẻ tấn công tiếp tục gửi nhiều gói tin SYN đến server thì cuối cùng server không thể tiếp nhận thêm kết nối nào nữa, dù đó là các yêu cầu kết nối hợp lệ. Việc này cũng đồng nghĩa với việc tiêu tốn tài nguyên vô ích và làm ngưng trệ hoạt động của hệ thống.

1.4.3.2 Tấn công Smurf

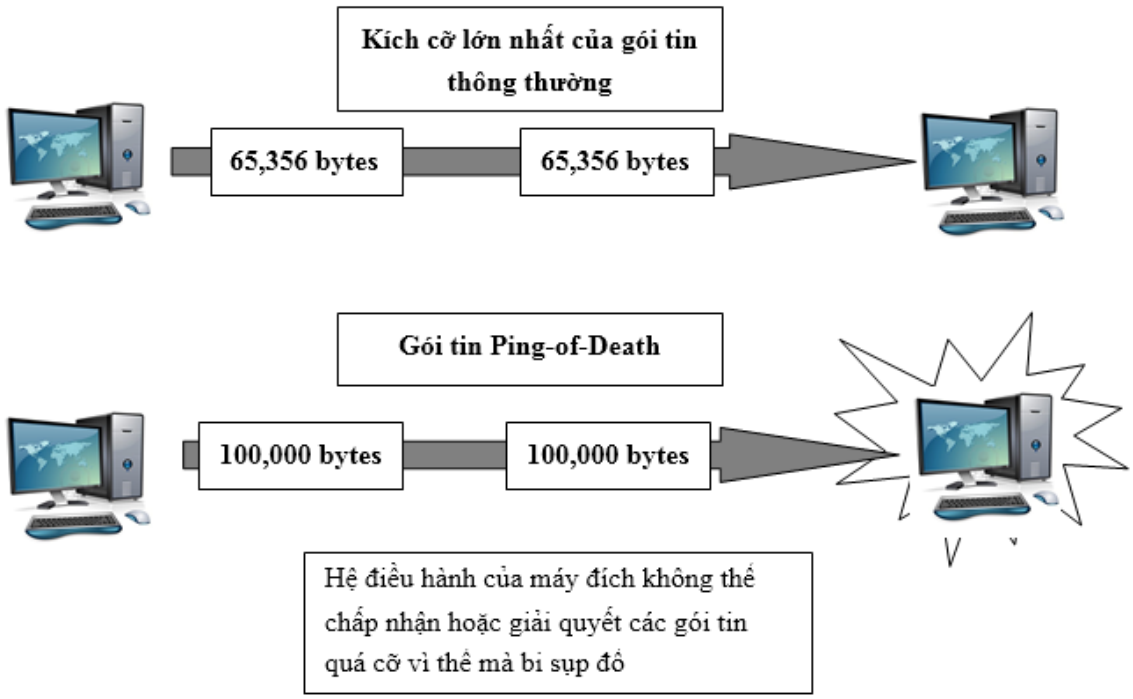


Hình 1.3 – Tấn công Smurf

Kiểu tấn công này cần một hệ thống hỗ trợ, gọi là mạng khuếch đại. Kẻ tấn công sẽ gửi các gói tin ICMP Echo Request đến địa chỉ Broadcast của mạng khuếch đại. Điều đặc biệt là các gói ICMP Echo Request này có địa chỉ IP nguồn chính là địa chỉ IP của nạn nhân. Khi các gói tin đó đến được địa chỉ Broadcast của mạng khuếch đại, lập tức tất cả các máy tính trong mạng khuếch đại sẽ nhận được các gói tin này. Các máy này tưởng rằng máy tính nạn nhân đã gửi gói ICMP Echo Request đến (do kẻ tấn công đã làm giả địa chỉ IP nguồn), lập tức chúng sẽ đồng loạt gửi trả lại hệ thống nạn nhân các gói ICMP Reply Echo Request. Hệ thống máy nạn nhân sẽ không chịu mỗi một khối lượng khổng lồ các gói tin này và nhanh chóng bị ngừng hoạt động, treo hoặc khởi động lại. Như vậy, kẻ tấn công chỉ cần gửi một lượng nhỏ các gói ICMP Echo Request đi và hệ thống mạng khuếch đại sẽ khuếch đại lượng gói ICMP Echo Request này lên gấp bội.

1.4.3.3 Tấn công Ping of Death

Kẻ tấn công gửi những gói tin IP lớn hơn số lượng bytes được phép là 65.536 bytes. Bởi vậy các gói tin được gửi có kích thước lớn hơn 65.536 bytes sẽ bị chia nhỏ để phù hợp với kích thước được phép, quá trình này được thực hiện ở lớp 2 và sau đó được tái tạo lại tại máy nhận. Tuy nhiên một số hệ điều hành tại máy nhận có thể không thể nhận biết được độ lớn của gói tin này và sẽ bị khởi động lại, hay đơn giản là sẽ bị gián đoạn giao tiếp.

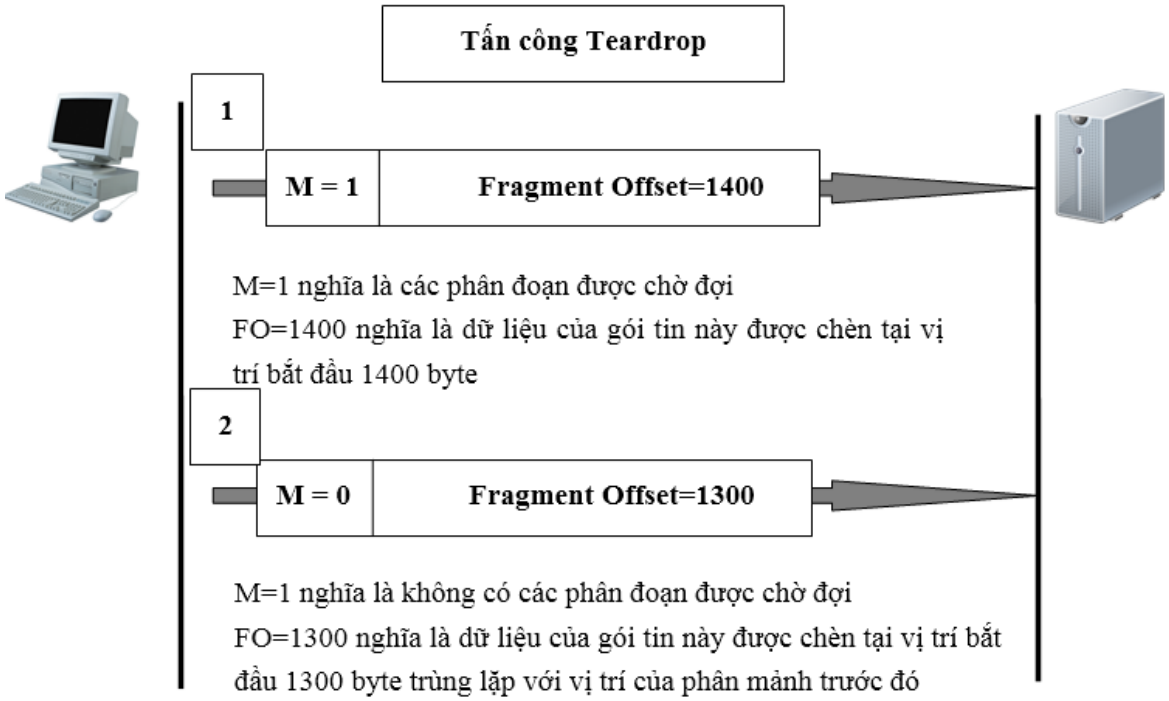


Hình 1.4 – Tấn công Ping-of-Death

1.4.3.4 Tấn công Teardrop

Trong mạng chuyển mạch gói, dữ liệu được chia thành nhiều gói tin nhỏ, mỗi gói tin có một giá trị offset riêng và có thể truyền đi theo nhiều con đường khác nhau để tới đích. Tại đích, nhờ vào giá trị offset của từng gói tin mà dữ liệu lại được kết hợp lại như ban đầu. Lợi dụng điều này, kẻ tấn công có thể tạo ra nhiều gói tin có giá trị offset trùng lặp nhau gửi đến mục tiêu muốn tấn công.

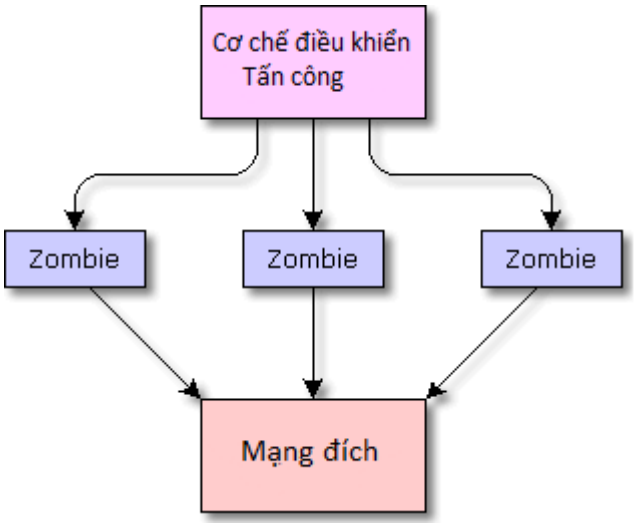
Nếu hệ điều hành nhận được các gói tin đã được chia nhỏ và không hiểu được, hệ thống sẽ mất một khoảng thời gian để cố gắng xây dựng lại gói tin mà không thành công, dẫn đến mất một phần tài nguyên hệ thống, nếu quá trình đó liên tục xảy ra thì hệ thống sẽ không còn tài nguyên cho các ứng dụng khác, phục vụ các người dùng khác và có thể dẫn đến bị treo.



Hình 1.5 – Tấn công Teardrop

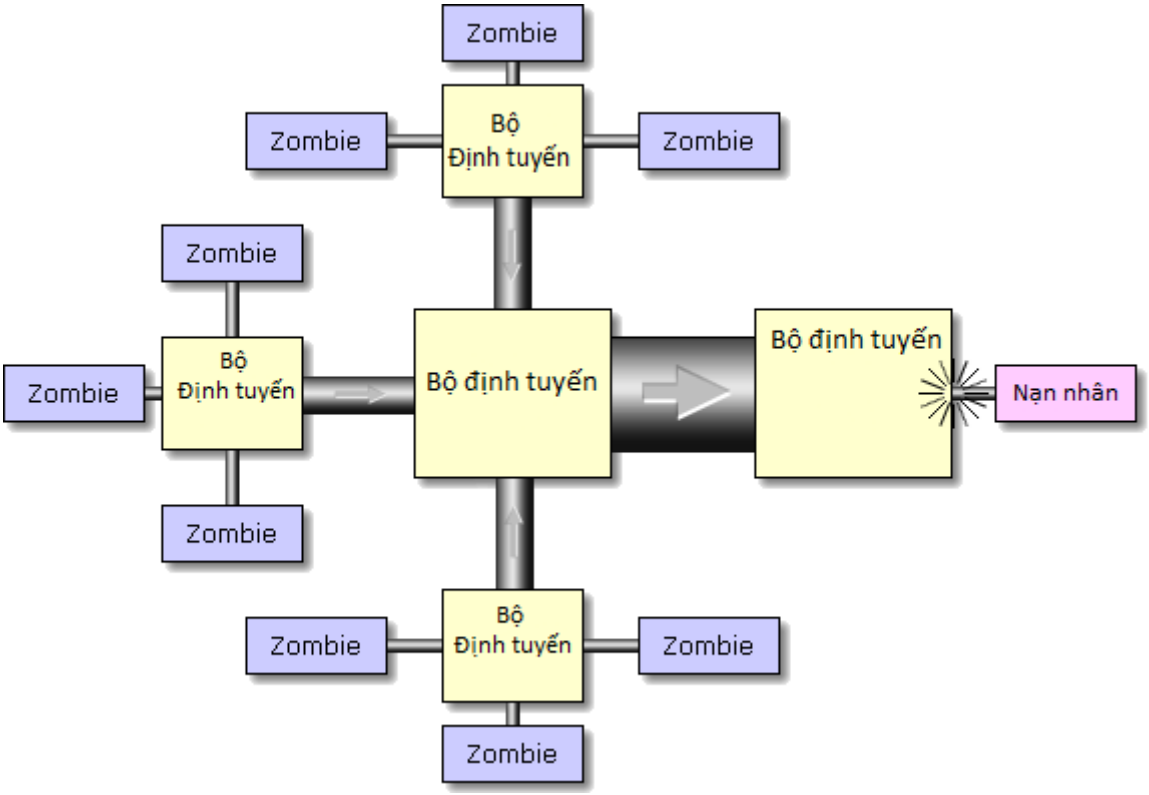
1.4.3.5 Tấn công từ chối dịch vụ phân tán

Xuất hiện vào năm 1999, so với tấn công DoS cổ điển, sức mạnh của tấn công từ chối dịch vụ phân tán DDoS cao hơn gấp nhiều lần. Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông gây nghẽn mạch hệ thống, dẫn đến hệ thống ngưng hoạt động. Để thực hiện các tấn công này, kẻ tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính trung gian khác nhau (đóng vai trò như zombie) để đồng loạt gửi các gói tin với số lượng rất lớn nhằm chiếm dụng tài nguyên và chiếm dụng băng thông của một mục tiêu xác định nào đó.



Hình 1.6 – Mô hình tấn công từ chối dịch vụ phân tán DDoS

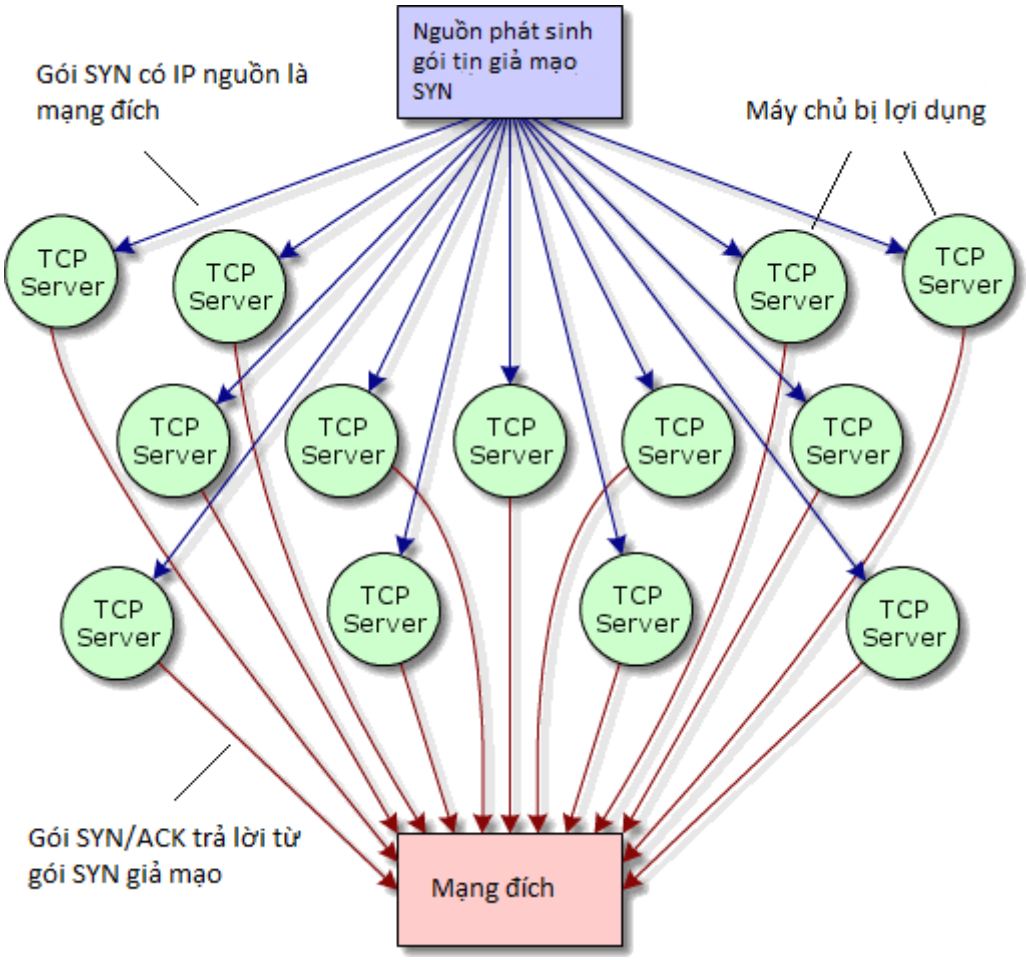
Hiện nay, đã xuất hiện dạng virus, worm có khả năng thực hiện các cuộc tấn công DDoS. Khi lây nhiễm vào các máy tính, chúng sẽ tự động gửi các yêu cầu phục vụ đến một mục tiêu xác định nào đó vào thời điểm xác định để chiếm dụng băng thông hoặc tài nguyên hệ thống máy chủ.



Hình 1.7 – Cách tin tặc thực hiện tấn công

1.4.3.6 Tấn công từ chối dịch vụ bằng phương pháp phản xạ (DRDoS)

Xuất hiện vào đầu năm 2002, là kiểu tấn công mới nhất, mạnh nhất trong họ DoS. Nếu được thực hiện bởi kẻ tấn công có trình độ thì nó có thể hạ gục bất cứ hệ thống nào trên thế giới một cách nhanh chóng. Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy chủ, tức là làm tắc nghẽn hoàn toàn đường kết nối từ máy chủ ra Internet và tiêu hao tài nguyên máy chủ. Trong suốt quá trình máy chủ bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy chủ đó. Tất cả các dịch vụ chạy trên nền TCP/IP như DNS, HTTP, FTP, POP3,... đều bị vô hiệu hóa. Về cơ bản, DRDoS là sự phối hợp giữa hai kiểu DoS và DDoS. Nó vừa là kiểu tấn công SYN với một máy tính đơn, vừa có sự kết hợp giữa nhiều máy tính để chiếm dụng băng thông như kiểu DDoS. Kẻ tấn công thực hiện bằng cách giả mạo địa chỉ của server mục tiêu rồi gửi yêu cầu SYN đến các mạng server lớn, chẳng hạn như Yahoo, Micorosoft để các server này gửi các gói tin SYN/ACK đến server mục tiêu. Các mạng server lớn có đường truyền mạnh đã vô tình đóng vai trò là các zombies cho kẻ tấn công DDoS.



Hình 1.8 – Mô hình tấn công DRDoS

Quá trình gửi cứ lặp lại liên tục với nhiều địa chỉ IP giả từ kẻ tấn công, với nhiều mạng server lớn tham gia nên server mục tiêu nhanh chóng bị quá tải, băng thông bị chiếm dụng bởi các mạng server lớn. Chỉ cần với một máy tính kết nối mạng Internet, một kẻ tấn công lành nghề có thể đánh bại bất cứ máy chủ nào trong giây lát mà không cần chiếm đoạt bất cứ máy nào để làm phương tiện thực hiện tấn công.

1.4.4. Tấn công thao tác dữ liệu

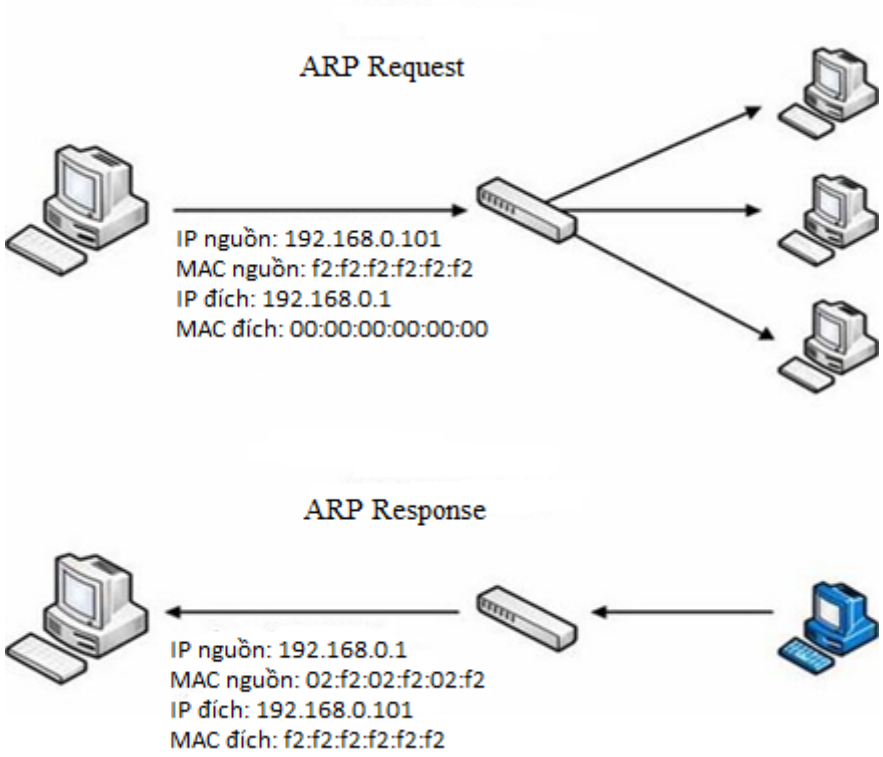
Thao tác dữ liệu, hoặc mạo danh có thể được thực hiện bởi các lỗ hổng trong giao thức IP và các ứng dụng liên quan. Các cuộc tấn công thao tác dữ liệu thường được gọi là các cuộc tấn công người đứng giữa vì cuộc tấn công này thường liên quan tới một đối tượng ở giữa để khai thác lỗ hổng. Các hình thức tấn công bao gồm giả mạo, phát lại phiên, cướp phiên, thay đổi định tuyến, ...

1.4.4.1 Tấn công giả mạo

Tấn công giả mạo là một phương pháp tấn công mạng để truy cập trái phép. Trong tấn công giả mạo, kẻ tấn công sẽ gửi các thông báo đến một máy tính cho biết thông báo này được gửi đến từ một hệ thống tin cậy. Để có thể thành công, kẻ tấn công đầu tiên phải xác định địa chỉ IP của hệ thống tin cậy đó và sau đó chỉnh sửa tiêu đề của gói tin để nó có vẻ là các gói tin đến từ hệ thống tin cậy. Về bản chất, kẻ tấn công lừa máy tình ở xa tin rằng nó là một thành viên hợp lệ của mạng. Mục tiêu là để thiết lập một kết nối mà cho phép kẻ tấn công truy cập đến các hệ thống.

Tấn công giả mạo địa chỉ IP: Tất cả các máy tính kết nối Internet đều được nhận diện bằng một địa chỉ IP duy nhất. Điều này cho phép các trang web nhận biết được các máy tính kết nối tới nó. Giả mạo địa chỉ IP cho phép một người đăng nhập vào một trang web với các địa chỉ IP khác nhau bằng cách sử dụng một Proxy server. Nói cách khác, giả mạo địa chỉ IP dùng để chỉ việc tạo ra các gói tin IP với địa chỉ IP nguồn được giả mạo với mục đích che giấu danh tính của người gửi hoặc mạo nhận một hệ thống máy tính khác.

Tấn công giả mạo ARP: Giao thức phân giải địa chỉ ARP(Address Resolution Protocol) được thiết kế để phục vụ cho nhu cầu thông dịch các địa chỉ giữa các lớp thứ hai và thứ ba trong mô hình OSI. Lớp thứ hai (lớp liên kết dữ liệu) sử dụng địa chỉ MAC để các thiết bị phần cứng có thể truyền thông với nhau một cách trực tiếp. Lớp thứ ba (lớp mạng), sử dụng địa chỉ IP để tạo các mạng có khả năng mở rộng trên toàn cầu. Lớp liên kết dữ liệu xử lý trực tiếp với các thiết bị được kết nối với nhau, còn lớp mạng xử lý các thiết bị được kết nối trực tiếp và không trực tiếp. Mỗi lớp có cơ chế phân định địa chỉ riêng, và chúng phải làm việc với nhau để tạo nên một mạng truyền thông.

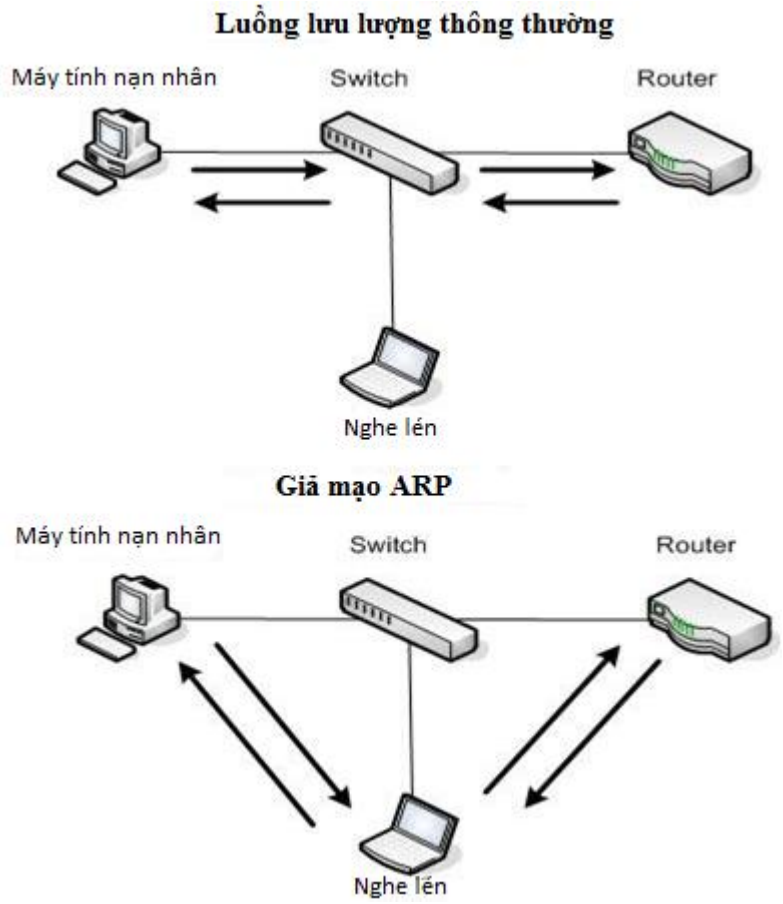


Hình 1.9 – Quá trình truyền thông ARP

Thực chất trong vấn đề hoạt động của ARP được tập trung vào hai gói: gói ARP Request và gói ARP Reply. Mục đích của ARP Request và ARP Reply là tìm ra địa chỉ MAC phần cứng có liên quan tới địa chỉ IP đã cho để lưu lượng có thể đến được đích của nó trong mạng. Gói ARP Request được gửi đến các thiết bị trong đoạn mạng. Đáp trả sẽ được gửi đi trong gói ARP Reply và cung cấp câu trả lời. Khi quá trình này hoàn tất, thiết bị phát sẽ cập nhật bảng ARP Cache của nó và hai thiết bị này có thể truyền thông với nhau.

Việc giả mạo bảng ARP chính là lợi dụng bản tính không an toàn của giao thức ARP. Không giống như các giao thức khác, chẳng hạn như DNS (có thể được cấu hình để chỉ chấp nhận các cập nhật động khá an toàn), các thiết bị sử dụng giao thức phân giải địa chỉ ARP sẽ chấp nhận việc cập nhật bất cứ lúc nào. Điều này có nghĩa rằng bất cứ thiết bị nào có thể gửi gói ARP Reply đến một máy tính khác và máy tính này sẽ cập nhật vào bảng ARP Cache của nó ngay giá trị mới này. Việc gửi một gói ARP Reply khi không có yêu cầu nào được tạo ra được gọi là việc gửi ARP "vu vơ". Khi các ARP Reply vu vơ này đến được các máy tính đã gửi yêu cầu, máy tính yêu cầu này sẽ nghĩ rằng

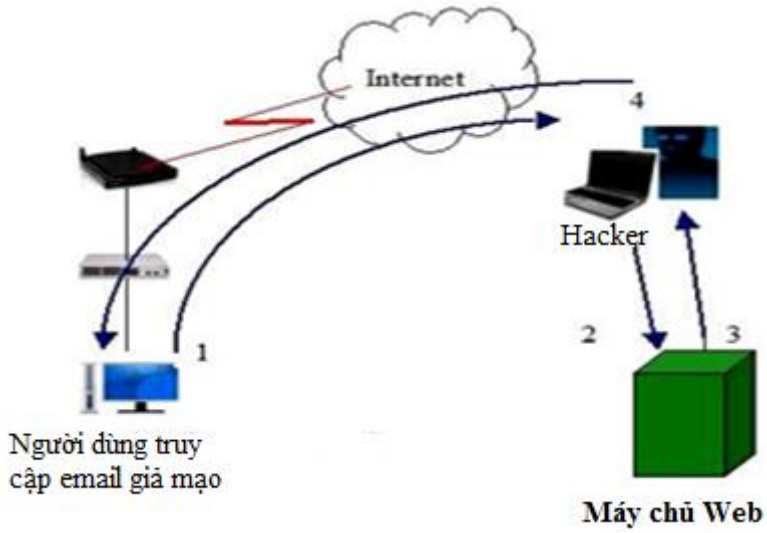
đó chính là đối tượng mình đang tìm kiếm để truyền thông, tuy nhiên thực chất họ lại đang truyền thông với một kẻ tấn công.



Hình 1.10 – Chặn truyền thông bằng các giả mạo ARP Cache

1.4.4.2 Phát lại phiên và cướp phiên

Phát lại phiên là một dạng của cuộc tấn công người đứng giữa, nơi mà kẻ xâm nhập bắt một loạt các gói tin và sửa đổi một phần dữ liệu trước khi chuyển tiếp như bình thường. Kiểu tấn công này nhằm vào một điểm yếu cố hữu trong chứng thực lưu lượng dữ liệu. Chẳng hạn như kẻ tấn công có thể thực hiện các bước lừa người dùng để đóng vai trò như một proxy trong suốt. Việc này có thể được thực hiện bằng cách gửi một email lừa đảo hoặc sửa đổi một trang web hợp lệ. Khi nạn nhân tải URL của trang web đã bị sửa đổi thì URL của kẻ tấn công được thêm vào trước URL của trang web đó. Ví dụ: http://www.hemantabaral.com là một URL hợp lệ, nhưng khi bị tấn công nó trở thành: http://www.theattacker.com/http://www.hemantabaral.com. Dưới đây là các bước chính của tấn công này:



Hình 1.11 – Tấn công Man-in-the-Middle

1. Khi nạn nhân yêu cầu trang web, nạn nhân sẽ gửi yêu cầu tới máy của kẻ tấn công.
2. Máy của kẻ tấn công nhận được yêu cầu và gửi yêu cầu đến web server.
3. Kẻ tấn công có thể thay thế hoặc áp dụng bất kỳ sự chuyển đổi dữ liệu nào mà họ muốn.
4. Kẻ tấn công sẽ chuyển tiếp trang web được yêu cầu tới máy nạn nhân.

1.4.4.3 Định tuyến lại

Các tấn công này cho phép truy cập tới bộ định tuyến để thay đổi bảng định tuyến, hoặc giả mạo danh tính của các bộ định tuyến chuyển gói tin tới một mạng khác.

1.5. KHÁI NIỆM VỀ QUẢN TRỊ AN TOÀN THÔNG TIN

Với các biện pháp an toàn thông tin người dùng có được công cụ trong tay để nhận thức được các điểm yếu, giảm thiểu các điểm yếu, ngăn chặn các nguy cơ tấn công, làm giảm các yếu tố rủi ro. Như vậy, các biện pháp và kỹ thuật đảm bảo an toàn thông tin chính là mang lại sự tin cậy cho các sản phẩm và hệ thống.

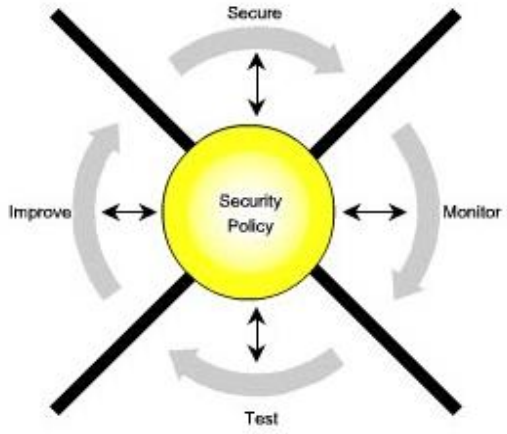
Quản trị an toàn hệ thống là đảm bảo an toàn kỹ thuật cho hoạt động của các cơ sở hạ tầng thông tin, trong đó bao gồm đảm bảo an toàn cho cả

phần cứng và phần mềm hoạt động theo các tiêu chuẩn kỹ thuật đã được công nhận; ngăn ngừa khả năng lợi dụng hệ thống và các cơ sở hạ tầng thông tin để thực hiện các hành vi trái phép gây hại cho cộng đồng, phạm pháp hay khủng bố; đảm bảo các tính chất bí mật, toàn vẹn, chính xác, sẵn sàng phục vụ của thông tin trong lưu trữ, xử lý và truyền tải trên mạng.

Như vậy khái niệm quản trị an toàn hệ thống là nhằm chỉ các hoạt động để đảm bảo an toàn cho cả phần cứng, phần mềm và mạng máy tính. An toàn phần cứng là bảo đảm hoạt động cho cơ sở hạ tầng thông tin. An toàn phần mềm gồm các hoạt động quản lý, kỹ thuật nhằm bảo vệ hệ thống thông tin, đảm bảo cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác, tin cậy. An toàn công nghệ thông tin là đảm bảo an toàn kỹ thuật cho các sản phẩm, dịch vụ và hệ thống công nghệ thông tin.

1.6. CÁC NHIỆM VỤ TRONG QUẢN TRỊ AN TOÀN HỆ THỐNG

An toàn hệ thống là một quá trình liên tục gắn liền với các hoạt động hàng ngày của các cán bộ chuyên trách, các hoạt động này có thể được mô tả theo các mô hình vòng đời an toàn hệ thống của Cisco. Mô hình này đã chỉ ra rằng việc thực hiện an ninh mạng là một quá trình được lặp đi lặp lại và được quản lý nhằm giảm thiểu các nguy cơ và nâng cao hiệu quả sử dụng của hệ thống. Quá trình này bao gồm bốn giai đoạn: secure (Đảm bảo an ninh), monitor (Giám sát), test (Đánh giá) và improve (Cải tiến).



- Đảm bảo an ninh: Là quá trình thực hiện, triển khai các giải pháp an toàn nhằm chặn đứng hoặc ngăn chặn những hành vi không được phép và đảm bảo an ninh thông tin. Nhiệm vụ cơ bản của giai đoạn này là việc thực hiện lên kế hoạch, triển khai và thiết lập an toàn cho hệ thống mạng, các công nghệ như an toàn mạng (VPN, firewall, IDS), hệ điều hành mạng và các dịch vụ mạng.
- Giám sát: Thực hiện các công việc giám sát dựa trên các công nghệ hỗ trợ, ví dụ IDS để theo dõi mạng nhằm đảm bảo độ an toàn của mạng. Nó giúp tìm ra các điểm yếu đang tồn tại trong mạng, từ đó giúp đưa ra giải pháp bảo vệ mạng.
- Đánh giá: Kiểm tra và quét các lỗ hổng. Đây là bước rất quan trọng. Nếu thực hiện tốt bước này sẽ hạn chế được nhiều nguy cơ bị tấn công.
- Cải tiến: Dùng những kết quả thu thập được từ giai đoạn theo dõi và đánh giá để điều chỉnh các chính sách an ninh cho phù hợp với hệ thống mạng.

1.7. CÁC YÊU CẦU CƠ BẢN TRONG VIỆC THIẾT LẬP AN TOÀN HỆ THỐNG

Một yêu cầu quan trọng trong việc quản trị hệ thống là cần cập nhật các bản tin về lĩnh vực an toàn thông tin của các hãng công nghệ, các tổ chức và cá nhân có uy tín trong lĩnh vực này, nhằm xác định đúng và thực hiện kịp thời các yêu cầu trong việc thiết lập an toàn cho các hệ thống. Ngoài ra, quá trình thiết lập an toàn cho một hệ thống cần tuân thủ các nguyên tắc cơ bản dưới dây:

1.7.1. Thay đổi tài khoản mặc định

Hầu như tất cả các thiết bị và hệ thống đều có tài khoản thiết lập mặc định và được sử dụng để thiết lập hệ thống một cách nhanh chóng và hiệu quả. Những tài khoản này được thiết lập công khai tên đăng nhập và mật khẩu và được thiết lập rất đơn giản. Vì vậy những tài khoản này thường không được thay đổi hoặc thiết lập lại, kẻ tấn công có thể lợi dụng điểm yếu này để khai thác vào hệ thống.

Để hiểu được ý nghĩa của việc cần phải thay đổi thiết lập mật khẩu mặc định. Xét một ví dụ cụ thể: Sâu máy tính Voyager Alpha Force nhắm đến máy chủ cơ sở dữ liệu Microsoft SQL, bởi vì hệ quản trị cơ sở dữ liệu này có tài khoản quản trị là SA với mật khẩu mặc định là rỗng. Dạng sâu máy tính loại này thực hiện quét hệ thống với cổng 1433 xem có được mở hay không (cổng mặc định của SQL server), sau đó nó thử đăng nhập sử dụng tài khoản SA với mật khẩu rỗng. Hoạt động quét của sâu này có thể làm ảnh hưởng đến đường truyền mạng.

Mật khẩu mặc định tài khoản quản trị của một số cơ sở dữ liệu:

Hệ quản trị CSDL	Tên tài khoản	Password
MySQL	root	Null
Oracle	sys	oracle
DB2	dlfm	ibmdb2

Trong trang web http://www.defaultpassword.com/ cung cấp tới 1812 mật khẩu mặc định về phần mềm cũng như thiết bị phần cứng của một số sản phẩm như Cisco Systems, 3Com, Linksys, Apache, Apple, D-Link…

Thay đổi tên hoặc ẩn tài khoản quản trị Administrator

Những tài khoản cao cấp để quản trị cho các hệ thống thường là administrator, admin, root. Nếu kẻ tấn công muốn xâm nhập vào hệ thống và bằng cách thử đăng nhập với một trong những tài khoản trên và mật khẩu mặc định của các hãng sản xuất. Hoặc sử dụng công cụ thực hiện tấn công từ điển hoặc vét cạn mật khẩu với những tài khoản trên. Vì vậy cần phải thay đổi tên hoặc ẩn những tài khoản quản trị này.

Nếu tên của tài khoản quản trị administrator đã được thay đổi, phải thực hiện ghi chép vào tài liệu kèm với mật khẩu tương ứng. Điều này thực sự cần thiết cho người quản trị mới khi người quản trị cũ không còn làm việc nữa.

1.7.2. Chỉ sử dụng tài khoản quản trị cho các nhiệm vụ quản trị

Nhiều quản trị hệ thống đăng nhập vào hệ thống của họ với tài khoản quản trị administrator hoặc tài khoản có quyền tương đương để thực hiện các hoạt động thông thường. Các hoạt động thông thường không phải là quản trị như: xem email, viết tài liệu, tìm kiếm phần mềm…Sử dụng tài khoản quản trị cho những hoạt động này rất nguy hiểm. Nếu một email có tệp tin gắn kèm chứa mã độc, khi chúng được tải xuống sẽ có quyền để cài đặt và thực thi lây nhiễm hoặc phá hoại hệ thống bởi vì chúng đang ở quyền administrator.

Sử dụng lệnh run as trong Microsoft Windows

Đăng nhập bằng tài khoản thông thường và người quản trị có thể sử dụng chức năng run as trong Windows để chạy với quyền administrator để cài đặt các chương trình và ứng dụng hoặc cấu hình hệ thống.

Sử dụng lệnh su hoặc sudo trong Unix hoặc Linux

Lệnh su (substitute user identity) có sẵn trong tất cả các phiên bản của Unix. Cung cấp khả năng chạy chương trình bằng tài khoản quản trị root khi đang ở người dùng thường. Với lệnh sudo cũng có khả năng tương tự.

1.7.3. Xác định các cổng không sử dụng hoặc không cần thiết

Các cổng TCP/UDP được xem là các "cánh cửa" mà một máy tính mở để truyền thông tin với các máy tính khác. Mỗi một cổng là một số cụ thể và được gắn với một dịch vụ hoặc một chương trình cụ thể. Ví dụ: Một máy tính muốn kết nối với một máy tính khác thông qua phần mềm SSH, thì một máy tính phải mở cổng 22 để máy tính còn lại kết nối tới.

Số hiệu cổng chạy từ 0 đến 65535, với các cổng từ 0-1024 là các cổng dành riêng cho dịch vụ đã được đăng ký. Bảng sau đây trình bày một số cổng phổ biến:

Bảng 1.1 – Một số cổng TCP/UDP dành riêng

Port	Service
20, 21	FTP
22	SSH

25	Simple Network Mail Protocol (SMTP)
53	Domain Name System (DNS)
80	HTTP
110	POP3 Mail
135, 137, 139	NetBIOS

Cùng với những cổng dành riêng cho các ứng dụng đã đăng ký. Một số chương trình độc hại sử dụng một trong những cổng còn lại để thực hiện kết nối. Ví dụ: Trojan "Back Orifice" sử dụng cổng 31337 để mở cửa hậu kết nối.

Một số chương trình độc hại khác lại không sử dụng các cổng mặc định mà nó được tùy chỉnh theo ý đồ của kẻ tấn công. Ví dụ: Trojan bo2k không có cổng mặc định.

Một trong những kỹ thuật của kẻ tấn công là xác định được các cổng đang mở của hệ thống đích để sử dụng các công cụ tấn công tương ứng. Vì vậy việc xác định các cổng đang mở trên hệ thống rất quan trọng. Những cổng nào không có mục đích sử dụng hoặc không có biện pháp phòng thủ cần phải đóng lại.

Sử dụng lệnh netstat để xác định các cổng mở. Công cụ dòng lệnh này cho phép người quản trị các cổng mở trên hệ thống. Các phiên bản của công cụ này có sẵn trên tất cả các hệ điều hành. Netstat hiển thị trạng thái mạng của một hệ thống, xác định các cổng mở, kết nối được thiết lập, và thống kê mạng.

1.7.4. Vô hiệu hóa/tắt/gỡ bỏ các dịch vụ hoặc Daemon không sử dụng hoặc không cần thiết

Xác định các ứng dụng, các dịch vụ, các tiến trình hoặc các cổng không cần thiết chỉ là phần đầu của việc gỡ bỏ các "điểm kết nối" cho kẻ tấn công. Phần còn lại là gỡ bỏ hoặc vô hiệu hóa các ứng dụng, dịch vụ, tiến trình tương ứng.

Vô hiệu hóa các dịch vụ không cần thiết trong Windows

Dựa vào thông tin quy định và chiến lược của hệ thống để vô hiệu hóa các dịch vụ trên máy tính. Có nhiều danh sách các khuyến cáo hướng dẫn vô hiệu hóa các dịch vụ, chúng tương đối dễ tìm thấy bằng cách sử dụng cụm từ "unnecessary services" kèm theo với phiên bản hệ điều hành. Vô hiệu hóa dịch vụ có thể được thực hiện bằng nhiều cách, lựa chọn các công cụ để sử dụng dựa vào việc xác định hệ thống và môi trường mạng cần phải được kiểm tra.

Trong môi trường Domain sử dụng mẫu MMC (Microsoft Management Console) cho phép tạo ra bản mẫu về các chính sách an toàn để áp dụng cho nhiều máy chủ hoặc máy trạm trong Domain.

Vô hiệu hóa các dịch vụ không cần thiết trong Unix

Có nhiều phương pháp có sẵn để cấu hình các dịch vụ trong hệ điều hành Unix. Với người dùng mới quản trị Unix có thể thực hiện thông qua chương trình có giao diện đồ họa như: Service Configuration Program trong phiên bản Red Hat. Trong trường hợp môi trường dòng lệnh, câu lệnh ntsysv khởi tạo giao diện đơn giản cho phép thay đổi tùy chọn khởi động cùng hệ thống của các dịch vụ và daemon. Một trong những chương trình hữu ích nhất là chkconfig, cập nhật và truy vấn thông tin run-level cho các dịch vụ hệ thống.

1.7.5. Loại bỏ các kết nối không được phép: Wireless và Dial-up

Với hệ thống mạng của tổ chức đã tồn tại, người dùng cuối sẽ làm mọi thứ nếu có thể để vượt qua các cơ chế an toàn nhằm thực hiện công việc dễ dàng hơn. Thường bao gồm các cơ chế cho phép kết nối tới hệ thống mạng. Một trong các thiết lập kết nối là thiết lập điểm truy cập cho mạng không dây trong tổ chức không ràng buộc bất kỳ địa điểm cụ thể, để cài đặt các phần mềm truy cập từ xa. Các cơ chế này được cài đặt mà không qua cơ chế kiểm tra bảo mật, vấn đền này làm cho mạng của tổ chức có nhiều nguy cơ về bảo mật.

Xác định tất cả các thiết bị và điểm truy cập mạng không dây: 802.11 và Bluetooth

Để xác định mạng không dây giả mạo trong tổ chức, cần theo các bước sau đây:

- Sử dụng một máy tính xách tay
- Sử dụng phần mềm NetStumbler

1.7.6. Thiết lập bộ lọc mã độc hại cho mỗi một hệ điều hành

Nhiều tổ chức, doanh nghiệp và quản trị hệ thống, khi hệ thống của họ đã có một số phương thức bảo vệ mã độc hại tại cổng giao tiếp vào ra, họ quan niệm rằng không phải bảo vệ thêm cho hệ thống và tài nguyên ở bên trong. Đây là một quan niệm sai lầm, với tổ chức có tài nguyên hạn chế, có thể áp dụng phương pháp bảo vệ tài nguyên này, nhưng không được xem là bảo vệ đầy đủ. Có một số lượng đáng kể mã độc hại tồn tại, và những loại mã độc mới hơn và nguy hiểm hơn được tạo ra một cách thường xuyên. Nếu một doanh nghiệp chỉ dựa trên một thiết bị ở cổng vào ra, vị trí này có thể xảy ra các sự cố về lỗi thiết bị hoặc phát hiện loại mã độc mới. Vì vậy cần phải có chương trình đặt trong mỗi một hệ thống để xác định, ngăn chặn, loại bỏ mã độc hại.

Một sản phẩm Anti-virus phải đáp ứng các yêu cầu sau:

1. Khả năng bảo vệ hệ thống máy tính và thiết bị truyền thông với máy tính khỏi sự xâm nhập của virus.
2. Cung cấp khả năng phát hiện các loại virus khi hệ thống máy tính và thiết bị truyền tin bị nhiễm.
3. Cung cấp khả năng phục hồi từ một máy tính bị nhiễm virus.

1.7.7. Kiểm tra chức năng sao lưu và phục hồi

Một trong những nhiệm vụ quan trọng của quản trị an toàn hệ thống là sao lưu và phục hồi hệ thống. Với một người quản trị hệ thống, không có cảm giác nào tồi tệ hơn khi cố gắng khôi phục dữ liệu sau khi hệ thống gặp sự cố và phát hiện ra dữ liệu phục hồi trống rỗng. Nhiều chuyên gia quản trị đã phải mất hàng tuần bằng biện pháp thủ công để khôi phục dữ liệu sau khi sử dụng biện pháp khôi phục từ một bản sao lưu đã có sẵn. Trong trường hợp tổ chức

có quy mô nhỏ thì có thể chấp nhận được, nhưng đối với tổ chức quy mô lớn nếu không có khả năng khôi phục dữ liệu thì sẽ phải trả giá đắt. Việc kiểm tra sao lưu nên được thực hiện thường xuyên, bằng cách lập lịch trình xác định tài nguyên cần sao lưu.

Chương 2.
THIẾT LẬP AN TOÀN CHO HỆ THỐNG MẠNG

2.1. PHÂN VÙNG HỆ THỐNG MẠNG

Một số doanh nghiệp có ý tưởng cho phép truy cập mạng nội bộ cũng như mạng công cộng với hình thức mở. Nhìn bề ngoài thì đây là một ý tưởng hay, bởi vì đây là một hệ thống mạng mở và không sử dụng một phương pháp nào ngăn chặn truy cập dữ liệu. Vì vậy mà nâng cao hiệu quả và tác động đáng kể tới doanh nghiệp kinh doanh. Nhưng, đây là một ý tưởng sai lầm. Ý tưởng này sẽ gây ra các nguy cơ mất an toàn đối với dữ liệu của doanh nghiệp, kẻ tấn công có thể xâm nhập vào hệ thống mạng bên trong nhằm đánh cắp dữ liệu, hoặc phá hủy dữ liệu và tài nguyên khác trong mạng. Một phương pháp để bảo vệ mạng bên trong từ các cuộc tấn công bên ngoài là cài đặt các thiết bị bảo mật ngay tại cổng vào mạng bên trong. Phương pháp này bảo vệ được các nguy cơ từ Internet, nhưng không thể phát hiện được các cuộc tấn công từ người dùng bên trong mạng nội bộ.

Các hình thức tấn công rất đa dạng, nhiều chuyên gia an toàn cho rằng các nguy cơ đối với thông tin chiếm 80% xuất phát từ mạng nội bộ. Trong trường hợp nhân viên trong các doanh nghiệp không có hiểu biết về tấn công hệ thống hoặc đánh cắp dữ liệu, thì sự thiếu hiểu biết về an toàn của nhân viên cũng là nguy cơ gây mất an toàn. Hệ thống mạng mở tạo cơ hội cho các đối tác truy cập hệ thống và lấy về dữ liệu mà họ không cần phải xác thực hay đảm bảo bất kỳ chính sách bảo mật nào. Vì vậy mà cũng tạo cơ hội cho kẻ tấn công khai thác dữ liệu từ mạng nội bộ.

Vì những lý do trên, việc phân vùng mạng là vô cùng quan trọng, mỗi phân vùng mạng tương ứng với các chức năng riêng. Khái niệm "bảo vệ theo chiều sâu" thường được áp dụng để bảo vệ các phân vùng mạng từ các tấn công mạng bên ngoài và cũng như các tấn công từ mạng bên trong.

2.1.1. Lựa chọn mô hình phân vùng mạng

Có nhiều cách để phân chia mạng, trong tất cả các phạm vi về an toàn mạng, thực hiện đánh giá hệ thống, lập kế hoạch nên được thực hiện trước khi

phân chia mạng. Xem xét những tác động nào sẽ ảnh hưởng tới từng phân vùng mạng. Khi chuẩn bị để phân chia vùng mạng, phân vùng có thể được tạo ra dựa vào các tiêu chuẩn sau đây:

- Trách nhiệm theo lĩnh vực công việc
- Mức độ bị đe dọa về an ninh, an toàn
- Mức độ rủi ro
- Các kiểu dịch vụ
- Như cầu kinh doanh

2.1.2. Phân vùng mạng dựa vào trách nhiệm theo lĩnh vực công việc

Phân vùng mạng dựa vào trách nhiệm theo lĩnh vực công việc của các bộ phận đặc biệt là bước quan trọng đầu tiên nhằm giảm thiểu các mối đe dọa tới dữ liệu và tài nguyên hệ thống mạng. Đây không chỉ là một phương pháp tốt trong lĩnh vực an toàn, mà còn đảm bảo các phân vùng mạng duy trì và tuân thủ các quy tắc an toàn. Nhiều quy tắc an toàn như HIPAA, GLBA yêu cầu các tổ chức, doanh nghiệp phải thực hiện các bước để giới hạn truy cập tới dữ liệu nhạy cảm. Những quy tắc này được thiết kế để bảo vệ "thông tin bí mật" của tổ chức, doanh nghiệp.

Trong quy tắc an toàn HIPAA, nội dung chính tập trung bảo vệ thông tin người dùng cá nhân, miêu tả ngắn trong phần 164.306 được trình bày ở bảng dưới đây. Phân vùng mạng sẽ đảm bảo tuân thủ với hai yêu cầu đầu tiên của HIPAA sau đây: đảm bảo tính bí mật, tính toàn vẹn, tính sẵn sàng của thông tin và bảo vệ chống lại tấn công thăm dò.

HIPAA Mục 164.306. Tiêu chuẩn an toàn: Những quy định chung Yêu cầu chung. Các tổ chức cần phải thực hiện như sau:

1. Đảm bảo tính bí mật, tính toàn vẹn, tính sẵn sàng của tất cả thông tin bảo vệ bằng điện tử của tổ chức hoặc doanh nghiệp được tạo ra, nhận, duy trì, truyền thông tin.
2. Bảo vệ chống lại bất kỳ mối đe dọa dự đoán hợp lý hoặc gây nguy hại tới an ninh hoặc tính toàn vẹn của thông tin đó.

3. Bảo vệ chống lại bất kỳ mục đích sử dụng dự đoán hợp lý hoặc tiết lộ thông tin mà không được phép hoặc theo yêu cầu của phần nhỏ E trong mục này.
4. Đảm bảo tuân thủ các chính sách an toàn bởi người dùng.

Trong quy tắc an toàn GLBA, các yêu cầu giải quyết các hồ sơ tài chính, bao gồm các hồ sơ ngân hàng, thông tin thẻ thanh toán, vv…, được trình bày trong phần 6801 (được trình bày ở bảng dưới đây). Cũng như HIPAA, đặc tính bí mật của thông tin trong một phân vùng mạng riêng biệt có thể tuân thủ với GLBA. Việc phân vùng mạng có lợi ích trong việc duy trì tính bí mật, bảo vệ chống lại các mối đe dọa an toàn thông tin, và giới hạn truy cập tới thông tin bí mật tới bên có thẩm quyền.

GLBA Mục 6801. Bảo vệ bí mật thông tin cá nhân

a. Chính sách nghĩa vụ bảo mật

Đây là chính sách của Quốc hội Mỹ, mỗi tổ chức tài chính có nghĩa vụ phải khẳng định và tiếp tục tôn trọng sự riêng tư của khách hàng và bảo vệ an ninh thông tin và bảo mật thông tin cá nhân không công khai của khách hàng.

b. Tổ chức tài chính bảo vệ

Để thực hiện chính sách trong tiểu mục (a) mỗi một cơ quan, tổ chức được miêu tả trong mục 6805(a) sẽ thiết lập các chuẩn phù hợp với các tổ chức tài chính để thẩm quyền của họ liên quan đến hành chính, kỹ thuật và biện pháp bảo vệ vật lý -

1. Để đảm bảo an ninh và bảo mật thông tin về hồ sơ của khách hàng.
2. Để bảo vệ chống lại bất kỳ mối đe dọa dự kiến hoặc mối nguy hiểm đối với an ninh toàn vẹn của hồ sơ khách hàng.
3. Để bảo vệ chống lại truy cập trái phép hoặc sử dụng các hồ sơ hoặc thông tin có thể gây nguy hại tới khách hàng.

Bởi tính độc lập sở hữu dữ liệu trong mỗi phân vùng mạng riêng biệt sẽ giới hạn đáng kể các truy cập tới từng phân vùng mạng. Mặc dù không có pháp luật đề cập đến yêu cầu trong phân vùng mạng nhưng có yêu cầu giới hạn truy cập tới thông tin bí mật. Đặt thông tin bí mật trong các vùng mạng đã phân chia là bước quan trọng đầu tiên cần phải thực hiện để giới hạn truy cập.

2.1.3. Phân vùng mạng dựa vào mức độ đe dọa và rủi ro về an toàn

Người quản trị hệ thống khi lập hồ sơ triển khai cũng như trong quá trình vận hành hệ thống cần phải xác định được các nguy cơ cũng như các mối đe dọa có thể xảy ra gây ảnh hưởng tới các tiêu chí của hệ thống như:

- Mất tính toàn vẹn: Tính toàn vẹn bị mất nếu dữ liệu hoặc hệ thống thông tin bị thay đổi trái phép do cố ý hay vô ý. Việc sử dụng dữ liệu hay hệ thống bị nhiễm hại sẽ dẫn đến các lỗi và các quyết định sai trái.
- Mất tính sẵn sàng: Nếu hệ thống không sẵn sàng cho người dùng thì tính đảm bảo hoạt động liên tục của tổ chức bị ảnh hưởng. Vận hành không hiệu quả hoặc mất các chức năng hệ thống dẫn tới giảm năng suất.
- Mất tính bí mật: Đề cập đến việc bảo mật thông tin không cho lộ ra ngoài. Hậu quả của việc để lộ thông tin mật có thể ảnh hưởng tới an ninh quốc gia. Việc trái phép và vô ý để lộ cũng làm giảm uy tín của cơ quan/tổ chức trước công chúng.

Dựa vào những tiêu chí trên đây mà một hệ thống thông tin đảm bảo an toàn cần phải đạt được. Vì vậy khi đánh giá hệ thống để triển khai cũng như vận hành cần phải xác định các mức độ đe dọa về an ninh, an toàn. Đảm bảo hệ thống tránh được các kiểu tấn công từ bên trong, bên ngoài. Một số ý chính khi phân vùng mạng dựa vào mức độ đe dọa và rủi ro về an toàn như sau:

- Đối với những máy tính, máy chủ cung cấp dịch vụ cho người dùng bên trong cũng như người dùng bên ngoài có thể truy cập sử dụng như các dịch vụ: Web, Mail, FTP, DNS, CA v.v. Những dịch vụ này cần phải được đặt tại phân vùng mạng DMZ (Demilitarized Zone). Bởi vì phân vùng này được áp dụng chính sách cho phép từ bên ngoài có thể truy cập vào và sử dụng dịch vụ. Tuy nhiên để tránh được tấn công cần phải có bức tường lửa và hệ thống phát hiện xâm nhập để lọc lưu lượng vào ra và phát hiện hành vi tấn công vào phân vùng này.

- Đối với những máy tính, máy chủ thuộc vùng mạng bên trong (vùng mạng nội bộ). Vùng mạng này chỉ dành cho nhân viên trong công ty/tổ chức truy cập làm việc. Phân vùng này cần phải triển khai chính sách ngăn chặn các kết nối khởi tạo từ bên ngoài vào. Và bên trong truy cập ra bên ngoài cần được kiểm soát chặt chẽ.
- Phân vùng quản trị: Phân vùng này dành cho máy tính, máy chủ cung cấp những dịch vụ bên trong như: máy chủ chia sẻ, máy chủ kiểm soát truy cập, máy chủ cơ sở dữ liệu. Phân vùng này nhóm quản trị viên có toàn quyền và người dùng mạng nội bộ chỉ được phép truy cập lưu trữ dữ liệu. Cấm các truy cập từ mạng bên ngoài vào.
- Đối với phân vùng mạng yêu cầu bảo mật tuyệt đối: Cần phải xây dựng tách biệt với mạng bên ngoài và đặc biệt ngắt kết nối Internet. Để đảm bảo tin tặc không thể tấn công được vào qua đường truyền mạng. Phân vùng này thêm các thiết bị xác thực mạnh khi truy cập như: xác thực vân tay, xác thực qua thẻ.

Cơ chế phân vùng mạng để đảm bảo an toàn là bước quan trọng giúp kiểm soát truy cập sử dụng mạng một cách chặt chẽ. Mỗi một phân vùng riêng lại xây dựng cơ chế, chính sách riêng đảm bảo ba tính chất của hệ thống đã nêu ở trên.

2.2. THIẾT LẬP AN TOÀN CHO HỆ ĐIỀU HÀNH MẠNG

2.2.1. Thiết lập các kiểm soát truy cập

Nguồn gốc các cơ chế kiểm soát truy cập trong cả hai loại hệ điều hành Unix và Windows đều cho phép chia nhỏ các mức độ truy cập tài nguyên. Khái niệm điều khiển truy cập của Unix và Windows khá giống nhau, nhưng việc thực hiện là khác nhau, các hoạt động bên trong tương ứng của chúng sẽ được trình bày ở các mục sau đây.

2.2.1.1 Kiểm soát truy cập trong hệ điều hành Unix

Unix ở mức độ cơ bản nhất sử dụng các quyền đối với tài nguyên để kiểm tra truy cập tới các tệp tin tương ứng. Trong Unix tất cả mọi thứ được xem là một tệp tin (ví dụ: các thiết bị, các thư mục, …), và các quyền chính dựa vào chủ sở hữu của tệp tin. Hầu hết các phiên bản của Unix là dựa vào phương thức kiểm soát truy cập tùy ý (DAC). Phương thức này cho phép chủ sở hữu của tệp tin thiết lập quyền truy cập tới tệp tin cho tất cả người dùng khác. Phương thức này đối lập với phương thức kiểm soát truy cập bắt buộc (MAC), ở phương thức này các mức kiểm soát truy cập dựa vào nhãn thông tin cung cấp bởi hệ thống hoặc thông tin được tạo ra bởi người dùng. Một người dùng không thể truy cập tới một tệp tin có nhãn bí mật nếu người dùng đó không có mức truy cập tương ứng.

Một số phiên bản của Unix có khả năng sử dụng mô hình kiểm soát truy cập MAC, bởi vì chúng đã được chỉnh sửa các mô-đun hoặc các chương trình cài thêm vào để hỗ trợ kiểm soát truy cập MAC.

Có ba quyền cơ bản mà người dùng có thể sử dụng khi cấp phát quyền truy cập tới các tệp tin trong Unix: quyền đọc, quyền ghi, quyền thực thi. Trong danh sách liệt kê của tệp tin những quyền này được thể hiện bằng các chữ cái viết tắt: **r** (read), **w** (write), **x** (excute). Mỗi một tệp tin đều được định nghĩa ba đối tượng truy cập: đầu tiên là chủ sở hữu tệp tin đó, thứ hai là nhóm chứa các thành viên, thứ 3 là người dùng còn lại. Sau đây là một ví dụ về ba quyền được thiết lập cho tệp tin /home/thuchanh/thuchanh1.txt; sử dụng lệnh **ls –l** để kiểm tra:

Ví dụ:

```
Linux1:  # ls –l  /home/thuchanh/thuchanh1.txt

-rwxr-xr-x  1  user1  users  11    Sep  9              06:30
thuchanh1.txt
```

Trong ví dụ trên các quyền và thông tin được phân chia vào trong các trường như sau:

- Trường thứ nhất xác định kiểu tệp tin đang được liệt kê. Trong ví dụ trên là một dấu trừ (-), có ý nghĩa đây là một tệp tin. Các ký tự đại diện này được trình bày trong bảng 2.1:
- Chín ký tự tiếp theo trong ví dụ trên trình bày quyền truy cập đã được thiết lập sẵn cho tệp tin tương ứng. Quyền đọc, quyền ghi, quyền thực thi là ba quyền truy cập chung nhất được áp dụng cho tất cả các tệp tin. Bảng 2.2 liệt kê và định nghĩa các ký tự đại diện có thể sử dụng để xác định các kiểu truy cập.

Bảng 2.1 – Các kiểu tệp tin

Ký tự đại diện	**Kiểu tệp tin**	**Định nghĩa**
-	Liên kết cứng tệp tin thông thường	Tệp tin thông thường.
b	Tệp tin khối đặc biệt	Tệp tin cho thiết bị vào/ra trong định dạng khối, cho phép truyền thông tới một thiết bị trong khối.
c	Tệp tin ký tự đặc biệt	Tệp tin cho thiết bị vào/ra trong định dạng ký tự, cho phép truyền thông tới một thiết bị bằng các ký tự.
d	Thư mục	Tệp tin chứa các thiết lập của tệp tin khác.
l	Link	Tệp tin trỏ tới các tệp tin khác cùng trong một tệp tin hệ thống (liên kết mềm), hoặc trỏ tới cùng một inode (liên kết cứng). Một inode là một số đại diện của một tệp tin được hệ thống sử dụng để tham chiếu tới tệp tin đó.
p	Named pipe	Tệp tin sử dụng cho truyền thông nhiều

		tiến trình.
s	Socket	Tệp tin sử dụng để truyền thông nhiều tiến trình giữa địa chỉ IP nguồn và đích, cổng nguồn và đích đã được xác định.

Bảng 2.2 – Các quyền truy cập

Ký tự đại diện	**Truy cập**	**Miêu tả**
r	Read	Cung cấp khả năng để xem một tệp tin hoặc liệt kê danh sách thư mục.
w	Write	Tệp tin có thể được chỉnh sửa hoặc có quyền xóa, quyền thêm các tệp tin vào một thư mục.
x	Execute	Tệp tin có thể được thực thi, hoặc có khả năng di chuyển đối với thư mục.
t	Stick bit	Đối với thư mục, thiết lập này ngăn chặn người dùng xóa các tệp tin khi người dùng đó không phải là chủ sở hữu của thư mục.
s	suid/sgid	Đối với người dùng thiết lập quyền trình bày là “set user id”; đối với nhóm thiết lập quyền là “set group id”. Tệp tin sẽ được thực thi với đặc quyền với người dùng hoặc nhóm chủ sở hữu của tệp tin.
l	File locking	Thiết lập bắt buộc khóa tệp tin nhằm ngăn chặn đọc và ghi tới tệp tin trong khi sử dụng.

Trở lại với ví dụ trên:

```
Linux1:  # ls –l  /home/thuchanh/thuchanh1.txt

-rwxr-xr-x  1  user1  users  11    Sep  9              06:30
thuchanh1.txt
```

Bảng 2.3 – Liệt kê và giải thích các trường

Trường	Tham số	Giải thích	Giải thích cho tệp tin
Trường đầu tiên	-	Kiểu của tệp tin	Liên kết cứng tệp tin thông thường
Ký tự 2-4	rwx	Quyền chủ sở hữu tệp tin	Đọc, ghi, thực thi
Ký tự 5-7	r-x	Quyền đối với nhóm	Đọc, thực thi
Ký tự 8-10	r-x	Người dùng khác	Đọc, thực thi
Trường 2	1	Số liên kết	Một
Trường 3	User1	Chủ sở hữu tệp tin	User1
Trường 4	Users	Nhóm sở hữu	User
Trường 5	11	Kích cỡ tệp tin	11Kb
Trường 6,7,8	Sep 9 06:30	Thời điểm tạo	Sep 9 06:30
Trường 9	Thuchanh1.txt	Tên tệp tin	Thuchanh1.txt

Kết quả các quyền của tệp tin thuchanh1.txt đối với người dùng: chủ sở hữu tên User1 có quyền đọc, ghi, thực thi tệp tin. Mọi người trong nhóm Users cũng như người dùng khác chỉ có quyền đọc và thực thi tệp tin.

Ngoài ra, một phương pháp khác để trình bày các quyền gọi là chế độ tuyệt đối. Phương pháp này người dùng có thể trình bày các quyền bằng số thay vì sử dụng các ký tự r, w, x. Các số được biểu diễn là hệ số bát phân (cơ số 8) và được trình bày trong bảng 2.4. Các số trình bày được tính bằng cách, cộng các số ứng với các quyền. Xét trong ví dụ trên quyền đối với tệp tin thuchanh1.txt là 755 bởi vì: r (4) + w (2) + e (1) = 7 cho chủ sở hữu, và r (4) + e (1) = 5 cho nhóm và người dùng khác.

Để thay đổi cho phép nhóm người dùng truy cập tới tệp tin sở hữu, và không cho phép người dùng khác ngoài nhóm truy cập tới tệp tin. Bằng cách thêm quyền cho nhóm người dùng đối với tệp tin. Sử dụng lệnh sau để thay đổi quyền:

```
Chmod g+rwx /home/thuchanh/thuchanh1.txt
```

Bảng 2.4 – Các quyền thể hiện trong cơ số 8

Quyền cơ số 8	**Ý nghĩa**
4	Đọc
2	Ghi
1	Thực thi

Nhằm giảm thiểu truy cập tới các tệp tin và thư mục, người dùng và đặc biệt là người quản trị phải hiểu rõ những hành động đang thực hiện và kết quả gây ảnh hưởng tới người dùng. Ví dụ: Thiết lập quyền cho thư mục quan trọng với quyền thực thi và không cho phép quyền đọc và ghi với tất cả người dùng (d--x--x--x hoặc 111), với cách thức này chỉ cho phép những người biết chính xác tên của tệp tin bên trong thư mục để thực thi nó, và không cho phép người dùng thực hiện liệt kê thư mục. Cách thức này đã thực hiện che dấu nội dung của thư mục nhưng đây không phải là biện pháp an toàn tối ưu. Trước hết người quản trị cũng như người dùng phải hiểu rõ việc thiết lập quyền cho tệp tin và thư mục sau đó thực hành kiểm tra ảnh hưởng của quyền đã thiết lập, cuối cùng mới thực hiện thiết lập quyền cho hệ thống.

Một phương pháp khác để kiểm soát truy cập là sử dụng danh sách điều khiển truy cập (ACLs). Phương thức tối ưu hơn khi thực hiện kiểm soát truy cập đối với tệp tin và thư mục. ACLs cho phép người dùng thay đổi quyền tới tệp tin. Người quản trị có thể sử dụng các quyền chuẩn của Unix để thiết lập các mức cao hơn, ví dụ: Cho phép một người dùng (user1) có quyền đọc và quyền ghi tới tệp tin và cho phép người dùng khác (user2) chỉ có quyền đọc tới tệp tin. Mỗi một phiên bản của Unix thì việc thực hiện ACLs khác nhau, một số phiên bản của Unix không hỗ trợ ACLs.

Sau khi đã tìm hiểu quyền truy cập cơ bản trên hệ thống Unix, bước tiếp theo người quản trị phải tìm kiếm các lỗ hổng bảo mật của các tệp tin trên hệ thống. Bước đầu tiên thực hiện tìm kiếm các tệp tin có suid/sgid. Những tệp tin này có khả năng mất an toàn bởi vì chúng có thể cho phép kẻ tấn công chạy các chương trình hoặc các đoạn mã lệnh để nâng quyền.

Sử dụng lệnh sau để tìm kiếm tệp tin suid/sgid:

```
Find / -type f\(-perm 04000 –o –perm -02000\) –exec
ls –la {}\
```

2.2.1.2 Kiểm soát truy cập trong hệ điều hành Windows

Kiểm soát truy cập trong các hệ thống Windows khác nhau tùy vào từng phiên bản và các đối tượng được bảo vệ. Phiên bản Windows 95/98 và Windows Me không cung cấp cơ chế kiểm soát truy cập tới tệp tin hệ thống và Registry.

Truy cập từ xa và chia sẻ dữ liệu được kiểm soát thông qua tài khoản người dùng và mật khẩu. Trong phiên bản Windows NT 4.0, Windows 2000, Windows XP Professional, Windows Server 2003 cung cấp cơ chế kiểm soát truy cập tùy ý cho các tệp tin, thự mục, chia sẽ dữ liệu, và truy cập tới Registry. Ngoài ra, kiểm soát truy cập tùy ý còn được sử dụng trên các đối tượng trong Active Directory Windows 2000, Server 2003, Server 2008 là máy chủ điều khiển miền.

Điều khiển truy cập tới các mức của thư mục và tệp tin có thể được gán tới người dùng hoặc nhóm người dùng cục bộ của Windows. Nhưng tài khoản

cục bộ này được lưu trong cơ sở dữ liệu cục bộ của máy tính. Khi máy tính được gia nhập vào miền thì những tài khoản này chứa trong cơ sở dữ liệu tập trung của miền. Và những tài khoản miền có thể truy cập tới các tệp tin, thư mục tới các máy tính cùng thuộc miền tương ứng với những quyền đã được gán.

Nếu một người dùng là thành viên của nhiều nhóm, người dùng này sẽ được gán quyền tương ứng của mỗi nhóm. Và người dùng này sẽ được sử dụng quyền cao nhất.

Tệp tin hệ thống, Registry, và cơ sở dữ liệu Active Directory là cấu trúc phân cấp, và tương ứng quyền cũng có tính kế thừa. Tính kế thừa là quá trình chuyển quyền được gán cho các đối tượng mức cao tới các đối tượng mức thấp hơn. Khi thiết lập quyền truy cập người quản trị phải xem xét tới tính kế thừa, quyền cho phép, hoặc quyền cấm truy cập để kết quả hiệu quả nhất.

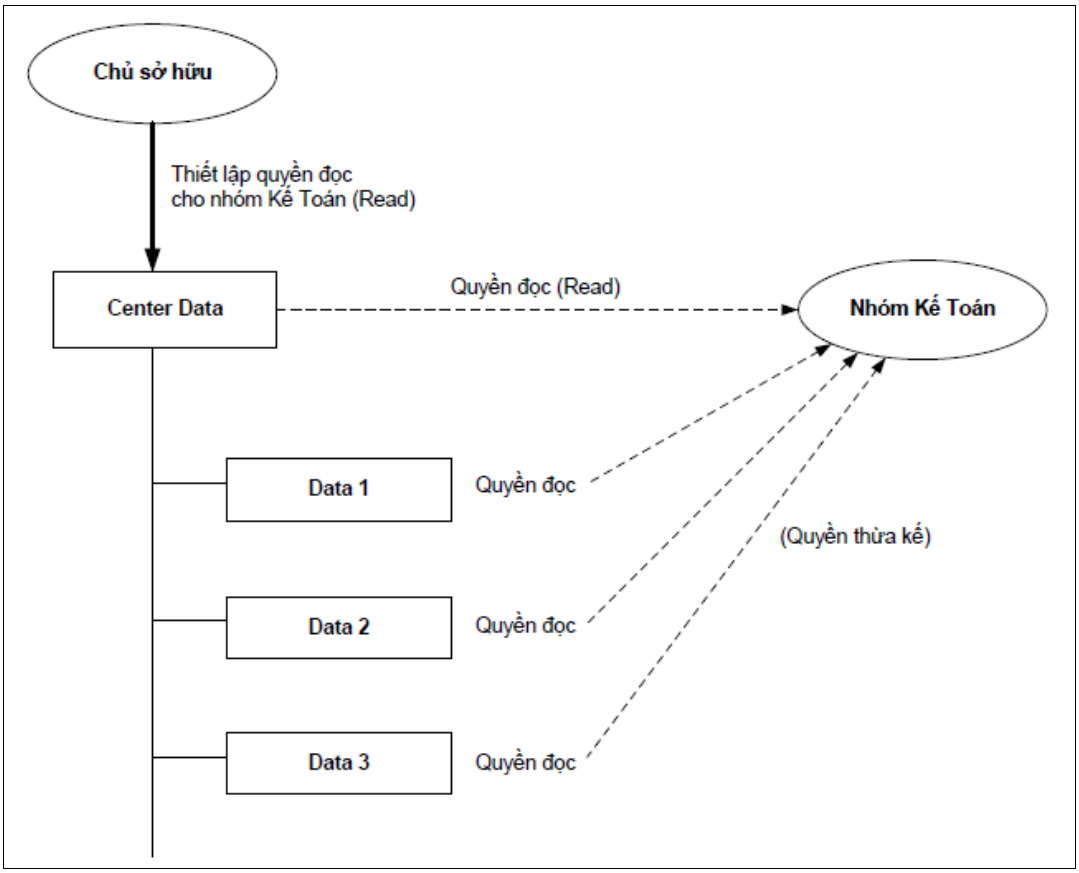
Tính kế thừa

Trong phiên bản Windows NT 4.0 các tệp tin và các thư mục luôn luôn kế thừa các quyền được gán tới thư mục mức cao hơn. Xét ví dụ ở hình 2.1:

Trong ví dụ này quyền đọc được gán cho nhóm KeToan tương ứng với thư mục là BaiViet, do đó các thành viên trong nhóm KeToan được quyền đọc tới các tệp tin trong thư mục con là Baiviet1, Baiviet2. Sử dụng tính kế thừa giúp việc thực hiện gán quyền dễ dàng hơn nhưng bên cạnh đó cũng gây các nguy cơ bị tấn công do cấu hình sai. Ví dụ, quyền truy cập tới tệp tin bên trong thư mục được lên kế hoạch và triển khai cẩn thận và các quyền truy cập được hạn chế, những quyền này có thể bị thay đổi bằng cách thiết lập ở thu mục chứa nó. Thư mục System32 chứa các tệp tin cấu hình hệ thống Windows, vì thế mà nó được bảo vệ bằng cách hạn chế quyền truy cập tới các tệp tin chứa trong thư mục System32. Nếu người quản trị thay đổi quyền lên phân vùng chứa thư mục System32 thì quyền này sẽ ảnh hưởng tới các thư mục con và tệp tin bên trong nó.

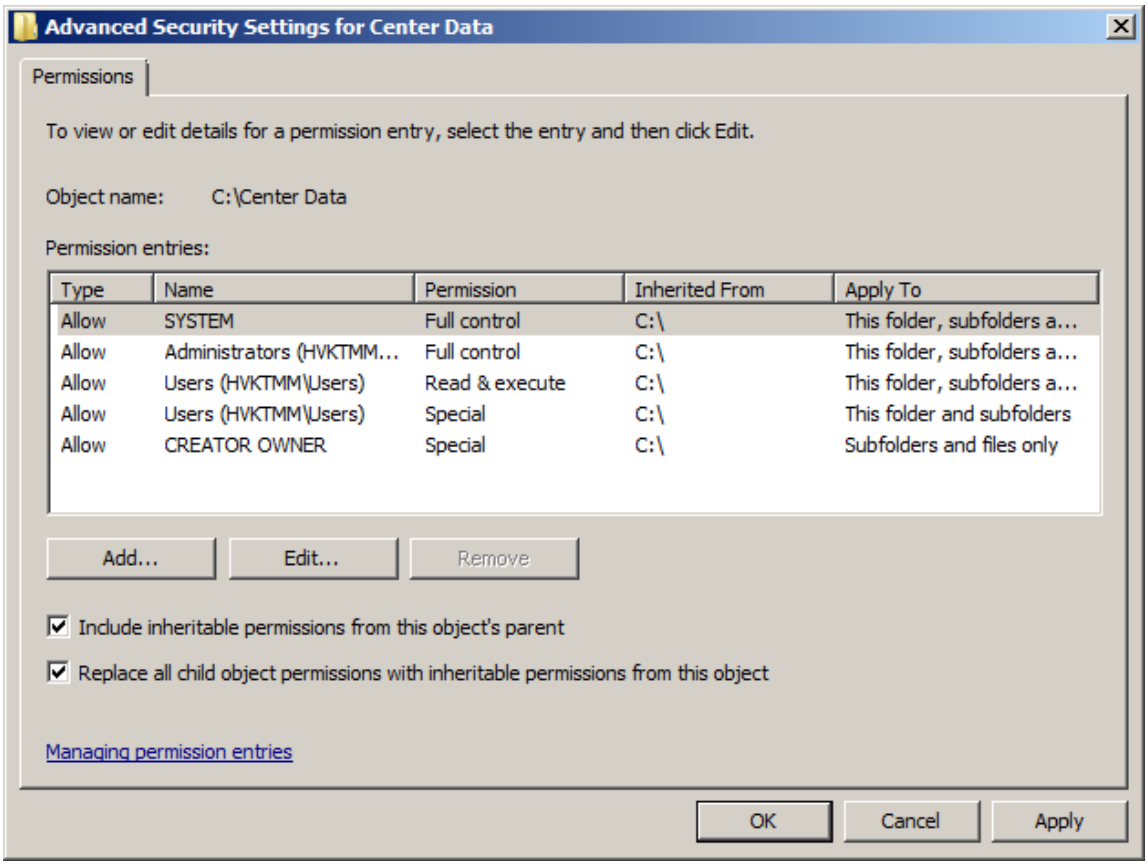
Trong các phiên bản Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008 các thư mục và tệp tin có thể được đánh dấu để

loại bỏ tính kế thừa từ các thư mục mức cao hơn. Tùy chọn này cho phép người quản trị cấu hình việc kiểm soát truy cập một cách chính xác tới từng thư mục và tệp tin nhạy cảm.



Hình 2.1 – Mô tả tính kế thừa quyền từ thư mục mức cao hơn

Đề thay đổi quyền kế thừa từ thư mục mức cao hơn người quản trị hoặc chủ sở hữu của thư mục đó chỉ cần bỏ tùy chọn trong mục Permission.



Hình 2.2 – Các tùy chọn của tính kế thừa

Liệt kê các quyền ảnh hưởng

Quy tắc sau đây người quản trị có thể sử dụng để xem xét trước khi thiết lập quyền …(kết hợp của các quyền sẽ được áp dụng, bao gồm quyền kế thừa và quyền tường minh) cho tất cả người dùng hoặc nhóm trên hệ thống Windows: Quyền "Cấm" được xem xét đầu tiên rồi sau đó thêm các quyền dựa vào vai trò của người dùng hoặc nhóm.

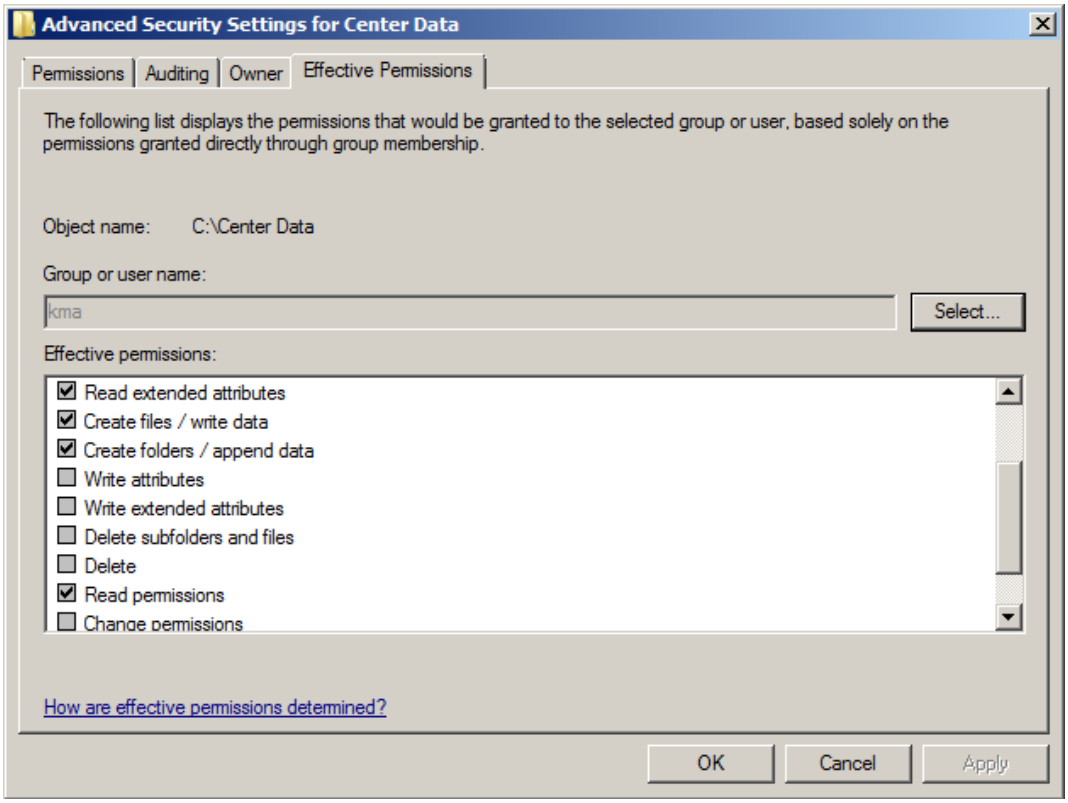
Trong phiên bản Windows NT 4.0 tự động thiết lập quyền Cấm lên trên cùng của danh sách kiểm soát truy cập (ACL). Danh sách kiểm soát truy cập là một cấu trúc lưu trữ chức năng kiểm soát truy cập đầu vào (ACEs), đây là một cấu trúc liệt kê các quyền và định danh người dùng và nhóm đã được cấp quyền. Khi một người dùng yêu cầu truy cập tới một tệp tin hoặc thư mục, danh sách này sẽ được kiểm tra, nếu người dùng đã bị cấm quyền truy cập thì đầu vào này sẽ không cần kiểm tra. Nếu người dùng không bị gán quyền Cấm thì ACE này sẽ được kiểm tra để nó cung cấp kiểm tra các quyền yêu cầu, nếu

có thì người dùng sẽ được quyền truy cập, nếu không thì người dùng sẽ bị cấm quyền truy cập.

Windows 2000 và các phiên bản trước đó đánh giá tính hiệu quả của thiết lập quyền khác nhau. Phiên bản Windows NT 4.0 áp dụng quyền kế thừa và quyền thiết lập trực tiếp là như nhau. Điều này có nghĩa là có thể quyền Cấm không được kiểm tra. Các quyền được đánh giá theo thứ tự dưới đây:

- Local Deny
- Local Allow
- Inherited Deny
- Inherited Allow

Trong phiên bản Windows NT 6.0, nếu một quyền "Cấm" đã được kiểm tra, sau đó nó tiếp tục xử lý quyền "Cho phép". Tuy nhiên nếu quyền Cấm được chia nhỏ thì quyền Cấm viết sẽ không ảnh hưởng đến quyền đọc khi người dùng yêu cầu. Quyền cho phép tường minh được kiểm tra trước khi xử lý quyền thừa kế "Cấm".



Hình 2.3 – Các quyền ảnh hưởng tới người dùng

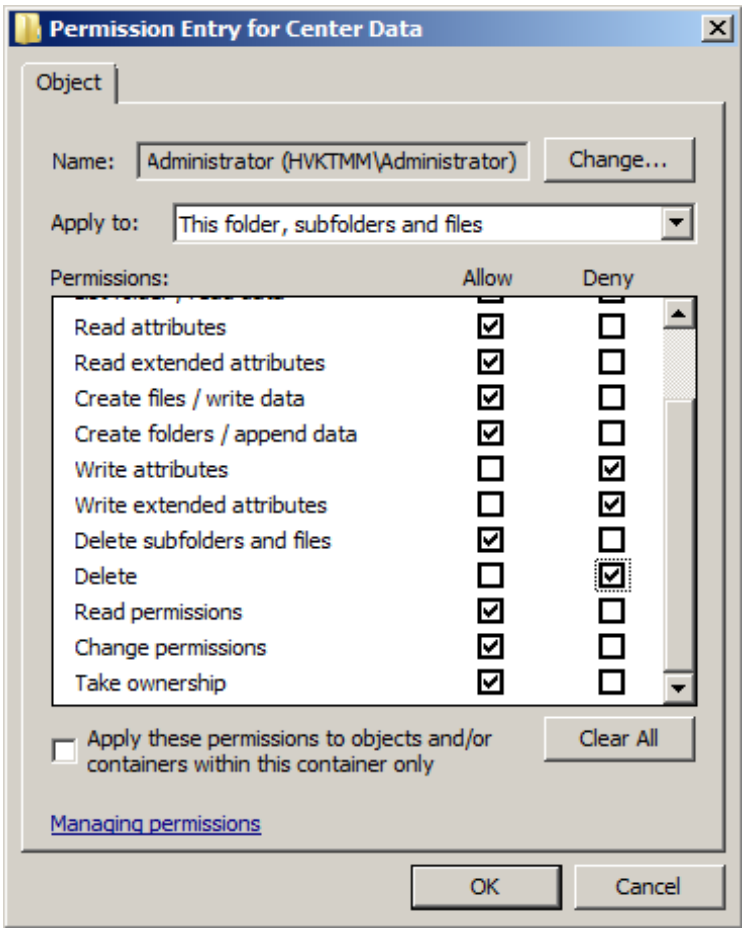
2.2.2. Xác định các quyền truy cập

Các quyền của tệp tin và thư mục trong hệ thống Windows được chia nhỏ hơn so với quyền trên hệ thống Unix. Các quyền trên Windows được chia làm bảy mục như trong bảng 2.5. Đối với quyền của mỗi mục thì có thể chia làm nhiều quyền nhỏ chứa trong nó, trình bày ở hình 2.4. Để gán quyền truy cập chi tiết tới tệp tin và thư mục người quản trị có thể chia nhỏ quyền của mỗi mục trong bảng 2.5.

Bảng 2.5 – Bảy hạng mục quyền trên Windows

Quyền truy cập	Đối với tệp tin	Đối với thư mục
Full Control	Cho phép tất cả các quyền	Cho phép tất cả các quyền
Modify	Quyền đọc, xóa, thay đổi, thực thi.	Liệt kê thư mục, đọc và thay đổi quyền và thuộc tính của thư mục, xóa thư mục, thêm tệp tin tới thư mục.
Read and Execute	Quyền đọc và thực thi tệp tin.	Liệt kê nội dung thư mục, xem quyền và thuộc tính của thư mục.
List Folder Contents	Quyền đọc và thực thi tệp tin.	Xem nội dung thư mục. Thực thi các tệp tin trong thư mục, đọc thuộc tính, đọc dữ liệu, liệt kê các tệp tin trong thư mục.
Read	Đọc nội dung tệp tin và thuộc tính.	Liệt kê danh sách thư mục. Đọc các thuộc tính và quyền.
Write	Ghi dữ liệu, thêm hoặc	Tạo tệp tin, tạo thư mục,

	xóa dữ liệu từ tệp tin. Thay đổi quyền và thuộc tính của tệp tin.	thay đổi quyền và thuộc tính thư mục.
Spectial Permissions	Quyền được chia nhỏ	Quyền được chia nhỏ



Hình 2.4 – Chia nhỏ quyền trên Windows

Quyền chia sẻ trên Windows

Chia sẻ dữ liệu trên Windows là điểm truy cập từ xa tới tệp tin và thư mục được chia sẻ. Phiên bản Windows 95/98 có hai mức chia sẻ:

- Mức chia sẻ: Thư mục chia sẻ được bảo vệ bằng mật khẩu. Mật khẩu được ứng với đối tượng chia sẻ, không áp dụng với người dùng cụ thể. Mọi người dùng biết mật khẩu chia sẻ có thể truy cập dữ liệu. Dữ liệu

chia sẻ không thể thiết lập bằng quyền cục bộ đối với tệp tin và thư mục.

- Mức người dùng: Thư mục chia sẻ được bảo vệ bằng cách gán quyền truy cập tới người dùng hoặc nhóm người dùng, phương thức này sử dụng tài khoản miền để xác thực. Người dùng phải sử dụng tài khoản miền và mật khẩu để xác thực trước khi truy cập dữ liệu chia sẻ.

Windows XP có năm mức chia sẻ và hai kiểu chia sẻ, đơn giản và nâng cao. Bảng 2.6 liệt kê và mô tả năm mức chia sẻ thư mục. Nếu hệ thống tệp tin NTFS được sử dụng, các quyền có thể thiết lập tùy ý. Nếu sử dụng chia sẻ nâng cao, các quyền chia sẻ có thể được thiết lập tùy ý.

Bảng 2.6 – Năm mức điều khiển chia sẻ Windows

Mức	Vị trí	Khả năng truy cập từ xa	Chủ sở hữu	Quyền khác
1	My Documents (private)	Remote Desktop	Full Control	No
2	My Documents	Remote Desktop	Full Control	Administrator- Full control
3	Shared Documents folder	Remote Desktop	Full Control	Administrator- Read, Write, Delete; Power Users- Change; Restricted Users- Read
4	Shared folders on the network (Read only)	Yes	Full Control locally	Administrator- Full Control locally; Everyone- Read network access

5	Shared folders on the network	Yes	Full Control locally	Administrator- Full Control locally; Everyone- Change network access

2.2.3. Kiểm soát truy cập dựa vào vai trò

Kiểm soát truy cập dựa vào vai trò (RBAC) là một khái niệm về kiểm soát truy cập đã trở nên phổ biến hơn do tầm quan trọng về an toàn thông tin trong các tổ chức trên thế giới. RBAC liên quan tới cấp quyền truy cập dựa vào vai trò hoặc nhóm người dùng. Các thành viên cùng một vai trò (cùng nhóm) được cung cấp các quyền dựa vào vai trò của người dùng đó trong tổ chức. Điều này làm giảm chi phí quản trị bởi vì người dùng được thiết lập quyền dựa vào khung chuẩn. Điều này có nghĩa khi thêm hoặc loại bỏ các quyền có thể áp dụng cho một nhóm lớn so với áp dụng cho mỗi người dùng riêng lẻ. Ví dụ: Nếu một người dùng là thành viên của nhóm Kế toán, thay vì cấp quyền truy cập cho mỗi một thành viên trong nhóm, người quản trị có thể đưa họ vào một khung vai trò chuẩn, tại đây các vai trò đã được định nghĩa sẵn. Sau đó thiết lập các ngoại lệ tương ứng với vai trò của mỗi người dùng. Khái niệm này rất quan trọng để hiểu rõ chức năng của một số sản phẩm đa nền tảng sử dụng vai trò để xác định một người dùng đã truy cập tới hệ thống.

Có nhiều gói phần mềm có sẵn để đạt tới RBAC và mỗi một phần mềm có các tùy chọn cấu hình và khả năng riêng. Sau đây là gói phần mềm phổ biến:

- RBAC bao gồm với Sun Solaris
- RBAC/Web Release 1.1 RBAC hệ thống dựa vào Unix – POSIX (Portable Operating System Interface), bao gồm Linux và hầu hết các phiên bản Unix.
- Sudo (Hầu hết các phiên bản Unix). Gói phần mềm này cho phép thực thi ở mức cao và dựa vào vai trò. Cho phép người quản trị truy cập sử dụng dòng lệnh với đầy đủ quyền trong trình điều khiển.

Hệ thống Windows dựa vào công nghệ NT nguyên bản không hỗ trợ kiểm soát truy cập dựa vào vai trò RBAC. Tuy nhiên, một RBAC đơn giản có thể được thực hiện bằng cách tạo các nhóm người dùng và gán yêu cầu truy cập với các quyền tương ứng với vai trò đã được định nghĩa sẵn. Mỗi một người dùng có thể được gán thêm các quyền ngoài vai trò đã được gán. Các ứng dụng của Microsoft SQL Server thực hiện các vai trò và cung cấp khả năng để định nghĩa thêm các vai trò dựa vào các yêu cầu của ứng dụng.

2.2.4. Thiết lập các công cụ nền tảng cho kiểm soát truy cập

Có rất nhiều công cụ có sẵn cho người quản trị sử dụng để điều khiển truy cập đa nền tảng. Trong phần này, tài nguyên được giới hạn và người quản trị sử dụng kết hợp các dịch vụ chuẩn mặc định như là FTP, các tiện ích thương mại hoặc các công cụ do người quản trị tạo ra. Nhiều hệ thống mạng không đồng nhất yêu cầu phải cấu hình nâng cao, khả năng tương thích phải an toàn, có rất nhiều các công cụ hỗ trợ cho chức năng này. Tuy nhiên, không phải tất cả các công cụ cung cấp đầy đủ các tính năng cho điều khiển truy cập.

2.2.4.1 Thiết lập cơ bản cho dịch vụ truyền và chia sẻ tệp tin

Có nhiều công cụ cung cấp chức năng truyền hoặc chia sẻ tệp tin. Một công cụ có sẵn trong hệ thống Windows là chia sẻ mạng và khả năng ánh xạ ổ đĩa từ xa của hệ thống Unix.

Thiết lập cho dịch vụ FTP

Truy cập tới máy chủ cung cấp dịch vụ FTP được bảo vệ bằng tên đăng nhập và mật khẩu, nhưng mật khẩu cũng như dữ liệu mặc định khi truyền trên mạng ở dạng không được mã hóa. Các quyền có thể được thiết lập ở mức thư mục để giới hạn truy cập sau khi kết nối đã được thiết lập. Thiết lập mặc định của dịch vụ FTP là cho phép truy cập từ bộ nhớ đệm, vì vậy đây cũng là một điểm yếu của giao thức. Tuy nhiên truy cập có thể được đảm bảo an toàn bằng phương pháp yêu cầu sử dụng các kênh mật mã như VPN hoặc SSH được thiết lập tại máy chủ dịch vụ FTP.

Một lựa chọn khác, bảo mật dữ liệu trên đường truyền thông qua FTPs, phương pháp này sử dụng giao thức bảo mật SSL để bảo mật phiên kết nối

FTP. Những phương thức trên chỉ bảo vệ dữ liệu khi truyền trên mạng, còn dữ liệu lúc lưu trữ thì người quản trị phải dùng những phương thức khác để bảo vệ nó.

Khóa chức năng truyền tệp tin thông qua tin nhắn nhanh

Các sản phẩm tin nhắn nhanh (Yahoo, Skype…) cho phép người dùng truyền tệp tin. Điều khiển truy cập tệp tin chỉ được cung cấp bởi người dùng mà đã cung cấp tệp tin. Mã độc tấn công có thể khởi tạo và lan truyền thông qua cơ chế này. Người dùng sẽ bị nhiễm mã độc khi họ mở tệp tin đính kèm. Cách duy nhất để ngăn chặn lây nhiễm là khóa tất cả tệp tin truyền qua tin nhắn nhanh thông qua tường lửa (Phương pháp này không thể ngăn chặn người dùng trong mạng nội bộ gửi tệp tin thông qua tin nhắn nhanh). Để khóa chức năng truyền tệp tin này, các chương trình tin nhắn nhanh bắt buộc phải sử dụng các cổng đặc biệt. Windows Messaging và Microsoft Network (MSN) sử dụng các cổng 6891 – 6900 để truyền tệp tin. Người quản trị bằng cách khóa các cổng này tại tường lửa sẽ ngăn chặn được truyền tệp tin thông qua tin nhắn nhanh. Tuy nhiên các chương trình tin nhắn nhanh cũng sử dụng cổng 80 để truyền tệp tin. Bước này người quản trị phải thực hiện kết hợp nhiều phương pháp khác để lọc mã độc gắn kèm với tệp tin.

Quản lý chia sẻ tệp tin giữa các máy tính ngang hàng

Tin nhắn nhanh cung cấp một phương pháp để chia sẻ tệp tin giữa các máy tính ngang hàng. Ở đây tệp tin không được duy trì trên máy chủ cung cấp dịch vụ chia sẻ tệp tin. Thay vì, mọi máy tính có thể truyền tệp tin tới và từ các máy tính khác. Vì vậy mà việc đảm bảo an toàn khi chia sẻ tệp tin giữa các máy tính là khó khăn. Ngoại trừ việc sử dụng các giao thức bảo mật như IPSEC. Trong các hệ thống Windows, các chính sách IPSEC có thể được cấu hình để yêu cầu các bên kết nối phải xác thực trước khi truyền thông với nhau. Một số phương thức xác thực và sử dụng mật mã để bảo vệ truyền tệp tin như: Xác thực sử dụng Kerberos, chứng chỉ, chia sẻ khóa. Phương pháp này ngăn chặn việc truyền tệp tin giữa các máy tính Windows xác nhận với các máy tính không được xác nhận hoặc các máy tính không tin cậy trên Internet.

Tuy nhiên, cũng có nhiều thuận lợi khi chia sẻ tệp tin giữa các máy tính ngang hàng. Nhiều ứng dụng có thể cung cấp khả năng tương thích cho các hệ thống Windows, Unix/Linux. Trước khi sử dụng những ứng dụng này người quản trị phải tìm hiểu các phương thức kiểm soát truy cập cũng như kiểm thử chức năng mà nó cung cấp.

2.2.4.2 Thiết lập kết hợp các dịch vụ của Microsoft với Unix

Các dịch vụ Microsoft Windows cho Unix (SFU) bao gồm các hệ thống con Interix, các công cụ, các tiện ích được thiết kế để hỗ trợ Unix tương thích với các phiên bản của Microsoft. SFU sử dụng Network File System để chia sẻ dữ liệu tới mọi hệ thống Unix/Linux hỗ trợ NFS. Quyền chia sẻ mặc định là Đọc và có thể được thiết lập tới các máy trạm và các nhóm. Chia sẻ không cung cấp quyền truy cập Root và người dùng nặc danh. Quyền mặc định của tệp tin đối với chủ sở hữu là Đọc, Viết, Thực thi. Quyền Đọc, Thực thi cho nhóm chỉ có thể truy cập tới tệp tin, và quyền Thực thi cho người dùng khác (`rwxr-x--x`). Windows DACLs được sử dụng để mô phỏng kiểm soát tệp tin Unix.

Thêm một dịch vụ bổ sung đó là: Gateway cho NFS, khi được cài đặt kích hoạt trên máy chủ Windows 2003, Windows server 2008, có thể cung cấp truy cập từ một máy Windows tới tài nguyên hệ thống tệp tin NFS Unix. Bản chất của phương thức này là máy chủ Unix ánh xạ tài nguyên NFS và chia sẻ nó với hệ thống Windows bằng cách sử dụng giao thức chia sẻ tệp tin (SMB).

Xác thực cho NFS được thực hiện thông qua máy chủ NFS. Dịch vụ phải được cài đặt trên máy chủ chia sẻ tệp tin và tất cả các máy chủ điều khiển miền (Domain Contronller). SFU có thể cung cấp PCNFS (NFS cho PC) nếu được yêu cầu bởi các hệ thống Unix. PCNFS thường được yêu cầu khi hệ thống Unix sử dụng các tệp tin bảo vệ mật khẩu trong Unix (Shadow Password). PCNFS được sử dụng để tạo các tệp tin khi ánh xạ các tệp tin mật khẩu/nhóm với mật khẩu đã được mã hóa trong tệp tin Shadow Password. Để ánh xạ tên người dùng trong Unix tới người dùng trong Windows IDs, dịch vụ ánh xạ tên người dùng được sử dụng để ánh xạ tên người dùng trong

Windows tới Unix và ngược lại. Khi một người dùng Unix yêu cầu truy cập tới tệp tin chia sẻ:

- Thực hiện kiểm tra để đảm bảo máy tính người dùng Unix được đăng nhập cục bộ để cấp quyền truy cập. Tên máy tính được giữ trong tệp tin .maphosts trong thư mục con Mapper của thư mục cài đặt SFUv3. Mặc định chỉ cho phép truy cập từ máy tính cục bộ. Với người quản trị phải được thêm các quyền khác.
- Dịch vụ ánh xạ tên người dùng (UNM – User Name Mapping) tìm kiếm tên người dùng Unix trong cơ sở dữ liệu của Windows và ánh xạ tên đăng nhập với Windows SID.
- Một yêu cầu truy cập được xác thực thông qua SID.
- Nếu người dùng Windows có quyền truy cập, thì người dùng Unix cũng được gán quyền truy cập.
- Nếu không có tên được ánh xạ hoặc không có người dùng có quyền truy cập, sau đó truy cập được gán tới một người dùng nặc danh.

Nếu dịch vụ ánh xạ tên (NMS) được sử dụng để hỗ trợ cổng giao tiếp, tài khoản người dùng Windows được ánh xạ tới cặp UID/GID của Unix. Dịch vụ truy cập từ xa Unix được cài đặt khi SFU cài đặt. Mặc định dịch vụ truy cập từ xa Windows Shell (WinRSH) chưa được kích hoạt, mặc dù khi cài đặt có thể đã được kích hoạt. Khả năng để sử dụng truy cập từ xa để kết nối chứa nhiều rủi ro lớn, và nhiều phiên bản truy cập từ xa của Unix có nhiều điểm yếu hoặc không có chức năng điều khiển truy cập.

WinRSH sử dụng tệp tin .rhosts để kiểm tra những máy tính nào có thể kết nối và không sử dụng đăng nhập miền. Vấn đề này luôn luôn chứa đựng mối nguy hiểm trong việc chỉ xác thực truy cập thông qua tên máy tính.

Inter-Unix các dịch vụ truy cập từ xa như: rsh, rstat, rdist cũng như Inter-Unix rshd (remote shell daemon) cho máy trạm và máy chủ và các dịch vụ rcp, rlogin có sẵn nhưng mặc định nó chưa được kích hoạt. Chức năng truy cập từ xa chứa nhiều rủi ro bị lợi dụng kể tấn công, vì vậy nó cần phải được bảo vệ.

Các bước thiết lập cho SFU phải được thực hiện thiết lập cho NFS. Vấn đề này bao gồm yêu cầu các tệp tin phù hợp và các quyền chia sẻ đã được thiết lập để cung cấp truy cập tới những người dùng yêu cầu truy cập. Khi thiết lập truy cập, người quản trị nên giới hạn quyền truy cập ít nhất có thể hạn chế tấn công leo thang đặc quyền.

Thiết lập an toàn cho dịch vụ Samba

Samba là một chương trình mã nguồn mở cung cấp dịch vụ chia sẻ dữ liệu và truy cập giữa các máy chủ Windows và Unix. Samba sử dụng rất nhiều giao thức phổ biến để chia sẻ tài nguyên gọi là SMB (Service Message Block) hoặc CIFS (Common Internet File System), những giao thức này được sử dụng trong chia sẻ của Microsoft.

Cũng như các chương trình khác, Samba là một ứng dụng đa nền tảng vì thế người quản trị cần phải hiểu rõ cấu trúc, chức năng nhằm đáp ứng việc cấu hình an toàn trong quá trình triển khai ứng dụng. Dưới đây là các bước thiết lập an toàn cho dịch vụ Samba:

- Đặt tệp tin cấu hình smb.conf bên trong thư mục được bảo vệ an toàn và thực hiện kiểm tra tính toàn vẹn theo định kỳ. Tệp tin này điều khiển giao thức SMB vì thế nó có thể được sử dụng trong các mục đích bất chính, bao gồm điều khiển cấu hình, nếu không được bảo vệ đúng đắn.
- Đảm bảo rằng tất cả các yêu cầu từ bên ngoài tới dịch vụ phải tuyệt đối cần thiết và phải sử dụng các phương pháp xác mạnh để xác định đúng người dùng có quyền truy cập.
- Cấu hình Samba để ngăn chặn tài khoản người dùng Windows có thể thay đổi hoặc xem quyền của tệp tin trên máy chủ cung cấp dịch vụ Samba. Khi một người dùng Windows kết nối, các quyền trên Unix được ánh xạ tới các quyền trên Windows. Bảng 2.7 trình bày các đặc điểm chuyển đổi các quyền giữa Unix và Windows.

Bảng 2.7 – Ánh xạ quyền từ Windows tới Samba

Windows	Samba
Full Control	rwx
Modify	rwx
Read & Execute	r-x
List Folder Contents	--x
Read	r--
Write	-w-

- Tùy chọn ngăn chặn người dùng không hợp lệ Samba: Tùy chọn này được sử dụng trong Samba để cho phép hoặc cấm người dùng truy cập tới dữ liệu chia sẻ. Trên Windows dữ liệu chia sẻ cũng được cấu hình để cho phép hoặc cấm truy cập thông qua tài khoản người dùng hoặc nhóm. Khi cấu hình quyền truy cập, người quản trị phải luôn luôn kiểm tra để xác định ảnh hưởng của các quyền đã thiết lập đối với tài khoản người dùng và dữ liệu chia sẻ.
- Hạn chế sử dụng tài khoản có quyền quản trị: Các thành viên trong nhóm quản trị có thể quản lý truy cập tới dữ liệu chia sẻ. Họ có thể thay đổi hoặc xóa bỏ dữ liệu của người dùng khác mà không quan tâm đến các quyền đã được thiết lập trước đó. Trong khi các thành viên của nhóm quản trị Windows được cung cấp quyền Full Control đối với dữ liệu chia sẻ. Người quản trị có thể thay đổi những quyền này để phù hợp với chính sách bảo mật, nhưng hạn chế truy cập hoặc xóa bỏ dữ liệu khi thực sự cần thiết.
- Thống nhất quy tắc đặt tên: Tên người dùng trong Windows không thực sự nhạy cảm. Tên người dùng trong Samba thực sự nhạy cảm. Bởi vì, trong Samba tên người dùng phân biệt ký tự hoa và ký tự thường, ANDY là một tên người dùng và khác với aNdy hoặc Andy.
- Quản lý các mức xác thực trong Samba: Samba có ba mức xác thực chia sẻ:

- Xác thực mức chia sẻ: Sử dụng các mật khẩu dùng cho chia sẻ (không phải mật khẩu người dùng). Xác thực mức chia sẻ trong Windows cũng tương tự xác thực mức chia sẻ trong Samba. Quyền truy cập được gán cho những người dùng biết mật khẩu chia sẻ này.
- Xác thực mức người dùng: Yêu cầu người dùng khi truy cập phải có quyền trên dữ liệu được chia sẻ.
- Xác thực mức máy chủ: Tương tự với truy cập mức người dùng nhưng ở đây sử dụng máy chủ miền để gán quyền truy cập.

- Không cho phép sử dụng mật khẩu ở dạng bản rõ: Người quản trị có thể cấu hình Samba để dụng mật khẩu ở dạng rõ. Đây là một lỗ hổng mà một kẻ tấn công có thể dò quét và phát hiện được mật khẩu khi truyền thông tin xác thực qua mạng.
- Cấu hình tệp tin smbpasswd trong thư mục /usr/local/samba/private và chỉ cho phép tài khoản Root có quyền đọc và ghi tới thư mục private và cấm tất cả người dùng khác truy cập vào thư mục này

Thiết lập bảo mật SMB – Server Message Block

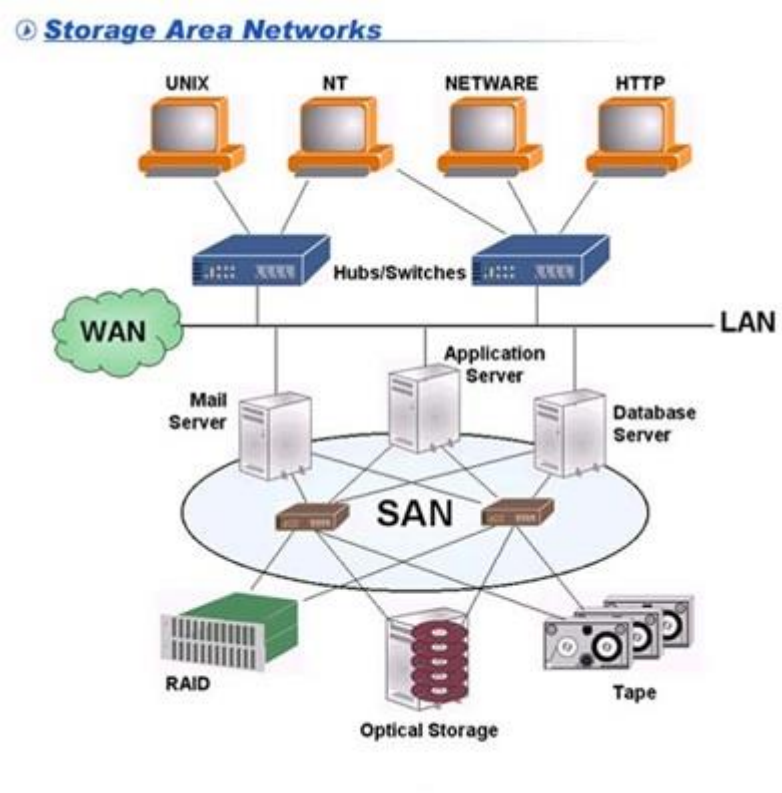
SMB là giao thức Windows sử dụng để chia sẻ dữ liệu và cũng được sử dụng bởi Samba để cho phép máy tính chạy hệ điều hành Windows truy cập tới dữ liệu chia sẻ trên máy chủ Samba. Tuy nhiên, nhiều kỹ thuật thiết lập bảo mật cho SMB không thể thực thi khi Samba sử dụng. Thiết lập an toàn chính cho SMB được thực hiện theo các bước sau đây:

- Khóa các truy cập tới các cổng SMB tại tường lửa. Phương thức này sẽ ngăn chặn truy cập dữ liệu chia sẻ trên Samba từ mạng bên ngoài vào mạng bên trong.
- Sử dụng nguyên tắc quyền tối thiểu: Chia sẻ dữ liệu với các quyền trên tệp tin và thư mục chỉ cho phép truy cập sau khi đã xác thực, yêu cầu truy cập là thực sự cần thiết.
- Thực hiện ký số SMB: Ký số SMB là một kỹ thuật được cung cấp trong Windows 2000, Windows XP, Windows Server 2003, Windows 7, Windows Server 2008. Gói tin SMB được ký bởi máy tính gửi. Máy

tính nhận có thể kiểm tra bằng chữ ký số và sẽ xác định được các gói tin được gửi bởi máy tính đã xác thực và cấp quyền truy cập.

Thiết lập bảo mật cho mạng lưu trữ SANS – Storage area networks

SANs cung cấp phương thức cho người dùng Windows và Linux truy cập dữ liệu lưu trữ dựa trên một mạng.



Hình 2.5 – Storage Area Network

Để đảm bảo an toàn khi truy cập dữ liệu SAN, người quản trị thiết lập theo các gợi ý sau:

- Định danh tất cả các giao diện mạng SAN.
- Sử dụng một mạng quản lý riêng biệt để truy cập tới SAN. Sử dụng công nghệ VPN hoặc tường lửa nếu cần thiết để truy cập tới SAN thông qua LAN.
- Sử dụng định danh người dùng dành riêng cho truy cập và định danh người dùng dành riêng cho quản trị.
- Thực thi chính sách mật khẩu mạnh.

- Phân chia các vùng SAN nhỏ cho quản lý và truy cập.
- Vô hiệu hóa các cổng không sử dụng trong SAN.
- Thay đổi mật khẩu mặc định trước khi kết nối thiết bị.
- Giám sát truy cập.
- Bảo vệ dữ liệu tránh các nguy cơ về sâu mạng và virút.
- Bảo vệ IP dùng để kết nối lưu trữ.
- Thiết lập an toàn tới các cổng truy cập.
- Sao lưu dự phòng dữ liệu.
- Triển khai các công nghệ an toàn như ảo hóa SAN, an toàn cổng, xác thực mạnh, IPSec.

Thiết lập an toàn NFS

NFS (Network File System) là một giao thức được tạo ra bởi hẵng Sun Microsystems trong những năm 1980, để chia sẻ tài nguyên hệ thống qua mạng máy tính. Giao thức này cho phép người dùng cuối truy cập từ xa tới dữ liệu trên máy chủ NFS. Hầu hết các phiên bản của Unix đều hỗ trợ NFS, và thực hiện trên nhiều hệ thống không phải Unix. Nếu người quản trị cấu hình không chính xác, NFS tồn tại nhiều lỗ hổng gây mất an toàn mà kẻ tấn công có thể khai thác. Các bước thiết lập an toàn cơ bản dưới đây giúp nâng cao bảo mật đối với máy chủ cung cấp dịch vụ NFS:

- Cài dịch vụ NFS tại phân vùng riêng trên máy chủ chia sẻ dữ liệu. Nếu kẻ tấn công thực hiện làm phá hủy hệ thống bằng cách làm đầy không gian lưu trữ với các tệp tin lớn, kẻ tấn công sẽ không thể thực hiện thành công bởi vì không gian đĩa đang còn trên các phân vùng khác.
- Gắn kết chia sẻ NFS chỉ với quyền đọc nếu có thể. Thiết lập này ngăn chặn thay đổi ngoài ý muốn hoặc mã độc sử dụng các tệp tin.
- Thiết lập tùy chọn **nosuid/nosgid** để ngăn chặn các chương trình suid/sgid từ các điểm gắn kết, ngăn chặn Trojan đang chạy trên các máy trạm.
- Sử dụng chương trình truy cập từ xa SSH để mã hóa luồng dữ liệu và truy cập an toàn. Thiết lập này ngăn chặn kẻ tấn công dò quét và chặn

bắt thông tin nhạy cảm như tài khoản đăng nhập và mật khẩu người dùng hoặc người quản trị.

- Sử dụng xác thực miền để hạn chế rủi ro giả mạo đăng nhập.
- Sử dụng phiên bản NFS 4: Phiên bản NFS4 cung cấp xác thực ACL (Access Control List) hỗ trợ Windows NT. NFS4 yêu cầu LIPKEY, sử dụng khóa công khai đơn giản chỉ có máy chủ có một cặp khóa công khai và khóa riêng để trao đổi khóa bí mật.

2.3. THIẾT LẬP NỀN TẢNG XÁC THỰC AN TOÀN

Xác thực (Authentication) là quá trình thiết lập hoặc chứng minh nguồn gốc của một người nào đó (hoặc một cái gì đó) là đáng tin cậy. Xác thực là một trong những thành phần nền tảng nhằm đảm bảo an ninh trong các hệ thống mạng. Để truy cập các nguồn tài nguyên yêu cầu thẩm quyền trong mạng (như đọc tập tin, chạy chương trình, cấu hình hệ thống…), người dùng cần phải có một định danh (ID), đồng thời phải chứng minh được tính tin cậy của định danh đó.Việc đảm bảo rằng chỉ người dùng tin cậy mới được phép chứng thực định danh của mình chính là mục đích của thiết lập xác thực. Quá trình xác thực trong một tổ chức có nhiều hệ điều hành và các thiết bị mạng khác nhau được gọi là thiết lập xác thực đa nền tảng. Để làm được điều đó cần phải nắm rõ kiến thức về các thuật toán cơ bản, các thiết bị cũng như các qui trình xác thực.

Phương pháp ủy quyền cơ bản nhất là thiết lập mật khẩu cho mỗi định danh người dùng. Định danh được coi là hợp lệ nếu như mật khẩu đăng nhập trùng với mật khẩu thiết lập ban đầu. Ngoài ra có thể sử dụng chứng chỉ số, thẻ bài, phương pháp sinh trắc học... để xác thực tính duy nhất của định danh người dùng.

Trong một môi trường mạng hỗn hợp, một số dạng xác thực được đánh giá là an toàn hơn so với các dạng khác. Tuy nhiên việc chuyển đổi từ dạng xác thực này sang dạng xác thực khác là không thể thực hiện do một số hệ điều hành và thiết bị mạng không tương thích với nhau hoặc do không đáp ứng được giá thành triển khai.

2.3.1. Thiết lập mật khẩu an toàn

Mật khẩu là phương pháp xác thực cơ bản nhất trong hệ thống. Để tránh được những nguy cơ tấn công, thì yêu cầu nhỏ nhất của hệ thống là thiết lập một mật khẩu đủ phức tạp, có độ dài từ sáu ký tự trở lên và phải bao gồm chữ cái (gồm cả chữ viết hoa và viết thường), chữ số và ít nhất một ký tự đặc biệt (-, _, @, +,..).

Một mật khẩu phức tạp còn quan trọng hơn là nhận thức của con người. Theo tính toán, nếu sử dụng ngẫu nhiên tất cả 94 ký tự có trong bảng mã ASCII thì có thể tạo được khoảng 690 tỉ mật khẩu có độ dài 6 ký tự ($\sim 94^6$). Nếu kẻ tấn công sử dụng máy tính có khả năng tính toán lên tới 100.000 tổ hợp ký tự ngẫu nhiên trong một giây thì sẽ cần khoảng 2 tháng rưỡi mới có thể dò hết tất cả số lượng mật khẩu nói trên. Phương pháp tấn công này gọi là *tấn công vét cạn (brute-force attack)*. Nếu may mắn, thời gian tìm kiếm có thể giảm xuống còn 1,25 tháng (~ 50%), 2.5 tuần (~ 25%) và 1.25 tuần (~12,5%)…Như vậy, mật khẩu càng phức tạp thì khả năng bị dò tìm càng thấp.

Bảng 2.8 đưa ra thời gian kẻ tấn công có thể dò tìm ra mật khẩu. Giả thiết kẻ tấn công có thể tính toán 100.000 nghìn tổ hợp ký tự trong một giây.

Bảng 2.8 – So sánh thời gian dò quét mật khẩu

Độ dài của mật khẩu (ký tự)	Thời gian dò tìm từ bộ 26 - ký tự	Thời gian dò tìm từ bộ 94 - ký tự
3	0,18 giây	8,3 giây
4	4,57 giây	13,0 giây
5	1,98 phút	20,4 giờ
6	51,5 phút	2,63 tháng
7	22,3 giờ	20,6 năm

8	24,2 giờ	1930 năm
9	1,72 năm	182,000 năm
10	44,8 năm	17,079,000 năm
11	1160 năm	1,605,461,000 năm
12	30,300 năm	150,913,342,000 năm

Thiết lập mật khẩu người dùng

Trong hầu hết các tổ chức đều có hai nhóm người dùng: nhóm người dùng nội mạng (ví dụ như nhân viên công ty) và nhóm người dùng ngoài mạng (ví dụ như khách hàng). Cần phải phân biệt rõ hai khái niệm này vì đối với mỗi nhóm người dùng cần thiết lập các chính sách mật khẩu khác nhau.

So với người dùng ngoài mạng, người dùng nội mạng sẽ truy cập tài nguyên hệ thống nhiều hơn. Do đó, việc quản lý cũng như thiết lập các chính sách mật khẩu cho nhóm này cũng cần phải chính xác, nghiêm ngặt hơn.

Đối với nhóm người dùng ngoài mạng, đặc biệt là các khách hàng của doanh nghiệp, cần phải thiết lập các chính sách mật khẩu một cách đơn giản, dễ hiểu để khách hàng có thể dễ dàng thực hiện các giao dịch. Một chính sách mật khẩu quá chặt chẽ có thể là nguyên nhân dẫn đến thất bại của doanh nghiệp trong kinh doanh.

2.3.2. Lựa chọn tiến trình xác thực an toàn

Khi một đối tượng được ủy quyền, nguồn xác thực sẽ kiểm tra và xác nhận tính xác thực của đối tượng đó. Có nhiều phương pháp cũng như công nghệ khác nhau để tiến hành xác thực các đối tượng trong hệ thống. Tuy nhiên, việc lựa chọn sử dụng phương pháp và công nghệ xác thực nào còn phụ thuộc vào thời gian, giá thành, quy mô, thậm chí cả môi trường sử dụng của hệ thống xác thực và đánh giá rủi ro. Dưới đây là ba phương pháp xác thực phổ biến có thể lựa chọn để triển khai:

- Xác thực dựa trên những gì ta biết
- Xác thực dựa trên tính năng vật lý không đổi
- Xác thực dựa vào những gì đã có

2.3.2.1 Xác thực dựa trên những gì đã biết

Như đã trình bày ở phần trước, phương pháp xác thực cơ bản nhất là sử dụng mật khẩu khi người dùng truy cập vào hệ thống. Một mật khẩu gồm sáu tham số chính, được mô tả trong bảng 2.9. Trong một vài trường hợp, việc tạo mật khẩu không yêu cầu đầy đủ các tham số này.

Bảng 2.9 – Các tham số của mật khẩu

Tham số	Mô tả	Ghi chú
Lịch sử mật khẩu (Password History)	Số lượng các mật khẩu cũ được lưu trữ. Khi các mật khẩu thay đổi, cả mật khẩu hiện thời và các mật khẩu lưu trữ đều không sử dụng được. Người dùng không được phép sử dụng các mật khẩu có trong danh sách này.	Yêu cầu lưu trữ ít nhất sáu mật khẩu riêng biệt trước khi cho phép sử dụng lại.
Thời gian sử dụng tối đa của mật khẩu (Maximum Password Age)	Thời gian lớn nhất mà mật khẩu có thể sử dụng trước khi buộc phải thay đổi.	Mật khẩu cho tài khoản người dùng có thể kéo dài 35 ngày, và 90 ngày đối với mật khẩu tài khoản dịch vụ.
Thời gian sử dụng tối thiểu của mật khẩu (Minimum Password Age)	Thời gian sử dụng ít nhất của mật khẩu trước khi được phép thay đổi. Nếu không có giá trị này, người dùng có thể thay đổi mật khẩu nhiều lần trong ngày để lấp đầy *Lịch sử mật khẩu* và lấy lại mật khẩu gốc ban đầu.	Nên thiết lập là 7 ngày. Người dùng sẽ không muốn thay đổi mật khẩu sau mỗi 7 ngày chỉ để lấy lại mật khẩu gốc ban đầu.

Độ dài của mật khẩu (Password Length)	Số ký tự bắt buộc tối thiểu của mật khẩu.	Mật khẩu phải dài ít nhất sáu ký tự. Độ dài càng lớn thì độ an toàn của mật khẩu càng cao.
Độ phức tạp của mật khẩu (Password Complexity)	Trong môi trường Windows, mật khẩu cần đáp ứng đủ ba điều kiện: 1. Chứa ba trong bốn thành phần: chữ hoa, chữ thường, chữ số và ký tự đặc biệt. 2. Không trùng với tên hoặc định danh. 3. Có độ dài ít nhất sáu ký tự.	Có thể tùy chọn *Enable* hoặc *Disable*. Khi chọn *Enable*, mật khẩu phải đáp ứng đầy đủ các yêu cầu đảm bảo an toàn.
Khóa tài khoản (Account Lockout)	Khi tài khoản đã khóa thì không có bất cứ mật khẩu nào hợp lệ. *Attacker* chỉ có thể dò quét hoặc bẻ khóa được mật khẩu trước khi tài khoản bị.	Thiết lập các tham số sau: *1. Account Lockout Threshold (Khóa tài khoản)* = 3: khóa tài khoản sau ba lần nhập sai mật khẩu. 2. *Account Lockout Duration (Thời gian khóa tài khoản) = 30*: mỗi lần tài khoản bị khóa kéo dài 30 phút. 3. *Reset Account Lockout Counter After* = 30: sau mỗi 30 phút, nếu số lần nhập sai mật khẩu nhỏ hơn tham số *khóa tài khoản* thì số lần truy cập trái phép sẽ trở về 0.

Sử dụng tham số *khóa tài khoản* làm nảy sinh một vài vấn đề. Trong một vài trường hợp, người dùng hợp pháp có thể quên hoặc nhầm lẫn mật khẩu khiến tài khoản bị đóng. Đồng thời nó cũng làm gia tăng số lượng tấn công từ chối dịch vụ (DOS) nhằm bẻ khóa mật khẩu hoặc khóa các tài khoản khiến người dùng hợp pháp không thể truy cập vào hệ thống. Để giảm các nguy cơ trên, nhiều tổ chức đã tăng số lần được phép nhập sai mật khẩu trước khi tài khoản bị đóng hoặc khiến cho việc thu thập các định danh người dùng của kẻ tấn công trở nên khó khăn. Ngoài ra, có thể ngăn chặn việc truy cập nặc danh (truy cập mà không cần tài khoản được ủy quyền) bằng cách không đặt tên các tài khoản người dùng theo quy luật tăng dần (ví dụ user1, user2, user3).

Giống như mật khẩu, các quy luật đặt tên tài khoản người dùng cũng cần phải giữ càng bí mật càng tốt. Hãy thử tưởng tượng, nếu kẻ tấn công nắm được quy luật đặt tên tài khoản (user1, user2, user3) và các tham số mật khẩu (ví dụ nhập sai mật khẩu ba lần sẽ khóa tài khoản…), chúng có thể viết các chương trình cho phép nhập mật khẩu lặp đi lặp lại cho đến khi tất cả tài khoản bị khóa. Việc tấn công có thể diễn ra tự động và trong thời gian rất ngắn, gây ra hậu quả khôn lường. Để giải quyết vấn đề này, nên chuẩn bị sẵn các tập lệnh nhằm khôi phục lại các tài khoản bị khóa.

Một phương pháp khác để khắc phục việc các tài khoản hợp pháp bị khóa đó là sử dụng tem thời gian để xác định được thời gian xảy ra các tấn công. Khi hàng loạt các tài khoản bị khóa, người quản trị có thể truy vấn đến các tài khoản cùng bị khóa trong một khoảng thời gian cụ thể (ví dụ trong 15 phút), sau đó sử dụng một tập luật để khôi phục lại các tài khoản đó. Phương pháp này không dùng để khôi phục lại tất cả các tài khoản vì có thể có những tài khoản được chủ động khóa bởi lý do an ninh.

Tuy nhiên, việc tấn công có thể xảy ra với các tài khoản ngẫu nhiên tại các thời điểm bất kỳ, đóng giả như một tấn công thực sự. Chỉ cần một tỉ lệ thành công thấp, kiểu tấn công này cũng có thể gây ra một vài hậu quả nghiêm trọng. Cách tốt nhất để ngăn chặn kiểu tấn công này đó là tránh sử dụng các định danh được đặt theo quy luật tăng dần (user1, user2, user3). Để

làm được điều đó, có thể cho phép người dùng tự thiết lập tài khoản của họ. Trong trường hợp bắt buộc phải tạo tài khoản người dùng với cấu trúc nhất định, nên sử dụng thêm các ký hiệu riêng cho từng tài khoản trước phần cấu trúc chung (Ví dụ A001, B002, E003). Khi muốn tấn công vào hệ thống, ngoài các ký tự theo cấu trúc chung (001, 002, 003), kẻ tấn công còn cần phải nắm được các ký hiệu riêng của từng người dùng (A, B, E).

2.3.2.2 Xác thực dựa trên tính năng vật lý không đổi

Con người có các nhân tố vật lý riêng không thay đổi như dấu vân tay, giọng nói, võng mạc mắt…. Quá trình xác thực hệ thống nhờ một trong số các nhân tố trên gọi là quá trình xác thực *sinh trắc học*. Trong hệ thống sinh trắc học, thay vì định danh và mật khẩu, người dùng chỉ cần sử dụng các nhận dạng riêng (nhân tố sinh trắc học) để truy cập vào hệ thống. Nhờ đặc tính không thay đổi của các nhân tố sinh trắc học, người dùng không cần phải lo lắng về việc quên hay nhầm lẫn nhận dạng của mình.

Ngoài tác dụng là thành phần cho quá trình xác thực, sinh trắc học còn được dùng trong hệ thống nhận dạng. Trong quá trình xác thực, người dùng nhập định danh của mình sau đó đưa ra nhân tố nhận dạng. Nếu nhân tố đưa ra trùng với nhận dạng của định danh lưu trong hệ thống thì người dùng được xác thực. Còn đối với hệ thống nhận dạng, người dùng chỉ cần đưa ra nhân tố nhận dạng mà không cần nhập định danh. Chỉ cần nhân tố đó có trong cơ sở dữ liệu thì quá trình nhận dạng thành công. Không giống như các nhân tố sinh trắc học, mật khẩu không được dùng để nhận dạng vì không có bất cứ sự ràng buộc vật lý nào giữa mật khẩu với người dùng.

Trước khi triển khai giải pháp sinh trắc học trên diện rộng, cần xem xét một vài vấn đề sau:

- Quá trình đăng ký sinh trắc học thực hiện như thế nào?
- Làm thế nào để bảo mật cho sinh trắc học?
- Việc chấp nhận sai và từ chối sai được giải quyết như thế nào?

Thiết lập một quá trình đăng ký an toàn

Sử dụng sinh trắc học được xem là phương pháp xác thực an toàn nhất, vì trên lý thuyết mỗi người dùng chỉ có một nhân tố nhận dạng riêng duy nhất. Một trong những vấn đề chủ yếu với sinh trắc học đó là quá trình đăng ký, tức là mỗi sinh trắc học của người dùng sẽ được cấp một biểu diễn số và liên kết với tài khoản người dùng. Nếu đăng ký xác thực bằng mật khẩu, người quản trị có thẩm quyền sẽ nhập định danh và mật khẩu, sau đó phân phối đến người dùng thông qua thư điện tử, đường bưu điện hoặc qua điện thoại. Nhưng với sinh trắc học, quá trình này là không cần thiết vì người dùng bắt buộc phải trực tiếp có mặt tại thời điểm đăng ký.

Mỗi người chỉ được phép đăng ký sinh trắc học một lần. Trước khi bắt đầu quá trình đăng ký, cần giải quyết các câu hỏi sau:

- Làm thế nào để xác nhận người đăng ký là hợp lệ?
- Việc đăng ký áp dụng cho những nhân tố nào?
- Chuyện gì sẽ xảy ra nếu đăng ký bị tổn hại?

Để giải quyết những câu hỏi trên, chúng ta cùng xem xét một ví dụ cụ thể là các tổ chức sử dụng dấu vân tay để xác thực trong hệ thống.

Làm thế nào để xác nhận người đăng ký là hợp lệ? Hầu hết các doanh nghiệp lớn đều có phương pháp riêng để xác nhận chính xác một người nào đó. Việc này có thể thực hiện nhờ đối chiếu người đó với khuôn mặt trên thẻ với một vài dấu hiệu lưu sẵn trong cơ sở dữ liệu nội bộ. Trong các tổ chức nhỏ, hầu hết mọi người đều quen biết lẫn nhau nên việc xác nhận trở nên dễ dàng hơn. Tại thời điểm đăng ký, các dấu hiệu và thông tin riêng sẽ liên quan đến sinh trắc học của từng người. Đối với các thành phần thứ ba muốn đăng ký, các tổ chức sẽ không có đủ tài nguyên chia sẻ để xác nhận tính hợp lệ của họ. Khi đó, việc xác nhận sẽ thực hiện thông qua các giấy phép cá nhân.

Những nhân tố nào được phép đăng ký? Giả sử một tổ chức sử dụng vân tay của ngón tay cái bên phải là nhận dạng đăng ký. Dĩ nhiên, những người bị cụt ngón tay cái bên phải sẽ phải dùng ngón tay khác. Nhưng những người mà ngón tay cái bên phải tạm thời không thể sử dụng ngay thời điểm đăng ký vì bị đứt, bị bỏng hoặc bị băng bó thì sao? Họ được phép dùng ngón tay khác hay sẽ phải đăng ký lại khi vết thương lành lặn? Vấn đề này không

chỉ xảy ra với dấu vân tay. Nó còn xảy ra với quét võng mạc, nhận dạng giọng nói…Yêu cầu của việc đăng ký là phải hoàn thành chỉ trong một lần. Vì vậy, khi muốn đăng ký một nhân tố sinh trắc học nào đó, cần phải tính đến tất cả những vấn đề có thể xảy ra khiến cho việc đăng ký không thể thực hiện.

Cũng cần phải xem xét trường hợp nếu một người đã đăng ký thành công nhưng sau đó nhân tố sinh trắc xong lại không có hiệu lực. Giả sử dùng ngón tay cái bên phải để đăng ký nhưng sau đó lại bị cụt hoặc bị bỏng thì thế nào? Đây là vấn đề xác thực và phải xem xét thời điểm đưa ra lựa chọn nhân tố sinh trắc học muốn đăng ký. Trong trường hợp này có thể đăng ký thêm một ngón tay, và sau đó chỉ cần sử dụng một trong hai ngón để xác thực.

Điều gì sẽ xảy ra nếu việc đăng ký bị tổn hại? Các thẩm quyền của một hệ thống sinh trắc học được lưu trữ ở dạng số nên vẫn có khả năng bị tấn công. Nếu một mật khẩu bị xâm phạm, nó có thể được cấp lại. Nhưng điều tương tự không xảy ra với sinh trắc học. Trên một bài báo năm 2002, Tsutomu Matsumoto, một nhà mật mã học Nhật Bản, đã công bố cách ông ta phá hỏng các sản phẩm của 11 công ty sinh trắc học hàng đầu thế giới chỉ với 10$ (http://cryptome.org/gummy.htm). Đó là ví dụ về một tấn công khiến cho việc thực hiện sinh trắc học trở nên vô ích, không phải vì sản phẩm không hoạt động mà vì có một phương pháp công khai có thể đánh bại độ khó của việc thực hiện sinh trắc học.

Bảo mật các thiết bị đọc sinh trắc học

Các bộ đọc sinh trắc học được phân làm hai loại: bộ đọc tập trung và bộ đọc phân tán. Giống như tên gọi, các bộ đọc sinh trắc học tập trung được bố trí và sử dụng một cách tập trung. Mỗi bộ đọc có thể xác thực cho nhiều người dùng, thường để truy cập vào các bộ phận như trung tâm dữ liệu… Do vậy các bộ đọc loại này chỉ được lắp ráp ở một vài nơi cố định. Có thể kể đến những bộ đọc tập trung điển hình như máy quét võng mạc hoặc thiết bị kiểm tra hình dạng bàn tay… Một ví dụ khác về bộ đọc tập trung đó là phần mềm nhận dạng giọng nói, có thể tích hợp trên điện thoại để phân tích giọng nói của những người gọi đến.

Việc triển khai các bộ đọc sinh trắc học tập trung cũng gặp phải một vài hạn chế. Ví dụ, nếu bộ đọc bị hư hỏng sẽ ảnh hưởng đến nhiều người dùng. Vì vậy trong hệ thống nên có sẵn một thiết bị sao lưu. Hầu hết các môi trường tập trung đều thiết kế một vị trí có chức năng dự trữ và mở rộng.

Bộ đọc sinh trắc học phân tán là bộ đọc chỉ sử dụng cho một người dùng và thường được dùng để xác thực mạng. Ví dụ như các bộ đọc vân tay và các máy quét mống mắt trên mỗi máy tính để bàn. Các bộ đọc phân tán có thể làm việc với một cơ sơ dữ liệu cục bộ (có trên máy tính cục bộ) hoặc dùng để bắt và chuyển tiếp các ủy quyền đến máy chủ trung tâm để xác nhận. Để giải quyết các sự cố hoặc lỗi thiết bị, khi xây dựng một giải pháp sinh trắc học phân tán cần có thêm các thủ tục sao lưu dữ liệu. Ngoài ra, cũng cần tính đến trường hợp người dùng không thể đăng nhập vào máy nếu máy chủ xác thực không sẵn dùng (ví dụ như bị ngắt kết nối).

2.3.2.3 Xác thực dựa trên những gì đã có

Một vài hệ thống xác thực yêu cầu người dùng sử dụng một đối tượng vật lý như thẻ khóa (key-card) hoặc thẻ bài (token). Đối tượng có thể liên kết đến định danh số hoặc chia sẻ thiết bị. Dạng xác thực này được gọi là xác thực dựa trên những gì đã có.

Ví dụ điển hình của hệ thống loại này là việc sử dụng các thẻ khóa để truy cập vào trong các tòa nhà. Trong nhiều hệ thống thẻ khóa, bất cứ ai sở hữu thẻ đều có thể truy cập vào bất cứ đâu mà thẻ cho phép. Giữa thẻ và người dùng không có mối ràng buộc cụ thể nào, trừ trường hợp thẻ được cấp riêng cho một cá nhân cụ thể. Khi đó đòi hỏi người dùng phải sử dụng thêm một đối tượng vật lý xác thực nào đó nhằm hai mục đích. Thứ nhất là để giới hạn số lượng người có thể xác thực. Thứ hai là khiến người dùng phải có trách nhiệm giám sát độ an toàn của thẻ. Trong trường hợp thẻ bị mất hoặc thất lạc, phải lập tức thông báo để vô hiệu hóa thẻ.

Một trong những ưu điểm của kiểu xác thực này là người dùng không cần phải nhớ mật khẩu. Khi cần xác thực, họ chỉ cần sử dụng các thiết bị vật lý được cấp quyền. Các thiết bị này được dùng để xác thực các hệ thống dựa trên ba phương diện chính:

- Giá trị mầm ngẫu nhiên
- Thách thức/ Phản hồi
- Khóa

Lựa chọn các hệ thống xác thực với giá trị mầm ngẫu nhiên

Giá trị mầm ngẫu nhiên (Random seed value) là sản phẩm số ngẫu nhiên của một quá trình. Mỗi một lần xác thực, người dùng có thể được quan sát để xác định mật khẩu hiện tại. Các số ngẫu nhiên được sinh ra là duy nhất đối với từng thiết bị, người dùng, và thời gian đăng nhập. Thiết bị sinh mầm ngẫu nhiên phổ biến nhất hiện nay đó là RSA securID (hình 2.6). RSA securID cho phép một khẩu mới hiện lên sau mỗi 60 giây và chỉ có hiệu lực trong một khoảng thời gian ngắn.

Hình 2.6 – RSA SecureID

Lựa chọn các hệ thống sử dụng thách thức/ phản hồi

Phương pháp xác thực dựa trên những gì đã có tiếp theo là thách thức/ phản hồi (challenge/ response). Trong các bộ phim, một điệp viên sẽ đến gặp người liên lạc và đưa ra ám hiệu. Dựa trên ám hiệu phản hồi, điệp viên biết được người liên lạc có đáng tin hay không. Đây là ví dụ điển hình của xác thực thách thức/ phản hồi. Nó cũng được sử dụng trong một số trang web khi một thành viên quên mật khẩu của mình. Trong quá trình đăng ký ban đầu, thành viên được yêu cầu một vài thông tin đặc biệt có thể dùng đến sau này, ví dụ như "tên đệm của mẹ bạn là gì". Trong trường hợp thành viên yêu cầu đặt lại mật khẩu, hệ thống sẽ đưa ra thách thức "hãy nhập tên đệm của mẹ bạn". Nếu nhập đúng, thành viên đó được phép thay đổi một mật khẩu mới.

Thách thức/ phản hồi cũng được sử dụng trong các hệ thống dựa trên mật khẩu như Microsoft Windows. Đầu tiên, người dùng sử dụng máy khách

gửi các thông tin đến hệ thống để yêu cầu xác thực. Hệ thống sẽ gửi ra một thách thức đến máy khách, đồng thời cũng tính toán câu trả lời nhờ các thông tin nhận được. Sau khi nhận được thách thức, máy khách tiến hành một vài thao tác và tính toán dựa trên các thông tin có sẵn và gửi phản hồi đến hệ thống. Thông tin mà cả máy khách và máy chủ đều biết có thể là mật khẩu người dùng hoặc một vài chữ số lưu trên thiết bị vật lý. Kết quả do hệ thống tính toán sẽ được so sánh với phản hồi của máy khách. Nếu chúng trùng nhau, người dùng được xác thực. Quá trình sử dụng thiết bị vật lý trong hệ thống thách thức/ phản hồi được thực hiện như sau:

1. Màn hình đăng nhập cho ứng dụng xuất hiện kèm theo yêu cầu xác thực thách thức/ phản hồi.
2. Người dùng nhập định danh.
3. Hệ thống xác thực dựa vào định danh người dùng để biết loại thẻ bài người dùng cần phải có, và gửi một thách thức đến màn hình đăng nhập.
4. Người dùng nhập các số thách thức vào thiết bị xác thực và nhận được một phản hồi.
5. Người dùng nhập phản hồi thu được từ thiết bị vào ứng dụng.
6. Nếu phản hồi của người dùng trùng với phản hồi do máy chủ tính toán thì người dùng được xác thực.

Các hệ thống khách cũng có thể được lập trình để sử dụng thách thức/ phản hồi cho việc xác thực. Ví dụ có thể tạo giá trị băm (*hash*) dạng số của ứng dụng và sử dụng một khóa mã hóa trên hệ thống cho ứng dụng đó. Mỗi lần hệ thống khách cố gắng xác thực, hệ thống chủ chịu trách nhiệm xác thực sẽ tiến hành tính toán dựa trên các giá trị băm và khóa của hệ thống khách và đưa ra câu hỏi (thách thức). Sau khi nhận thách thức từ hệ thống chủ, hệ thống khách sử dụng các thành phần của nó để tạo ra câu trả lời (phản hồi) cho thách thức. Nếu giá trị băm hoặc khóa trong cả hai hệ thống không có hiệu lực (trường hợp chương trình bị thay đổi) thì quá trình xác thực không thực hiện được. Với kiểu xác thực này, hệ thống không bao giờ phải gửi các chứng thực dựa trên mật khẩu vào trong mạng, vì quá trình chỉ đơn giản là so sánh những thành phần đã biết của cả hai hệ thống.

Lựa chọn các hệ thống sử dụng chứng chỉ số

Phương pháp xác thực thứ ba dựa trên những gì đã có đó là sử dụng các chứng chỉ số (*digital certificates)*. Các chứng chỉ số có thể được dùng cho máy tính và người dùng, sử dụng các giao thức bảo mật khác nhau như chứng thực, mã hóa thư điện tử, chữ ký số và mã hóa tập tin.

Các hệ thống xác thực dạng này sử dụng mật mã đối xứng (hay mật mã khóa bí mật), nghĩa là khóa mã hóa và khóa giải mã là giống nhau. Trong khi đó, mật mã bất đối xứng (còn gọi là mật mã khóa công khai) sử dụng một cặp khóa gồm khóa công khai (có thể công khai cho tất cả mọi người) và khóa riêng (chỉ người sở hữu cặp khóa mới biết). Nếu dùng khóa công khai để mã hóa thì khóa bí mật được dùng để giải mã và ngược lại. Các chứng chỉ số là sự ràng buộc giữa chủ thể và cặp khóa. Chứng chỉ số bao gồm thông tin về đối tượng sử dụng, khóa công khai của cặp khóa và được ký bởi trung tâm thẩm quyền chứng chỉ (*Certification Authority* – CA). CA là quá trình chạy trên máy chủ để quản lý và cấp các chứng chỉ cho các đối tượng thẩm quyền (máy tính hoặc người dùng). Khóa bí mật của cặp khóa không có trong chứng chỉ.

Khi sử dụng mã hóa bất đối xứng để xác thực, người dùng đưa ra chứng chỉ cho máy chủ xác thực để chứng minh tính hợp lệ của mình. Máy chủ xác thực chỉ chấp nhận chứng chỉ nếu nó được ký bởi một CA tin cậy và xác nhận chữ ký số trong chứng chỉ là hợp lệ. CA tạo chữ ký số cho chứng chỉ bằng cách sử dụng khóa riêng của mình để mã hóa cho một bản tin tóm lược (bản rút gọn của một vài dữ liệu) của chứng chỉ. Nếu CA là tin cậy, máy chủ xác thực sẽ sử dụng khóa công khai của CA để giải mã chữ ký số và thu được nội dung bản tin rút gọn.

Vì các chứng chỉ số là dữ liệu dạng điện tử, nên chúng cũng gặp phải các vấn đề xảy ra với dữ liệu điện tử như sao chép, sửa đổi… Phương án hiệu quả nhất để khắc phục những nguy cơ trên là lưu các chứng chỉ số trong một thiết bị vật lý như thẻ thông minh (*smart card*) hoặc thẻ bài xác thực tích hợp trên usb (*token*).

Nếu sử dụng thẻ thông minh thì cần bố trí một đầu đọc thẻ tại vị trí xác thực người dùng. Tương tự, đối với thẻ bài xác thực tích hợp trên usb, các máy truy cập cũng phải có cổng usb để người dùng cắm thiết bị. Phương pháp xác thực này có thể không được áp dụng cho người dùng di động, sử dụng các máy tính công cộng. Ví dụ, một người đang đi du lịch, sử dụng máy tính không có đầu đọc thẻ hoặc cổng usb để truy cập hệ thống, sẽ không được xác thực.

Trong khi các máy tính được lập trình để lưu trữ và sử dụng mật khẩu, việc sử dụng mã hóa bất đối xứng cung cấp một phương pháp quản lý xác thực từ máy tính đến máy tính an toàn hơn. Thông thường, khi tiến hành quá trình xác thực, cả hệ thống xác thực lẫn hệ thống thực hiện xác thực đều biết được bí mật. Nếu xảy ra sự cố rò rỉ thông tin hoặc mất mát dữ liệu thì rất khó để quy trách nhiệm cho một bên cụ thể nào. Tuy nhiên, nếu sử dụng mật mã bất đối xứng thì mọi chuyện trở nên vô cùng đơn giản. Khi đó, mỗi bên tham gia xác thực đều có một cặp khóa gồm một khóa riêng và một khóa công khai. Nếu khóa riêng bị tiết lộ và giao dịch lừa đảo được thực hiện với khóa đó thì có thể biết được chính xác đối tượng nào đã tiết lộ bí mật.

2.3.3. Các phương pháp xác thực mạnh

Xác thực mạnh (strong authentication) là phương pháp xác thực hệ thống sử dụng hai hoặc nhiều hơn các dạng xác thực nêu trên (xác thực dựa trên những gì đã biết, đã có hoặc nhân tố vật lý không đổi). Trong cộng đồng bảo mật, xác thực mạnh thường yêu cầu những yếu tố *đã có* và *đã biết*. Ví dụ như trường hợp sử dụng thẻ ATM: người sử dụng chỉ có thể rút tiền ra khỏi máy ATM nếu như *có* một cái thẻ và *biết* được mã PIN của nó. Tuy nhiên, xác thực mạnh cũng có thể dựa trên *nhân tố vật lý* và *những gì đã biết* (ví dụ như sinh trắc học và mật khẩu) hoặc *nhân tố vật lý* và *những gì đã có* (sinh trắc học và thẻ thông minh). Xác thực mạnh còn được gọi là *xác thực đa nhân tố*.

Trong thực tế, hầu hết các sản phẩm thương mại đều sử dụng xác thực hai nhân tố để xác thực người dùng. Người dùng phải sử dụng đồng thời một cái gì đó mà họ có (thường là sản phẩm cấu hình sẵn) kèm theo một cái gì đó

mà họ biết mới có thể được xác thực. Ví dụ, nếu sử dụng RSA SecurID, người dùng sẽ phải nhập mật khẩu và các giá trị được hiển thị trên thẻ để xác thực. Đối với thẻ thông minh, hầu hết các giải pháp xác thực đều buộc người dùng phải nhập mã PIN hoặc mật khẩu để mở khóa.

Xác thực mạnh bao gồm hai lớp bảo mật có sẵn:

- Một thiết bị vật lý phải đưa ra tại thời điểm xác thực. Trong trường hợp bị mất thiết bị, người dùng có thể yêu cầu đóng tài khoản cho đến khi được cấp thiết bị mới.
- Ngay cả khi thiết bị bị đánh cắp, kẻ trộm cũng cần phải có mã PIN hoặc mật khẩu để xác thực.

2.3.4. Thiết lập các dịch vụ xác thực

Nguồn xác thực (*authentication sources*) là một trong những khía cạnh quan trọng nhất của môi trường xác thực vì chúng lưu trữ một số lượng lớn các thông tin mật khẩu người dùng. Ngày nay, khi các cuộc tấn công nhằm vào các nguồn xác thực ngày càng nhiều, các quy định của chính phủ tiếp tục xác định rõ việc củng cố, bảo vệ các nguồn xác thực đang là nhiệm vụ cấp bách hơn bao giờ hết.

Thông thường, một tổ chức nào đó có quyền không thực hiện các giải pháp bảo mật cho nguồn xác thực của mình. Tuy nhiên, các cơ quan quản lý Nhà nước đang bắt đầu gặp phải những vấn đề nghiêm trọng hơn gây nên những hậu quả nhất định đối với các nguồn xác thực có tính bảo mật kém. Các công ty thường phải nộp những khoản tiền phạt lớn do không có phương pháp thỏa đáng bảo mật các nguồn xác thực của mình, nơi lưu trữ hàng loạt thông tin cá nhân của khách hàng. Trước đây, tập đoàn Microsoft từng phải chấp nhận 20 năm kiểm toán độc lập và phải sửa đổi báo cáo mô tả hệ thống của mình mới tránh được một khoản tiền phạt do trình bày sai lạc về mức độ an ninh của hệ thống xác thực hộ chiếu trực tuyến.

Ngoài ra, để cứng hóa các hệ điều hành sử dụng tại các nguồn xác thực cũng như vá lỗi cho các hệ điều hành và các qui trình xác thực, cần định kỳ kiểm tra tính tuân thủ đối với chính sách xác thực của tổ chức và các hệ

thống, dựa trên quá trình xác thực được sử dụng. Nếu sử dụng các hệ thống xác thực mật khẩu, cần phải đáp ứng một số yêu cầu cụ thể để thiết lập an toàn nơi lưu trữ mật khẩu. Mật khẩu sau khi được tạo thì không thể chuyển đổi ngược trở lại dạng văn bản rõ. Điều này thường được thực hiện bằng cách áp dụng một thuật toán hàm băm để mã hóa mật khẩu. Mã hóa hàm băm là một quá trình mã hóa một chiều và không thể giải mã ngược trở lại. Để đối chiếu mật khẩu, thay vì giải mã các mật khẩu được lưu trữ, người ta sẽ mã hóa mật khẩu nhập vào bằng một thuật toán hàm băm tương tự. Giá trị mã hóa sau đó có thể được so sánh trực tiếp với các mật khẩu được lưu trữ hoặc sử dụng trong quá trình xác thực thách thức/ phản hồi.

Đối với trường hợp sử dụng một ứng dụng của bên trung gian có nơi lưu trữ mật khẩu riêng, cần yêu cầu các nhà cung cấp giải thích rõ các phương pháp cũng như các tiêu chuẩn lưu trữ mật khẩu để đánh giá và độ bảo mật. Khi đánh giá nơi lưu trữ mật khẩu của một sản phẩm trung gian, hãy yêu cầu các nhà cung cấp trả lời một số câu hỏi sau:

- *Có thể chuyển đổi mật khẩu trở lại dạng rõ được không?* Nếu có, trong mọi trường hợp (kể cả khi mật khẩu được lưu ở dạng rõ) hãy dừng ngay việc thực hiện giải pháp.
- *Có sử dụng thuật toán hàm băm mật mã không?* Như đã nêu ở trên, một mật khẩu sau khi tạo ra sẽ được mã hóa bằng thuật toán hàm băm. Hàm băm là hàm mã hóa một chiều nên không thể giải mã ngược lại được. Nếu bên trung gian có sử dụng mã hóa hàm băm thì cần yêu cầu sử dụng một thuật toán hàm băm nổi tiếng như SHA1 hoặc MD5 vì chúng có độ bảo mật cao hơn so với các thuật toán riêng, độc quyền.
- *Giải pháp có cung cấp một giá trị băm mật mã muối (salted cryptographic hash)? Muối* là yếu tố duy nhất được thêm vào giá trị băm nhằm giảm rủi ro trước các tấn công. Ví dụ, nếu một mật khẩu chỉ đơn giản được băm với thuật toán SHA1, bất cứ ai truy cập vào SHA1 đều có thể tính trước một danh sách các mật khẩu tiềm năng để so sánh với mật khẩu hàm băm trong ứng dụng. Nhưng nếu SHA1 kết hợp với các muối, kẻ tấn công phải biết đồng thời cả thuật

toán và muối mới có thể thực hiện được mục đích của mình. Sự kết hợp này làm giảm thiểu các rủi ro khi nguồn xác thực bị tấn công. Với mỗi ứng dụng khác nhau nên sử dụng muối khác nhau, tránh tình trạng mật khẩu của ứng dụng này bị phá làm ảnh hưởng đến nguồn xác thực của ứng dụng khác.

2.3.5. Sử dụng các phương pháp xác thực đa nền tảng

Trong phần này chúng ta sẽ thảo luận làm thế nào để tăng hiệu quả cho quá trình xác thực thông qua môi trường triển khai. Trong các hệ thống thường hỗ trợ hai phương pháp xác thực sau: *xác thực gốc (native authentication)* và *xác thực qua bên trung gian (third-party authentication).* Xác thực gốc là dạng xác thực được tích hợp sẵn trên hệ thống. Còn xác thực qua bên trung gian là khả năng một hệ thống bỏ qua nguồn sẵn có của nó và các thẩm quyền hiện tại để xác thực với một hệ thống trung gian nhằm thu được một phản hồi về các thẩm quyền đã được cung cấp.

Điều đầu tiên cần làm khi muốn tăng hiệu suất của hệ thống xác thực thông qua môi trường triển khai đó là xem xét những hệ thống nào có số lượng lớn người dùng đăng nhập vào. Nếu đang sử dụng hệ điều hành Microsoft và đã triển khai cơ sở dữ liệu trung tâm (*Active Directory* – AD), thì cần thực hiện xác thực cho nhiều hệ thống, ứng dụng và các chương trình như là đối với AD. Điều yêu cầu người dùng phải ghi nhớ mật khẩu và đưa ra một địa điểm trung tâm để thực thi hoặc như vô hiệu hóa các tài khoản. Trong trường hợp nhiều hệ thống cùng sử dụng chung một nguồn xác thực duy nhất, nếu bị vô hiệu hóa tại một nguồn xác thực cụ thể, thì người dùng cũng không thể truy cập trên tất cả các nguồn xác thực còn lại.

Một tùy chọn khác để tận dụng các nguồn xác thực đó là chỉ ra những hệ thống hỗn hợp cho một nguồn xác thực mạnh, ví dụ như *RSA ACE/Server* – thành phần quản trị của giải pháp bảo mật RSA. Nhiều ứng dụng hiện nay có sẵn một tùy chọn để tích hợp trực tiếp vào RSA ACE/Server để thực hiện xác thực hai yếu tố. Điều này không làm gia tăng mức độ bảo mật mà đôi khi còn khiến người dùng khó chịu khi bị yêu cầu thêm một mã thông báo mỗi lần đăng nhập hoặc tái đăng nhập vào một ứng dụng. Tuy nhiên, ưu điểm của

phương pháp này là một tài khoản có thể bị vô hiệu hóa tại một nguồn xác thực nhưng vẫn dùng được trong các hệ thống còn lại.

Một cách khác để thực hiện xác thực đa nền tảng hiệu quả là sử dụng một ứng dụng quản lý mật khẩu, chẳng hạn như ứng dụng *TFS ApplicationControl* sử dụng công nghệ TFS. TFS ApplicationControl cho phép lưu mật khẩu trên màn hình dưới định dạng bảo mật. Tại thời điểm người dùng truy cập ứng dụng, mật khẩu sẽ được đưa vào TFS ApplicationControl. Điều đó cho phép người dùng chỉ cần xác thực mật khẩu một lần mà không cần tham gia vào các lần sau do đã có TFS ApplicationControl quản lý. Bất cứ lúc nào cần thay đổi mật khẩu, người dùng phải tạo hoặc ghi nhớ mật khẩu vì TFS ApplicationControl có thể thực hiện toàn bộ quá trình.

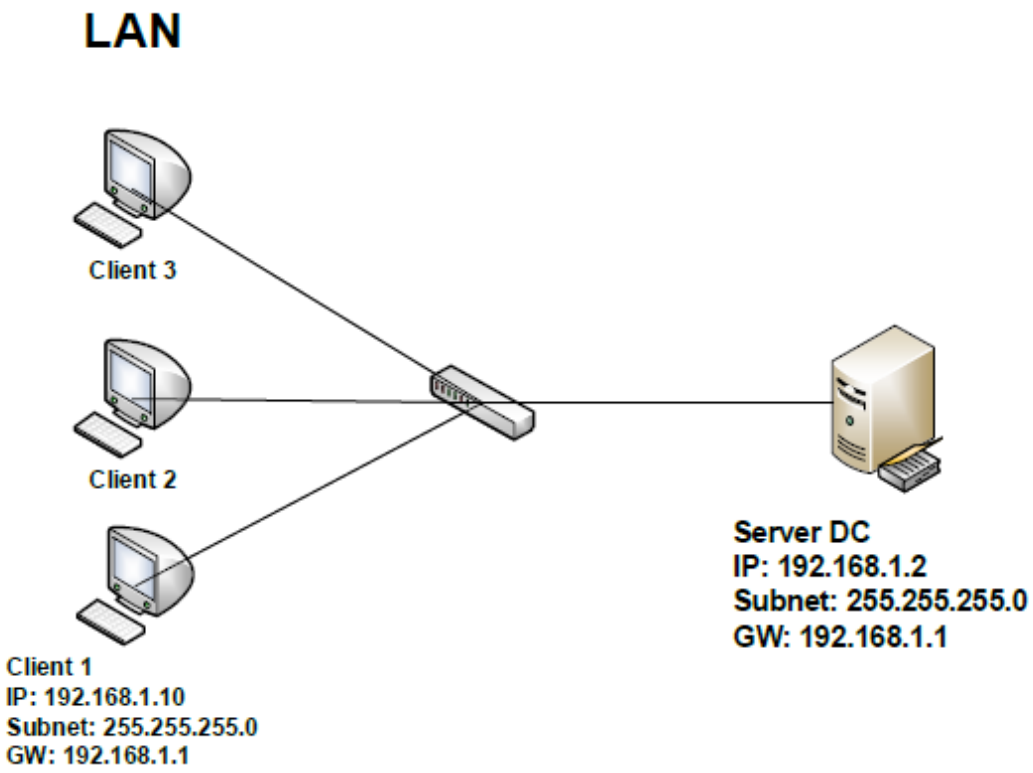
Giải pháp tiếp theo có thể được sử dụng thông qua môi trường xác thực là *Kerberos* – giao thức xác thực sử dụng "phiếu" (*ticket*). Sau khi tiến hành xác thực, người dùng sẽ được cấp một phiếu xác thực. Mỗi lần người dùng muốn truy cập vào các tài nguyên như các tập tin, máy in, và các ứng dụng, hệ điều hành sẽ kiểm tra phiếu xác thực và sau đó cấp cho người dùng một phiếu khác có chức năng thay thế cho mật khẩu truy cập. Sử dụng phiếu thay cho mật khẩu đem lại mức độ bảo mật cao hơn, bởi vì người dùng không cần phải nhớ mật khẩu cho tất cả các hệ thống mà họ truy cập vào. Về cơ bản, phiếu có độ an toàn cao hơn mật khẩu vì nó dựa trên cơ sở của mật mã. Để triển khai giải pháp Kerberos trong hệ thống, cần phải đảm bảo rằng tất cả các ứng dụng sử dụng đều hỗ trợ Kerberos.

CÁC BÀI THỰC HÀNH

1. Bài thực hành thiết lập kiểm soát truy cập

Mục đích bài thực hành: Xây dựng máy chủ kiểm soát tập trung với hệ điều hành Windows Server, tại máy chủ này chứa cơ sở dữ liệu về người dùng trong toàn bộ mạng, dữ liệu về phần mềm và tài liệu của mạng nội bộ. Khi người dùng muốn làm việc phải thực hiện xác thực vào miền với tên đăng nhập và mật khẩu tương ứng. Khi tương tác với tài nguyên chia sẻ phải có quyền thích hợp.

Bước 1: Thiết lập mô hình mạng như sau:



- Thiết lập địa chỉ IP tương ứng với máy chủ và máy trạm

Bước 2: Nâng cấp máy chủ DC lên chức năng Domain Controler.

Bước 3: Join các máy Client vào miền.

- Tại mỗi máy trạm thực hiện gia nhập vào miền (đã tạo trên máy Domain Controler), ở bước này cần phải có tài khoản quản trị miền.

Bước 4: Tạo tài khoản người dùng miền: user1, user2, user3, thực hiện trên máy chủ DC. Tạo thư mục dùng chung Data Center của miền trên máy chủ DC.

Với mỗi người dùng user1, user2, user3 khi sử dụng tài nguyên trong thư mục Data Center phải thực hiện xác thực miền trước khi sử dụng tài nguyên này.

Bước 5: Đăng nhập bằng user1 từ máy trạm Client 1:

Như vậy ở bước này tại máy chủ DC đã kiểm soát toàn bộ truy cập của máy tính và người dùng từ mạng nội bộ thông qua máy chủ quản lý tập trung DC.

Bước 6: Chia sẻ thư mục Data Center, bây giờ kiểm soát người dùng truy cập tới tài nguyên này bằng cách phân quyền đối với thư mục này:

- Người quản trị: administrator có toàn quyền
- Người dùng thường: user1, user2, user3 chỉ có quyền đọc (tương ứng với quyền cho phép xem và tải dữ liệu về)

Như vậy ở bước này, khi người dùng muốn sử dụng tài nguyên mạng phải có quyền tương ứng. Đây là chức năng kiểm soát truy cập tài nguyên chia sẻ.

2. Bài thực hành thiết lập kiểm soát truy cập trên Linux

Mục đích bài thực hành: Kiểm soát truy cập vào hệ điều hành Linux, ứng dụng phân quyền người dùng vào thư mục chia sẻ trên Linux.

Bước 1: Cài đặt máy chủ với hệ điều hành Linux, ví dụ: CentOS hoặc Ubuntu.

Bước 2: Tạo người dùng User1, User2, User3 trên Linux. User1 và User2 cùng nhóm kma.

Bước 3: Đăng nhập bằng quyền root

- Tạo thư mục /kma
- Tạo file thuchanh.txt trong thư mục /kma
- Thay đổi chủ sở hữu thư mục /kma là User1.

Bước 4: Cấp quyền: Toàn quyền với User1, cho phép User2 quyền ghi, Other quyền đọc lên file thuchanh.txt

- Logon vào các User để kiểm tra kết quả.

Bước 5: Thiết lập bit Sticky:

- Được sử dụng cho các thư mục chia sẻ, nhằm ngăn chặn người dùng đổi tên hay xóa file của người dùng khác.

- Những user có quyền: root, owner file, owner của thư mục chứa file.
- Khi stickby được thiết lập thì sẽ xuất hiện chữ "t" nằm ở vị trí cuối cùng của câu lệnh hiển thị permission
- Lệnh:

#Chmod +t *[đường dẫn]*

Bước 6: Thực hiện như sau:

- Cấp quyền 777 cho thư mục **/kma**
- Lần lượt login vào User1, User2, User3
- Mỗi người dùng tạo thư mục riêng trong thư mục **/kma**.
- Kiểm tra người dùng này thay đổi, xóa thư mục của người khác?
- Login vào root thiết lập Stickey cho thư mục **/kma**
- Login vào từng người dùng kiểm tra xem người dùng này có thay đổi, xóa thư mục của người khác?

Chương 3.
THIẾT LẬP AN TOÀN CHO CÁC DỊCH VỤ MẠNG

3.1. THIẾT LẬP AN TOÀN CHO DỊCH VỤ WEB

3.1.1. Thiết lập an toàn cho môi trường dịch vụ Web

Mặc dù các dịch vụ Web là các công nghệ mới, chúng phụ thuộc vào cơ sở các công nghệ đã có trước đó, một trong số đó đã có thời gian khoảng mười năm hoặc nhiều hơn. Một chuyên gia an toàn đã cấu hình bảo mật cho dịch vụ Web mà một kẻ tấn công luôn luôn tìm kiếm điểm yếu nhất của hệ thống mạng để khai thác và tấn công. Kẻ tấn công sẽ gặp thất bại nếu như người quản trị thực hiện cập nhật theo định kỳ các bản vá hoặc cấu hình an toàn cho hệ điều hành, môi trường mạng, quy trình phát triển. Nếu dịch vụ Web được triển khai trên máy chủ dành riêng cho Web thì phải đảm bảo rằng máy chủ đó phải được cập nhật bản vá định kỳ và phải được bảo vệ theo nhiều lớp.

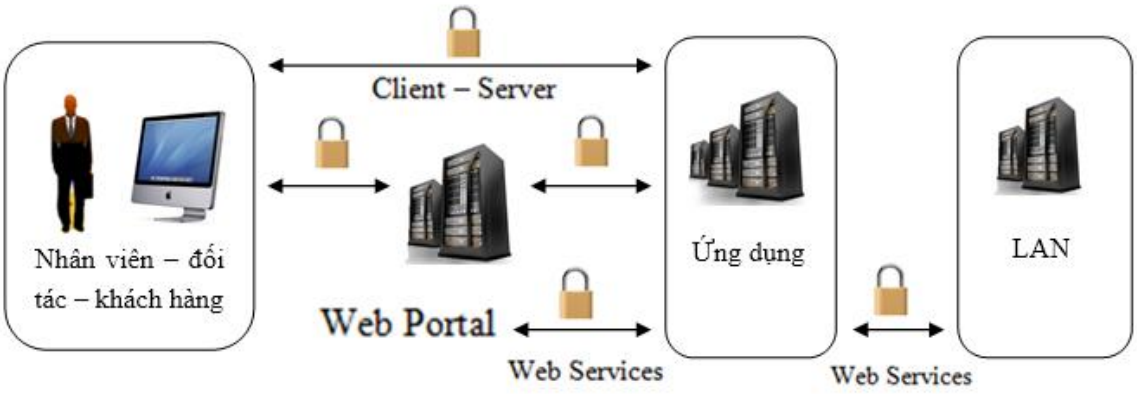
3.1.2. Cơ bản về dịch vụ Web

Người quản trị không thể cấu hình an toàn một hệ thống thông tin, các ứng dụng, các dịch vụ khi chỉ biết chút ít về nó. Trước khi bắt tay vào cấu hình an toàn cho dịch vụ Web, người quản trị cần phải hiểu được họ đang làm cái gì, họ đang tác động vào những vị trí nào, và làm thế nào để họ gắn kèm dịch vụ nào vào trong hệ thống thông tin. Thuật ngữ "Web services - dịch vụ Web" được định nghĩa là một dịch vụ trên "World Wide Web - WWW". Có nhiều định nghĩa có sẵn về dịch vụ Web, nhưng chính xác nhất, các đối tượng được định nghĩa, định nghĩa dịch vụ Web từ tập đoàn W3C (World Wide Web Consortium).

Một dịch vụ Web là một hệ thống phần mềm được thiết kế để hỗ trợ tương thích máy tính này tới máy tính kia tương tác với nhau qua đường mạng. Đó là một giao diện được trình bày trong một định dạng mà một máy tính có thể xử lý (WSDL). Các hệ thống khác tương tác với dịch vụ Web thông qua cách truyền lệnh bằng cách miêu tả sử dụng thông điệp SOAP

(Simple Object Access Protocol), phương thức truyền điển hình với HTTP sử dụng ngôn ngữ XML kết hợp với các chuẩn khác liên quan tới XML.

Dịch vụ Web được xử lý giữa các máy tính, không phải giữa người với máy tính. Một dịch vụ Web là sự tương tác giữa máy tính với máy tính. Người dùng cuối không thể tương tác trực tiếp với dịch vụ Web. Dịch vụ Web được truy cập từ các máy trạm, được W3C định nghĩa là "Một thực thể hệ thống thực hiện sử dụng một dịch vụ Web". Người dùng cuối sẽ không tham gia tất cả quá trình xử lý Web hoặc người dùng cuối truy cập gián tiếp dịch vụ Web. Trong thiết kế hệ thống Web theo mô hình doanh nghiệp tới người tiêu dùng, một kiến trúc n-lớp (một hệ thống có các phần của một ứng dụng cư trú trên một số hoặc *n* hệ thống máy tính) có thể được sử dụng. Dịch vụ Web cũng được xem là bên phát triển thứ ba của kiến trúc hệ thống, được phát triển từ mô hình máy trạm-máy chủ và kiến trúc n-lớp. Hình 3.1 trình bày kiến trúc này:



Hình 3.1 – Mô hình kiến trúc n-lớp

Sự khác nhau giữa "máy trạm" và "người dùng cuối" là rất quan trọng trong quản trị an toàn dịch vụ Web. Nếu một dịch vụ Web được cấu hình chỉ cho phép số lượng người dùng cuối xác định truy cập vào nó, thông điệp XML thông qua dịch vụ Web phải chứa đựng thông tin về người dùng cuối, như là thông tin xác thực, các thuộc tính…Phương pháp này phức tạp hơn so với xác thực một người dùng cuối tại một trang Web, kể từ khi người dùng cuối trực tiếp thao tác với trang Web. Các chuẩn SAML và WS-Security là thích hợp để giải quyết vấn đề trong kiến trúc này (các chuẩn này sẽ được trình bày trong các phần tiếp theo).

Ngôn ngữ miêu tả dịch vụ Web – WSDL

Trong ý thứ hai về định nghĩa của W3C, một giao diện của một dịch vụ Web có thể được miêu tả sử dụng WSDL và cũng được sử dụng cho miêu tả chức năng cung cấp bởi dịch vụ Web. Một miêu tả WSDL của một dịch vụ Web (cũng được gọi là một tập tin WSDL) cung cấp miêu tả khả năng đọc của một máy để dịch vụ có thể được gọi, các tham số chờ đợi, cấu trúc dữ liệu được trả về. Vì vậy WSDL phục vụ mục đích tương ứng với khả năng đó là phương pháp chữ ký trong một ngôn ngữ lập trình. Ví dụ về WSDL:

```
<?xml version="1.0" encoding="UTF-8"?>
<description xmlns="http://www.w3.org/ns/wsdl"
             xmlns:tns="http://www.tmsws.com/wsdl20sample"
             xmlns:whttp="http://schemas.xmlsoap.org/wsdl/http/"
             xmlns:wsoap="http://schemas.xmlsoap.org/wsdl/soap/"
             targetNamespace="http://www.tmsws.com/wsdl20sample">

<!-- Abstract type -->
   <types>
      <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
                 xmlns="http://www.tmsws.com/wsdl20sample"
                 targetNamespace="http://www.example.com/wsdl20sample">

         <xs:element name="request"> ... </xs:element>
         <xs:element name="response"> ... </xs:element>
      </xs:schema>
   </types>
```

Cũng như chủ thể của việc bảo vệ an toàn, WSDL cũng được sử dụng để trình bày các chính sách an toàn. WSPA (WS-Policy Attachment) là một tính năng kỹ thuật cho phép thêm các chính sách an toàn thông tin tới tệp tin WSDL, gồm các chỉ dẫn trên những phần nào của thông điệp SOAP phải được ký, những phần nào phải được mã hóa, các khóa mã và định dạng thẻ bài được sử dụng. Đây là thông tin được sử dụng trên các máy trạm phải thực hiện gửi các thông điệp an toàn.

REST và dịch vụ Web XML

Trong ý cuối cùng về định nghĩa của W3C: "Các hệ thống khác tương tác với dịch vụ Web thông qua cách truyền lệnh bằng cách miêu tả sử dụng thông điệp SOAP, phương thức truyền điển hình với HTTP sử dụng ngôn ngữ

XML kết hợp với các chuẩn khác liên quan tới XML". Quan điểm của một số chuyên gia cho rằng sử dụng SOAP là một yêu cầu khắc nghiệt cho một hệ thống gọi là một "dịch vụ Web". Một số ứng dụng trước đây không sử dụng SOAP, và vì vậy khi gửi thông điệp XML mà không có "vỏ bọc" SOAP. Một hình thức khác của REST (kiểu kiến trúc phần mền) - một dịch vụ Web nên được gọi bằng cách gửi các hình thức GETs và POSTs của giao thức HTTP tới một URI, kết quả trả về đơn giản là XML. Nhìn từ khía cạnh an toàn sẽ thấy lựa chọn không sử dụng SOAP thì các chuẩn an toàn nằm trong SOAP không được sử dụng, ví dụ như chuẩn WS-Security.

Truyền độc lập

Điểm cuối cùng liên quan tới định nghĩa của W3C là trong khi XML là "phương thức truyền điển hình là HTTP", HTTP không bắt buộc. SOAP được thiết kế để có thể truyền độc lập. XML được gửi đã sử dụng giao thức FTP hoặc SMTP cũng được tính là dịch vụ Web. Khái niệm này thường bị hiểu nhầm ở chỗ hai giao thức FTP hoặc SMTP hoạt động ở cổng riêng 21 và 25 nhưng chúng cũng hoạt động thông qua dịch vụ Web ở cổng 80. Hiện tại, sử dụng các tài khoản HTTP cho đại đa số lưu lượng các dịch vụ Web, làm gia tăng các vấn đề về an toàn thông tin như: các thiết bị tường lửa rất khó khăn để phân biệt lưu lượng dịch vụ Web từ lưu lượng trình duyệt Web thông thường cùng đi qua cổng TCP giống nhau.

Đây là vấn đề không phải nghiêm trọng như trong một số trường hợp, lưu lượng của dịch vụ Web được phân biệt bằng chính phần đầu của gói tin HTTP (Content-type: text/xml hoặc application/soap+xml) và có các đặc trưng khác được cảnh báo bởi các tường lửa, chẳng hạn như trong thực tế dòng đầu tiên của mã lệnh XML (<?xml version=1.0?> hoặc <?xml version=1.1?> phụ thuộc vào từng phiên bản XML). Truyền dữ liệu nên kết hợp các chuẩn như WS-Security.

3.1.3. Các chuẩn và tham số kỹ thuật

Ngôn ngữ XML và SOAP đã được phát triển bên trong nền tảng của W3C. Khi trở thành dịch vụ Web an toàn, W3C đã gia nhập vào tổ chức của Các chuẩn thông tin có cấu trúc tiên tiến gọi tắt là OASIS. W3C là cơ sở phát

triển cho mã hóa XML và ký số XML, cũng như các đặc điểm kỹ thuật quản lý khóa XML (XKMS – XML Key Management Specification). OASIS là cơ sở phát triển cho SAML và WS-Security.

Ngoài những chuẩn chủ yếu, khả năng tương tác các dịch vụ Web (WS-I) tổ chức thực hiện các chuẩn từ OASIS và W3C và trình bày sử dụng "hồ sơ" miêu tả các tiêu chuẩn sẽ được sử dụng với nhau để đạt được các nhiệm vụ chung. WS-I đã đưa ra một hồ sơ cơ bản SOAP để các nhà cung cấp dịch vụ Web có thể sử dụng để kiểm tra sản phẩm của họ có tương thích với các sản phẩm của nhà cung cấp khác hay không. WS-I cũng đưa ra một hồ sơ an toàn cơ bản, bao gồm các hồ sơ cho giao thức SSL và xác thực HTTP, bên cạnh các hồ sơ sử dụng cho WS-Security. Điều này cho thấy bảo mật cho dịch vụ Web là không giới hạn cho các công nghệ mới của dịch vụ Web, nhưng các công nghệ cụ vẫn được áp dụng. Bản dự thảo hồ sơ an toàn cơ bản WS-I dành nhiều sự chú ý tới vấn đề an toàn của chính các công nghệ an toàn đó. Ví dụ: một nhà cung cấp dịch vụ Web triển khai xác thực sử dụng thẻ bài chứng chỉ X.509 WS-Security phải đảm bảo không thể chặn bắt một thông điệp hợp lệ và gửi lại nó tới hệ thống máy chủ dịch vụ Web. Tấn công chặn bắt-dùng lại là một hình thức tấn công tương đương với tìm kiếm một hồ sơ đã ký và sử dụng máy fax để fax lại nó. Nếu bên nhận không kiểm tra lại cẩn thận thông điệp nhận được bằng các giá trị như thời gian gửi, số tuần tự thì bên nhận cũng tin cậy vào thông điệp gửi lại này. WS-I miêu tả mức triển khai an toàn nhất phải lưu ý đến nhẫn thời gian và số tuần tự của thông điệp.

3.1.4. Thiết lập các yêu cầu an toàn

Các mục trên đã nêu lên tổng quan về dịch vụ Web, người quản trị hệ thống đứng trong vị trí kiểm tra các yêu cầu an toàn của dịch vụ Web. Các công nghệ sử dụng để đảm bảo yêu cầu về an toàn như mật mã, xác nhận thông điệp, xác thực…

Bất kỳ hệ thống nào, bao gồm cả hệ thống dựa vào dịch vụ Web cũng phải tuân theo các yêu cầu cơ bản về an toàn như sau:

- Xác thực – Ai gửi thông điệp này?

- Thẩm quyền – Đối tượng đã được xác thực có những quyền hạn gì trên hệ thống đích?
- Toàn vẹn – Thông điệp này có bị giả mạo hay không?
- Tính bí mật – Thông tin đã bị đọc trong quá trình truyền hay lưu trữ hay chưa?
- Ghi nhật ký – Các giao dịch đã được ghi chép lại hay chưa?
- Tính quản trị – Cách đơn giản để quản lý chính sách?
- Tính sẵn sàng – Các lỗ hổng hệ thống có bị tấn công DoS hay không?

Đây là những yêu cầu quan trọng cần phải ghi nhớ và tránh chỉnh sửa với các chuẩn cụ thể. Điều này có nghĩa là nghĩ đến cách người quản trị có thể đảm bảo tính toàn vẹn của những thông điệp hơn là suy nghĩ làm thế nào có thể xây dựng ký số XML vào trong hệ thống.

3.1.4.1 Thực hiện xác thực cho dịch vụ Web

Có hai kiểu xác thực quan trọng cho dịch vụ Web:

- Xác thực máy trạm: Xác thực các ứng dụng đã gửi thông điệp XML tới dịch vụ Web.
- Xác thực người dùng cuối: Gắn thông tin về người dùng cuối vào trong thông điệp gửi tới dịch vụ Web.

Khi triển khai dịch vụ người quản trị nên chọn giữa truyền dữ liệu – hoặc thông điệp – dựa vào xác thực máy trạm, đảm bảo người quản trị có quyền truy cập từ xa sau khi xác thực, và tạo ra một hệ thống cho phép xác định các thông điệp xác thực hoặc không xác thực.

Làm thế nào để lựa chọn giữa truyền dữ liệu – và thông điệp – dựa vào xác thực máy trạm. Xác thực máy trạm có thể thực hiện sử dụng các giao thức truyền an toàn như là SSL, SSL với xác thực HTTP, SSL với xác thực ký số HTTP. Xác thực máy trạm có thể thực hiện sử dụng xác thực mức-thông điệp, hình thức này độc lập với xác thực lúc truyền dữ liệu. WS-Security được sử dụng cho xác thực mức-thông điệp; đặc biệt thẻ bài chứng chỉ X.509 WS-

Security cho xác thực dựa vào chứng chỉ, WS-Security Kerberos cho xác thực Kerberos, và thẻ bài WS-Security Username cho xác thực dựa vào định danh.

Vì vậy, khi nào thì sử dụng phương thức xác thực dựa vào truyền dữ liệu và khi nào sử dụng phương thức xác thực dựa vào thông điệp? Câu trả lời là khi dịch vụ Web là điểm nối điểm, với các máy trạm gửi trực tiếp mã XML tới dịch vụ Web, kiểu xác thực mức vận chuyển là thích hợp. Khi trung gian SOAP được sử dụng, tạo ra nhiều điểm liên kết giữa máy trạm và dịch vụ Web thì xác thực mức-thông điệp nên được sử dụng để đảm bảo an toàn từ đầu cuối tới đầu cuối.

Xác thực dựa vào chứng nhận được sử dụng để thiết lập định danh. Ví dụ của chứng nhận bao gồm định danh/mật khẩu kết hợp với chứng chỉ X.509.

Xóa bỏ chứng nhận sau khi xác thực

Một thẻ bài định danh WS-Security có cấu trúc chứa đựng cả một tên và một mật khẩu là một chứng nhận. Nếu không tin cậy các ứng dụng xử lý thông điệp ở phía đầu cuối, xem xét xóa bỏ chứng nhận từ thông điệp xác thực sau đó. Ví dụ sau đây sử dụng XSLT (– Extensible Stylesheet Language Transformations) sẽ gỡ bỏ nội dung của phần đầu SOAP, bao gồm xác thực chứng nhận từ một thông điệp SOAP:

```
<?xml version="1.0"?>
<xsl:stylesheet exclude-result-prefixes=”SOAP-ENV SOAP”
xmlns: SOAP-ENV=”http://schemas.xmlsoap.org/soap/envelope”
xmlns: xsl=”http://www.w3.org/2009/XSL/Transform” version=”1.0”>
<xsl:output method=”xml”/>
<xsl:strip-space elements=”*”/>
<xsl:template match=”/”>
      <xsl:appy-template select=”//SOAP-ENV:Envelope”/>
</xsl:template>
<xsl:template match=”*”>
    <xsl:if test=”not (name(.)=’soapenv:Header’)”>
       <xsl:element name=”{name(.)}” namespace=”{namespace-uri(.)}”>
          <xsl:apply-templates select=”@*|*|text()”/>
       </xsl:element>
    </xsl:if>
</xsl:template>
```

```
<xsl:template match="@*">
  <xsl:copy/>
</xsl:template>
</xsl:stylesheet>
```

Sử dụng sự lan truyền chính để cho phép các thông điệp xác thực hoặc không xác thực

Trong ví dụ xác thực sau đây, một thẻ SAML được đưa ra để xác định máy trạm đã được xác thực, cấp quyền cho một dịch vụ cụ thể, hoặc có một thuộc tính nhất định. Trong phương thức này, việc xác thực thông tin dựa trên nguyên tắc đặt tên và được truyền tới dịch vụ Web để xử lý các thông điệp XML. Nếu không có chức năng "lan truyền chính" thông tin về máy trạm có thể bị mất trong quá trình xác thực. Những thuận lợi khác của phương thức này bao gồm:

- Một ứng dụng phải đảm bảo các thông điệp XML thông qua nó phải đi qua cổng an toàn XML, bằng cách kiểm tra thông điệp cho một thẻ an toàn XML đã được ký số bởi cổng an toàn XML. Nếu thẻ an toàn này không được trình bày, thông điệp sẽ được cổng an toàn XML chuyển tới các phương pháp cách ly hoặc loại bỏ.
- Một ứng dụng thực thi một luật giống như "chỉ có máy trạm đã được xác thực với chứng chỉ X.509 là cho phép truy cập tới dịch vụ", thông tin về phương thức xác thực có trong tài liệu về SAML.
- Các thông điệp liên quan với nhau thông qua các ứng dụng đa xử lý XML, dựa vào định danh các thẻ an toàn bên trong.

Một ví dụ của một thông điệp SOAP sử dụng nguyên tắc lan truyền, bằng cách gắn một thẻ xác thực SAML:

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap=
"http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2009/XMLSchema"
xmlns:xsi=
"http://www.w3.org/2009/XMLSchema-instance">
<soap:header>
<wsse:Security soap:actor="current" xmlns:wsse="http://docs.oasis-
open.org/wss/2009/01/oasis-200901-wss-wssecurity-secext-1.0.xsd">
```

```
<saml:Assertion AssertionID=”vordel-1087530254730” IssueInstant=”2009-06-
18T03:44:14Z” Issuer=”Corporate CA”
MajorVersion=”1”xmlns:saml=”urn:oasis:names:tc:SAML:1.0:assertion”>
<saml:Conditions NotBefore=”2009-06-18T12:00:00Z” NotOnOrAfter=”2009-06-
18T12:10:00Z”/>
<saml:AuthenticationStatament AuthenticationInstant=”2009-06-
18T03:44:14Z” AuthenticationMethod=”urn:ietf:rfc:2246”>
<saml:SubjectLocality DNSAddress=”client.com” IPAddress=”192.168.1.10”/>
<saml:Subject>
<saml:NameIdentifier Format=”urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName”>
CN=Client Name, O=Client Organisation,C=SE</saml:NameIdentifier>
  </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
</wsse:Security>
</soap:Header>
<soap:Body>
<StockQouteRequest xmlns=”http://www.mystockquoteexample.com”>
<symbols>
<Symbol>BENO</Symbol>
<Symbol>KSTN</Symbol>
</Symbol>
</StockQouteRequest>
</soap:Body>
</soap:Envelope>
```

Trong ví dụ mã lệnh XML trên đây, đoạn “urn:ietf:rfc:2246” trong câu lệnh AuthenticationMethod tham chiếu tới phương thức xác thực máy trạm sử dụng SSL/TSL. Thông tin của máy trạm được chứa trong các trường Subject/NameIdentifier (CN=Client Name, O=Client Oganization, C=SE). Các ứng dụng xử lý thông điệp trên được biết là định danh các bên xác thực. Thông tin này cũng giải thích và xác định SAML đã được ký số, kết hợp với thông điệp SOAP để xác định mã lệnh đã được đánh dấu để phát hiện tấn công sử dụng lại sử dụng thông điệp SOAP.

Nhúng các thẻ xác thực người dùng

Xác thực người dùng cuối đạt được thông qua cách thức tương tự với nguyên tắc lan truyền. Một thẻ được nhúng vào trong thông điệp SOAP, truyền thông tin về người dùng cuối. Đây là một kỹ thuật cơ bản được hãng Project Liberty sử dụng (www.projectliberty.org), trong kỹ thuật này một người dùng đăng nhập một lần tới dịch vụ được cung cấp, và sau đó họ vẫn

được dùng các dịch vụ khác trong cùng một nhà cung cấp, vì họ không cần phải xác thực lại. Giải pháp này an toàn hơn so với phương thức Single-Sign-On, sử dụng cơ chế lan truyền ủy nhiệm (mật khẩu của người dùng được bỏ qua khi có yêu cầu xác thực bên trong khi sử dụng các dịch vụ khác), hoặc sử dụng cookies (đây là phương thức truyền thông qua HTTP vì vậy mà không sử dụng cho thông điệp SOAP).

Khi các thẻ an toàn phải chuyển đổi từ định dạng này sang định dạng khác, ví dụ chuyển đổi một vé xác thực đầu vào Kerberos tới cấu trúc UsernameToken để thay thế các thông điệp đi ra, có thể sử dụng WS-Trust. WS-Trust bao gồm một thông điệp RequestSecurityToken được sử dụng để yêu cầu một thẻ an toàn nhất định. WS-Trust được thiết kế để cho phép quan hệ tin cậy giữa các miền an toàn.

Triển khai xác thực dịch vụ Web sử dụng SAML và liên kết tới trang Web có thẩm quyền

Một khi người gửi và người dùng cuối được xác thực, bước tiếp theo được xác định xem người dùng cuối có được cho phép để truy cập tới tài nguyên mà họ yêu cầu hay không, bước này gọi là quyền hạn. Quyền hạn thông thường đi sau xác thực, trong mô hình điều khiển truy cập dựa vào vai trò (RBAC) thì đây là một bước trung gian. Trong mô hình RBAC, quyền hạn không dựa vào trực tiếp định danh của người dùng mà thuộc tính của người dùng (vai trò của họ). Mô hình này có khả năng mở rộng và dễ dàng quản lý hơn so với mô hình điều khiển truy cập dựa vào danh sách.

Như đã trình bày ở phần "Thực hiện xác thực cho dịch vụ Web", SAML sử dụng để xác nhận các thuộc tính của người dùng, để cung cấp quyền hạn tương ứng. Ngoài ra SAML cũng sử dụng để yêu cầu quyền hạn. Có nhiều công cụ có sẵn trong các trang Web cấp quyền (Netegrity SiteMinder, Entrust GetAccess, RSA ClearTrust, Oblix COREid).

Ngôn ngữ đánh dấu điều khiển truy cập XML viết tắt là XACML, được sử dụng để hiển thị quy định quyền hạn trong định dạng XML. XACML là một ví dụ điển hình về kỹ thuật an toàn XML và đó không phải thiết kế đặc biệt cho an toàn dịch vụ Web, đó là một ví dụ về công nghệ XML được sử

dụng để giải quyết các vấn đề về tương tác an toàn. Trước khi có chuẩn XACML, không có phương thức chuẩn của sự hiển thị điều khiển truy cập thông tin trong một cấu trúc. Khi chuẩn XACML được công bố, đó là một sự lựa chọn thích hợp cho các tổ chức mong muốn đưa ra các chính sách điều khiển truy cập của họ tới bên thứ ba kiểm tra, hoặc cho các tổ chức mong muốn di chuyển các quy định điều khiển truy cập từ một hệ thống tới các hệ thống khác mà không cần phải xây dựng lại.

Đảm bảo tính toàn vẹn thông điệp sử dụng – ký số XML, ký số PKCS#7, SSL/TLS, IPSec

Có nhiều quan niệm sai lầm về sử dụng mật mã, toàn vẹn thông điệp là một lợi ích phụ có được do miễn phí. Một thông điệp đã được mã hóa có thể bị thay đổi mà không cần phải tương tác để giải mã. Vấn đề này rất quan trọng đối với mọi hệ thống truyền nhận, bao gồm dịch vụ Web, đảm bảo tính toàn vẹn thông điệp. Giao thức SSL/TLS đảm bảo tính toàn vẹn tại tầng vận chuyển. IPSec đảm bảo tính toàn vẹn ở tầng thấp hơn, ký số được sử dụng trực tiếp lên thông điệp. Ký số PKCS#7 là phương pháp cơ bản trong bảo mật e-mail (S/MIME).

Ký số XML là một chuẩn ký số của W3C và IETF cho phép một ký số được thể hiện sử dụng XML. Ký số XML không có các thuật toán ký số mới vì thế mà không thể nói rằng nó là "mạnh" hoặc "yếu" hơn so với định dạng ký số trước nó, như là PKCS#7. WS-Security miêu tả một thông điệp SOAP khi đã được ký số. WS-Security chỉ ra cấu trúc ký số XML được đặt bên trong các yếu tố an toàn, và lần lượt được thay thế vào trong phần đầu của thông điệp SOAP (giống như gói tin TCP, có header và body).

Ký số XML hỗ trợ ký số nhiều hơn so với tham chiếu chuẩn. Đây là một thuận lợi khi ký số thông điệp SOAP, cũng như ký vào phần body của thông điệp. Tem thời gian cũng phải được ký để tránh tấn công sử dụng lại. Ký số XML cung cấp tính bền vững về toàn vẹn cho XML, nghĩa là tính toàn vẹn vẫn được đảm bảo sau khi thông điệp XML đã được nhận, xử lý, và lưu trữ.

Thông báo cho máy trạm về yêu cầu an toàn sử dụng WS-Policy

Nếu người quản trị đã cài đặt một dịch vụ Web và yêu cầu các thông điệp đi vào và tem thời gian của thông điệp phải được ký số, làm thế nào để truyền thông tin yêu cầu này tới máy trạm? Để làm được việc này người quản trị sử dụng WS-Policy. Phương thức này cho phép một dịch vụ Web truyền thông tin về chính sách an toàn của nó tới các máy trạm. Ví dụ WS-Policy sau đây miêu tả miêu tả một chính sách cho dịch vụ Web, mục đích của chính sách này là tất cả các thông điệp gửi tới dịch vụ Web phải được ký số vào phần body SOAP và phải ký số vào nhẫn thời gian.

```
<?xml version=”1.0” encoding=”utf-8”?>
<policyDocument xmlns=”http://schemas.microsoft.com/wse/2006/06/Policy”>
<mappings xmlns:wse=”https://schemas.microsoft.com/wse/2006/06/Policy”>
<endpoint uri=”http://www.mycompany.com/StockService”>
<defaultOperation>
<request policy=”#Sign-X.509”/>
<response policy=””/>
<fault policy=””/>
</defaultOperation >
</endpoint>
</mappings>
<policies xmlns:wsu=”http://docs.oasis-open.org/wss/2006/01/oasis-200601-
wss-wssecurity-utility-1.0.xsd”
xmlns:wsp=”http://schemas.xmlsoap.org/ws/2006/12/policy”
xmlns:wssp=”http://schemas.xmlsoap.org/ws/2006/12/secext”
xmlns:wse=”http://schemas.microsoft.com/wse/2007/06/Policy”
xmlns:wsse=” http://docs.oasis-open.org/wss/2006/01/oasis-200601-wss-
wssecurity-secext-1.0.xsd”
xmlns:wsa=”http://schemas.xmlsoap.org/ws/2006/03/addressing” >
<wsp:Policy wsu:Id=”Sign-X.509”>
<!-- MessagePredicate is used to require headers.
This assertion should be used along with the Integrity assertion when the
presence of the signed element is required -->
<wsp:MessagePredicate wsp:Usage=”wsp:Required”
Dialect=”http://schemas.xmlsoap.org/2006/12/wsse#part” >
Wsp:Body() wsp:Header(wsa:MessageID) wse:Timestamp()
</wsp: MessagePredicate >
<!-- The Integrity assertion is used to ensure that the message is signed
with X.509. Many Web service will also use the token for authorization,
such as by using the <wse:Role> claim or specific X.509 claims.-->
<wssp:Integrity wsp:Usage=”wsp:Required”>
<wssp:TokenInfo>
<wssp:SecurityToken wse:IdentityToken=”true”>
<wssp:TokenType>http://docs.oasis-open.org/wss/2006/01/oasis-200601-wss-
X509-token-profile-1.0#X509v3</wssp:TokenType >
```

```
<wssp:Claims>
<wssp:SubjectName MatchType=”wssp:Exact”>
StockClient
</wssp:SubjectName>
<wssp:X509Extension OID=”1.2.23.44”MatchType=”wssp:Exact”>
The Web Servie
</wssp:X509Extension>
</wssp:Claims>
</wssp:SecurityToken>
</wssp:TokenInfo>
</wssp:MessageParts
Dialect=”http://schemas.xmlsoap.org/2006/12/wsse#part”>
Wsp:header(wsa:MessageID) wse:Timestamp()
</wssp:MessageParts>
</wssp:Integrity>
</wsp:Policy>
</policies>
</policyDocument>
```

Trên đây là danh sách các mã WS-Policy, theo quy tắc thì cả phần body SOAP và tem thời gian đều được ký. Ngoài ra, còn có quy tắc một chứng chỉ X.509 là một định dạng thẻ để gửi các thông điệp đi vào tới dịch vụ Web. Bộ công cụ Microsoft WSE 2.0 hỗ trợ phương thức WS-Policy và cho phép người quản trị tự động tạo tài liệu WS-Policy như ví dụ trên đây và gắn vào dịch vụ Web sử dụng WSE.

Triển khai tính bí mật: Mã hóa XML, SSL/TLS, IPSec

Nhiều người mới tiếp cận với an toàn thông tin có suy nghĩ không chính xác về tính bí mật là tương đương với an toàn và mật mã tương đương với tính bí mật. Một ví dụ, một tài liệu được đảm bảo an toàn nghĩa là tài liệu được mã hóa. Mã hóa XML được đưa ra là chuẩn an toàn dịch vụ Web quan trọng nhất. Bởi vì nó cho phép một phần của thông điệp SOAP được mã hóa, phần còn lại ở dạng bản rõ. Lý do không mã hóa toàn bộ thông điệp SOAP để cho phép SOAP trung gian có thể đọc thông điệp và phân biệt thông tin định tuyến mà chúng yêu cầu. Cũng như ký số XML, việc thực thi mã hóa XML tới SOAP sử dụng WS-Security. Và chính WS-Security cũng là nơi mà cấu trúc mã hóa XML được đặt tại đó, lần lượt được đặt vào trong phần đầu của thông điệp SOAP. WS-Policy có thể cũng được sử dụng để truyền quy tắc mà một phần, hoặc nhiều phần của thông điệp SOAP phải được ký, ngoài ra WS-

Policy còn được sử dụng để truyền khóa công khai dùng cho mã hóa phần body SOAP của các thông điệp SOAP đi vào.

Mã hóa XML hoạt động ở tầng Message (Tầng ứng dụng) và độc lập với các tầng vận chuyển phía dưới. Các thông điệp ở tầng Message có liên quan với WS-SecureConversation, phương thức này thiết lập kết nối an toàn giữa bên yêu cầu dịch vụ Web và máy chủ dịch vụ Web. Phiên này được khởi tạo bằng cách đàm phán một khóa bí mật, khóa này sử dụng để mã hóa cho tất cả các thông điệp sau đó và những thông điệp này thuộc cùng một phiên khởi tạo.

Giao thức IPSec và SSL/TLS cũng cung cấp tính bí mật. Trong môi trường cần phải đảm bảo tính bí mật hoàn toàn và môi trường không tin cậy vào các điểm trung gian hoặc yêu cầu truyền hoàn toàn độc lập các thông điệp XML, lúc này người quản trị xem xét thực hiện triển khai mã hóa XML từ đầu cuối tới đầu cuối. Một lợi thế đặc biệt của mã hóa XML là tính bí mật không giới hạn thời gian khi các thông điệp đang truyền, tới thời gian khi một tài liệu XML được lưu trữ. Với tính năng này, mã hóa XML cung cấp khả năng bảo mật lâu dài.

Tránh cấu hình an toàn thông thường bằng cách chỉnh sửa tệp tin XML

Quản trị một chính sách an toàn cho dịch vụ Web bao gồm hai hoạt động chính:

- **Dữ liệu**: Nhiệm vụ của việc gán các chính sách an toàn mới và các cấu hình máy trạm mới tới hệ thống.
- **Quản lý chính**: bao gồm các việc thay đổi chính sách, khôi phục chính sách, thêm mới chính sách. Vì vậy mà quản lý chính sách là một nhiệm vụ cấp bách khi một chính sách an toàn cần phải thay đổi nhanh. Ví dụ, khi một hệ thống đã bị tấn công, người quản trị chính sách an toàn dịch vụ Web cần phải thực hiện các biện pháp trực quan và đơn giản nhất có thể. Một khuyến cáo là người quản trị không nên tác động trực tiếp sử dụng các tệp tin XML để cấu hình chính sách an toàn cho dịch vụ Web. Như đã giới thiệu ở các phần trước các công nghệ được sử dụng là WS-

Policy và XACML được sử dụng để thao tác với các chính sách an toàn.

3.1.4.2 Đảm bảo tính sẵn sàng cho dịch vụ Web

Tính sẵn sàng bao gồm việc bảo vệ dịch vụ Web bằng cách ngăn chặn các thông điệp tấn công "storms". Đây là nhiệm vụ cơ bản của tường lửa. Ngoài ra, các thông điệp được thiết kế để gây ra các vấn đề về xử lý XML phải được ngăn chặn. Đây gọi là tấn công DoS XML (Từ chối dịch vụ XML). Một tấn công DoS XML khác với tấn công DoS thông thường bởi vì nó không đồng bộ. Một thông điệp XML đơn có thể làm thiệt hại đáng kể, sẽ được trình bày ở các phần tiếp theo.

3.1.5. Ngăn chặn các XML độc hại

Việc khai thác sử dụng lỗ hổng XML được coi là một hình thức tấn công mới. Những tấn công này sẽ làm cho hệ thống xử lý XML bị hư hại hoặc truy cập không cần quyền hạn tới dữ liệu. Trong phần này kiểm tra những tấn công và cung cấp những công việc mà người quản trị cần phải thực hiện để ngăn chặn chúng. Có nhiều sản phẩm tường lửa về XML có khả năng ngăn chặn những tấn công này. Trong các tiểu mục sau đây trình bày về những kiểu tấn công đó là gì, biện pháp đối phó, làm thế nào sử dụng tường lửa XML để ngăn chặn.

Ngăn chặn tiêm nhiễm truy vấn SQL của dịch vụ Web (SQL Injection)

Tấn công tiêm nhiễm truy vấn SQL là một hình thức tấn công mà chèn các câu truy vấn SQL vào trong các trường nhập dữ liệu hoặc trên đường dẫn của trang Web để thực thi với cơ sở dữ liệu và lấy về kết quả dữ liệu không phù hợp hoặc tiết lộ về thông tin truy cập cơ sở dữ liệu. Tấn công tiêm nhiễm SQL một dịch vụ Web cũng theo nguyên lý tương tự, ngoại trừ các truy vấn cộng thêm dữ liệu SQL tới các tham số bên trong một thông điệp SOAP, trong phạm vi truy vấn SQL sẽ được biên dịch bởi cơ sở dữ liệu phía sau máy chủ Web.

Một tấn công tiêm nhiễm SQL thành công yêu cầu hai nhân tố sau đây:

- Dữ liệu nhận được từ một kết nối mạng được chèn trực tiếp vào trong một truy vấn SQL.
- Truy vấn SQL được thực thi trong hoàn cảnh một người dùng với đầy đủ quyền để thực thi tấn công.

Ví dụ:

```
<SOAP-ENV:Envelope
     Xmlns:SOAP-
     ENV=”http://schemas.xmlsoap.org/soap/envelope/”>
     <SOAP-ENV:Header></SOAP-ENV:Header >
     <SOAP-ENV:Body
     <BookLookup:searchByIBSN
     Xmlns:BookLookup=”https://www.books.com/Lookup”>
     <BookLookup:IBSN>0072224711<BookLookup:IBSN>
     </BookLookup:searchByIBSN>
</SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Đoạn mã lệnh trên được xử lý bởi ngôn ngữ VB.NET, với chèn nội dung của ISBN vào trong một truy vấn SQL:

```
Set myRecordset = myConnection.excute (“SELECT * FROM
myBooksTable WHERE ISBN =’” & ISBN_Element_Text & “’”)
```

Trong trường hợp của thông điệp SOAP trước đó sẽ trở thành:

```
SELECT * FROM myBooksTable WHERE IBSN = ’0072224711’
```

Bây giờ xem chuyện gì xảy ra khi thông điệp SOAP nhận được:

```
<SOAP-ENV:Envelope
     Xmlns:SOAP-
     ENV=”http://schemas.xmlsoap.org/soap/envelope/”>
     <SOAP-ENV:Header></SOAP-ENV:Header >
     <SOAP-ENV:Body
     <BookLookup:searchByIBSN
     Xmlns:BookLookup=”https://www.books.com/Lookup”>
     <BookLookup:IBSN>0072224711’; exec
```

```
     master..xp_cmdshell ' net user Joe pass /ADD'; --
     <BookLookup:IBSN>
     </BookLookup:searchByIBSN>
</SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Trong trường hợp này truy vấn SQL sẽ đọc

```
SELECT * FROM myBooksTable WHERE IBSN = '0072224711';
exec master..xp_cmdshell ' net user Joe pass /ADD'; --
```

Đoạn mã sau truy vấn SELECT thực hiện tạo một người dùng tên Joe với mật khẩu PASS. Một kẻ tấn công cố gắng thực hiện tạo tài khoản người dùng mới để truy cập tới máy tính từ xa.

Để ngăn chặn tấn công này, phải đảm bảo dữ liệu nhận được từ người dùng không tin cậy không được chèn trực tiếp vào các truy vấn SQL. Để đặt được điều này bằng cách sử dụng các thủ tục lưu trữ hơn là truy vấn SQL. Tiêm nhiễm truy vấn SQL cũng có thể ngăn chặn bằng cách thực thi các luật xác nhận nội dung đầu vào. Trong trường hợp này, cổng an toàn XML sẽ thực thi một luật Schema-based, chứa đựng một biểu thức chính quy (RegEx), như ví dụ sau đây:

```
<simpleType name="ibsn"><restriction base="string"> <pattern
value="[0-9]{10}"/></restriction></simpleType>
```

Schema này sẽ kiểm tra lại dữ liệu đã được cô lập theo đường dẫn:

```
/Body/BookLookup:searchByIBSN/BookLookup:IBSN
```

Như ví dụ trên `0072224711` được đi qua biểu thức chính quy trong Schema, nhưng giá trị `0072224711'; exec master..xp_cmdshell ' net user Joe pass /ADD'; --` bị ngăn chặn.

Sử dụng thủ tục lưu trữ của SQL là một giải pháp hữu hiệu để ngăn chặn vấn đề tiêm nhiễm truy vấn SQL. Là một người quản trị an toàn hệ thống, phải đảm bảo rằng nhân viên phát triển phần mềm trong tổ chức có hiểu biết về tiêm nhiễm truy vấn SQL và biết cách ngăn chặn dạng tấn công này đối với dịch vụ Web. Biện pháp tiếp theo để ngăn chặn là giải pháp sử dụng tường lửa XML để ngăn chặn tiêm nhiễm truy vấn SQL bằng cách phát hiện các truy vấn SQL trong các thông điệp XML đi vào.

Bảo vệ dịch vụ Web chống lại tấn công chặn bắt và sử dụng lại

Mô tả dạng tấn công này: Một dịch vụ Web được bảo vệ bởi cổng an toàn XML nhằm quét các yêu cầu đi vào bao gồm chứng chỉ X.509 chứa đựng bên trong thông điệp SOAP và đảm bảo thông điệp được mã hóa và ký số. Hệ thống này tồn tại lỗ hổng để tấn công chặn bắt và sử dụng lại, bằng cách chặn bắt một thông điệp hợp lệ sau đó sử dụng lại mà không cần phải xác thực.

Giải pháp để ngăn chặn vấn đề này là sử dụng tem thời gian. Công cụ hỗ trợ để gắn tem thời gian là WS-Security, một ví dụ đã được trình bày trong phần WS-Policy ở trên đây, để bảo vệ dịch vụ Web có thể bắt buộc ký tem thời gian để hiển thị trong thông điệp đi vào. Một gói tin sử dụng lại đã gán tem thời gian sẽ tương tự với gói tin gốc. Nếu gói tin đến có thời gian ngắn sau gói tin đầu tiên, thì cả hai phải loại bỏ, bởi vì gói tin không thể được thiết lập với những gói tin là bản gốc và đây là một gói tin sử dụng lại. Đây là lý do tại sao phải thiết lập cẩn thận khoảng thời gian tin cậy của tem thời gian. Khoảng thời gian phải đủ ngắn để một kẻ tấn công không có đủ thời gian để chặn bắt, giải mã, và sử dụng lại một gói tin hợp lệ. Và cũng phải đủ dài để phân biệt giữa các đồng hồ hệ thống của dịch vụ web. Các yêu cầu của dịch vụ web không có kết quả trong các gói tin hợp lệ phải bị chặn.

Cập nhật các bản vá để ngăn chặn tấn công từ chối dịch vụ XML - XDoS

Tấn công XDoS sử dụng tính năng của DTDs (Document type definition entry). Trong đó tấn công XDoS dựa trên hành vi mà các thực thể được định nghĩa trong DTD có thể kéo trong. Ví dụ: Người phát triển mã nguồn HTML sẽ quen thuộc với cách sử dụng `<` và `>` thay vì sử dụng dấu ngoặc nhọn, vì vậy mà các trình duyệt web không phân tích được mã nguồn HTML. Sử dụng các ký hiệu chỉ dẫn trình duyệt web tìm kiếm `lt` và `gt` trong HTML DTD và thay thế bằng bất cứ cái gì mà nó tìm thấy.

Vậy nếu một thực thể đã được định nghĩa đệ quy thì chuyện gì sẽ xảy ra. Giả sử `&x100` đã tìm được trong một DTD và tìm ký hiệu `&x99;&x99;`. Bộ phận phân tích DTD sau đó phải tìm kiếm `&x99;`. Giả sử nó tìm được ký hiệu `&x98;&x98;`. Phần còn lại của gói tin XML làm bộ

nhớ tràn ngập và đây là lý do của tấn công từ chối dịch vụ. Đoạn mã tấn công XML DTD được trình bày ở dưới đây:

```
<!DOCTYPE foobar [
    <!ENTITY x0 "hello">
    <!ENTITY x1 "&x0;&x0;">
    <!ENTITY x2 "&x1;&x1;">
    <!ENTITY x3 "&x2;&x2;">
    <!ENTITY x4 "&x3;&x3;">
    ...
    <!ENTITY x98 "&x97;&x97;">
    <!ENTITY x99 "&x98;&x98;">
    <!ENTITY x100 "&x99;&x99;">
]>
<foobar>&x100;</foobar>
```

Việc thực hiện SOAP đã yêu cầu bằng sự chỉ định SOAP không để tiến trình DTD không ngăn chặn nhiều nhà cung cấp SOAP xử lý DTD trong sản phẩm của họ, vì vậy đây là một lỗ hổng để tấn công XDoS. Các bản vá ngăn chặn dạng tấn công này được cung cấp sẵn từ các nhà cung cấp Microsoft, IBM, Macromedia, Sybase và một số nhà cung cấp khác. Người quản trị phải đảm bảo rằng việc triển khai SOAP trong hệ thống phải thực hiện cập nhật các bản vá nhằm ngăn chặn hình thức tấn công từ chối dịch vụ web.

3.1.6. Thực hiện các chính sách an toàn

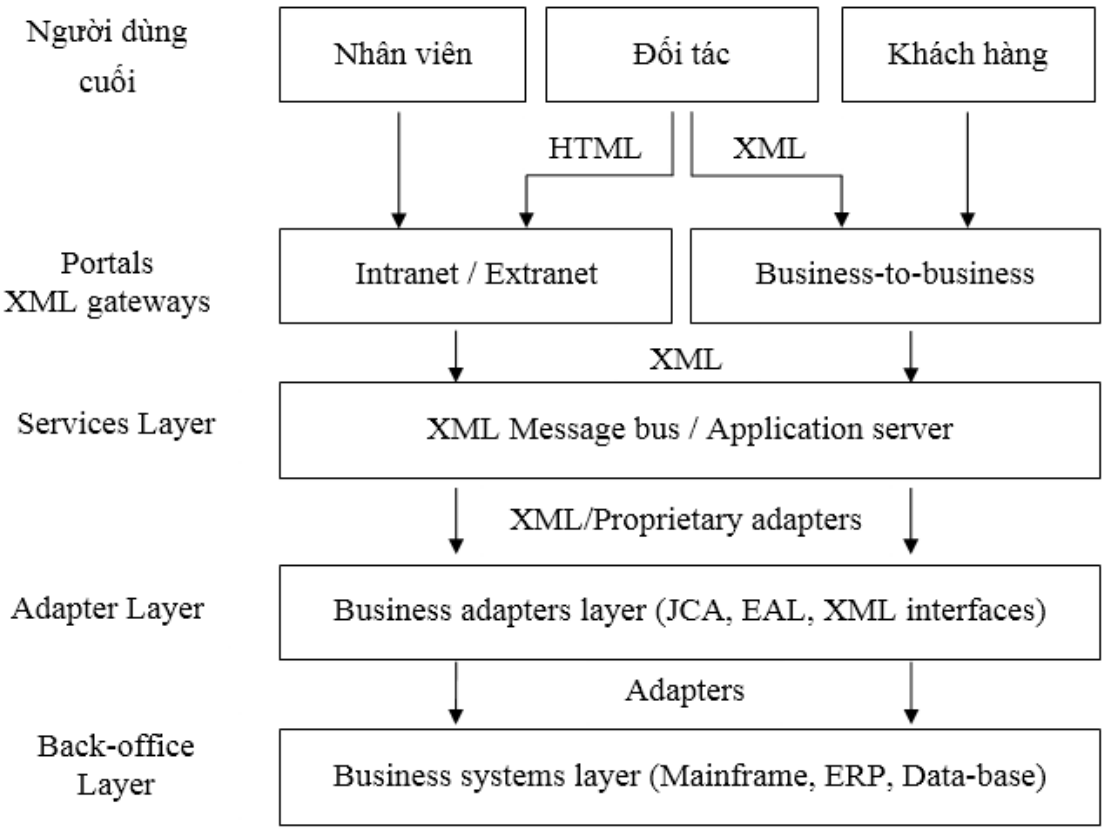
Kiến trúc hướng dịch vụ (SOA – Service Oriented Architecture) và phần mềm hướng dịch vụ là những cơ hội lớn để các doanh nghiệp dễ dàng về các vấn đề hội nhập và nâng cao năng suất kinh doanh. Mặc dù có nhiều định nghĩa, với một mô hình SOA là mô hình cơ bản của tính toán phân tán, sử dụng các dịch vụ là yếu tố cơ bản để phát triển ứng dụng. Dịch vụ trở thành các khối cơ bản với các ứng dụng mới được tạo ra. Dịch vụ web là một ví dụ điển hình của dịch vụ đó. Thực thi dịch vụ như dịch vụ web trong thành phần hỗ trợ một SOA bên trong các ứng dụng phân tán.

Hình 3.2 trình bày vị trí của một kiến trúc SOA trong hệ thống mạng của một tổ chức. SOA đặt một lớp dịch vụ phía trước hệ thống back-office và thường được triển khai là máy chủ dịch vụ. Lớp dịch vụ này bảo vệ các nhà phát triển từ sự phức tạp ở mức thấp hơn và cho phép các ứng dụng được phát

triển nhanh chóng. Mô hình SOA rất phù hợp là "bảng điều khiển" các ứng dụng, bởi vì nó cho phép truy cập vào thông tin mà trước đó bị khóa bên trong hệ thống back-office. Trong hình 3.2 – phía trên góc bên trái - trình bày bảng điều khiển cho nhân viên truy cập thông tin thông qua cổng thông tin điện tử.

Áp dụng chính sách an toàn tới SOA trong hình 3.2 có ba thách thức sau:

- Duy trì một phạm vi an toàn từ người dùng cuối hoặc máy trạm tới các hệ thống của doanh nghiệp (Từ đầu đến cuối của mô hình), vì vậy người quản trị có thể điều khiển những ai truy cập vào dịch vụ web.
- Đảm bảo một kẻ tấn công khi gửi mã độc XML (như tấn công XDoS) bị ngăn chặn tại lớp dịch vụ.
- Ngăn chặn giả mạo gói tin XML để vượt qua cổng XML.



Hình 3.2 – Kiến trúc hướng dịch vụ

Sử dụng các thẻ an toàn để cho phép các đối tượng an toàn tới lớp dịch vụ

Tại lớp hệ thống, các ứng dụng của doanh nghiệp có các tài liệu an toàn phải được chuyển tới người dùng cuối hoặc các ứng dụng của dịch vụ web tại máy trạm. Để tránh mất mát dữ liệu an toàn của khách hàng hoặc người sử dụng giữa lớp truy cập (Nơi định danh của khách hàng hoặc người sử dụng đã được xác thực) và lớp dịch vụ (Nơi các ứng dụng được phép và đáp ứng tới người dùng cuối), các thẻ an toàn như xác nhận SAML hoặc WS-Security (UsernameToken) nên được chèn vào trong gói tin XML để cho phép tới lớp dịch vụ.

3.2. THIẾT LẬP AN TOÀN CHO HỆ QUẢN TRỊ CƠ SỞ DỮ LIỆU

3.2.1. Bảo vệ hệ quản trị cơ sở dữ liệu trong quá trình cài đặt

Cài đặt hệ quản trị cơ sở dữ liệu đảm bảo an toàn người quả trị phải tuân thủ những quy tắc sau đây:

- ✓ Lựa chọn máy chủ có cấu hình phù hợp với lượng dữ liệu mà hệ quản trị cơ sở dữ liệu cần xử lý.
- ✓ Cập nhật các bản vá lỗi cho hệ điều hành máy chủ cài cơ sở dữ liệu, bước này nhằm ngăn chặn các hiểm họa bị tấn công từ bên ngoài.
- ✓ Đảm bảo cung cấp nguồn điện liên tục để quá trình cài đặt diễn ra thông suốt.
- ✓ Cần phải xem xét kỹ các yêu cầu nhà cung cấp khuyến cáo đối với hệ quản trị cơ sở dữ liệu đó trước khi cài đặt.
- ✓ Lập tài liệu quản trị ngay trước khi bước vào cài đặt, vận hành cũng như bảo trì cơ sở dữ liệu khi xảy ra sự cố.

3.2.2. Phân quyền sử dụng hệ quản trị cơ sở dữ liệu

Với mục đích tăng tính bảo mật dữ liệu, tùy vào các hệ quản trị cơ sở dữ liệu mà hỗ trợ các tính năng cho phép người quản trị thiết lập cơ chế bảo vệ cơ sở dữ liệu trong môi trường đa người dùng, bao gồm các yếu tố chính sau:

- Vai trò của người dùng trong hệ thống và cơ sở dữ liệu.

- Quyền sử dụng các ứng dụng cơ sở dữ liệu trong hệ quản trị cơ sở dữ liệu.
- Quyền tạo và sửa đổi cấu trúc các đối tượng CSDL.
- Quyền truy cập, xử lý dữ liệu.

Khi đăng nhập vào một hệ thống CSDL đa người dùng, người sử dụng cần phải cung cấp UserID (tài khoản) và Password (mật khẩu). Dựa trên UserID hệ thống có khả năng kiểm soát tất cả các hành vi của người sử dụng trên CSDL.

Để thực hiện được chức năng này, người quản trị CSDL cần phải thiết lập các quyền xử lý và truy cập vào CSDL khi tạo ra UserID, ngoài ra còn có một số thuộc tính khác như chuyển quyền sao lưu và phục hồi dữ liệu, trao đổi dữ liệu với các ứng dụng CSDL khác…

Khi nói đến phân quyền, người quản trị cần quan tâm đến các thông tin sau của người dùng:

- ✓ Một người dùng chỉ có một UserID và một mật khẩu.
- ✓ Thời gian có hiệu lực của mật khẩu.
- ✓ Giới hạn chiều dài của mật khẩu.
- ✓ Giới hạn người sử dụng theo thẩm quyền hay mở rộng.
- ✓ Thông tin về người sử dụng.

Khi tạo người sử dụng, tên tài khoản cần rõ ràng, dễ hiểu dễ gợi nhớ, và không cho phép các ký tự đặc biệt, không nên có khoảng trắng.

Quyền người dùng và quản trị quyền người dùng

Quyền người dùng được định nghĩa như mức độ người dùng có thể hay không thể thực thi trên CSDL, quyền được chia thành 4 loại như sau:

- Quyền truy cập vào máy chủ CSDL.
- Quyền truy xuất vào CSDL.
- Quyền thực hiện trên các đối tượng của CSDL.
- Quyền xử lý dữ liệu.

Bảng tóm tắt các truy vấn trong hệ cơ sở dữ liệu

Bảng 3.1 – Truy vấn trong cơ sở dữ liệu

Quyền	Diễn giải
SELECT	Cho phép người sử dụng nhìn thấy dữ liệu, nếu người sử dụng có quyền này thì họ chỉ có thể thực thi những phát biểu select để truy vấn dữ liệu trên các bảng hay các view được cho phép.
INSERT	Cho phép người sử dụng thêm dữ liệu, nếu người sử dụng có quyền này thì họ có thể thực thi phát biểu insert.
UPDATE	Quyền này cho phép người sử dụng chỉnh sửa dữ liệu bằng phát biểu Update.
DELETE	Quyền này cho phép người sử dụng xóa dữ liệu.
REFERENCE	Cho phép người sử dụng thêm dữ liệu vào bảng có khóa ngoại.
EXECUTE	Quyền này cho phép người sử dụng thực thi các thủ tục (SP) trong CSDL.

Đối với hệ quản trị cơ sở dữ liệu SQL Server vai trò của người sử dụng trong cơ sở dữ liệu như sau:

Bảng 3.2 – Vai trò người dùng trong SQL Server

Vai trò (Role)	Diễn giải
sysadmin	Có các quyền tương đương với sa.
serveradmin	Cấu hình một số tham số và tắt server.
setupadmin	Bị giới hạn bớt một số chức năng liên kết server và khởi động một số thủ tục.
securityadmin	Quản lý người dùng và tạo CSDL.
processadmin	Được phép dừng các thao tác đang thực hiện trên CSDL và một số quá trình thực hiện khác của SQL Server.
dbcreator	Được phép tạo CSDL.

diskadmin	Quản lý các tập tin liên quan đến CSDL SQL Server.

Vai trò trên CSDL:

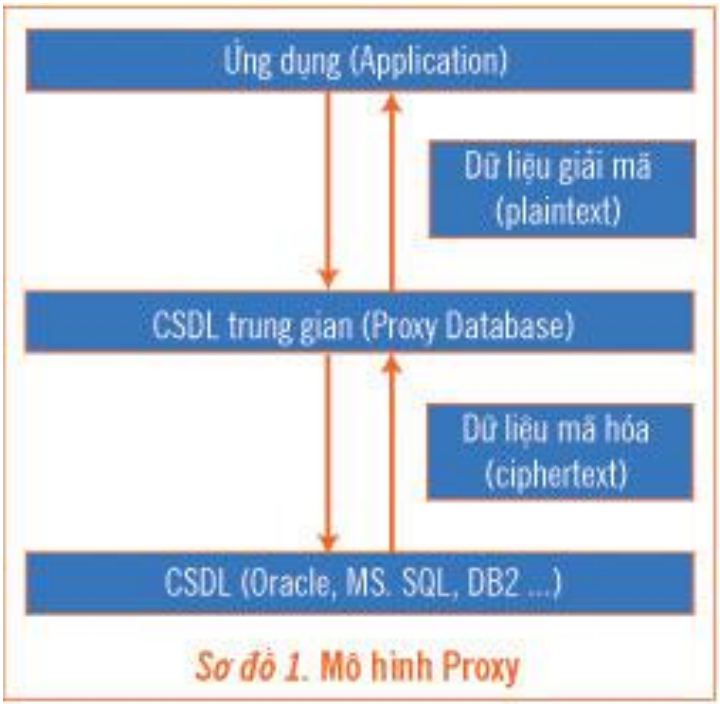
Vai trò	Diễn giải
db _owner	Với vai trò này, người sử dụng (NSD) thuộc nhóm sở hữu CSDL mới có thể truy cập vào CSDL.
db_accessadmin	Thực hiện các chức năng giống như securityadmin.
db _datareader	NSD được phép select trên các bảng dữ liệu của người dùng khác trong CSDL.
db _datawriter	NSD được phép insert, update, delete trên các bảng dữ liệu của người dùng khác trong CSDL.
db _ddladmin	NSD có thể thêm hay chỉnh sửa các đối tượng của CSDL.
db _securityadmin	NSD có quyền tương đương với quyền securityadmin.
db_backupoperator	NSD có thể thực hiện chức năng backup dữ liệu.
db _denydareader	Không cho phép sử dụng phát biểu SELECT trên tất cả các bảng dữ liệu của CSDL.
db_denydawriter	Không cho phép sử dụng phát biểu INSERT, UPDATE, DELETE trên tất cả các bảng dữ liệu của CSDL.

3.2.3. Mã hóa cơ sở dữ liệu

Trong chiến lược bảo mật dữ liệu, đa số các công ty hiện nay tập trung nguồn lực vào bảo vệ dữ liệu trên đường truyền. Trong khi đó vấn đề bảo vệ dữ liệu nằm trong cơ sở dữ liệu (CSDL, database) chưa được quan tâm đúng mức.

Thực tế cho thấy, sự cố về an ninh xảy ra với CSDL có thể ảnh hưởng nghiêm trọng đến danh tiếng của công ty và quan hệ với khách hàng. Sự cố an ninh mất cắp 40 triệu thẻ tín dụng của khách hàng gần đây xảy ra với Master Card và Visa Card đã phần nào gia tăng sự chú ý đến các giải pháp bảo mật CSDL.

Trong mục này, giáo trình trình bày các giải pháp bảo mật CSDL bằng phương pháp xây dựng tầng mã hóa.



Hình 3.3 – Mô hình Proxy

Giải pháp đơn giản nhất bảo vệ dữ liệu trong CSDL ở mức độ tập tin, chống lại sự truy cập trái phép vào các tập tin CSDL là hình thức mã hóa. Tuy nhiên, mã hóa dữ liệu ở mức độ này là giải pháp mang tính "được ăn cả, ngã về không", giải pháp này không cung cấp mức độ bảo mật truy cập đến CSDL ở mức độ bảng (table), cột (column) và dòng (row). Một điểm yếu nữa của giải pháp này là bất cứ ai với quyền truy xuất CSDL đều có thể truy cập vào tất cả dữ liệu trong CSDL. Điều này phát sinh một nguy cơ nghiêm trọng, cho phép các đối tượng với quyền quản trị (admin) truy cập tất cả các dữ liệu nhạy cảm. Thêm vào đó, giải pháp này bị hạn chế vì không cho phép phân quyền khác nhau cho người sử dụng CSDL.

Giải pháp thứ hai, đối nghịch với giải pháp mã hóa cấp tập tin nêu trên, giải quyết vấn đề mã hóa ở mức ứng dụng. Giải pháp này xử lý mã hóa dữ liệu trước khi truyền dữ liệu vào CSDL. Những vấn đề về quản lý khóa và quyền truy cập được hỗ trợ bởi ứng dụng. Truy vấn dữ liệu đến CSDL sẽ trả kết quả dữ liệu ở dạng mã hóa và dữ liệu này sẽ được giải mã bởi ứng dụng. Giải pháp này giải quyết được vấn đề phân tách quyền an ninh và hỗ trợ các

chính sách an ninh dựa trên vai trò (Role Based Access Control – RBAC). Tuy nhiên, xử lý mã hóa trên tầng ứng dụng đòi hỏi sự thay đổi toàn diện kiến trúc của ứng dụng, thậm chí đòi hỏi ứng dụng phải được viết lại. Đây là một vấn đề đáng kể cho các công ty có nhiều ứng dụng chạy trên nhiều nền CSDL khác nhau.

Từ những phân tích hai giải pháp nêu trên, có thể dễ dàng nhận thấy một giải pháp bảo mật CSDL tối ưu cần hỗ trợ các yếu tố chính sau:

- Hỗ trợ mã hóa tại các mức dữ liệu cấp bảng, cột, hàng.
- Hỗ trợ chính sách an ninh phân quyền truy cập đến mức dữ liệu cột, hỗ trợ RBAC.
- Cơ chế mã hóa không ảnh hưởng đến các ứng dụng hiện tại.

Dưới đây là hai mô hình thỏa mãn các yêu cầu trên, đặc biệt là yêu cầu thứ ba.

1. Xây dựng tầng CSDL trung gian

Trong mô hình này, một CSDL trung gian (proxy) được xây dựng giữa ứng dụng và CSDL gốc (Sơ đồ 1). CSDL trung gian này có vai trò mã hóa dữ liệu trước khi cập nhật vào CSDL gốc, đồng thời giải mã dữ liệu trước khi cung cấp cho ứng dụng. CSDL trung gian đồng thời cung cấp thêm các chức năng quản lý khóa, xác thực người dùng và cấp phép truy cập.

Giải pháp này cho phép tạo thêm nhiều chức năng về bảo mật cho CSDL. Tuy nhiên, mô hình CSDL trung gian đòi hỏi xây dựng một ứng dụng CSDL tái tạo tất cả các chức năng của CSDL gốc.

2. Sử dụng cơ chế sẵn có trong CSDL

Mô hình này giải quyết các vấn đề mã hóa cột dựa trên các cơ chế sau:

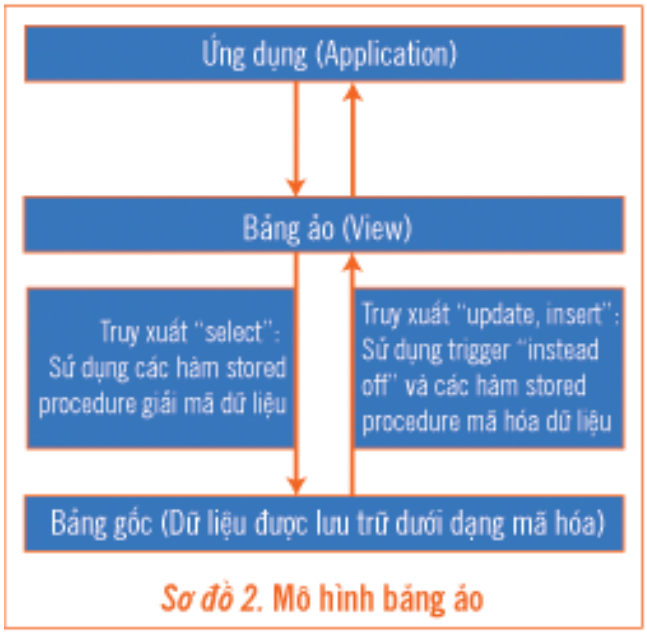
a. Các hàm Stored Procedure trong CSDL cho chức năng mã hóa và giải mã

b. Sử dụng cơ chế View trong CSDL tạo các bảng ảo, thay thế các bảng thật đã được mã hóa.

c. Cơ chế "instead of" trigger được sử dụng nhằm tự động hóa quá trình mã hóa từ View đến bảng gốc.

Trong mô hình này, dữ liệu trong các bảng gốc sẽ được mã hóa, tên của bảng gốc được thay đổi. Một bảng ảo (View) được tạo ra mang tên của bảng gốc, ứng dụng sẽ truy cập đến bảng ảo này.

Truy xuất dữ liệu trong mô hình này có thể được tóm tắt như sau:



Hình 3.4 – Mô hình bảng ảo

Các truy xuất dữ liệu đến bảng gốc sẽ được thay thế bằng truy xuất đến bảng ảo. Bảng ảo được tạo ra để mô phỏng dữ liệu trong bảng gốc. Khi thực thi lệnh "select", dữ liệu sẽ được giải mã cho bảng ảo từ bảng gốc (đã được mã hóa). Khi thực thi lệnh "Insert, Update", "instead of" trigger sẽ được thi hành và mã hóa dữ liệu xuống bảng gốc.

Quản lý phân quyền truy cập đến các cột sẽ được quản lý ở các bảng ảo. Ngoài các quyền cơ bản do CSDL cung cấp, hai quyền truy cập mới được định nghĩa:

1. Người sử dụng chỉ được quyền đọc dữ liệu ở dạng mã hóa (ciphertext). Quyền này phù hợp với những đối tượng cần quản lý CSDL mà không cần đọc nội dung dữ liệu.
2. Người sử dụng được quyền đọc dữ liệu ở dạng giải mã (plaintext).

Giải pháp nêu trên có lợi điểm đơn giản, dễ phát triển. Tuy nhiên, do các giới hạn về cơ chế view, trigger và cách thức quản trị dữ liệu, giải pháp này có những hạn chế sau:

- ✓ Những cột index không thể được mã hóa, do đó hạn chế các ứng dụng cần hỗ trợ index.
- ✓ Dữ liệu mã hóa có kích thước lớn so với dữ liệu gốc. Sự chênh lệch này không đáng kể đối với các dữ liệu chữ (text), nhưng rất đáng kể đối với các dữ liệu số và dạng nhị phân. Ví dụ, dữ liệu số 1 byte sẽ bị tăng lên 2 byte sau khi mã hóa.
- ✓ Tốc độ truy cập CSDL giảm do quá trình thực thi tầng mã hóa.

Hiện nay, trên thị trường sản phẩm mã hóa CSDL, DBEncrypt (www.appsecinc.com) và nCypher (www.ncypher.com) phát triển theo mô hình trên.

3.2.4. Giám sát và kiểm toán cơ sở dữ liệu

Một cơ bản của một hệ thống an toàn bao gồm cả cơ sở dữ liệu là giám sát kỹ lưỡng các hoạt động như truy cập, những phiên đăng nhập, những thay đổi cơ sở dữ liệu, quản lý thay đổi, cấu hình hệ điều hành v.v… Hệ thống giám sát mở rộng vượt ra ngoài an toàn, và nó thường là một ý tưởng tốt để tận dụng. Ví dụ, công cụ hoặc thực hành sử dụng để giám sát hoạt động. Quản trị cơ sở dữ liệu và các ứng dụng được yêu cầu của chính sách MISP theo dõi rủi ro vốn có của hệ thống. Điều này có thể đơn giản như thường xuyên kiểm tra các quyền và danh sách kiểm soát truy cập hoặc như phức tạp như ghi lại các bản ghi bao gồm kích hoạt cho các sự kiện bất thường. Cho các máy chủ hệ thống, giám sát với Microsoft Operations Manager (MOM) hoặc Tripwire có thể chỉ ra các vấn đề tiềm năng về bảo mật. Ngoài ra còn có một số sản phẩm của bên thứ ba cho các ứng dụng giám sát, cơ sở dữ liệu và máy chủ. Tuy nhiên, xin lưu ý rằng giám sát quan trọng nhất của bất kỳ hệ thống là khả năng chuyên môn và kinh nghiệm của người quản trị, và không có thay thế cho đánh giá định kỳ các tài liệu đăng nhập bằng các chuyên gia có kiến thức.

- Thường xuyên giám sát tất cả các thư mục chia sẻ trên máy chủ cơ sở dữ liệu để đảm bảo rằng tất cả các quyền là tối thiểu và không có chia

sẻ nếu không cần thiết. Đặc biệt thận trọng với những thư mục chia sẻ mà cho phép truy cập có quyền Write.

- Thường xuyên giám sát thành viên có vai trò quản trị và mật khẩu của tất cả các tài khoản và thông tin khi họ đăng nhập.
- Lập tài liệu về các quyền cơ sở dữ liệu nâng cao.

3.2.5. Sao lưu và phục hồi dữ liệu

Những nguyên nhân gây ra mất mát dữ liệu

- Đĩa cứng hỏng
- Vô ý hay cố ý sửa đổi dữ liệu như xóa hay thay đổi dữ liệu.
- Trộm cắp
- Virus

Để tránh việc mất dữ liệu, chúng ta nên thường xuyên sao lưu cơ sở dữ liệu. Nếu như dữ liệu hay cơ sở dữ liệu bị hư thì ta có thể dùng bản sao lưu (backup) này để khôi phục lại cơ sở dữ liệu bị mất.

Sao lưu cơ sở dữ liệu

Sao lưu - backup một cơ sở dữ liệu (CSDL) là tạo một bản sao CSDL, ta có thể dùng bản sao để khôi phục lại CSDL nếu CSDL bị mất. Bản sao gồm tất cả những tệp tin có trong CSDL kể cả transaction log.

Transaction log (hay log file) chứa những dữ liệu thay đổi trong CSDL (Ví dụ như khi ta thực hiện các lệnh INSERT, UPDATE, DELETE). Transaction log được sử dụng trong suốt quá trình khôi phục để roll forward những transaction hoàn thành và roll back những transaction chưa hoàn thành. Sao lưu một transaction log là chỉ sao lưu những thay đổi xảy ra trong transaction log kể từ lần sao lưu transaction log cuối cùng.

Roll back là hủy bỏ giao dịch chưa hoàn thành khi hệ thống xảy ra sự cố,… (hoặc trong trường hợp sao lưu, khi đã thực hiện xong việc sao lưu mà giao dịch chưa hoàn thành).

Roll forward là khôi phục tất cả giao dịch đã hoàn thành khi hệ thống xảy ra sự cố,… (hoặc trong trường hợp sao lưu, những giao dịch đã hoàn thành khi đã thực hiện xong việc sao lưu).

Checkpoint là thời điểm ghi lại tất cả những trang dữ liệu thay đổi lên đĩa.

Sao lưu một CSDL ghi lại toàn bộ trạng thái của dữ liệu tại thời điểm thực hiện xong sao lưu.

Lập kế hoạch để sao lưu thường xuyên

Nếu cơ sở dữ liệu có nhiều người sử dụng, trước khi thực hiện một bản sao lưu, cần phải đảm bảo rằng tất cả người dùng không truy vấn tới cơ sở dữ liệu để tất cả các thay đổi trong dữ liệu được lưu lại.

Về mức độ thường xuyên phải tạo các bản sao lưu cơ sở dữ liệu, nó thường phụ thuộc vào mức độ cơ sở dữ liệu thường xuyên có thay đổi lớn. Dưới đây là một số hướng dẫn chung để giúp người quản trị quyết định tần suất sao lưu:

- Nếu cơ sở dữ liệu là một kho lưu trữ, hoặc nếu CSDL chỉ được sử dụng để tham chiếu và hiếm khi thay đổi, cần thực hiện sao lưu chỉ khi thiết kế hoặc dữ liệu được thay đổi.
- Nếu cơ sở dữ liệu đang hoạt động và dữ liệu thường xuyên thay đổi, tạo ra một lịch trình thường xuyên sao lưu cho cơ sở dữ liệu.
- Nếu cơ sở dữ liệu có nhiều người sử dụng, tạo ra một bản sao lưu của cơ sở dữ liệu bất cứ khi nào có sự thay đổi thiết kế.

Đối với mỗi hệ quản trị cơ sở dữ liệu khác nhau thì có các phương pháp sao lưu khác nhau. Sau đây trình bày một số ví dụ sao lưu trong hệ quản trị cơ sở dữ liệu MySQL:

Khi sao lưu hệ quản trị cơ sở dữ liệu MySQl có thể sử dụng dòng lệnh trực tiếp hoặc sử dụng đồ họa gián tiếp thông qua trình duyệt web - phpMyAdmin. Phương thức này thích hợp với việc sao lưu một phần của cơ sở dữ liệu hoặc chọn các định dạng dữ liệu khi sao lưu.

Đăng nhập vào cPanel, kích hoạt hệ thống Quản lý cơ sở dữ liệu phpMyAdmin và làm theo các bước sau:

1. Chọn cơ sở dữ liệu cần sao lưu (hiển thị trong danh mục bên trái nếu có nhiều cơ sở dữ liệu).
2. Bấm vào tab Export, để cấu hình mặc định (trong mục Export chọn định dạng SQL, Select All để sao lưu tất cả các bảng trong cơ sở dữ liệu hoặc chọn từng bảng theo yêu cầu; trong mục Options chọn Structure và Data).
3. Đánh dấu vào mục Save as file, điền tên file muốn sao lưu (nếu để trống sẽ dùng tên của cơ sở dữ liệu) và định dạng nén (nên chọn zipped hoặc gzipped để giảm dung lượng file cần tải).
4. Bấm nút Go, phpMyAdmin sẽ để tải file sao lưu về máy.

Phục hồi dữ liệu

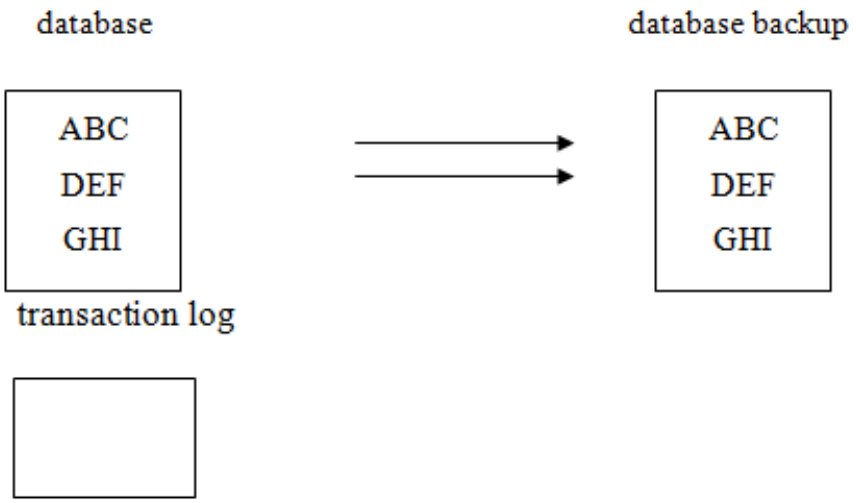
Việc khôi phục một bản sao lưu CSDL sẽ trả về CSDL cùng trạng thái của CSDL khi ta thực hiện việc sao lưu. Giao dịch (transaction) nào không hoàn thành trong khi sao lưu (backup) CSDL được roll back để đảm bảo tính nhất quán CSDL.

Khôi phục một bản sao lưu transaction log là áp dụng lại tất cả giao dịch (transaction) hoàn thành trong transaction log đối với CSDL. Khi áp dụng bản sao lưu transaction log, SQL Server đọc trước transaction log, roll forward tất cả các transaction. Khi đến cuối bản sao lưu transaction log, SQL Server roll back tất cả transaction mà không hoàn thành khi ta bắt đầu thực hiện sao lưu, tạo lại trạng thái chính xác của CSDL tại thời điểm bắt đầu thực hiện sao lưu.

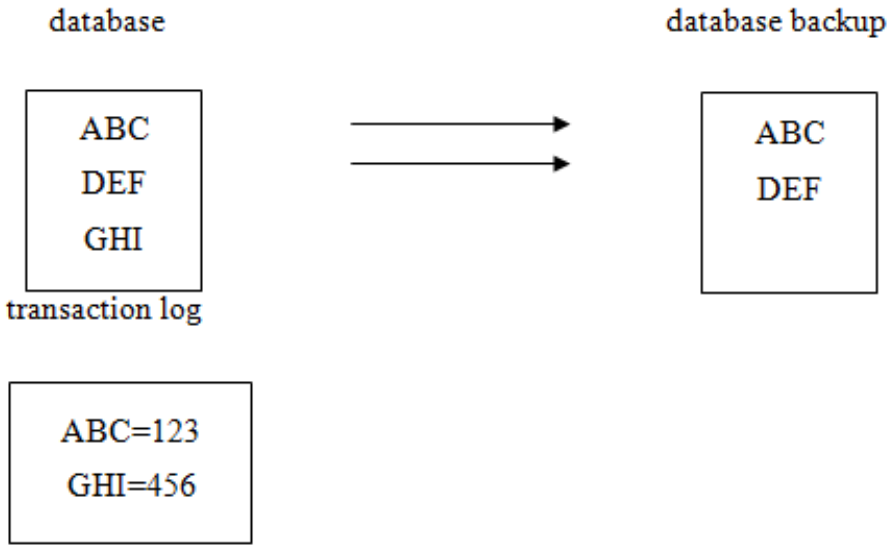
Ví dụ minh họa sao lưu (backup) và khôi phục (restore) một CSDL có xảy ra giao dịch (transaction) khi thực hiện sao lưu:

1. Bắt đầu backup: Giả sử CSDL gồm có các dữ liệu ABC, DEF, GHI, JKL, transaction log file không có dữ liệu vì không có giao dịch nào xảy ra. Khi đang thực hiện sao lưu (backup) được một phần dữ liệu thì xảy ra giao dịch, SQL Server 2000

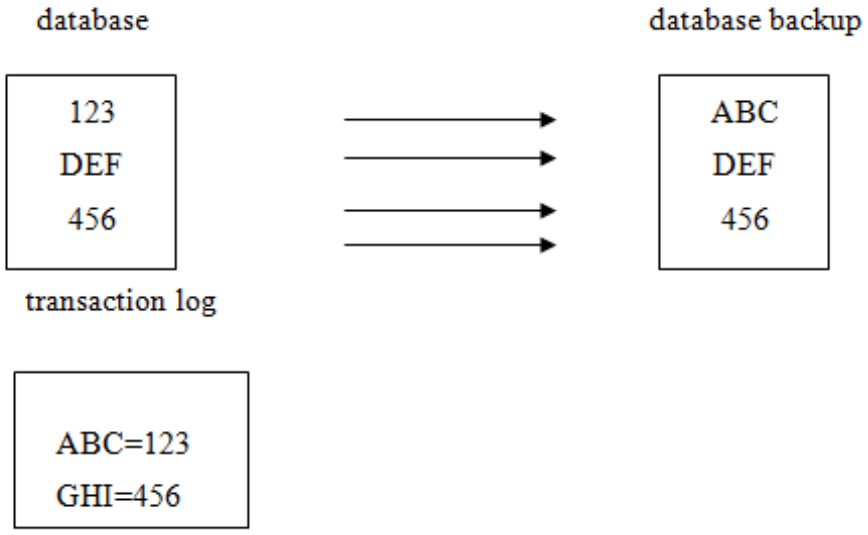
sẽ ưu tiên cho việc giao dịch trước, việc sao lưu (backup) tạm thời dừng lại.



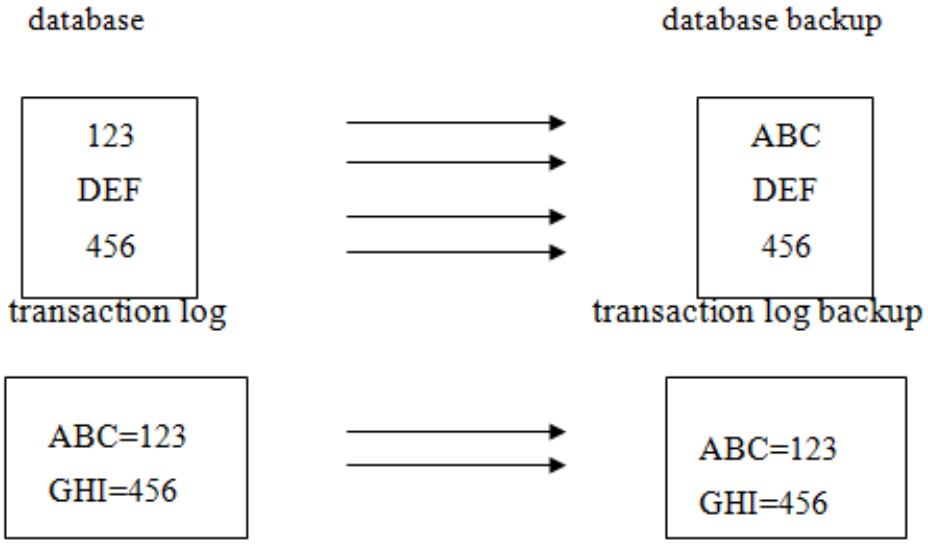
2. Xảy ra giao dịch (transaction), dữ liệu ABC được thay bằng 123, GHI được thay bằng 456.



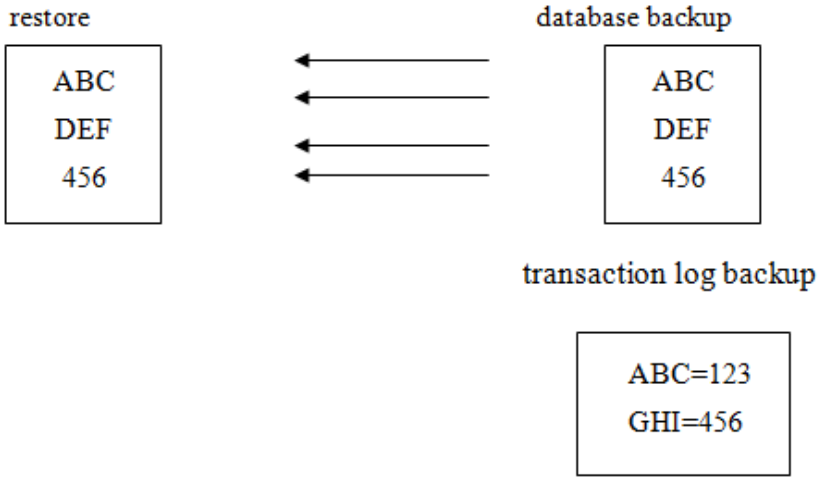
3. Khi thực hiện giao dịch (transaction) xong, SQL Server thực hiện tiếp việc sao lưu (backup), sẽ chép phần còn lại của dữ liệu nhưng dữ liệu đã thay đổi do xảy ra giao dịch.



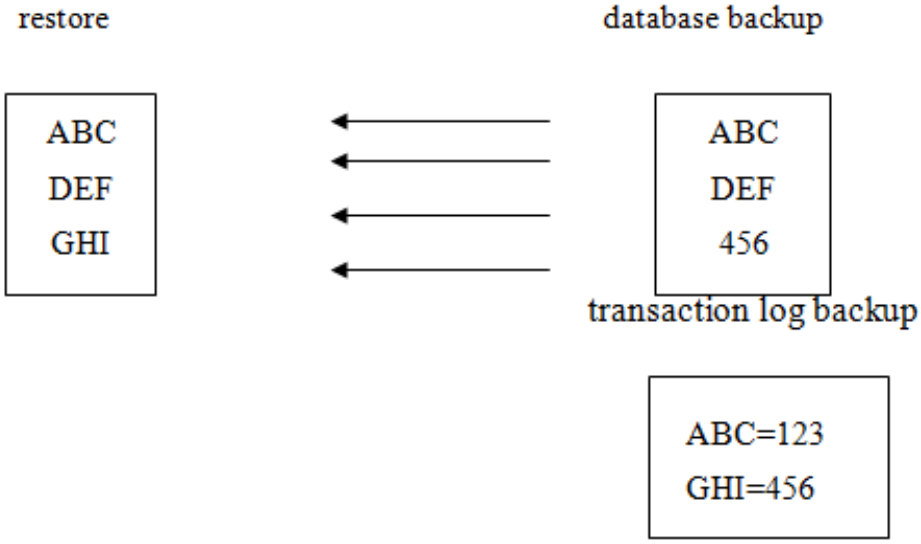
4. Khi sao lưu xong phần dữ liệu thì sẽ chép tiếp phần transaction log.



5. Khi có yêu cầu khôi phục (restore) CSDL , CSDL được khôi phục trước, chép lại toàn bộ CSDL của bản sao lưu CSDL đó.



6. Sau đó SQL Server sẽ khôi phục tiếp phần transaction log. Trước tiên sẽ roll forward nhưng khi đọc đến dữ liệu thứ ba thì nó thấy dữ liệu này đã được thay đổi rồi do đó nó sẽ roll back (trả về dữ liệu ban đầu khi chưa thực hiện giao dịch) để nhất quán dữ liệu.



Các loại sao lưu và phục hồi

- Các loại sao lưu
  - ✓ **Full Database Backups**: Copy tất cả data files, user data và database objects như system tables, indexes, user-defined tables trong một database.

- ✓ **Differential Database Backups:** Copy những thay đổi trong tất cả data files kể từ lần full backup gần nhất.
- ✓ **File or File Group Backups:** Copy một data file đơn hay một file group.
- ✓ **Transaction Log Backups:** Ghi nhận một cách thứ tự tất cả các transactions chứa trong transaction log file kể từ lần transaction log backup gần nhất. Loại backup này cho phép ta phục hồi dữ liệu trở ngược lại vào một thời điểm nào đó trong quá khứ mà vẫn đảm bảo tính nhất quán.

- Các mô hình khôi phục
  - ✓ **Full Recovery Model**: Đây là model cho phép phục hồi dữ liệu với ít rủi ro nhất. Nếu một database ở trong mode này thì tất cả các hoạt động không chỉ insert, update, delete mà kể cả insert bằng **Bulk Insert**, hay **Bcp** đều được log vào transaction log file. Khi có sự cố thì ta có thể phục hồi lại dữ liệu ngược trở lại tới một thời điểm trong quá khứ. Khi data file bị hư nếu ta có thể backup được transaction log file thì ta có thể phục hồi database đến thời điểm transaction gần nhất được commited.
  - ✓ **Bulk-Logged Recovery Model**: Ở mode này các hoạt động mang tính hàng loạt như Bulk Insert, bcp, Create Index, WriteText, UpdateText chỉ được log minimum vào transaction log file đủ để cho biết là các hoạt động này có diễn ra mà không log toàn bộ chi tiết như trong Full Recovery Mode. Các hoạt động khác như Insert, Update, Delete vẫn được log đầy đủ để dùng cho việc phục hồi sau này.
  - ✓ **Simple Recovery Model**: Ở mode này thì Transaction Log File được rút ngắn thường xuyên và không cần backup. Với mode này chỉ có thể phục hồi tới thời điểm backup gần nhất mà không thể phục hồi tới một thời điểm trong quá khứ.

3.3. THIẾT LẬP AN TOÀN CHO DỊCH VỤ THƯ TÍN ĐIỆN TỬ

3.3.1. Thiết lập an toàn máy chủ ứng dụng thư tín

3.3.1.1 Cài đặt an toàn cho máy chủ thư tín

Trong quá trình cài đặt thiết lập cấu hình cho máy chủ thư nếu thấy bất kỳ ứng dụng, dịch vụ hay script nào không cần thiết nên loại bỏ ngay trước khi kết thúc quy trình cài đặt.

Trong quá trình cài đặt máy chủ thư, những bước sau cần được thực hiện:

- Cài đặt phần mềm máy chủ thư trên máy chủ chuyên dụng.
- Cài đặt ở mức tối thiểu các dịch vụ Internet cần có.
- Áp dụng các công nghệ vá lỗ hổng và nâng cấp hệ thống để chống các hiểm họa biết trước.
- Tạo các phân vùng đĩa (logic hoặc vật lý) sử dụng cho việc cài đặt ứng dụng thư.
- Loại bỏ hoặc vô hiệu hóa tất cả các dịch vụ được cài đặt bởi ứng dụng chủ thư không cần thiết (ví dụ: thư dựa trên web, FTP, tiện ích quản lý từ xa…)
- Loại bỏ tất cả những tiện ích không rõ nguồn gốc khỏi máy chủ thư.
- Áp dụng các cơ chế an toàn có sẵn đối với một máy chủ thư.
- Thiết lập lại cấu hình cho các giao thức SMTP, POP3, IMAP.

3.3.1.2 Cấu hình an toàn ứng dụng máy chủ thư tín

Hầu hết các hệ điều hành trên các máy chủ thư đã cung cấp khả năng phân quyền cho việc truy cập đến hệ thống các tệp tin, các thiết bị, và nguồn tài nguyên trên máy chủ đó. Bất cứ nguồn tài nguyên nào trên máy chủ mà mail server có thể truy nhập đến đều là tiềm năng có thể chia sẻ cho tất cả người sử dụng trong hệ thống thư tín. Phần mềm mail server hỗ trợ bổ sung việc truy cập đến các tệp tin, các thiết bị, và nguồn tài nguyên nhằm quản lý và vận hành các hoạt động của nó. Quan trọng nhất là việc làm sao có thể đồng nhất các quyền được thiết lập bởi hệ điều hành và chính bản thân phần

mềm mail server. Bên cạnh đó phải đảm bảo được rằng các đối tượng sử dụng mail không được trao quá nhiều hoặc quá ít quyền.

Như vậy người quản trị máy chủ thư cần tìm ra phương pháp làm thế nào để thiết lập cấu hình tốt nhất việc quản lý truy nhập để bảo vệ thông tin được lưu trữ trên máy chủ thư công khai trong hai mối quan hệ dưới đây:

- Hạn chế sự truy cập của ứng dụng mail server tới các nguồn tài nguyên phụ của máy tính.
- Hạn chế sự truy cập của người sử dụng đến hệ thống thông qua các quyền bổ sung được hỗ trợ bởi máy chủ thư, nơi mà những mức điều khiển truy cập được thiết lập chi tiết hơn.

Việc thiết lập cấu hình quản lý truy nhập có thể ngăn cấm các thông tin nhạy cảm, riêng tư khỏi những hiểm hoạ khi một máy chủ thư được công khai hoá. Hơn nữa, quản lý truy nhập có thể được sử dụng nhằm giới hạn việc sử dụng nguồn tài nguyên trong trường hợp máy chủ thư bị tấn công từ chối dịch vụ (DoS).

Cũng cần thiết phải đảm bảo rằng mail server không thể lưu các tệp ngoài các cấu trúc tệp đã được xác định bởi mail server. Điều này có thể được cấu hình trên chính mail server hoặc cấu hình hệ điều hành trong việc quản lý tất cả các tiến trình chạy trên máy chủ. Phải đảm bảo được rằng các thư mục và các tệp (bên ngoài cây thư mục đã được xác định) không thể bị truy nhập, ngay cả khi người dùng biết được đường dẫn của chúng.

Trên các máy chủ Unix và Linux, nên sử dụng "chroot jail" cho ứng dụng mail server. Sử dụng chroot thay đổi view của mail server trên hệ thống file của máy chủ, cụ thể là thư mục root được hiển thị sẽ không phải là thư mục root thực sự của hệ thống mà nó chỉ là một phần con của thư mục root hệ thống. Bởi vậy, nếu mail server bị đánh sập, kẻ tấn công chỉ có thể truy nhập trong giới hạn phần con của hệ thống file trên máy chủ. Đây là một hình thức nâng cao độ an toàn rất hiệu quả.

Nhằm giảm ảnh hưởng của các loại tấn công DoS, nên thiết lập cấu hình máy chủ thư nhằm hạn chế số lượng nguồn tài nguyên hệ thống mà trong quá trình vận hành có thể gây tổn hại.

3.3.1.3 Bảo vệ thư tín điện tử trước tấn công của mã độc hại

Thư điện tử đã và đang được sử dụng như một công cụ cho việc gửi các tệp dữ liệu dạng nhị phân dưới hình thức các tệp đính kèm. Ban đầu, chúng không gây ra các rủi ro cho sự an toàn bởi vì các tệp đính kèm thường chỉ là các tài liệu hoặc các tệp hình ảnh dung lượng nhỏ. Ngày càng có nhiều tổ chức, cá nhân sử dụng thư điện tử cho việc giao dịch hàng ngày, dung lượng và kiểu định dạng của các tệp đính kèm từ đó mà cũng ngày một gia tăng. Ngày nay, rất nhiều thư điện tử được gửi với các tệp đính kèm là các chương trình chạy, tranh ảnh, nhạc và âm thanh. Vấn đề đặt ra ở đây là loại tệp đính kèm nào được phép, hay một tệp với định dạng bất kỳ nào đó cũng có thể được trao đổi qua thư điện tử dưới dạng tệp đính kèm.

Quyết định khi nào thì cho phép đính kèm có thể là một quyết định không phải dễ. Không cho phép gửi theo các tệp đính kèm trong thư điện tử sẽ làm đơn giản hoá một hệ thống và làm cho hệ thống an toàn hơn; Tuy nhiên, sẽ làm giảm sự hữu dụng vốn có của hệ thống thư tín điện tử. Nói chung việc cho phép đính kèm là một nhu cầu thực tế của người sử dụng. Tuy nhiên, người quản trị hệ thống thư cần xác định trước các kiểu định dạng dữ liệu sẽ được cho phép đính kèm.

Virus có thể được truyền qua các thư điện tử theo dạng virus thư hoặc là virus đính kèm. Nếu một máy chủ thư không được cài đặt phần mềm chống virus, hoặc đã được cài đặt nhưng phần mềm chống virus hoạt động không hiệu quả, khả năng đe dọa sự an toàn cho người sử dụng đầu cuối sẽ tăng lên. Một số phần mềm thư điện tử máy trạm phổ biến hiện nay có nguy cơ cao trong việc lây nhiễm và truyền các virus sinh ra từ thư điện tử. Các loại virus trên là đặc trưng cho kết quả hỗ trợ các nội dung tích cực của các trạm thư điện tử, chẳng hạn các thông điệp HTML. Việc ngăn cấm hoặc cho phép các nội dung có tính hoạt động như trên cần được thực hiện bởi các nhà xây dựng các ứng dụng thư điện tử.

Nhiều loại nội dung có thể được xem là nội dung hoạt động. Điển hình là các nội dung dưới dạng các script hoặc các control object. Các kiểu nội dung hoạt động phổ biết nhất được biết đến hiện nay là ActiveX, Java, JavaScrip, và Visual Basic Script. Các vi rút dưới dạng nội dung hoạt động và

mã phá hoại có thể ảnh hưởng đến MUA. Để khắc phục điều đó, người quản trị nên cấu hình nhằm quản lý chặt chúng và đưa ra những thông báo cho người sử dụng đầu cuối.

Quét Virus

Chống sự phá hoại xuất phát từ nội dung hoạt động chỉ là bước đầu tiên nhằm bảo vệ người sử dụng đầu cuối. Bước tiếp theo là bảo vệ việc sinh virus từ những tệp đính kèm. Để bảo vệ khỏi virus và các mã nguy hiểm khác, nhất thiết phải thực thi việc quét virus tại một hay nhiều khâu trong quá trình phân phối thư điện tử. Việc quét virus có thể được thực hiện trên bức tường lửa nơi dữ liệu thư điện tử bắt đầu vào mạng của một cơ quan hay tổ chức nào đó, ngay trên máy chủ thư điện tử hay trên các máy trạm của người sử dụng đầu cuối. Mỗi lựa chọn có điểm mạnh và điểm yếu riêng. Nếu nguồn tài nguyên cho phép, việc sử dụng nhiều hơn một sự lựa chọn ở trên sẽ đem lại sự an toàn cao hơn.

Dưới đây là một số lợi ích quét virus cho thư điện tử tại bức tường lửa:

- Thư điện tử có thể được quét virus theo cả hai hướng (trong và ngoài mạng của một tổ chức hoặc công ty nào đó)
- Virus có thể bị chặn lại trước khi xâm nhập mạng.
- Có thể quét virus các thư vào mạng mà không cần thay đổi lớn cấu hình máy chủ thư điện tử hiện tại.
- Có thể quản lý tập trung việc quét virus để đảm bảo sự tuân thủ chính sách an toàn của tổ chức.
- Các bức tường lửa thường hỗ trợ nhiều giao thức khác nhau, vì vậy chúng ta có thể sử dụng chương trình quét virus cho các giao thức khác (ví dụ như HTTP, FTP).

Nhược điểm của việc cài đặt trình quét virus trên bức tường lửa:

- Yêu cầu sửa đổi lớn cấu hình máy chủ thư điện tử hiện tại khi quét virus cho thư điện tử theo hướng ra ngoài mạng.
- Không thể quét virus các thư điện tử đã mã hoá.

- Không bảo vệ được người sử dụng nội bộ khi xuất hiện virus ở mạng trong của công ty hay tổ chức trừ khi mạng được cấu hình để tất cả dòng dữ liệu truyền qua giao thức SMTP được định tuyến qua một bộ quét chuyên dụng trước khi đến máy chủ thư điện tử của công ty hay tổ chức đó.
- Yêu cầu tường lửa có cấu hình cao để chịu tải.

Lựa chọn thứ hai là cài đặt trình quét virus cho thư điện tử trên chính máy chủ thư điện tử. Lựa chọn này rất hữu ích cho việc bảo vệ thư điện tử khỏi các virus được người sử dụng trong mạng nội bộ gửi cho người sử dụng ở một mạng khác vì các thông điệp đó thường không được bức tường lửa quét virus.

Dưới đây là một số ưu nhược điểm của phương án này.

Ưu điểm:

- Thư điện tử có thể được quét virus theo cả hai hướng (trong và ngoài).
- Có thể thực hiện việc quản lý trung tâm để đảm bảo tuân thủ chính sách bảo mật của tổ chức.
- Có thể bảo vệ người sử dụng nội bộ khi có một virus trong mạng nội bộ của tổ chức hay công ty.

Nhược điểm:

- Quét virus yêu cầu biến đổi lớn về cấu hình máy chủ thư điện tử hiện tại.
- Không thể quét virus được các thư điện tử đã được mã hoá.
- Yêu cầu máy chủ thư phải có cấu hình cao khi sử dụng cho công ty hay tổ chức có nhiều người sử dụng.

Dù lựa chọn phương án quét virus trên bức tường lửa hay trên chính các máy chủ thư điện tử, người quản trị cần:

- Phát hiện và quét tất cả các virus đã biết và các loại mã nguy hiểm khác.

- Hỗ trợ quét thông minh (trợ giúp một số biện pháp bảo vệ khỏi các virus mới hoặc chưa được biết).
- Trợ giúp việc lọc nội dung.
- Kết hợp với cơ chế ngăn ngừa khả năng phá vỡ hệ thống bởi các nguy cơ khác.
- Dễ dàng trong việc quản lý.
- Hỗ trợ việc cập nhật tự động.
- Cập nhật thường xuyên (yếu tố bắt buộc).
- Có thể định danh và áp dụng quy tắc cho các loại nội dung khác nhau.

Một lựa chọn nữa là cài đặt trình quét virus trên các máy trạm, tức trên chính các máy của người sử dụng đầu cuối. Thư điện tử được quét khi người sử dụng mở. Ưu điểm lớn của phương án này là việc quét virus được phân tán trên nhiều máy, do đó sẽ có ảnh hưởng rất ít đến hiệu suất làm việc của mỗi hệ thống riêng.

Lợi ích của việc quét virus trên các máy khách:

- Không yêu cầu bất kỳ sửa đổi nào trên mail server.
- Có thể quét các thư điện tử được mã hoá khi người sử dụng giải mã chúng.
- Việc quét virus được phân tán trên nhiều máy và do đó hạn chế tối đa ảnh hưởng của việc quét đối với máy chủ.
- Cung cấp khả năng bảo vệ cho những người sử dụng bên trong thậm chí khi nguồn gốc của virus xuất phát từ một người sử dụng bên trong.

Các bất lợi khi quét virus máy khách như sau:

- Khó quản lý tập trung.
- Những người sử dụng có thể cập nhật chậm các bộ quét virus, dẫn đến việc ảnh hưởng đến cả một tập thể.
- Người sử dụng có thể loại bỏ các chức năng của trình quét virus.
- Chỉ quét các thông điệp vào.

- Không xử lý được virus trên bức tường lửa hoặc trên máy chủ thư điện tử trung tâm.

Lọc nội dung thư

Trên thực tế, việc lọc nội dung làm việc theo nguyên lý tương tự thực hiện quét vi rút trên bức tường lửa hoặc máy chủ thư. Về bản chất, đây là quá trình thực hiện việc tìm một đặc tính nào đó có xuất hiện trong nội dung thư hay không. Khi thực thi việc quét virus hoặc ngăn cấm một loại tệp nào đó (căn cứ vào phần mở, tên tệp hay định dạng tệp) thì chỉ đảm bảo được một mức độ an toàn nào đó. Thực tế đã chứng minh khả năng gây tổn hại cho hệ thống, xuất phát từ các nội dung thư và các tệp đính kèm còn lớn hơn nhiều so với virus hay các loại mã phá hoại khác. Chính vì thế, một số biện pháp lọc nội dung cần được triển khai đối với một hệ thống thư điện tử.

Nói chung, các quy tắc được định nghĩa nhằm cách ly, làm sạch, ngăn chặn hoặc xoá bất kỳ dữ liệu nào đi qua máy chủ cần căn cứ vào kết quả của quá trình quét.

Dưới đây là một số thành phần tiêu biểu có thể bị chặn và xử lý bởi các bộ lọc:

- Thư điện tử chứa nội dung đáng ngờ (Ví dụ: Active X, JavaScript), chúng sẽ được gỡ bỏ phần mã gây nên sự nghi ngờ trước khi chuyển đến người sử dụng.
- Thư dạng bom thư có thể bị xoá.
- Các tệp có dung lượng lớn có thể bị dừng phân phát tại các giờ cao điểm (tại thời điểm lượng dữ liệu giao dịch nhiều).

Một đặc điểm chính nữa của các gói lọc nội dung là cho phép việc quét dữ liệu được gửi ra bên ngoài mạng. Việc phân tích từ vựng có thể được thực hiện, như vậy sẽ quét được các thông điệp chứa từ và cụm từ được xem là tương ứng với chức năng sử dụng thư điện tử của một tổ chức hay công ty nào đó. Việc phân tích từ vựng cũng có thể được sử dụng nhằm lưu lại các thông tin trao đổi qua thư điện tử có nội dung chống lại công ty, hoặc các thư có mục đích tấn công theo kiểu bom thư xuất phát từ tổ chức hay công ty đó. Mặt khác, việc phân tích từ vựng còn có thể được sử dụng để quản lý các

thông tin nhạy cảm của một công ty hay tổ chức, khi chúng có nguy cơ bị rò rỉ theo đường thư điện tử.

Hiện tại có nhiều ứng dụng lọc nội dung khác nhau có thể hỗ trợ cho hầu hết các hệ thống truyền thông điệp thư điện tử. Một bộ lọc nội dung được xem là hiệu quả nhất là bộ lọc có thể lọc được tất cả các thư đi và đến một mạng của một công ty hay tổ chức nào đó. Nhiều sản phẩm mới đã kết hợp được các chức năng như lọc nội dung, quét virus và hạn chế kiểu tệp được phép gửi qua thư điện tử. Việc kết hợp các tính năng trên trong cùng một sản phẩm sẽ giúp giảm nhẹ việc quản trị cơ chế an toàn của một mạng.

Ngăn ngừa việc gửi thư hàng loạt

Ngày nay luôn có các đối tượng muốn khai thác các phương tiện truyền thông để công khai hoá các ý tưởng hoặc sản phẩm của họ. Trong đó, thư điện tử không phải là trường hợp ngoại lệ. Thuật ngữ chung nhất dùng cho các thông điệp kiểu này là thư điện tử thương mại tự nguyện (UCE – Unsolicited Comercial Email) hoặc Spam. Hầu hết người sử dụng thư điện tử đều ít nhất một lần nhận được các thư điện tử không mong muốn trên. Để khắc phục hiện tượng trên các nhà quản trị có thể buộc phải quản lý lưu lượng thư đi qua server. Lợi ích trong việc thực hiện kiểm soát UCE là giảm dung lượng hộp thư từ đó giảm các yêu cầu về không gian lưu trữ trên các máy chủ thư.

Để kiểm soát các thông điệp UCE, các nhà quản trị cần phải giải quyết hai vấn đề chính:

- Đảm bảo rằng các UCE không được gửi từ các máy chủ thư mà họ quản lý.
- Thực hiện việc kiểm soát các thông điệp thư điện tử đến, đây cũng chính nội dung chính của mục này.

Vì Internet không có cơ quan nào có đủ thẩm quyền kiểm soát chung, nên các nhà quản trị các máy chủ thư đã thiết lập ra các danh sách gồm các máy chủ thư thường được sử dụng để gửi các thư điện tử kiểu spam. Các danh sách này được các nhà quản trị xem là các danh sách đen mang tính mở (ORBs - Open Relay Blacklists). Nhiều ứng dụng máy chủ thư phổ biến hiện nay có tính năng từ chối không nhận các thông điệp xuất phát từ các ORBs

nào đó. Các danh sách trên được cập nhật thường xuyên; do đó, máy chủ được thiết lập cấu hình từ chối không nhận thư điện tử xuất phát từ các máy chủ có trong danh sách đen sẽ làm giảm đi sự phiền toái mà spam có thể gây ra cho người sử dụng.

Dưới đây là trích dẫn phần nội dung của tệp cấu hình Sendmail nhằm quản lý các ORB.

```
.....

Feature      ('dnsbl',      relays.mail-
abuse.org')
```

Bên cạnh đó, phần lớn các máy chủ thư có thể được cấu hình để từ chối việc nhận các thông điệp điện tử được gửi đến từ một tập tên miền xác định nào đó. Dưới đây là phần trích dẫn từ một tệp cấu hình truy nhập của sendmail có chức năng kiểm soát UCE thông qua việc cho phép hoặc từ chối các thông điệp thư điện tử được chuyển tiếp từ một tập tên miền nào đó.

```
local.com            Relay # cho phÐp r¬ le tõ local.com

Spammers.net     Reject # ng¨n c¸c th- tõ spammers.net

(127.0.0.1)          OK# b¶o vÖ th- tõ m¸y chñ ri²ng nµy

10.                        Reject # ng¨n c¸c th- tõ miÒn IP
nµy
```

Chuyển tiếp thư có xác nhận

Như được đề cập đến trong phần trước, việc thiết lập cấu hình xác thực các thư chuyển tiếp sẽ làm giảm khả năng gửi thư hàng loạt qua một máy chủ thư. Một lợi ích nữa trong việc xác thực các thư chuyển tiếp là làm tăng khả năng an toàn và tính khả dụng của hệ thống.

Hiện có hai phương pháp được hỗ trợ việc quản lý các thư chuyển tiếp. Phương pháp thứ nhất là kiểm soát các mạng con hoặc tên miền mà từ đó các thông điệp thư điện tử được gửi đi. Phương pháp này rất hiệu quả trong

trường hợp hệ thống thư điện tử được thiết lập trong một dải địa chỉ cho trước. Tuy nhiên, nếu trong hệ thống có những người dùng từ xa với các dải địa chỉ khác nhau thì việc áp dụng phương pháp này sẽ không mang lại hiệu quả. Để giải quyết vấn đề người sử dụng từ xa, cần có một cấu hình mạnh hơn.

Phương pháp thứ hai là yêu cầu người sử dụng tự xác nhận họ trước khi họ muốn một thông điệp nào đó. Phương pháp này được gọi là chuyển tiếp thư có xác nhận hoặc SMTP AUTH, là một mở rộng của giao thức SMTP nhằm hỗ trợ việc xác thực người sử dụng. Nhưng rất tiếc rằng, cấu hình mặc định của hầu hết các máy chủ thư là không thực thi việc xác nhận chuyển tiếp. Do đó, người quản trị máy chủ thư phải tự thiết lập cấu hình chức năng này. Xác nhận chuyển tiếp là một trong các tính năng được sử dụng ít nhất nhưng tác dụng trong việc nâng cao độ an toàn cho các máy chủ thư là rất lớn.

3.3.1.4 Truy cập an toàn

Giống như nhiều giao thức Internet khác, hầu hết các giao thức trên chưa được tích hợp sẵn các chức năng mã hoá và xác thực. Việc chưa được tích hợp các tính năng bảo mật và xác thực có thể dẫn đến ba vấn đề người sử dụng có thể gặp phải. Thứ nhất, đối với người sử dụng gửi các thông điệp thư điện tử, nội dung của chúng có thể bị chặn bắt và đọc bất hợp pháp trên đường truyền, thậm chí các nội dung đó có thể bị giả mạo hoặc thay đổi. Thứ hai, người nhận không thể kiểm tra xuất xứ cũng như tính toàn vẹn của các thông điệp thư điện tử. Thứ ba, nếu không sử dụng cơ chế thông tin xác thực sử dụng một lần thì khi một người dùng truy nhập vào hộp thư của mình mọi thông tin được sử dụng để đăng nhập được gửi dưới dạng rõ trên mạng, như vậy các đối tượng tấn công có thể nghe lén và sử dụng lại. Hiện nay, cấu hình mặc định cho hầu hết các phần mềm thư điện tử khách được thiết lập ở chế độ gửi mật khẩu rõ tạo điều kiện chặn bắt cho các máy tính khác trong bản thân mạng cục bộ của người dùng hoặc bất kỳ một máy nào đó có chức năng chuyển mật khẩu đến máy chủ thư điện tử có thể.

Vấn đề cuối cùng có thể được giải quyết thông qua việc áp dụng phương pháp thường được sử dụng để bảo vệ dịch vụ Web - sử dụng giao

thức bảo mật tầng vận tải (TLS - Transport Layer Security). TLS được thiết kế dựa trên giao thức bảo mật tầng socket phiên bản 3 (SSLv3 - Secure Socket Layer version 3). Chúng ta có thể sử dụng TLS kết hợp với các giao thức POP3, IMAP, và SMTP để bảo mật cho dữ liệu giao dịch giữa các máy khách thư điện tử và máy chủ thư điện tử.

Dưới đây là một ví dụ trong tệp cấu hình của Sendmail, thiết lập việc sử dụng giao thức TLS:

```
….
define ('CERT_DIR','MAIL_SETTING_DIR''certs')dnl
define('confCACERT_PATH','CERT_DIR')dnl
define('confCACERT','CERT_DIR/CAcert.pem')dnl
define('confSERVER_CERT','CERT_DIR/mycert.pem')dnl
define('confSERVER_KEY','CERT_DIR/mykey.pem')dnl
define('confCLIENT_CERT','CERT_DIR/cert.pem')dnl
define('confCLIENT_KEY','CERT_DIR/mykey.pem')dnl
….
```

Truy cập thư thông qua web

Ngày càng có nhiều tổ chức cung cấp trình duyệt web có thể truy nhập vào hệ thống thông điệp thư tín điện tử. Khả năng truy nhập thư điện tử thông qua giao diện Web cho phép chúng ta thực hiện cơ chế an toàn cho cả phía client và phía máy chủ. Lĩnh vực bảo đảm an toàn cho các trang Web nằm ngoài phạm vi của giáo trình này. Tuy nhiên khi sử dụng giao diện Web để truy nhập đến hệ thống thư tín điện tử, chúng ta cần chú ý:

- Không nên cài đặt cả phần mềm Web server và phần mềm mail server trên cùng một máy chủ.
- Cần thiết lập cơ chế bảo mật giao dịch Web sử dụng giao thức SSL/TLS.

3.3.1.5 Thiết lập cấu hình ghi nhật ký

Khả năng ghi nhật ký của các sản phẩm thư máy chủ là rất khác nhau, dưới đây chỉ đề cập đến các cấu hình chung nhất. Nên thiết lập chế độ ghi nhật ký cho phần mềm thư máy chủ ở mức chi tiết nhất ("maximum" , "detailed", …). Khi đó các sự kiện dưới đây sẽ được ghi lại:

- Nhật ký của máy cục bộ.
  - ✓ Các lỗi thiết lập IP.
  - ✓ Các vấn đề liên quan đến cấu hình khác (DNS, Windows Internet Naming Service)
  - ✓ Các lỗi cấu hình phần mềm thư (không tương thích với DNS: lỗi cấu hình cục bộ, lỗi bí danh).
  - ✓ Cơ sở dữ liệu bí danh quá hạn.
  - ✓ Thiếu nguồn tài nguyên hệ thống (dung lượng đĩa trống, bộ nhớ, CPU)
  - ✓ Xây dựng lại cơ sở dữ liệu bí danh
- Nhật ký liên quan đến các kết nối
  - ✓ Đăng nhập (thành công hoặc không thành công)
  - ✓ Các vấn đề an toàn
  - ✓ Lỗi giao diện
  - ✓ Mất kết nối (các vấn đề về mạng)
  - ✓ Giao thức có vấn đề
  - ✓ Thời gian chờ kết nối
  - ✓ Từ chối kết nối
  - ✓ Sử dụng các câu lệnh VRFI và EXPN
- Đăng nhập liên quan đến thông điệp
  - ✓ Gửi thay (send on behalf of)
  - ✓ Gửi như (send as)

- ✓ Các địa chỉ không đúng định dạng
- ✓ Thống kê thư
- ✓ Tạo các thông báo lỗi
- ✓ Không thực hiện được việc phân phát thư
- ✓ Thư chưa gửi được

Phần mềm máy chủ truyền thư cung cấp khả năng cho phép hoặc vô hiệu hoá việc các điều khiển truy nhập xác định trong quá trình khởi động. Mức điều khiển này có ích cho việc bỏ qua sự thay đổi vô tình các tệp nhật ký do các lỗi trong việc quản lý truy nhập tệp.

Các công cụ phân tích tự động tệp nhật ký

Lưu lượng dữ liệu truyền qua máy chủ thư là rất lớn, dung lượng các tệp nhật ký vì thế cũng sẽ tăng lên rất nhanh. Bởi vậy cần cài đặt các công cụ phân tích các tệp nhật ký tự động trên các máy chủ thư nhằm làm giảm gánh nặng cho các nhà quản trị. Các dụng cụ này phân tích các tệp nhật ký trên máy chủ thư và xác định các sự kiện đáng ngờ và bất thường.

Hiện nay có rất nhiều công cụ (có công cụ là các sản phẩm thương mại, cũng có những công cụ được cung cấp miễn phí) hỗ trợ việc phân tích một cách chính qui. Một số tổ chức muốn sử dụng hai hoặc nhiều hơn các bộ phân tích tự động tệp nhật ký nhằm giảm nguy cơ bỏ qua hiểm hoạ hoặc các sự kiện quan trọng khác đã được ghi lại trong các tệp nhật ký.

3.3.2. Thiết lập an toàn đối với người dùng cuối

3.3.2.1 Cập nhật các bản vá cho phần mềm thư máy trạm

Bước quan trọng nhất trong việc thiết lập cơ chế an toàn các phần mềm thư điện tử máy trạm là đảm bảo rằng tất cả người sử dụng đang được sử dụng phiên bản mới nhất, có độ an toàn cao nhất của phần mềm thư máy trạm với việc áp dụng tất cả công nghệ lấp lỗ hổng cần thiết. Để định danh các điểm yếu của phần mềm thư máy trạm cụ thể nào đó chúng ta có thể tham khảo từ trang Web http://icat.nist.gov, của viện tiêu chuẩn công nghệ (NIST) quốc gia Mỹ.

Dưới đây là danh sách các trang Web cung cấp các công cụ lấp lỗ hổng cho từng loại phần mềm thư máy trạm:

- Edura: http://www.edura.com/
- Lotus Notes: http://www.lotus.com/home.nsf/welcome/downloads
- Microsoft Outlook:http://www.microsoft.com/office/outlook/default.htm
- Microsoft Outlook Express:http://windowsupdate.microsoft.com/
- Netscape:http://home.netscape.com/smartupdate/

Việc cập nhật cho Outlook là khá phức tạp hơn bởi vì đây là một phần mềm thư điện tử máy trạm hoạt động trong sự liên kết với trình duyệt Microsoft Internet Explorer. Các cấu hình được thiết lập và điểm yếu của Internet Explorer có thể có sự ảnh hưởng tới sự an toàn của Outlook; do vậy, bên cạnh việc cập nhật cho Outlook chúng ta cũng cần thực hiện việc cập nhật cho cả Internet Explorer. Nếu việc chạy một phiên bản an toàn của một phần mềm thư điện tử máy trạm không thành công sẽ giảm tính hiệu quả của các biện pháp thiết lập cơ chế an toàn sẽ được bàn trong các mục tiếp theo.

3.3.2.2 Trạm thư an toàn

Nói chung các công ty khi xây dựng phần mềm thư điện tử cho máy trạm thường đã tích hợp sẵn các tính năng an toàn, và các tính năng này có khả năng thực thi cao trên thực tế. Nhưng nếu chỉ dừng lại ở mức sử dụng cấu hình mặc định của các phần mềm thư điện tử máy trạm người sử dụng sẽ chưa lợi dụng hết được các cơ chế an toàn vốn có của chúng.

Nói chung với mỗi phần mềm thư điện tử máy trạm chúng ta cần thực hiện cấu hình một số tính năng sau:

- Vô hiệu hoá khả năng mở thư tự động.
- Vô hiệu hóa việc mở tự động thư tiếp theo.
- Vô hiệu hoá việc xử lý thư có nội dung tích cực. Điều này sẽ xuất hiện những rắc rối đối với các phần mềm thư điện tử hoạt động trong mối liên hệ với trình duyệt, vì khi vô hiệu hoá tính năng này sẽ ảnh hưởng

đến chức năng của trình duyệt trong việc hiện thị các trang Web. Trong những trường hợp như vậy, việc lựa chọn chức năng nào sẽ bị vô hiệu hoá, chức năng nào không phải được thực hiện một cách hết sức cẩn thận. Một công việc khác là cần xác định những vùng an toàn riêng biệt cho phần mềm thư điện tử và trình duyệt. Như vậy sẽ cho phép trình duyệt bị có ít chức năng bị cấm hơn so với các phần mềm thư máy trạm.

- Thiết lập " vùng an toàn" cho Outlook:
  - ✓ Vô hiệu hoá khả năng tải các ActiveX không được ký.
  - ✓ Vô hiệu hoá các quyền Java.
  - ✓ Vô hiệu hoá các script tích cực.
  - ✓ Vô hiệu hoá các script của Java Applet.

Lưu ý rằng việc thiết lập ở trên là dành cho Outlook trình duyệt Internet Explorer 5.5. Những phiên bản khác của ứng dụng trên cũng có các bước thiết lập cấu hình tương tự. Ngoài ra, việc thực hiện các thao tác cấu hình trên sẽ có tác dụng đối với cả Outlook và trình duyệt Internet Explorer.

- Thiết lập cấu hình cho Eudora:
  - ✓ Vô hiệu hoá việc "Cho phép thực thi trong nội dung HTML".
  - ✓ Vô hiệu hoá Microsoft viewer.
  - ✓ Vô hiệu hoá MAPI.
- Thiết lập cấu hình Netscape:
  - ✓ Không lựa chọn "Enable Java"
  - ✓ Không lựa chọn "Enable JavaScript for Mail and News"
  - ✓ Không lựa chọn "Send email address as anonymous FTP Password"
  - ✓ Loại bỏ "Microsoft ActiveX Portability Container for Netscape" như các plug-in hỗ trợ ActiveX khác.

3.3.2.3 Truy cập an toàn thư điện tử dựa trên web

Theo quan điểm của người sử dụng, việc truy nhập đến máy chủ thư điện tử thông qua việc sử dụng một máy chủ Web sẽ đem đến sự hiệu quả và giao diện sử dụng thân thiện hơn. Tuy nhiên, vấn đề an toàn cho hệ thống thư cần được xem xét một cách cẩn thận trước khi đưa ra quyết định sử dụng giao diện Web để thực hiện giao dịch thư điện tử. Hầu hết các vấn đề liên quan đến cơ chế an toàn trong trường hợp này cũng tương tự như đối với các phần mềm thư điện tử thông thường. Ví dụ, việc truy nhập thư điện tử dựa trên Web với cấu hình mặc định việc gửi mật khẩu và dữ liệu khác cũng ở dạng rõ như khi sử dụng POP và IMAP. Đối với nơi có yêu cầu an toàn cao, người quản trị cần thiết lập cấu hình để máy chủ thư chỉ chấp nhận các kết nối Web thông qua các giao thức bảo mật SSL/TLS hỗ trợ thuật toán mã hoá 128-bit. Với việc sử dụng các giao thức trên mọi dữ liệu (thông tin đăng nhập, nội dung thư điện tử) sẽ được mã hoá trong các giao dịch giữa máy chủ Web (sử dụng cho thư) và các máy trạm người sử dụng chạy trình duyệt. Chú ý rằng dữ liệu chỉ được bảo mật trong giao dịch, còn dữ liệu thư điện tử lưu trên các máy chủ và máy trạm là không được bảo mật. Trong trường hợp này, chúng ta có thể sử dụng các phương pháp mã hoá thư điện tử như S/MINE hoặc PGP. Tuy nhiên các hệ thống truyền thư dựa trên Web không hỗ trợ trực tiếp việc sử dụng phương pháp trên. Một giải pháp có thể thực hiện được là mã hoá dữ liệu một cách offline sau đó dán nó vào trong trình duyệt truyền (phương pháp này có thể dễ dàng thực hiện với PGP).

Rủi ro lớn của các hệ thống thư điện tử dựa trên Web là chúng có thể được truy nhập từ các máy tính công cộng (có thể là từ các máy tính trong phòng thí nghiệm, trong thư viện, hoặc ngay trong các quán caffe Internet). Trong các tình huống này, trình duyệt có thể được thiết lập cấu hình để nhớ tên người sử dụng và mật khẩu. Nếu người sử dụng không chú ý đến cấu hình trên, người sử dụng không được cấp quyền cũng có thể sử dụng chính máy tính đó để truy nhập vào hệ thống thư điện tử của một công ty hay tổ chức nào đó. Một nguy hiểm khác, đối với các máy tính công cộng có thể bộ ghi nhật ký bàn phím, thao tác gõ bàn phím của người dùng khi làm việc một hệ thống thư sẽ được ghi lại, trong đó có cả thông tin về tên người sử dụng và mật khẩu

đăng nhập. Dữ liệu này có thể sẽ được khai thác nhằm tấn công hệ thống thư hoặc ăn cắp thông tin của người dùng. Các trình duyệt Web cũng lưu lại một số thông tin trong quá trình người sử dụng thao tác ở dạng các tệp tạm, các thông tin này chỉ tồn tại ở một giai đoạn nhất định. Nhưng sau mỗi phiên làm việc nếu người sử dụng không xoá chúng đi trước khi đóng trình duyệt, thì kẻ xấu có thể sử dụng chính các thông tin đó để đăng nhập vào hệ thống thư với vai trò của người sử dụng. Việc dùng các giao thức SSL/TLS nói chung có thể khắc phục được các mối nguy hiểm trên.

Sự an toàn của các hệ thống thư điện tử dựa trên Web bị ảnh hưởng rất lớn từ yếu tố con người trong quá trình sử dụng. Do đó, mọi người sử dụng trong hệ thống cần được đào tạo một cách cẩn thận, và họ phải hiểu rõ vai trò của mình đối với sự an toàn chung, trước khi được trao quyền truy nhập hệ thống.

3.3.3. Thiết lập an toàn thư tín sử dụng mật mã

3.3.3.1 Giới thiệu các lược đồ an toàn thư tín

Hai lược đồ đầu tiên cho việc bảo mật nội dung thư đầu cuối là Prety Good Privacy (PGP) và Secure Multipurpose Internet Mail Extension (S/MIME). Cả hai đều dựa trên cùng một yếu tố là mật mã khoá công khai, trong đó mỗi người sử dụng có một cặp khoá: một khoá công khai mà ai cũng có thể có và một khoá bí mật mà chỉ người sử dụng là chủ hữu cặp khoá mới có. Khoá công khai của đối tượng nhận được sử dụng để mã hoá dữ liệu cần gửi, và dữ liệu đã được mã hoá này chỉ được giải mã khi sử dụng khoá bí mật tương ứng. Khoá bí mật của người gửi sẽ được sử dụng để tạo chữ ký điện tử trên dữ liệu được gửi đi, việc xác nhận chữ ký điện tử trên sẽ được kiểm tra bởi bất kỳ ai có khoá công khai tương ứng. Công nghệ chữ ký điện tử có sử dụng đến việc tạo một bản tóm lược dữ liệu cần ký thông qua việc sử dụng các hàm băm (hàm hash), với việc sử dụng hàm băm dữ liệu sẽ được ký một cách hiệu quả hơn (để hiểu rõ hơn cần có nhiều kiến thức hơn trong lĩnh vực mật mã).

Xuất phát từ nhiều lý do, trong đó lý do quan trọng nhất là khi sử dụng mật mã khoá công khai sẽ phải trả giá về thời gian tính toán. Để làm giảm

thời gian xử lý, mật mã khoá đối xứng cũng được sử dụng trong việc bảo mật nội dung thư điện tử. Mật mã khoá đối xứng yêu cầu có một khoá đơn được chia sẻ trước giữa các đối tượng cần trao đổi thông tin, đối với thư điện tử là các đối tượng nhận và các đối tượng gửi. Như vậy, khắc phục được nhược điểm của mật mã khoá công khai là thời gian xử lý, thì mật mã khoá đối xứng lại vướng phải nhược điểm là cần phân phối khoá trước.

Một lược đồ tiêu biểu kết hợp giữa hai hệ mật trên ra đời sử dụng cho thư điện tử, lược đồ này có thể được tóm tắt như sau:

Bên đối tượng gửi

- Sinh ra một khoá ngẫu nhiên
- Mã hoá thông điệp cần gửi sử dụng một thuật toán mã hoá khoá đối xứng (khoá sinh ngẫu nhiên ở trên).
- Mã hoá khoá đối xứng sử dụng khoá công khai của đối tượng nhận với thuật toán mã hoá khoá công khai tương ứng.
- Gửi cả thông điệp đã được mã và khoá đối xứng đã được mã cho đối tượng nhận.

Bên phía đối tượng nhận

- Sử dụng khoá bí mật giải mã khoá đối xứng đã được mã (với thuật toán mã hoá khoá công khai tương ứng)
- Dùng khoá đối xứng để giải mã thông điệp đã được mã hoá (với thuật toán tương ứng như bên gửi)

Ưu điểm của lược đồ này là:

- Thuật toán mã hoá khoá công khai chỉ được sử dụng để mã khoá đối xứng.
- Khoá dùng cho thuật toán mã hoá đối xứng không phải phân phối trước.

Mặc dù S/MIME và PGP là hai lược đồ mã hoá thư điện tử được dùng phổ biến hiện nay, nhưng cũng có nhiều lược đồ khác đã được đề xuất kể từ khi phát minh ra thư điện tử. Hai trong số đó chúng ta có thể kể đến là lược đồ PEM (đầu tiên được phát triển năm 1987) và MIME Object Security Services

(MOSS). Tuy nhiên trong phạm vi tập bài giảng này chúng ta sẽ không đề cập sâu hơn đến chúng.

Mặc dù mã hoá thư điện tử nâng cao độ an toàn, nhưng khi sử dụng dịch vụ này cần chú ý:

- Việc quét virus và lọc nội dung thư tại bức tường lửa và ngay trên máy chủ thư sẽ gặp rắc rối với nội dung thư đã được mã hoá. Nếu trên bức tường lửa và máy chủ thư không có phương pháp để giải mã thư điện tử thì chúng không thể thực hiện việc quét virus và lọc nội dung.
- Các thao tác mã, giải mã sẽ cần thời gian xử lý. Các tổ chức có hệ thống máy tính lạc hậu sẽ không muốn sử dụng tính năng mã hoá, trừ khi họ có khả năng nâng cấp hệ thống máy tính.
- Các thư điện tử được mã hoá sẽ có dung lượng lớn hơn và bởi vậy yêu cầu thêm về băng thông mạng. Thực tế dung lượng tăng lên bao nhiêu phụ thuộc vào rất nhiều yếu tố: thuật toán mã hoá, cỡ khoá, dung lượng thư cần mã,...
- Để sử dụng tính năng mã hoá sẽ kéo theo một số tác vụ khác như: phân phối khoá, khôi phục khoá, và huỷ bỏ các khoá mã.

3.3.3.2 Mã hóa thư điện tử sử dụng PGP – Pretty Good Privacy

PGP ra đời lần đầu tiên vào năm 1991. Khởi đầu PGP là một phần mềm miễn phí, nhưng sau đó nó được phát triển thành hai phiên bản: phiên bản thương mại và phiên bản miễn phí. Việc tải phiên bản miễn phí, hoặc đăng ký mua phiên bản thương mại có thể được thực hiện thông qua rất nhiều địa chỉ Web, bảng dưới đây liệt kê một số trang Web chính mà ở đó người sử dụng có thể tải PGP. OpenPGP hiện tại được định nghĩa bởi IETF (Internet Engineering Task Force).

Danh sách các trang web cung cấp PGP:

Tổ chức	**URL**
International PGP Site	http://www.pgpi.org

MIT PGP Freeware Distribution	http://web.mit.edu/network/pgp.html
PGP site (Phiên bản thương mại)	http://www.pgp.com
OpenPGP site	http://www.openpgp.org

Phiên bản PGP là phiên bản 7.0, được xây dựng bởi công ty PGP. Phiên bản này hỗ trợ một số thuật toán mật mã được đề xuất bởi NIST, bao gồm:

- Chuẩn mã hoá dữ liệu (DES - Data Encryption Standard), 3 DES, cho việc mã hoá dữ liệu.
- Chuẩn mã hoá tiên tiến (AES - Advanced Encryption Standard) cho việc mã hoá dữ liệu.
- Thuật toán chữ ký điện tử (DSA - Digital Signature Algorithm) cho các chữ kỹ số.
- RSA cho các chữ ký số
- Thuật toán băm an toàn (SHA-1 - Secure Hash Algorithm) cho việc băm dữ liệu.
- Chú ý:
  - ✓ Để biết thêm chi tiết về chuẩn mã hoá dữ liệu DES và 3DES có thể truy nhập vào trang: http://csrc.ncsl.nist.gov/cryptval
  - ✓ Để biết thêm chi tiết về thuật toán AES có thể truy nhập vào trang: http://csrc.nist.gov/encryption/aes
  - ✓ Để biết thêm chi tiết về DSA và DSS có thể truy nhập vào trang: http://www.itl.nist.gov/fipspub/fip186.html
  - ✓ Để biết thêm chi tiết về SHA và SHS có thể truy nhập vào trang: http://csrc.nist.gov/cryptval/shs.html

Các phiên bản khác của PGP có thể hỗ trợ các lược đồ mã hoá khác. Các tổ chức thuộc liên bang Mỹ được yêu cầu sử dụng các thuật toán mà chính phủ liên bang Mỹ đã chấp nhận, các tổ chức khác cũng thường sử dụng

các thuật toán trên vì chúng đã kiểm tra và kiểm định tính an toàn. Thực tế đã có rất nhiều thuật toán mã hoá không được chấp nhận đã bị phá, đây cũng có thể xem là một trong các lỗ hổng cho thư điện tử khi chúng được sử dụng.

Nếu một tổ chức hay công ty nào đó lựa chọn PGP, họ cần áp dụng các hướng dẫn được liệt kê trong bảng dưới đây:

Bảng 3.3 – Bảng liệt kê phân cấp bảo mật của PGP

	Bộ các thuật toán mật mã
An toàn mức cao nhất	✓ Mã hoá: Sử dụng AES với 256 bít khoá. ✓ Chữ ký số và hàm băm: Chuẩn chữ ký số DSS với độ dài khoá là 1024 bít hoặc lớn hơn, thuật toán băm SHA-1.
An toàn và thực thi	✓ Mã hoá: Sử dụng AES với 128 bít khoá. ✓ Chữ ký số và hàm băm: DSS với khoá có độ dài 1024 bít hoặc lớn hơn, SHA-1.
An toàn và tương thích	✓ Mã hoá: 3DES, 168/112 bít khoá. ✓ Chữ ký số và hàm băm: DSS với khoá có độ dài 1024 bít hoặc lớn hơn, SHA-1.
Xác thực và phát hiện giả mạo	✓ Chữ ký số và hàm băm: DSS với khoá có độ dài 1024 bít hoặc lớn hơn, SHA-1.

Mặc dù PGP đã sử dụng mật mã khoá công khai, nhưng chỉ trong việc ký các bản tóm lược của thông điệp, còn việc mã hoá nhiều thành phần thực sự của thông điệp được thực hiện bởi thuật toán mã hoá khoá đối xứng như đã đề cập ở phần trước. Dưới đây là các mô tả vắn tắt về qui trình ký và mã hoá thư điện tử sử dụng PGP (các bước có thể xuất hiện theo thứ tự khác nhau):

- PGP tạo một khoá phiên ngẫu nhiên (trong một vài cài đặt của PGP, nguồn sinh ngẫu nhiên được lấy từ sự di chuyển chuột trên màn hình của người sử dụng)
- Thông điệp thư điện tử được mã hoá bằng khoá phiên sinh ngẫu nhiên và một thuật toán mã hoá khoá đối xứng (3DES, AES).
- Khoá phiên được mã hoá bằng khoá công khai của đối tượng nhận.
- Sử dụng hàm băm SHA-1 để sinh bản tóm lược của thông điệp điện tử, và giá trị tóm lược này sẽ được thực hiện ký điện tử sử dụng khoá bí mật của đối tượng gửi.
- Khoá phiên đã mã hoá được đính kèm theo thông điệp thư điện tử.
- Thông điệp thư điện tử được gửi cho đối tượng nhận.

Đối tượng nhận thực hiện ngược lại qui trình trên để nhận được khoá phiên và giải mã và kiểm tra chữ ký thông điệp thư điện tử. Các phần mềm thư điện tử máy trạm phổ thông như Netscape Messenger, Eudora, Microsoft Outook yêu cầu việc cài đặt plug-in để thiết lập khả năng gửi nhận các thông điệp thư điện tử được mã hoá bởi PGP. Các địa chỉ Web cung cấp PGP cũng hỗ trợ các hướng dẫn về việc sử dụng PGP với các ứng dụng thư máy trạm khác nhau.

3.3.3.3 Mã hóa thư điện tử sử dụng S/MIME

S/MIME lần đầu tiên được giới thiệu vào năm 1995 bởi RSA Data Security. S/MIME dựa trên chuẩn mật mã khoá công khai tương ứng PKCS#7 (Public Key Cryptography Standard #7) sử dụng cho định dạng dữ liệu các thông điệp thư điện tử đã được mã hoá, và chuẩn X.509 phiên bản 3 cho các chứng chỉ điện tử. Các thông tin về các chuẩn RSA PKCS có thể tra cứu từ trang chủ của PKCS: http://www.rsasecurity.com/rsalabs/pkcs/index.html

S/MIME phiên bản 2 đã được chấp nhận một cách rộng rãi từ nền công nghiệp thư điện tử trên Internet. Mặc dù nó không xem là một chuẩn (theo IETF), nhưng nó được xác định trên các RFCs dưới đây:

- RFC 2311: S/MIME Version 2 Message Specification

- RFC 2312: S/MIME Version 2 Certificate Handling
- RFC 2313: PKCS#1- RSA Encryption Version 1.5
- RFC 2314: PKCS#10 - Certification Request Syntax Version 1.5
- RFC 2315: PKCS#7 - Cryptographic Message Syntax Version 1.5
- RFC 2268: Mô tả thuật toán mã hoá RC2

S/MIME phiên bản 3 được phát triển bởi IETF S/MIME Working Group và được chấp nhận là chuẩn của IETF vào tháng 7 năm 1999. S/MIME phiên bản 3 được xác định bởi các RFC:

- RFC 2630: Cryptographic Message Syntax
- RFC 2633: S/MIME Version 3 Message Specification
- RFC 2632: S/MIME Version 3 Certificate Handling
- RFC 2631: Diffie-Hellman Key Agreement Method
- RFC 2634: Enhanced Security Services for S/MIME

Trang chủ của S/MIME Working Group có địa chỉ: http://www.ietf.org/html.chaters/smime-charter.html.

Bởi vì phiên bản đầu tiên của S/MIME được phát triển vào năm 1995, nên chuẩn S/MIME phải tuân theo cơ chế quản lý xuất khẩu mật mã hiện của nước Mỹ. Điều này có nghĩa là các cài đặt S/MIME bị áp đặt hỗ trợ thuật toán mã hoá không có độ an toàn cao là RC2 với 40 bít khoá. Việc quản lý cơ chế xuất khẩu mật mã bây giờ đã mở hơn rất nhiều. Tuy nhiên, do từng đã bị yêu cầu chỉ hỗ trợ thuật toán RC2 40-bít, nên S/MIME thường được xem như là một sản phẩm hỗ trợ mật mã yếu, hiện nay điều này chỉ đúng nếu như một thuật toán yếu được chọn, S/MIME đã được tích hợp nhiều thuật toán mã hoá, cho phép hỗ trợ phương pháp mã hoá có độ bảo mật cao.

Đặc tính có giá trị nhất của S/MIME là nó được xây dựng ngay bên trong các phần mềm thư máy trạm và gần như trong suốt với người sử dụng. Bởi tính đóng gói của các ngành công nghiệp phần mềm ngày nay rất cao (đặc biệt là sản phẩm của các hãng lớn như Microsoft, Netscape, ...), nên S/MIME đã tồn tại một cách mặc định trong các bộ cài đặt của các phần mềm thư máy

trạm phổ thông hiện nay như Netscape Messager và Outlook, Outlook Express. Tương tự như PGP, không có một sai lầm thực sự nào được phát hiện trong giao thức S/MIME. Tuy nhiên, như trên các URL đã mô tả, S/MIME sử dụng thuật toán RC2 40-bít đã bị phá trên các máy Windows (có thể tham khảo thông tin này ở trang:

http://www.counterpane.com/smime.html)

S/MIME phiên bản 3 hỗ trợ hai thuật toán mã hoá dữ liệu được giới thiệu bởi NIST là DES và 3DES, và một thuật toán do IETF bổ sung là AES. Để làm tương thích được với các phiên bản thấp hơn, bị hạn chế bởi việc quản lý cơ chế xuất khẩu mật mã, S/MIME cũng hỗ trợ các thuật toán RC2 40-bít và RC2 64-bít.

Nói chung, các tổ chức không nên sử dụng thuật toán RC2 40 bít (độ an toàn thấp nhất) hoặc DES (độ an toàn thấp) cho các thư tín điện tử hay các cuộc trao đổi dữ liệu khác có tính chất nhạy cảm. Cả hai thuật toán trên được cho là rất yếu trong môi trường hiện nay và chỉ nên dùng nó khi không còn cách nào khác (ví dụ trong trường hợp bắt buộc, hoặc phải làm việc với các phiên bản cũ của S/MIME). RC2 64 bít có độ an toàn cao hơn RC2 40 bít và DES và tốc độ của nó cũng cao hơn DES và 3DES. Tuy nhiên, RC2 64 bít có độ an toàn thấp hơn 3DES, nên chỉ nên giới hạn việc dùng nó trong trường hợp tương thích là yêu cầu số một. Việc thực thi các thuật toán dường như chỉ là một công bố của S/MIME từ khi các thao tác mã hoá và giải mã được thực hiện trên các máy trạm. Khi an toàn là yêu cầu số một, 3DES là thuật toán có độ an toàn cao nhất hiện được hỗ trợ bởi S/MIME, và hy vọng trong tương lai AES sẽ nhanh chóng được tích hợp cho các phần mềm thư máy trạm hiện đang được sử dụng phổ thông.

3.3.3.4 Sự lựa chọn giữa PGP và S/MIME

Việc lựa chọn giữa PGP và S/MIME phụ thuộc vào một số yếu tố. Các phiên bản thương mại mới nhất của PGP đã được bổ sung các tính năng nhằm hoàn thiện sản phẩm như S/MIME, tạo nên sự khác biệt rất ít giữa chúng. Khi triển khai cả hai chuẩn trên cũng cung cấp các tính năng bổ sung như mã hoá

đĩa hoặc mã hoá tệp, như vậy có thể sử dụng để bảo vệ các thông tin ngoài thư điện tử trên các máy.

Các ưu điểm của PGP gồm

- Tương thích với các nhóm người sử dụng nhỏ.
- An toàn hơn với sự trợ giúp của thuật toán mã hoá dữ liệu AES, trong khi S/MIME chưa tích hợp thuật toán này cho các phần mềm thư điện tử phổ thông.
- Có phiên bản miễn phí.
- Không yêu cầu (có hỗ trợ nếu yêu cầu) một cơ sở hạ tầng khoá công khai bên ngoài (PKI - Public Key Infrastructure), trong khi S/MIME yêu cầu các tổ chức phải trả một khoản kinh phí để có được các chứng chỉ điện tử hoặc tự họ phải sở hữu một trung tâm cấp phát và quản lý chứng chỉ.
- Có thể dùng với bất kỳ một phần mềm thư điện tử máy trạm nào.

Các ưu điểm của S/MIME

- Thích hợp với các nhóm người sử dụng lớn như các tổ chức hoặc các công ty.
- Là chuẩn mã hoá thư điện tử được sử dụng rộng rãi nhất.
- Hỗ trợ sẵn trong hầu hết các ứng dụng thư điện tử máy trạm.
- Trong suốt hơn đối với người sử dụng đầu cuối.

3.3.4. Sao lưu và phục hồi máy chủ thư tín

Việc duy trì tính toàn vẹn của dữ liệu trên máy chủ thư là một trong các chức năng quan trọng nhất của người quản trị. Đây là một chức năng cực kỳ quan trọng bởi vì các máy chủ thư thường là khâu dễ bị gây hại nhất trong mạng chung của một tổ chức hay công ty. Bên cạnh đó, trong quá trình hoạt động phần cứng hoặc phần mềm cấu thành các máy chủ thư rất có thể sẽ bị hư hỏng hoặc không hoạt động.

Máy chủ thư cần được người quản trị sao lưu dự phòng một cách thường xuyên vì một số lý do:

- Một máy chủ thư có thể không hoạt động được do bị tấn công hoặc do nguyên nhân phần cứng hoặc phần mềm có vấn đề.
- Thông thường việc giải quyết tranh chấp trong một số trường hợp người ta căn cứ vào dữ liệu được sao lưu dự phòng chứ không căn cứ vào dữ liệu hiện tại trên máy chủ thư.

Để thực hiện việc sao lưu dữ liệu trên các máy chủ thư, các tổ chức cần thiết lập chính sách cho vấn đề này. Nội dung của chính sách chịu ảnh hưởng của ba yếu tố:

- Các yêu cầu pháp lý.
  - ✓ Các luật và qui định hiện hành(áp dụng cho các chủ thể là Chính phủ, nhà nước và các tổ chức quốc tế).
  - ✓ Các yêu cầu kiện tụng, tranh chấp.
- Các yêu cầu về nhiệm vụ
  - ✓ Bằng hợp đồng.
  - ✓ Thực hành chung.
  - ✓ Đánh giá dữ liệu cho tổ chức.
- Các chính sách và hướng dẫn có tổ chức

Mặc dù chính sách dự phòng máy chủ thư của từng tổ chức là khác nhau, nhưng các chính sách đó cần phải giải quyết được một số vấn đề sau:

- Mục đích của chính sách dự phòng máy chủ thư.
- Ai sẽ chịu ảnh hưởng bởi chính sách dự phòng máy chủ thư.
- Máy chủ thư nào được cần thực hiện chính sách dự phòng.
- Định nghĩa các thuật ngữ chính, đặc biệt là các thuật ngữ về kỹ thuật và pháp luật.
- Mô tả một cách chi tiết các yêu cầu theo ngôn ngữ pháp luật, thương mại, ...
- Phác thảo tần số dự phòng.

- Phác thảo các thủ tục nhằm bảo đảm dữ liệu sẽ hoàn toàn được bảo vệ và lưu trữ.
- Phác thảo các thủ tục nhằm bảo đảm dữ liệu khi không có yêu cầu lưu thêm sẽ bị huỷ hoàn toàn (không có khả năng khôi phục lại).
- Có văn bản rõ ràng về việc xử lý kiện tụng tranh chấp.
- Liệt kê các trách nhiệm cho việc duy trì, bảo vệ và huỷ dữ liệu.
- Tạo bảng phân loại thông tin và giai đoạn sao lưu tương ứng của nó.
- Có văn bản về qui định trách nhiệm cho các trung tâm, phòng ban chịu trách nhiệm sao lưu dữ liệu nếu chúng tồn tại

Có ba kiểu sao lưu dự phòng chính hiện đang tồn tại:

- ***Sao lưu đầy đủ***: là sao lưu dự phòng hoàn chỉnh một máy chủ thư bao gồm hệ điều hành, các ứng dụng và dữ liệu lưu trữ trên máy chủ thư đó.
  - ✓ Thuận lợi của việc sao lưu dự phòng toàn bộ là chúng ta có một bản sao dự phòng đầy đủ (các tham số cấu hình, dữ liệu, ...), như vậy sẽ rất dễ cho việc khôi phục trang thái khi gặp sự cố.
  - ✓ Bất lợi của việc sao lưu dự phòng toàn bộ là vấn đề thời gian và nguồn tài nguyên để thực hiện.
- ***Sao lưu dự phòng tăng***: chỉ thực hiện sao lưu đối với dữ liệu có sự thay đổi so với lần sao lưu trước đó (có thể là sao lưu đầy đủ).
- ***Sao lưu dự phòng sai khác:*** thực hiện sao lưu dự phòng cả dữ liệu cũng như các tham số cấu hình đã bị thay đổi so với lần sao lưu dự phòng đầy đủ cuối cùng.

Trong ba kiểu sao lưu dự phòng trên, việc sao lưu dự phòng toàn bộ được thực hiện với chu kỳ dài thời gian hơn (thường là theo hàng tuần, hàng tháng hoặc khi xuất hiện ra sự thay đổi quan trọng), còn sao lưu dự phòng tăng và sao lưu dự phòng sai khác được thực hiện thường xuyên hơn (thường là theo ngày hoặc theo từng tuần).

Tần số của việc sao lưu dự phòng được quyết định bởi các yếu tố dưới đây:

- Sự thay đổi thông tin và các tham số cấu hình trên các máy chủ thư.
- Lượng dữ liệu sẽ được sao lưu dự phòng.
- Khả năng hỗ trợ của các thiết bị dự phòng.
- Thời gian có thể cho việc thực hiện sao lưu dự phòng.
- Tính quan trọng của dữ liệu.
- Mức đe dọa mà máy chủ thư gặp phải.
- Khả năng khôi phục lại dữ liệu mà không cần đến dữ liệu đã được sao lưu dự phòng.
- Các công cụ sao lưu dự phòng khác.

Khi thực hiện việc sao lưu dự phòng, cần thoả mãn một số tiêu chí dưới đây:

- Chỉ thực hiện đọc một lần.
- Phải có khả năng lưu trữ và kiểm tra tính đúng đắn của dữ liệu được sao lưu dự phòng.
- Phải có khả năng sắp xếp và gắn nhãn thời gian cho thông tin được sao lưu dự phòng.
- Hỗ trợ khả năng khai thác, tìm kiếm, thống kê dễ dàng đối với thông tin được sao lưu dự phòng.
- Duy trì ít nhất hai bản copy ở hai địa điểm địa lý khác nhau.

Quản trị từ xa một máy chủ thư

Một khuyến cáo rất quan trọng từ các chuyên gia là không nên cho phép việc quản trị các máy chủ thư từ xa khi chưa đánh giá hết các khả năng rủi ro có thể. Cấu hình an toàn nhất là không cho bất kỳ một sự quản trị nào từ xa (tất nhiên, điều này không thể áp dụng cho tất cả các tổ chức sử dụng thư điện tử trên thực tế). Rủi ro của việc quản trị từ xa phụ thuộc vào vị trí của máy chủ thư trong mạng chung. Đối với một máy chủ thư được đặt sau bức

tường lửa, việc quản trị từ xa hoặc cập nhật nội dung có thể được thực hiện từ các máy mạng bên trong mà không làm phát sinh thêm rủi ro. Nói chung trong mọi trường hợp không nên cho phép việc quản trị máy chủ thư từ một vị trí nằm ngoài mạng được bảo vệ.

Nếu một tổ chức hay công ty nào đó có nhu cầu quản trị hoặc cập nhật thông tin từ xa trên một máy chủ thư, cần đảm bảo rằng các bước dưới đây được thực hiện trong điều kiện an toàn có thể:

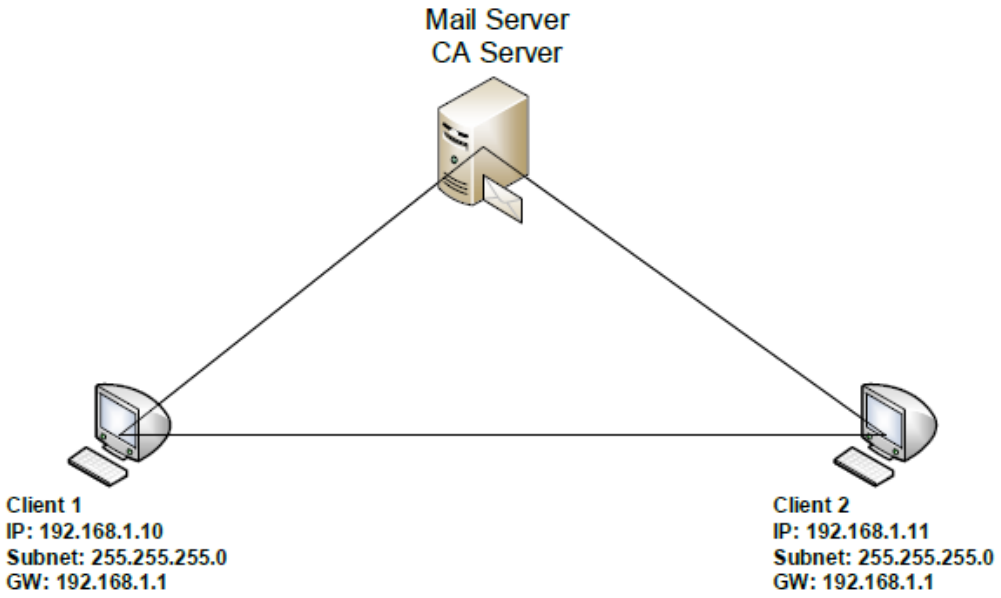
- Sử dụng lược đồ xác thực an toàn cao (như sử dụng mật mã khoá công khai, xác thực hai yếu tố)
  - ✓ Hạn chế các máy có thể được sử dụng để quản trị từ xa hoặc cập nhật nội dung trên máy chủ thư.
  - ✓ Hạn chế thông qua các user được uỷ quyền.
  - ✓ Hạn chế thông qua địa chỉ IP.
  - ✓ Hạn chế ngay cả với các máy thuộc mạng trong.
- Sử dụng các giao thức an toàn hơn (như secure shell, HTTPS,) và không sử dụng các giao thức có độ an toàn thấp (như Telnet, FTP, HTTP).
- Cấp quyền tối thiểu cho việc quản trị từ xa hay cập nhật nội dung
- Không cho phép việc quản trị từ xa trên Internet xuyên qua bức tường lửa trừ khi được thực hiện thông qua một cơ chế bảo mật mạnh, ví dụ như đường hầm mạng riêng ảo.
- Thay đổi các tài khoản và mật khẩu mặc định của các ứng dụng hay tiện ích quản trị từ xa.
- Không ánh xạ bất kỳ một tệp nào ở mạng trong từ máy chủ thư.

CÁC BÀI THỰC HÀNH

1. Thực hành thiết lập an toàn cho dịch vụ thư tín điện tử

Mục đích bài thực hành: sử dụng kỹ thuật mật mã để mã hóa thư điện tử nhằm đảm bảo tính bí mật và toàn vẹn khi gửi và nhận thư điện tử.

Bước 1: Chuẩn bị theo mô hình sau:



Máy chủ	IP: 192.168.1.2 Subnet: 255.255.255.0 GW: 192.168.1.1 DNS: 192.168.1.2
Client 1	IP: 192.168.1.10 Subnet: 255.255.255.0 GW: 192.168.1.1 DNS: 192.168.1.2
Client 2	IP: 192.168.1.11 Subnet: 255.255.255.0 GW: 192.168.1.1 DNS: 192.168.1.2

Bước 2:

- Tại máy chủ thực hiện cài đặt dịch vụ DNS, mục đích của dịch vụ này là cung cấp tên miền cho người dùng khi gửi mail.
- Cài đặt dịch vụ web: dịch vụ này cung cấp khả năng yêu cầu chứng chỉ bởi CA thông qua trình duyệt web.

- Cài đặt dịch vụ Certification Authority (CA): dịch vụ này cung cấp chứng chỉ bảo mật cho người dùng. Trong chứng chỉ có chứa thông tin người dùng và khóa mã để mã hóa cho mail của người dùng.

Bước 3: Tạo tài khoản người dùng mail trong mail server

Bước 4: Tại máy trạm Client1 và Client 2 sử dụng Outlook express đăng nhập bằng tài khoản người dùng là user1 và user2 tương ứng đã tạo trong máy chủ mail.

Bước 5: Thực hiện kiểm tra gửi và nhận thư bằng cách từ user1 gửi thư cho user2.

Tiếp tục ta sử dụng mật mã để mã hóa và xác thực thư.

Bước 6: Cấp chứng chỉ cho 2 máy trạm Client1 và Client2

- Tại máy trạm Client1 và Client2 sử dụng trình duyệt IE để truy cập vào máy chủ CA.
- Yêu cầu chứng chỉ cho 2 người dùng user1 và user2.
- Nhập thông tin người dùng, tiến hành submit và cài đặt chứng chỉ cho người dùng user1 và user2.
- Soạn mail và sử dụng chức năng ký số và mã hóa cho mail này.

Kết quả của bài thực hành là hướng dẫn người dùng sử dụng chức năng ký số và mã hóa cho thư điện tử.

2. Thực hành thiết lập an toàn cho dịch vụ Web

Thực hiện thiết lập an toàn cho dịch vụ Web chạy trên máy chủ Apache theo các bước sau:

Bước 1: Cài đặt an toàn cho máy chủ Web Apache

Bước 2: Lựa chọn những module cần thiết cho Apache bao gồm:

- httpd_core: Chứa các chức năng cốt lõi của Apache, cần thiết cho bất cứ Apache nào.

- mod_access: Cung cấp chế độ điều khiển dựa trên tên máy, địa chỉ IP, hoặc các tính chất yêu cầu thuộc về các clients. Bởi vì module này cần cho các điều khiển "order", "allow" và "deny", cần được cho phép.
- mod_auth: Cần thiết để ứng dụng vấn đề khai báo người dùng cho việc sử dụng các hồ sơ nguyên bản (khai báo căn bản cho HTTP).
- mod_dir: Cần thiết để tìm kiếm và phục vụ các hồ sơ thư mục: "index.html", "default.htm", v..v..
- mod_log_config: Cần thiết để ứng hiệu báo cáo những yêu cầu thực hiện đến server.
- mod_mime: Cần thiết để chỉnh lý nhóm chữ cái, mã hoá nội dung, tùy tác, ngôn ngữ nội dung và các loại MIME đại diện cho các loại tài liệu.

Bước 3: Phân quyền cho các tệp tin cấu hình Apache như: httpd.conf với quyền: chủ sở hữu có quyền đọc, ghi; nhóm chỉ có quyền đọc; người dùng khác chỉ có quyền đọc.

Bước 4: Cài đặt thêm các module bảo mật cho apache như:

- ModSecurity: Có chức năng lọc các request với http header, chống các kỹ thuật tấn công SQL injection, paths, parameters
- Mod reqtimeout: Chống tấn công từ chối dịch vụ lên máy chủ Web Apache

Chương 4.
THIẾT LẬP AN TOÀN CHO MẠNG KHÔNG DÂY

4.1. XÂY DỰNG CHÍNH SÁCH AN TOÀN CHO MẠNG KHÔNG DÂY

Nhiều công nghệ có cách tiếp cận cài đặt đơn giản, không đòi hỏi nhiều về nỗ lực thiết kế, chúng được gọi là cách tiếp cận đơn giản. Kết quả là, người ta có thể hoàn thành việc cài đặt chỉ với vài lần nhấn bấm Next và Finish mà không cần phải suy nghĩ về việc lập kế hoạch và thiết kế, cũng như vận hành các hoạt động công nghệ. Không phải tất cả các công nghệ đều được cài đặt theo phương pháp đơn giản trên, đặc biệt là các WLAN, nếu người dùng muốn chúng được an toàn. Ngày nay, WLAN có thể dễ dàng được cài đặt trên hầu hết các hệ thống mạng và theo mặc định phần lớn trong số chúng là không an toàn, do đó sẽ làm suy yếu hệ thống an ninh của tổ chức nếu chúng không được lên kế hoạch một cách chặt chẽ. Ví dụ, có những người nhận xét rằng mạng không dây của họ là an toàn bởi vì nó đã được cài đặt sau tường lửa. Tuy nhiên, sự thật là phía sau tường lửa cũng có khả năng bị tấn công cao vào mạng không dây. Việc quy hoạch mạng không dây sẽ làm sáng tỏ vấn đề này. Bước đầu tiên trong quy hoạch mạng không dây là xác định chính sách an ninh mà mạng không dây cần phải tuân theo.

Trước khi thiết kế một mạng không dây an toàn, người quản trị phải xác định được các phương tiện không dây an toàn cần thiết cho công ty, tổ chức. Chính sách an ninh mạng không dây phải định nghĩa các tiêu chuẩn, các chính sách và các thủ tục cụ thể sẽ được tuân theo để đảm bảo rằng bất kỳ mạng không dây nào đều được thực hiện trong khả năng an toàn nhất có thể.

Đồng thời, điều quan trọng là phải phân biệt được chính sách bảo mật không dây và các thủ tục thực thi. Cách dễ dàng để nhận biết đó là chính sách bảo mật sẽ cho biết phải làm gì bằng các chi tiết được nêu cụ thể trong các văn bản.Ví dụ, chính sách bảo mật không dây yêu cầu phải xác thực bằng thẻ thông minh mà không cung cấp các chi tiết cụ thể về các thủ tục thực thi để cài đặt và cấu hình RSA SecureID. Trong chương này, chúng ta sẽ xem xét

cách xác định các yếu tố của các thành phần chính sách bảo mật mạng không dây, bao gồm:

- Người nào có thẩm quyền đối với các mạng không dây
- Các yêu cầu phân đoạn mạng không dây
- Các yêu cầu về phần cứng và phần mềm
- Lệnh cấm trên thiết bị và phần mềm không dây không được cấp phép
- Phương pháp xác thực
- Phương pháp mã hóa
- Các yêu cầu về đăng nhập và tính toán
- Các yêu cầu về định danh dịch vụ (SSID)
- Các yêu cầu bảo mật cho điểm truy cập không dây (WAP)
- Chính sách thực thi

Xác định người có thẩm quyền đối với mạng không dây

Một trong những vấn đề quan trọng nhất của tất cả các cam kết an ninh mạng là phải xác định một cách rõ ràng và dứt khoát người có thẩm quyền đối với cam kết đó. Mạng không dây cũng không ngoại lệ. Người được lựa chọn để chịu trách nhiệm quản lý mạng không dây phải là người có khả năng lãnh đạo, tầm nhìn xa, và có thể đưa ra quyết định để đảm bảo rằng các biện pháp an ninh thích hợp đã được thực hiện. Ngoài ra, nếu tổ chức có các hệ thống mạng không dây chi nhánh hoặc kết nối từ xa, người quản trị cần phải xác định người có thẩm quyền đối với các hệ thống đó và làm thế nào mà chúng có thể phù hợp với hệ thống phân cấp toàn cầu.

Xác định các yêu cầu về phân đoạn mạng không dây

Xác định các yêu cầu phân đoạn mạng không dây là khía cạnh khó khăn hơn khi thiết kế mạng không dây. Phân tách mạng không dây từ mạng có dây để đảm bảo rằng một hành vi xâm phạm trên mạng không dây không được tự động cho phép truy cập vào mạng có dây. Nghĩa là, mạng không dây phải được coi là mạng không tin cậy, trong khi mạng có dây được coi là mạng tin cậy.

Đồng thời, việc cung cấp mạng không dây tại một địa điểm từ xa có thể khiến việc thiết kế gặp nhiều khó khăn hơn. Ví dụ, phân đoạn mạng WLAN trong các văn phòng trung tâm với một mạng VLAN chuyên dụng là tương đối dễ dàng, nhưng để làm như vậy tại văn phòng chi nhánh có thể gặp nhiều khó khăn hơn và khá tốn kém. Nếu văn phòng chi nhánh có kết nối đầy đủ với hệ thống mạng của tổ chức, thì việc phân chia tại các chi nhánh từ xa cũng không kém quan trọng so với việc phân chia tại trụ sở chính.

Thay vì tìm cách xác định vị trí cần phải phân đoạn mạng trong hệ thống mạng không dây, chính sách an ninh không dây nên xác định thời điểm cần thiết cũng như phương pháp để thực hiện phân đoạn mạng. Ví dụ như sử dụng mạng LAN ảo đơn giản (VLAN), sử dụng VLAN với danh sách điều khiển truy cập (ACL), sử dụng VLAN với tường lửa, hoặc thậm chí yêu cầu phân đoạn với tất cả các kết nối không dây và áp dụng công nghệ mạng riêng ảo (VPN) để cung cấp truy cập. Khuyến nghị an toàn nhất, như bạn sẽ thấy sau trong chương tiếp theo, là thực hiện phân đoạn vật lý và sử dụng VPN để cung cấp truy cập vào mạng tin cậy.

Xác định các yêu cầu về phần cứng và phần mềm

Tiêu chuẩn hóa là một yếu tố chủ chốt của an toàn mạng. Tiêu chuẩn hóa các phần cứng và phần mềm được sử dụng trong mạng không dây giúp quản lý và duy trì hệ thống tốt hơn. Nó cũng làm giảm các trường hợp thiết bị không tương thích (có thể dẫn đến giảm độ an toàn) và hỗ trợ xử lý sự cố hiệu quả hơn bằng cách khiến việc so sánh các thiết bị trở nên đơn giản hơn để xác định sự khác biệt giữa các hệ thống. Cuối cùng, tiêu chuẩn hóa giúp việc hỗ trợ mạng không dây trở nên dễ dàng hơn ngay cả khi các kỹ thuật viên không nắm được nhiều loại phần cứng và các phiên bản phần mềm khác nhau. Ví dụ, chính sách an toàn không dây nên xác định các nhà cung cấp phần cứng cụ thể và các mô hình sẽ được hỗ trợ trong hệ thống mạng. Đồng thời cũng cần cung cấp một phiên bản phần mềm yêu cầu tối thiểu, cho phép các nhân viên kỹ thuật nâng cấp phần mềm theo yêu cầu để giải quyết vấn đề an ninh và các vấn đề khác mà không cần phải tốn thời gian để cập nhật cả chính sách bảo mật chỉ để triển khai một bản vá mới.

Lệnh cấm tất cả thiết bị và phần mềm không dây không được cấp phép

Việc cấm tất cả các thiết bị và phần mềm không dây, được triển khai mà không được phê chuẩn IT trước, cung cấp thẩm quyền cần thiết để định vị và loại bỏ bất kỳ điểm truy cập giả mạo nào của các cá nhân cụ thể.

Xác định phương pháp xác thực

Mạng không dây rất dễ bị tấn công và truy cập vào mạng nội bộ, do đó việc sử dụng một phương pháp xác thực là rất cần thiết. Phương pháp xác thực thích hợp sẽ đảm bảo rằng chỉ có người dùng được ủy quyền mới có thể kết nối vào mạng. Có một vài yếu tố mà chính sách an toàn không dây cần phải giải quyết, bao gồm các tiêu chuẩn xác thực phải tuân thủ, các phương pháp xác thực và các yêu cầu triển khai.

Thứ nhất, chính sách an toàn không dây cần xác định tiêu chuẩn xác thực thích hợp. Áp dụng một tiêu chuẩn xác thực không độc quyền sẽ giúp công ty, tổ chức giảm bớt nguy cơ bị kìm hãm bởi một nhà cung cấp nhất định. Thứ hai, chính sách an toàn không dây cần xác định phương pháp xác thực sẽ được thực hiện. Ví dụ, người quản trị cần phải xác định xem công ty, tổ chức sẽ sử dụng chứng chỉ, khóa chia sẻ trước hay xác thực người dùng… Một khía cạnh khác của phương pháp xác thực đó là tiến hành xác thực lẫn nhau (máy khách với máy chủ và ngược lại) hay chỉ đơn giản là xác thực các hệ thống đơn lẻ. Xác thực lẫn nhau sẽ đem lại tính bảo mật cao hơn cho hệ thống.

Sau đây là một vài phương pháp xác thực phổ biến được dùng cho mạng không dây:

- Khóa chia sẻ trước (Preshared keys – PSKs): người quản trị sử dụng các khóa tự tạo để nhận dạng người dùng. PSKs cũng thường được dùng để thiết lập các hàm mã hóa.
- IEEE 802.1x: chuẩn giao thức xác thực mở rộng PPP (EAP), được định nghĩa trong RFC 2284. Thông thường, IEEE 802.1x sử dụng các máy chủ xác thực như RADIUS hoặc TACACS+ để xác thực người dùng với điểm truy cập không dây.

- Chứng chỉ (Certificates): Một kiểu xác thực điện tử, sử dụng một hạ tầng khóa công khai (PKI) và các thẩm quyền chứng chỉ tin cậy (CA) để nhận dạng người dùng hoặc thiết bị. Chứng chỉ thường chứa thông tin cần thiết để mã hóa và giải mã dữ liệu.
- Xác thực người dùng (User authentication): Chuẩn sử dụng username/password để xác thực người dùng. Phương pháp xác thực này thường được dùng như một thành phần của 802.1x thay vì triển khai độc lập.

Cuối cùng, chính sách an toàn cần phải xác định giải pháp thực hiện xác thực. Ví dụ, cần chỉ ra người dùng và nhóm ở cấp độ nào được sử dụng, làm thế nào để quản lý mật khẩu, phân phối và quản lý chứng chỉ ra sao...

Xác định phương pháp mã hóa

Mã hóa là phương pháp thứ hai, sau xác thực, được dùng để bảo vệ mạng không dây. Xác thực sẽ xác nhận của người dùng được cấp quyền và cho phép người đó truy cập vào mạng. Trong khi đó, mã hóa đảm bảo rằng dữ liệu được truyền một cách bí mật và toàn vẹn, bằng cách sử dụng các cấu hình bổ sung có sẵn cho các giao thức mã hóa.

Chính sách an toàn cần xác định rõ thời điểm cần thiết cũng như phương thức thực hiện mã hóa. Có một vài phương pháp mã hóa có sẵn cho mạng không dây như WEP, WAP, 802.11i và mã hóa dựa trên VPN. Khi xác định phương pháp mã hóa, thực hiện hạn chế các chi phí bổ sung khi truyền dữ liệu bằng cách sử dụng nhiều phương pháp mã hóa. Ví dụ, nếu chính sách an toàn của công ty, tổ chức yêu cầu tất cả các kết nối không dây phải sử dụng VPN để truy cập vào mạng tin cậy, thì không cần phải sử dụng thêm một giải pháp mã hóa không dây cụ thể nào, vì công nghệ VPN đã cung cấp cả mã hóa và xác thực.

Có 4 giải pháp mã hóa thông dụng thường dùng cho mạng không dây:

- WEP: được thiết kế để đảm bảo tính riêng tư của dữ liệu trong mạng không dây. Đáng tiếc là WEP đã bị bẻ khóa và không nên sử dụng.

- WPA: là thành phần của chuẩn 802.11i, được phát triển để giải quyết các vấn đề bảo mật liên quan đến WEP trước khi chuẩn 802.11i được thông qua. WPA sử dụng tập hợp nhiều công nghệ để giảm bớt các vấn đề mà WEP mắc phải: chuẩn xác thực 802.1x giải quyết các vấn đề về xác thực; giao thức toàn vẹn khóa thời gian (TKIP) xử lý các vấn đề về mã hóa; và MIC giúp đảm bảo tính toàn vẹn cho các bản tin.
- 802.11i: ngoài các công nghệ dùng trong WPA, 802.11i còn sử dụng các công nghệ mã hóa mạnh hơn như chuẩn mã hóa tiên tiến (AES). Từ khi được thông qua vào năm 2004, 802.11i đã trở thành giải pháp mã hóa được yêu thích cho mạng không dây mà không sử dụng VPN.
- Mã hóa dựa trên VPN: dùng để xác thực một máy khách không dây và sử dụng VPN để truy cập vào mạng tin cậy. Mã hóa dựa trên VPN thường triển khai IPSec trên giao thức đường hầm lớp 2 (L2TP), IPSec đơn thuần, hoặc giao thức đường hầm kết nối điểm đến điểm (PPTP), mã hóa điểm đến điểm của Microsoft (MPPE). Khi một máy khách không dây sử dụng VPN để truy cập vào mạng tin cậy, thì hầu như không cần thiết phải sử dụng thêm một dạng mã hóa không dây cụ thể nào như WEP, WPA hay 802.11i.

Xác định các yêu cầu về đăng nhập và kiểm toán

Ghi nhật ký (logging) và kiểm toán (*accounting)* là những thành phần quan trọng được dùng để giám sát các hoạt động trên mạng không dây cũng như phát hiện việc sử dụng trái phép. Accounting giúp biết danh sách người dùng đang kết nối với mạng không dây kèm theo thời điểm họ kết nối. Accounting thường được triển khai cùng với các công nghệ như RADIUS hoặc TACACS +.

Trong khi đó, logging có chức năng giám sát người dùng, tìm và khắc phục lỗi, và phát hiện các sử dụng sai trái. Ví dụ, người quản trị có thể sử dụng các bản ghi (log) để phát hiện những lần thử xác thực không thành công,

từ đó có thể nhận biết đối tượng không đủ thẩm quyền đã cố gắng truy cập vào hệ thống. Tương tự như vậy, có thể sử dụng các log để nhận dạng và theo dõi người đã truy cập thành công vào hệ thống mạng.

Ngoài việc xác định công nghệ logging và accounting thích hợp sẽ được sử dụng, chính sách an toàn cũng cần chỉ ra tần suất đọc log, ai được phép đọc chúng, và làm thế nào để cảnh báo khi xảy ra các sự kiện quan trọng.

Xác định các yêu cầu định danh dịch vụ

Định danh dịch vụ (SSID) được dùng để nhận dạng và đặt tên cho một mạng WLAN duy nhất. Nó cho phép người dùng truy cập vào mạng không dây có thể kết nối với điểm truy cập không dây (WAP) để truy cập vào mạng. Tuy nhiên, việc quảng bá SSID khiến cho WAP dễ dàng bị các tin tặc phát hiện và tấn công. Do đó, chính sách an toàn không dây cần xác định xem sẽ quảng bá SSID hay là không. Ngoài ra, cũng nên chỉ ra một quy ước để đặt tên cho WAP, nhưng không nên quá rõ ràng đến nỗi bất cứ ai cũng có thể nhận ra. Ví dụ, một tin tặc đang cố gắng tiếp cận với tập đoàn Cocacola để ăn cắp dữ liệu. Nếu tin tặc đó dò tìm được một WAP có SSID là Cocacola_Wap, hắn có thể dễ dàng kết luận rằng đây là một điểm tấn công cần truy cập và khai thác.

Xác định các yêu cầu bảo mật WAP

Giống như đối với tất cả các thiết bị mạng khác, chính sách an toàn không dây cần đưa ra các yêu cầu bảo mật WAP nhằm đảm bảo an toàn cho thiết bị cả về mặt vật lý lẫn logic. Ngoài ra, chính sách bảo mật cũng phải làm rõ làm thế nào để cấp quyền truy cập quản trị, ai được phép khởi tạo một phiên quản trị với thiết bị, và ai có thể cấu hình thiết bị đó. Xác định phương pháp cấu hình một cơ chế an toàn cho thiết bị bất kỳ cũng là một yêu cầu cần thiết đối với chính sách an toàn không dây.

Xác định chính sách thực thi

Để một chính sách an toàn bất kỳ có thể làm việc hiệu quả, nó phải có một chính sách thực thi rõ ràng, trong đó bao gồm các cơ chế kỹ thuật được

sử dụng. Chẳng hạn như sử dụng thiết bị phần cứng để dò tìm và phát hiện các mạng không dây giả mạo. Ngoài ra, chính sách thực thi cũng cần đưa ra biện pháp xử lý đối với các hành vi vi phạm chính sách bảo mật. Các biện pháp này phải được trình bày một cách rõ ràng bằng văn bản. Làm việc với đội ngũ pháp lý của công ty để đảm bảo rằng các chính sách thực thi là phù hợp về mặt pháp lý.

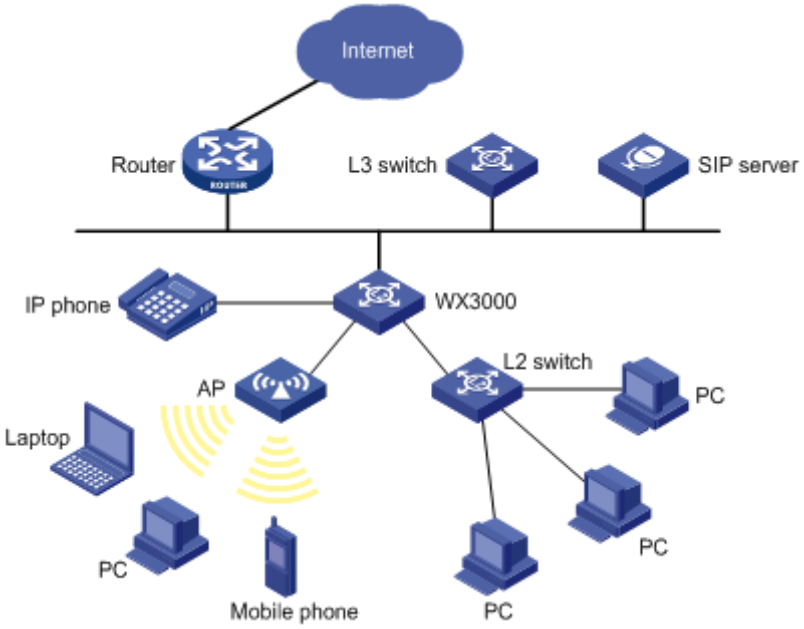
4.2. THIẾT KẾ MÔ HÌNH CHO MẠNG LAN KHÔNG DÂY

Khi viết các chính sách an toàn, người quản trị cần phải xác định làm thể nào thể triển khai mạng không dây trong hệ thống mạng của công ty, tổ chức. Bước tiếp theo là thiết kế một mô hình WLAN an toàn. Có bốn nguyên tắc chính khi thiết kế mô hình mạng WLAN:

- Kết hợp mạng không dây và mạng hữu tuyến
- Thiết lập các phân vùng mạng
- Sử dụng VPN để kết nối mạng không dây với mạng hữu tuyến
- Xây dựng mạng WLAN cho văn phòng từ xa

4.2.1. Kết hợp mạng không dây và mạng hữu tuyến

Mặc dù mô hình kết hợp mạng không dây và mạng có dây có độ an toàn kém nhất, nó vẫn cần phải được thực hiện, bởi vì trong nhiều trường hợp lý do tài chính có thể sẽ ngăn cản việc triển khai một mô hình an toàn hơn. Hình 4.1 mô tả một sơ đồ mạng kết hợp, mạng WLAN được kết nối trực tiếp đến cơ sở hạ tầng của mạng LAN có dây.



Hình 4.1 - Mô hình mạng kết hợp WLAN và LAN

Các thiết bị kết nối qua WAP được kết nối trực tiếp với cùng mạng mà các khách hàng và máy chủ khác kết nối tới. Trong dạng thiết kế này, vì không có các nguồn tài nguyên cụ thể đáng tin cậy (có dây) và không tin cậy (không dây), nên điều quan trọng là phải có các biện pháp dự phòng để đảm bảo rằng chỉ cho phép các kết nối thẩm quyền tới mạng không dây. Khi thiết kế mô hình này, khuyến cáo thực hiện những điều sau đây:

- Cơ chế xác thực an toàn: Ngoại trừ WAP, không có gì đảm bảo rằng giữa người dùng không dây và các tài nguyên mạng có dây thực hiện các cơ chế xác thực chặt chẽ. Khuyến cáo chỉ thực hiện cơ chế xác thực 802.1x.
- Cơ chế mã hóa nghiêm ngặt nhất: Chỉ duy nhất việc bảo vệ dữ liệu truyền qua mạng không dây sẽ được cung cấp bởi cấu hình WAP. Do đó, thực hiện 802.11i cho việc mã hóa không dây, hoặc WPA nếu thiết bị không hỗ trợ 802.11i. Chú ý không bao giờ sử dụng WEP trong trường hợp này, vì WEP đã bị bẻ khóa.
- Đăng nhập rộng: Như đã đề cập ở phần trước, đăng nhập là một khía cạnh quan trọng để phát hiện việc sử dụng sai. Do người dùng không dây kết nối trực tiếp tới mạng có dây nên người quản trị cần đảm bảo rằng đã cấu hình đăng nhập rộng và cảnh báo để

sớm phát hiện khả năng xâm phạm cũng như thông tin pháp lý để điều tra sự cố.

- Giới hạn địa chỉ MAC: Giới hạn địa chỉ MAC cho phép đưa ra các địa chỉ MAC cụ thể được phép kết nối tới WAP. Trong khi các địa chỉ MAC có thể giả mạo, nó vẫn cung cấp một giải pháp bổ sung đủ an toàn để đảm bảo rằng chỉ những hệ thống được cho phép cụ thể bởi người quản trị mới được kết nối tới hạ tầng WLAN.
- Cấu hình SSID an toàn: Để ví trí WAP không bị phát hiện, cần tắt bỏ tính năng phát SSID khi cấu hình WAP. Trong khi hầu hết các thẻ mạng không dây (Wireless NIC – WNIC) vẫn có thể kết nối đến WAP bằng cách nhập thủ công chuỗi SSID chính xác, thì một số WNIC lại gặp vấn đề với phương pháp này. Ngoài ra, để tắt tính năng phát SSID, người quản trị không được phép sử dụng tên công ty hoặc vị trí cụ thể trong SSID, vì chúng có thể được sử dụng bởi tin tặc để dò tìm các tài nguyên tấn công.

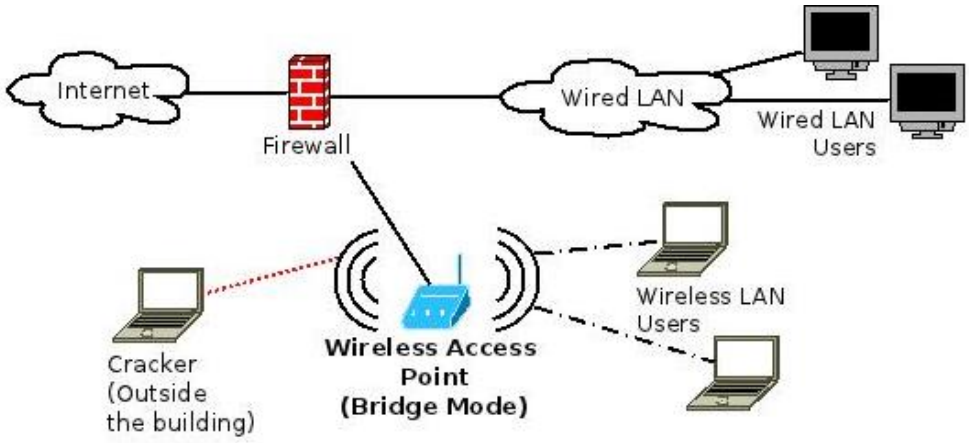
4.2.2. Thiết lập các phân vùng mạng

Phân chia hệ thống mạng thành các phân vùng đáng tin cậy và không tin cậy, trong đó mạng hữu tuyến là mạng đáng tin cậy và mạng không dây là mạng không tin cậy. Mục đích của loại hình thiết kế mạng là cung cấp một phương pháp để hạn chế lưu lượng truy cập từ các mạng không tin cậy tới mạng đáng tin cậy. Có hai phương pháp chủ yếu để phân vùng mạng đáng tin cậy và không tin cậy:

- Thực hiện phân vùng vật lý
- Thực hiện phân vùng logic bằng VLAN

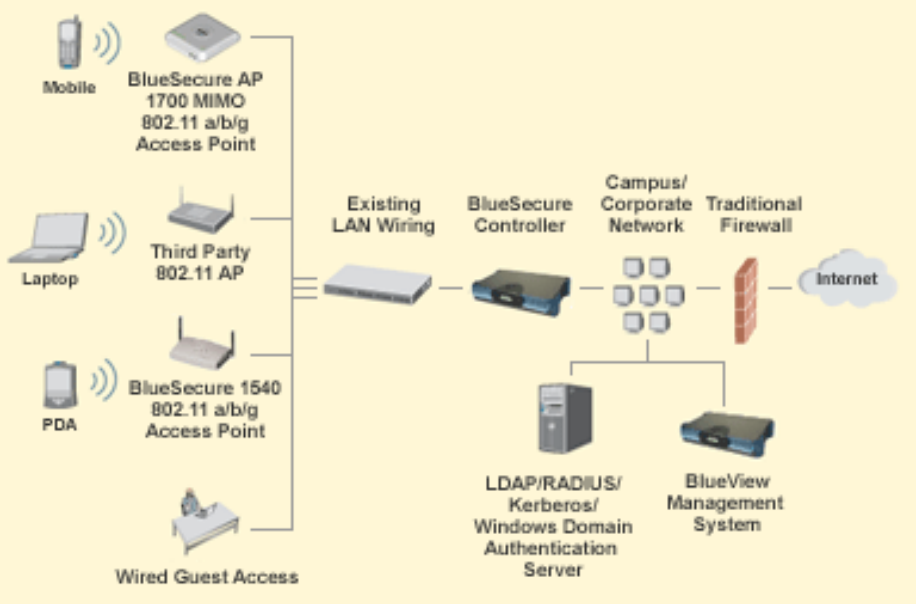
Thực hiện phân vùng vật lý

Thực hiện phân chia vật lý cũng đơn giản như việc đảm bảo rằng các mạng WLAN và mạng LAN có dây có thể tách rời nhau bởi một thiết bị định tuyến hay một bức tường lửa. Trong cấu hình này, các mạng WLAN không khác gì một phân vùng DMZ. Hình 4.2 minh họa mô hình thiết kế này.



Hình 4.2 – Phân vùng vật lý WLAN và mạng hữu tuyến

Trong thiết kế này, vẫn nên tuân theo tất cả các khuyến nghị thiết kế cho một mạng lưới thống nhất. Bây giờ, câu hỏi đặt ra là, "Nếu tôi thực hiện điều tương tự, tại sao không triển khai một mạng thống nhất, nơi mà việc quản lý trở nên đơn giản và dễ dàng hơn?" Điều mà phân vùng vật lý mang lại là khả năng kiểm soát chặt chẽ hơn đối với các lưu lượng được phép truy cập giữa các mạng đáng tin cậy và mạng không tin cậy. Bằng cách sử dụng mô hình mạng phân vùng, việc có thể cấu hình ACL (Access Control List – danh sách điều khiển truy cập) tại các bộ định tuyến hoặc tường lửa, cho phép lưu lượng truy cập vào các thiết bị trong mạng tin cậy qua các cổng cụ thể. Ví dụ, nếu thiết bị không dây cần truy cập vào chỉ có sáu máy chủ, người quản trị có thể cấu hình một ACL chỉ cho phép lưu lượng truy cập đến sáu máy chủ này. Ngoài ra, có thể hạn chế việc truy cập đến sáu máy chủ trên qua các cổng cụ thể của giao thức TCP hoặc UDP bằng cách sử dụng các ứng dụng. Hình 4.3 là một thiết kế mạng WLAN chi tiết mà người sử dụng thiết kế dự phòng để cung cấp truy cập không dây an toàn và tính sẵn sàng cao tới mạng đáng tin cậy.



Hình 4.3 – Phân vùng WLAN và mạng hữu tuyến sử dụng tường lửa

Trong thiết kế này, các mạng WLAN được xem như một DMZ, bao gồm việc triển khai các IDS sensor cả hai phía trước và phía sau tường lửa để cung cấp khả năng giám sát và báo cáo mở rộng. Bất kỳ một mong muốn truy cập vào các nguồn tài nguyên nội bộ nào đều phải truyền qua bức tường lửa, và phải được các ACL thông qua.

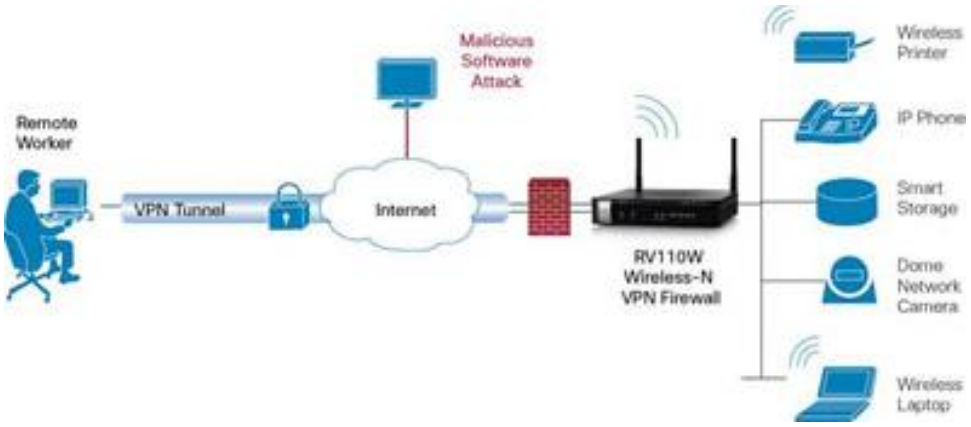
Thực hiện phân vùng logic bằng VLAN

Mặc dù phân vùng vật lý được coi là phương pháp phân vùng an toàn nhất, nhưng cũng là phương pháp tốn kém nhất vì nó thường đòi hỏi các tài nguyên phần cứng bổ sung. Để giảm chi phí, có thể sử dụng VLAN để cung cấp một mức độ bảo mật tương tự trong khi vẫn tận dụng được các tài nguyên phần cứng có sẵn. Để kết nối các VLAN với nhau đòi hỏi phải có một bộ định tuyến hoặc tường lửa, được cấu hình sẵn các ACL để đảm bảo an toàn cho các VLAN.

4.2.3. Kết nối mạng không dây với mạng hữu tuyến sử dụng VPN

Mô hình thiết kế an toàn nhất để cung cấp truy cập vào mạng đáng tin cậy là sử dụng VPN, công nghệ mạng riêng ảo rất an toàn và đáng tin cậy, kết hợp với các mạng WLAN. Trong thiết kế này, tất cả lưu lượng muốn truy cập vào mạng đáng tin cậy phải đi qua một VPN, do đó đảm bảo rằng kết nối đã

được chứng thực và các dữ liệu được bảo vệ. Hình 4.4 mô tả một cấu trúc liên kết mạng WLAN chi tiết sử dụng truy cập VPN.



Hình 4.4 – Mô hình WLAN sử dụng truy cập VPN

Các khách hàng không dây trong trường hợp này được cấu hình với các máy khách VPN thích hợp. Vì bản chất của VPN là đảm bảo lưu lượng đi qua mạng tin cậy, nên không cần thiết phải luôn sử dụng các biện pháp an ninh không dây như 802.1x hoặc 802.11i. Mạng không dây trong trường hợp này thực sự trở thành một phương tiện trung gian không an toàn, cho phép các khách hàng thiết lập kết nối VPN với mạng tin cậy, ví dụ như một khách hàng từ xa có thể thiết lập một kết nối VPN thông qua mạng Internet.

4.2.4. Xây dựng mạng WLAN cho văn phòng từ xa

Vì cơ sở hạ tầng thường có các văn phòng trung tâm, nên tương đối dễ dàng để tuân thủ các khuyến nghị thiết kế được cung cấp từ trước. Các văn phòng, chi nhánh từ xa thường có vấn đề trong việc thiếu cơ sở hạ tầng hoặc nhân viên kỹ thuật thích hợp để thực hiện các thiết kế tương tự. Ví dụ, hầu hết các văn phòng chi nhánh không có các bộ tập trung VPN nội bộ để cung cấp cho các dịch vụ VPN. Tại cùng một thời điểm, *tin tặc* có thể vừa truy cập vào mạng WLAN tại các văn phòng từ xa vừa kết nối với văn phòng chính của tổ chức, như là truy cập vào cùng các nguồn tài nguyên giống nhau.

Mặc dù phương pháp thiết kế này được hoàn toàn chấp nhận trong một số trường hợp, song nó vẫn bị coi là kém an toàn hơn so với các lựa chọn thay thế. Có một số cách tương đối rẻ tiền để có thể phân vùng vật lý cho các mạng có dây và không dây của tổ chức, như sử dụng Cisco PIX 501 có khả năng

chấm dứt một số ít các kết nối VPN. Điều này không chỉ cung cấp việc phân vùng vật lý hay logic, mà còn cho phép yêu cầu sử dụng VPN cho tất cả các truy cập không dây vào mạng đáng tin cậy.

4.3. THIẾT LẬP AN TOÀN CHO MẠNG LAN KHÔNG DÂY

4.3.1. Thiết lập chức năng mã hóa

4.3.1.1 WEP

WEP (Wired Equivalent Privacy) có nghĩa là bảo mật không dây tương đương với có dây. Thực ra, WEP đã đưa cả xác thực người dùng và đảm bảo an toàn dữ liệu vào cùng một phương thức không an toàn. WEP sử dụng một khoá mã hoá không thay đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khoá mã hoá, nên độ dài khoá chỉ còn 40 bit hoặc 104 bit) được sử dụng để xác thực các thiết bị được phép truy cập vào trong mạng và cũng được sử dụng để mã hoá truyền dữ liệu.

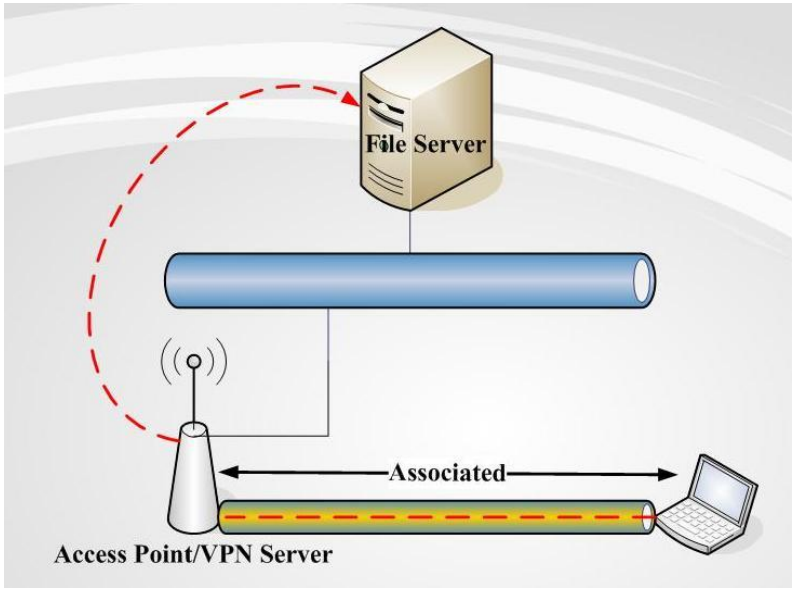
Rất đơn giản, các khoá mã hoá này dễ dàng bị phá bởi thuật toán brute-force và kiểu tấn công thử lỗi (trial-and-error). Các phần mềm miễn phí như Airsnort hoặc WEPCrack sẽ cho phép tin tặc có thể phá vỡ khoá mã hoá nếu họ thu thập đủ từ 5 đến 10 triệu gói tin trên một mạng không dây. Với những khoá mã hoá 128 bit cũng không khá hơn: 24 bit cho khởi tạo mã hoá nên chỉ có 104 bit được sử dụng để mã hoá, và cách thức cũng giống như mã hoá có độ dài 64 bit nên mã hoá 128 bit cũng dễ dàng bị bẻ khoá. Ngoài ra, những điểm yếu trong những vector khởi tạo khoá mã hoá giúp cho tin tặc có thể tìm ra mật khẩu nhanh hơn với ít gói thông tin hơn rất nhiều.

Không dự đoán được những lỗi trong khoá mã hoá, WEP có thể được tạo ra cách bảo mật mạnh mẽ hơn nếu sử dụng một giao thức xác thực mà cung cấp mỗi khoá mã hoá mới cho mỗi phiên làm việc. Khoá mã hoá sẽ thay đổi trên mỗi phiên làm việc. Điều này sẽ gây khó khăn hơn cho tin tặc thu thập đủ các gói dữ liệu cần thiết để có thể bẻ gãy khoá bảo mật.

WLAN VPN

Mạng riêng ảo VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chắn dữ liệu khỏi các truy cập trái phép. VPN tạo ra một tin cậy cao thông

qua việc sử dụng một cơ chế bảo mật như IPSec (Internet Protocol Security). IPSec dùng các thuật toán mạnh như Data Encryption Standard (DES) và Triple DES (3DES) để mã hóa dữ liệu và dùng các thuật toán khác để xác thực gói dữ liệu. IPSec cũng sử dụng thẻ xác nhận số để xác nhận khóa mã (public key). Khi được sử dụng trên mạng WLAN, cổng kết nối của VPN đảm nhận việc xác thực, đóng gói và mã hóa.



Hình 4.5 – Mô hình WLAN VPN

TKIP

TKIP (Temporal Key Integrity Protocal) là giải pháp của IEEE được phát triển năm 2004. Là một nâng cấp cho WEP nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm (hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC (message integrity check) để đảm bảo tính chính xác của gói tin. TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo.

AES

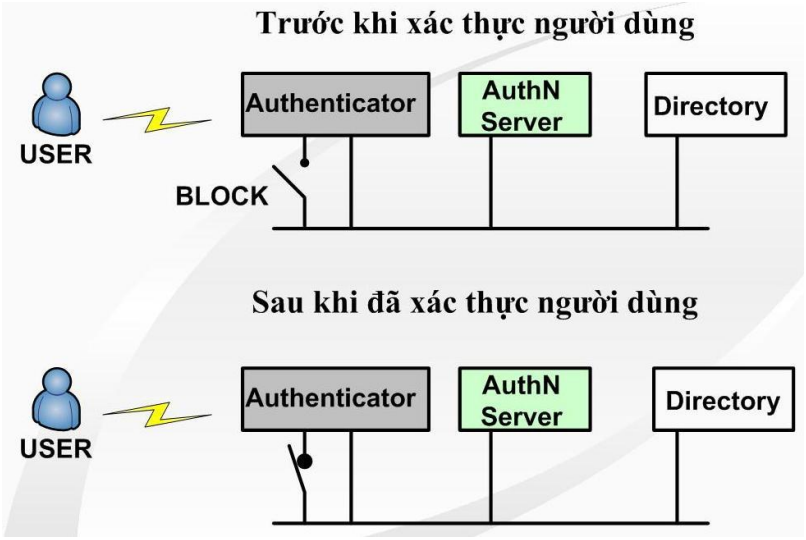
Trong mật mã học, AES (Viết tắt của từ tiếng Anh: Advanced Encryption Standard, hay Tiêu chuẩn mã hóa tiên tiến) là một thuật toán mã hóa khối được chính phủ Hoa kỳ áp dụng làm tiêu chuẩn mã hóa. Giống như tiêu chuẩn tiền nhiệm DES, AES được kỳ vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kỹ lưỡng. AES được chấp thuận làm tiêu chuẩn

liên bang bởi Viện tiêu chuẩn và công nghệ quốc gia Hoa kỳ (NIST) sau một quá trình tiêu chuẩn hóa kéo dài 5 năm.

Thuật toán được thiết kế bởi hai nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen (lấy tên chung là "Rijndael" khi tham gia cuộc thi thiết kế AES). Rijndael được phát âm là "Rhine dahl" theo phiên âm quốc tế (IPA).

802.1X VÀ EAP

802.1x là chuẩn đặc tả cho việc truy cập dựa trên cổng (port-based) được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Việc điều khiển truy cập được thực hiện bằng cách: Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn (blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.



Hình 4.6 – Mô hình hoạt động xác thực 802.1x

EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng (password, cetificate,…), giao thức được sử dụng (MD5, TLS_Transport Layer Security, OTP_ One Time Password,…) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.

Quá trình chứng thực 802.1x-EAP như sau:

1. AP sẽ chặn lại tất cả các thông tin của client cho tới khi client log on vào mạng, khi đó Client yêu cầu liên kết tới AP

2. AP đáp lại yêu cầu liên kết với một yêu cầu nhận dạng EAP
3. Client gửi đáp lại yêu cầu nhận dạng EAP cho AP
4. Thông tin đáp lại yêu cầu nhận dạng EAP của client được chuyển tới Server chứng thực
5. Server chứng thực gửi một yêu cầu cho phép tới AP
6. AP chuyển yêu cầu cho phép tới client
7. Client gửi trả lời sự cấp phép EAP tới AP
8. AP chuyển sự trả lời đó tới Server chứng thực
9. Server chứng thực gửi một thông báo thành công EAP tới AP
10. AP chuyển thông báo thành công tới client và đặt cổng của client trong chế độ forward.

4.3.1.2 WPA

WEP được xây dựng để bảo vệ một mạng không dây tránh bị nghe trộm. Nhưng nhanh chóng sau đó người ta phát hiện ra nhiều lỗ hỏng ở công nghệ này. Do đó, công nghệ mới có tên gọi WPA (Wi-Fi Protected Access) ra đời, khắc phục được nhiều nhược điểm của WEP.

Trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP. WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên tin tặc không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu.

Không những thế, WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hóa lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết

bị máy trạm. Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc.

4.3.1.3 WPA2

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES. AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Để đánh giá chuẩn mã hoá này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mỹ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã đối xứng này.

FILTERING

Filtering (Lọc) là cơ **c**hế bảo mật cơ bản có thể sử dụng cùng với WEP. Lọc hoạt động giống như Access list trên router, cấm những cái không mong muốn và cho phép những cái mong muốn. Có 3 kiểu lọc cơ bản có thể được sử dụng trong WLAN:

- Lọc SSID
- Lọc địa chỉ MAC
- Lọc giao thức

Lọc SSID

Lọc SSID là một phương thức cơ bản của lọc và chỉ nên được sử dụng cho việc điều khiển truy cập cơ bản.

SSID của client phải khớp với SSID của AP để có thể xác thực và kết nối với tập dịch vụ. SSID được quảng bá mà không được mã hóa trong các Beacon nên rất dễ bị phát hiện bằng cách sử dụng các phần mềm. Một số sai lầm mà người sử dụng WLAN mắc phải trong việc quản lí SSID gồm:

- ✓ Sử dụng giá trị SSID mặc định tạo điều kiện cho hacker dò tìm địa chỉ MAC của AP.
- ✓ Sử dụng SSID có liên quan đến công ty.
- ✓ Sử dụng SSID như là phương thức bảo mật của công ty.

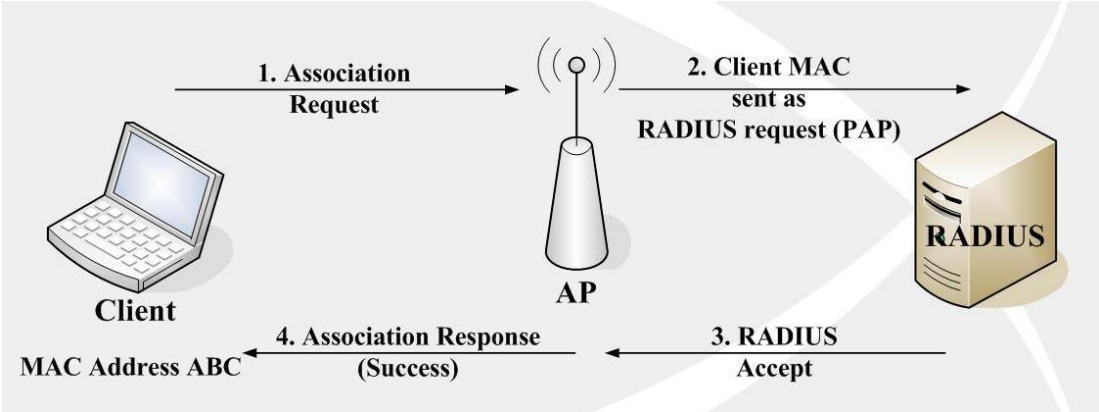
✓ Quảng bá SSID một cách không cần thiết.

Lọc địa chỉ MAC

Hầu hết các AP đều có chức năng lọc địa chỉ MAC. Người quản trị có thể xây dựng danh sách các địa chỉ MAC được cho phép.

Nếu client có địa chỉ MAC không nằm trong danh sách lọc địa chỉ MAC của AP thì AP sẽ ngăn chặn không cho phép client đó kết nối vào mạng.

Nếu công ty có nhiều client thì có thể xây dựng máy chủ RADIUS có chức năng lọc địa chỉ MAC thay vì AP. Cấu hình lọc địa chỉ MAC là giải pháp bảo mật có tính mở rộng cao.



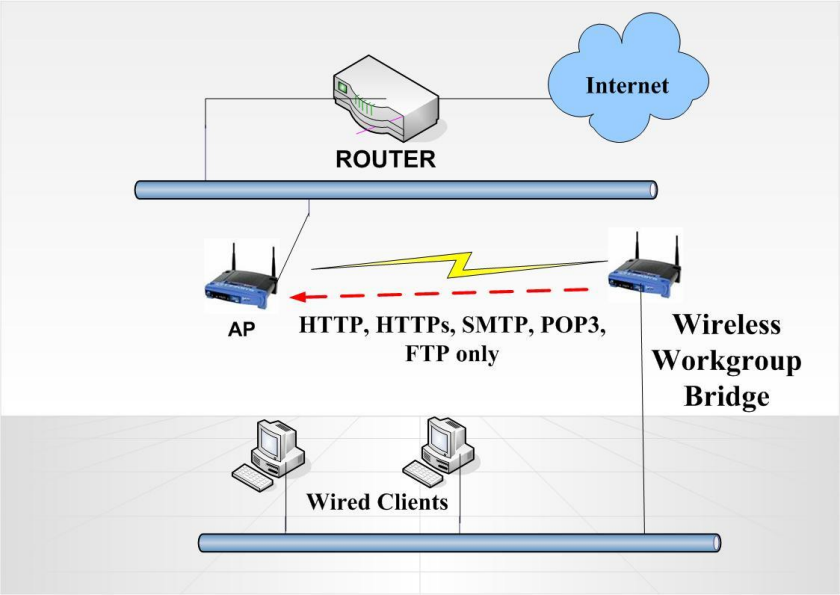
Hình 4.7 – Tiến trình xác thực MAC

Lọc giao thức

Mạng Lan không dây có thể lọc các gói đi qua mạng dựa trên các giao thức từ lớp 2 đến lớp 7. Trong nhiều trường hợp người quản trị nên cài đặt lọc giao thức trong môi trường dùng chung, ví dụ trong trường hợp sau:

- Có một nhóm cầu nối không dây được đặt trên một Remote building trong một mạng WLAN của một trường đại học mà kết nối lại tới AP của tòa nhà kỹ thuật trung tâm.
- Vì tất cả những người sử dụng trong remote building chia sẻ băng thông 5Mbs giữa những tòa nhà này, nên một số lượng đáng kể các điều khiển trên các sử dụng này phải được thực hiện.

- Nếu các kết nối này được cài đặt với mục đích đặc biệt của sự truy nhập Internet của người sử dụng, thì bộ lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ HTTP, SMTP, HTTPS, FTP…



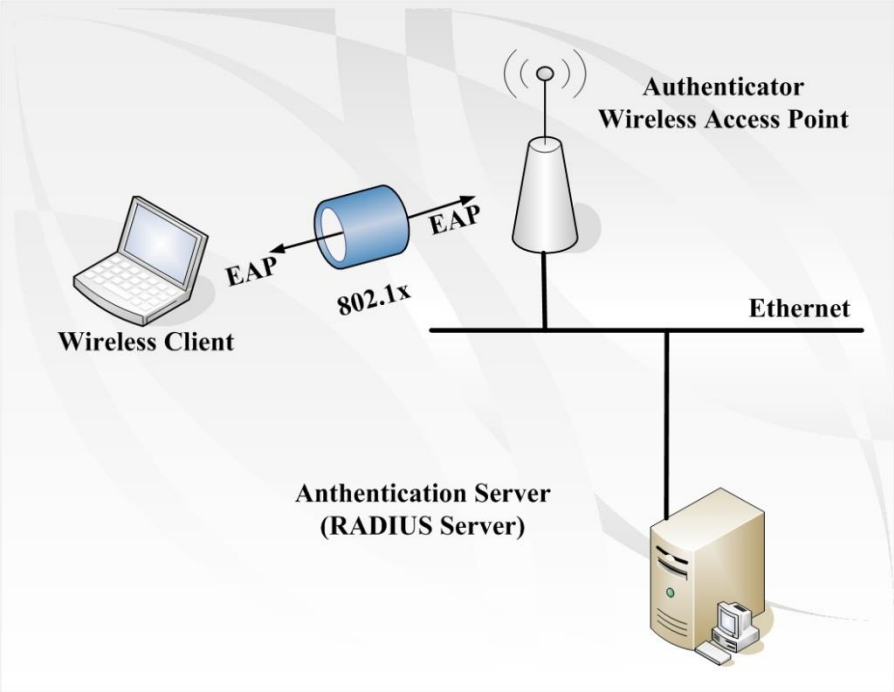
Hình 4.8 – Lọc giao thức

4.3.2. Sử dụng máy chủ xác thực Radius Server

Radius (Remote Authentication Dial-in User Service) Server là một máy chủ cung cấp dịch vụ xác thực người dùng từ xa. Nguyên lý xác thực của WLAN kết hợp với Radius Server đó là: việc xác thực người dùng sẽ không được thực hiện trên AP nữa mà thực hiện trên Radius Server, quản lý các thông tin như tên đăng nhập, mật khẩu… Khi người dùng gửi yêu cầu chứng thực, server này sẽ tra cứu dữ liệu để xem người này có hợp lệ không, được cấp quyền đến mức nào…

Xác thực, cấp phép và kiểm toán

- Giao thức RADIUS được định nghĩa trong RFC 2865 như sau: Với khả năng cung cấp xác thực tập trung, cấp phép và điều khiển truy cập (Authentication, Authorization, và Accounting – AAA) cho các phiên làm việc với SLIP và PPP Dial-up – như việc cung cấp xác thực của các nhà cung cấp dịch vụ Internet (ISP) đều dựa trên giao thức này để xác thực người dùng khi họ truy cập Internet.



Hình 4.9 – Mô hình xác thực giữa Wireless Clients và RADIUS Server.

- Nó cần thiết trong tất cả các Network Access Server (NAS) để làm việc với danh sách tên đăng nhập và mật khẩu cho việc cấp phép, yêu cầu truy cập RADIUS sẽ chuyển các thông tin tới một máy chủ xác thực, thông thường nó là một máy chủ AAA (AAA – Authentication, Authoriztion, và Accounting). Trong kiến trúc của hệ thống nó tạo ra khả năng tập trung các dữ liệu, thông tin của người dùng, các điều kiện truy cập trên một điểm duy nhất (single point), trong khi có khả năng cung cấp cho một hệ thống lớn, cung cấp giải pháp NASs.
- Khi một người dùng kết nối, NAS sẽ gửi một gói tin dạng yêu cầu truy cập RADIUS tới máy chủ AAA, chuyển các thông tin như tên đăng nhập và mật khẩu, thông qua một cổng xác định, định danh NAS, và một thông điệp xác thực.
- Sau khi nhận được các thông tin máy chủ AAA sử dụng các gói tin được cung cấp như định danh NAS, và trung tâm xác thực thẩm định lại việc NAS đó có được phép gửi các yêu cầu đó không. Nếu có khả năng, máy chủ AAA sẽ tìm kiếm tra thông tin tên đăng nhập và mật khẩu mà người dùng yêu cầu truy cập trong

cơ sở dữ liệu. Nếu quá trình kiểm tra là đúng thì nó sẽ mang một thông tin trong gói tin yêu cầu truy cập quyết định quá trình truy cập của người dùng đó là được chấp nhận.

- Khi quá trình xác thực bắt đầu được sử dụng, máy chủ AAA có thể sẽ trả về một thách thức truy cập (Access-Challenge) RADIUS mang một số ngẫu nhiên. NAS sẽ chuyển thông tin đến người dùng từ xa (với ví dụ này sử dụng CHAP). Khi đó người dùng sẽ phải trả lời đúng các yêu cầu xác nhận (trong ví dụ này, đưa ra lời đề nghị mã hoá mật khẩu), sau đó NAS sẽ chuyển tới máy chủ AAA một gói tin yêu cầu truy cập RADIUS.
- Nếu máy chủ AAA sau khi kiểm tra các thông tin của người dùng hoàn toàn thoả mãn sẽ cho phép sử dụng dịch vụ, nó sẽ trả về một gói tin dạng chấp nhận truy cập RADIUS. Nếu không thoả mãn máy chủ AAA sẽ trả về một tin từ chối truy cập RADIUS và NAS sẽ ngắt kết nối với người dùng.
- Khi một gói tin chấp nhận truy cập được nhận và RADIUS Accounting đã được thiết lập, NAS sẽ gửi một gói tin RADIUS Accounting-Request (Start) tới máy chủ AAA. Máy chủ sẽ thêm các thông tin vào tệp tin Log của nó, với việc NAS sẽ cho phép phiên làm việc với người dùng bắt đầu khi nào, và kết thúc khi nào, RADIUS Accouting làm nhiệm vụ ghi lại quá trình xác thực của người dùng vào hệ thống, khi kết thúc phiên làm việc NAS sẽ gửi một thông tin RADIUS Accounting-Request (Stop).

Sự an toàn và tính mở rộng

Tất cả các gói tin của RADIUS đều được đóng gói bởi UDP datagrams, nó bao gồm các thông tin như: message type, sequence number, length, Authenticator, và một loạt các Attribute-Value.

Trung tâm xác thực (Authenticator): Tác dụng của Authenticator là cung cấp một chế độ bảo mật. NAS và máy chủ AAA sử dụng Authenticator để hiểu được các thông tin đã được mã hóa của nhau như mật khẩu chẳng hạn. Authenticator cũng giúp NAS phát hiện sự giả mạo của gói tin RADIUS

Responses. Cuối cùng, Authenticator được sử dụng làm cho để biến mật khẩu thành một dạng nào đó, ngăn chặn việc làm lộ mật khẩu của người dùng trong các gói tin RADIUS.

Authenticator gửi gói tin yêu cầu truy cập trong một số ngẫu nhiên. MD5 sẽ băm (hash) số ngẫu nhiên đó thành một dạng riêng là OR'ed cho mật khẩu của người dùng và gửi trong gói tin yêu cầu truy cập chứa thông tin mật khẩu của người dùng. Toàn bộ gói tin trả lời RADIUS sau đó được MD5 băm (hash) với cùng thông số bảo mật của Authenticator, và các thông số trả lời khác.

Authenticator giúp cho quá trình giao tiếp giữa NAS và máy chủ AAA được bảo mật nhưng nếu kẻ tấn công bắt được cả hai gói tin yêu cầu truy cập và trả lời truy cập RADIUS thì có thể thực hiện "dictionary attack" để phân tích việc đóng gói này. Trong điều kiện thực tế để việc giải mã khó khăn cần phải sử dụng những thông số dài hơn, toàn bộ vấn đề có khả năng nguy hại cho quá trình truyền tải này được miêu tả rất kỹ trong RFC 3580.

Cặp giá trị thuộc tính: Thông tin được mang bởi RADIUS được miêu tả trong một dạng giá trị thuộc tính, để hỗ trợ cho nhiều công nghệ khác nhau, và nhiều phương thức xác thực khác nhau. Một chuẩn được định nghĩa trong cặp giá trị thuộc tính, bao gồm tên đăng nhập, mật khẩu, địa chỉ IP của NAS, cổng của NAS, kiểu dịch vụ. Các nhà sản xuất (vendors) cũng có thể định nghĩa cặp giá trị thuộc tính để mang các thông tin của mình như Vendor-Specific toàn bộ ví dụ này được miêu tả trong RFC 2548 - Định nghĩa Microsoft Attribute-Value pair trong MS-CHAP.

Thêm vào đó, rất nhiều chuẩn cặp giá trị thuộc tính được định nghĩa trong nhiều năm để hỗ trợ giao thức xác thực mở rộng (EAP), một dạng khác cũ hơn của nó là giao thức PAP và CHAP. Thông tin có thể tìm thấy trong tài liệu RFC 3579 cho phiên bản mới nhất của RADIUS hỗ trợ EAP. Trong phần này sẽ nói rất rõ về hỗ trợ xác thực cho WLAN, từ khi chuẩn EAP được sử dụng cho cổng điều khiển truy cập 802.1x để cho phép xác thực từ bên ngoài cho wireless.

Áp dụng RADIUS cho WLAN

Trong một mạng Wireless sử dụng cổng điều khiển truy cập 802.1x, các máy trạm sử dụng wireless với vai trò người dùng truy cập từ xa và điểm truy cập Wireless làm việc như một máy chủ truy cập mạng (NAS). Để thay thế cho việc kết nối đến NAS với dial-up như giao thức PPP, máy trạm kết nối wireless kết nối đến Access Point bằng việc sử dụng giao thức 802.11.

Trong quá trình được thực hiện, máy trạm kết nối wireless gửi một gói tin EAP-Start tới Access Point. Access Point sẽ yêu cầu máy trạm nhận dạng và chuyển các thông tin đó tới một máy chủ AAA với thông tin là tên đăng nhập yêu cầu truy cập RADIUS.

Máy chủ AAA và máy trạm wireless hoàn thành quá trình bằng việc chuyển các thông tin thách thức xác thực và yêu cầu truy cập RADIUS qua Access Point. Được quyết định bởi phía trên là một dạng EAP, thông tin này được chuyển trong một đường hầm được mã hoá TLS (Encypted TLS Tunnel).

Nếu máy chủ AAA gửi một gói tin chấp nhận truy cập, Access Point và máy trạm wireless sẽ hoàn thành quá trình kết nối và thực hiện phiên làm việc với việc sử dụng WEP hay TKIP để mã hoá dữ liệu. Và tại điểm đó, Access Point sẽ không cấm cổng và máy trạm wireless có thể gửi và nhận dữ liệu từ hệ thống mạng một cách bình thường.

Cần lưu ý là mã hoá dữ liệu từ máy trạm wireless tới Access Point khác với quá trình mã hoá từ Access Point tới máy chủ AAA Server (RADIUS Server).

Nếu máy chủ AAA gửi một gói tin từ chối truy cập, Access Point sẽ ngắt kết nối tới máy trạm. Máy trạm có thể cố gắng thử lại quá tình xác thực, nhưng Access Point sẽ cấm máy trạm này không gửi được các gói tin tới các Access Point ở gần đó. Chú ý là máy trạm này hoàn toàn có khả năng nghe được các dữ liệu được truyền đi từ các máy trạm khác – Trên thực tế dữ liệu được truyền qua sóng radio và đó là câu trả lời tại sao phải mã hoá dữ liệu khi truyền trong mạng không dây.

Cặp thuộc tính giá trị bao gồm trong gói tin của RADIUS có thể sử dụng bởi máy chủ AAA để quyết định phiên làm việc giữa Access Point và

máy trạm wireless, như Sesstion-Timeout hay VLAN Tag (Tunnel-Type=VLAN, Tunnel-Private-Group-ID=tag). Chính xác các thông tin thêm vào có thể phụ thuộc vào máy chủ AAA Server hay Access Point và máy trạm mạng sử dụng.

4.4. TÌM KIẾM VÀ LOẠI BỎ CÁC MẠNG KHÔNG DÂY GIẢ MẠO

Trong một thế giới hoàn hảo, việc ngăn chặn cụ thể các mạng không dây giả mạo trong chính sách an toàn không dây là đủ để giải quyết vấn đề. Tuy nhiên, trong thế giới thực hiện nay, người quản trị cần phải có những bước bổ sung để phát hiện, ngăn chặn và loại bỏ các mạng WLAN lừa đảo kết nối vào mạng. Các bước đó bao gồm:

- *Triển khai và thực thi một chính sách an toàn không dây*. Chính sách an toàn không dây định nghĩa cách thức để mạng không dây sẽ được hoặc không được thực hiện trong tổ chức. Cần phải đảm bảo rằng chính sách an toàn đó được thi hành. Ví dụ, chính sách đó định nghĩa rằng việc sử dụng một WAP trực tuyến giả dụng là sai trái và cần phải chấm dứt. Chính sách cũng chỉ ra những việc cần làm nếu phát hiện ra một WAP giả mạo và ai là người có trách nhiệm giải quyết các việc đó.
- *Cung cấp an toàn mang tính vật lý*. Vì hầu hết các mạng WLAN có một phạm vi giới hạn, nên điều quan trọng là thực hiện các biện pháp an ninh thích hợp để tránh người khác có thể thu được phạm vi đó để phân phối trực tuyến một WAP giả mạo bất kỳ. Tùy chọn khác sử dụng *paint* và *window screening* có thể ngăn chặn được các lưu lượng không dây truyền qua. Những sản phẩm này có thể đảm bảo rằng một người nào đó bên ngoài sẽ không thể kết nối tới bất kỳ mạng không dây nào hoạt động trong các tòa nhà.
- *Cung cấp một hạ tầng WLAN đảm bảo*. Một phương pháp hiệu quả nhằm ngăn chặn các mạng giả mạo WLAN là cung cấp một hạ tầng mạng WLAN thích hợp sao cho người dùng không cần thiết phải đi ra ngoài để làm những việc riêng của họ.

- *Cô lập mạng WLAN giả mạo bằng cách thực hiện bảo mật các cổng trên thiết bị chuyển mạch mạng LAN*. Mặc dù vẫn tồn tại một vài vấn đề cần giải quyết, song bảo mật cổng trên thiết bị chuyển mạch vẫn có thể được thực hiện để đảm bảo rằng chỉ những hệ thống xác thực mới có thể kết nối được với hệ thống mạng. Vì các WAP giả mạo không có thông tin xác thực nên chúng không có hiệu lực trong hệ thống mạng.

Dò quét các mạng WLAN giả mạo, loại bỏ chúng, và ngăn chặn những kẻ thực hiện. Để làm được điều đó thì một chính sách bảo mật đơn thuần là không đủ.

4.4.1. Thực hiện quy trình khám phá

Nhiều người thường nghĩ rằng, nếu không thể ngăn chặn việc tiến hành một WLAN giả mạo thì đó là nguyên nhân mất an toàn mạng không dây. Nhưng thực tế không phải như vậy. Việc người quản trị không thể thực sự ngăn chặn các WAP trái phép thực hiện trong mạng không có nghĩa là không thể phát hiện và loại bỏ chúng.

Có hai phương pháp chủ yếu để phát hiện các mạng WLAN trái phép trong mạng. Phương pháp đầu tiên là cố gắng để phát hiện ra tính không dây của chúng. Phương pháp thứ hai cố gắng để phát hiện ra chúng từ mạng có dây.

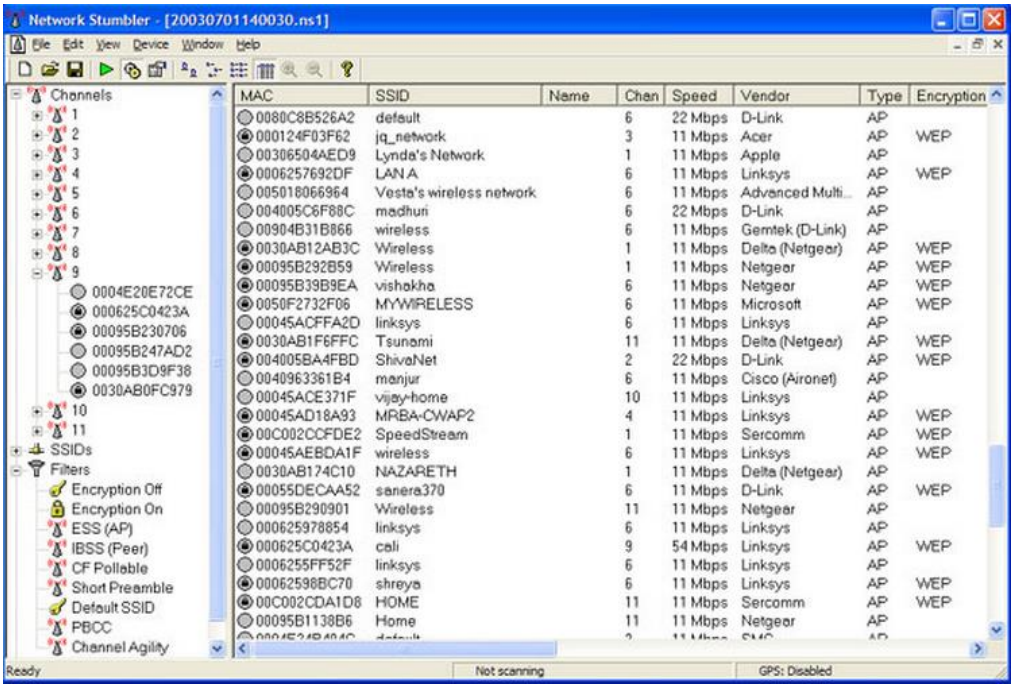
Phát hiện tính không dây của các mạng WLAN trái phép.

Một phương pháp hiệu quả đáng ngạc nhiên để có thể phát hiện các mạng WLAN trái phép bằng cách đơn giản là sử dụng một máy trạm truy cập không dây và định vị các WAP phát sóng trong môi trường của hệ thống mạng. Tuy nhiên, có một vài lời cảnh báo cần được xem xét khi sử dụng phương pháp này:

- ✓ Vì các mạng WLAN có một phạm vi giới hạn, nên máy trạm truy cập phải nằm trong phạm vi của WAP mới có thể phát hiện ra nó.
- ✓ Việc phát hiện một WAP mà không phát SSID là rất khó khăn.

✓ Rất khó khăn để khảo sát các trang web từ xa.

Công cụ NetStumbler cung cấp một trong những phương pháp đơn giản nhất để phát hiện một AP giả mạo trên mạng không dây. Sau khi cài đặt NetStumbler, chương trình sẽ tự động quét WAP mà không yêu cầu các thông tin về cấu hình thiết bị (ngoại trừ cung cấp các NIC không dây). Ví dụ, hình 4.10 mô tả NetStumbler bắt 175 WAP, trong đó có 113 mạng không sử dụng phương pháp mã hóa nào, số còn lại đều sử dụng WEP thay vì WPA.



Hình 4.10 – NetStumbler

Phát hiện WAP trái phép từ mạng có dây

Việc sử dụng một quá trình phát hiện có dây có thể làm giảm bớt những khó khăn trong việc cố gắng phát hiện một WAP không dây trái phép. Ví dụ, một quá trình phát hiện có dây không dễ dàng bị thiếu mất các WAP kể cả khi chúng không phát SSID. Ngoài ra, quá trình phát hiện có dây có thể được sử dụng để khảo sát các trang web từ xa và thậm chí có thể được lên kế hoạch và kịch bản để làm tăng tính dễ sử dụng.

Tuy nhiên, phương pháp này cũng có một số nhược điểm nhất định. Việc định vị tất cả các điểm truy cập trái phép có thể khó khăn, chủ yếu là do thiếu các thiết bị chuyên dụng để thực hiện. Hiện nay, hầu hết các kỹ thuật

đều dựa trên cách sử dụng địa chỉ MAC của WAP (bởi vì tất cả nhà cung cấp được chỉ định một phạm vi địa chỉ MAC cụ thể) hoặc hệ điều hành quét vân tay để xác định các WAP. Dưới đây là hai công cụ có thể giúp người quản trị trong việc xác định một WAP trái phép nhờ theo dõi địa chỉ MAC:

- APTools: APTools không chỉ có thể phát hiện ra một điểm truy cập dựa trên địa chỉ MAC của WAP, nó còn có thể cố gắng kiểm tra để xác minh rằng các điểm truy cập là một WAP trái ngược với bất kỳ một thiết bị khác mà có một địa chỉ MAC.
- Arpwatch: Arpwatch có thể giám sát mạng và duy trì một cơ sở dữ liệu về địa chỉ MAC và địa chỉ IP theo từng cặp, cho phép bạn xác định địa chỉ MAC mới cũng như địa chỉ MAC từ các nhà cung cấp không đạt tiêu chuẩn.

Dưới đây là một số công cụ có thể giúp người quản trị trong việc thực hiện quét mạng:

- ✓ Nmap: Nmap có thể được sử dụng để xác định hệ điều hành mà một thiết bị được dò tìm ra đang chạy.
- ✓ Xprobe: Xprobe có khả năng tương tự như Nmap trong xác định hệ điều hành thông qua việc sử dụng quét dấu vân tay.
- ✓ Nessus: Nessus là một công cụ đánh giá điểm yếu nổi tiếng mà có thể được sử dụng để phát hiện các WAP giả mạo. Được sử dụng để phát hiện các WAP giả mạo.

Cả hai phương pháp trên, sử dụng địa chỉ MAC của WAP và hệ điều hành quét vân tay, đều gặp những vấn đề chung trong việc sinh ra các xác thực lỗi. Ví dụ, Nmap nhận một Linksys WAP54G như một thiết bị Linux bởi vì nó thực sự chạy hệ điều hành Linux. Điều này khiến việc xác định xem thiết bị đó thực sự là một WAP hay chỉ là một máy chủ Linux có một địa chỉ MAC đã được giao cho một nhà cung cấp không dây trở nên khó khăn hơn. Điều đó có thể gây khó khăn để phân biệt giữa một AP Cisco và một switch Cisco nếu cơ sở dữ liệu các địa chỉ MAC không được cập nhật chính xác.

4.4.2. Loại bỏ các điểm giả mạo

Một khi đã phát hiện được một WAP giả mạo, bước tiếp theo cần làm là hãy tìm cách tắt nó đi. Một lựa chọn là cố gắng xác định vị trí vật lý và ngắt kết nối của WAP đó khỏi hệ thống mạng; tuy nhiên, điều này có thể tốn thời gian và dễ bị thất bại. Những khó khăn rõ ràng của phương pháp này là việc định vị các WAP, thường được thực hiện thông qua một quá trình thử nghiệm và báo lỗi, có thể rất khó khăn vì hầu hết các WAP khá nhỏ và dễ dàng dấu kín.

Một lựa chọn khác là để xác định vị trí các cổng của switch mà có địa chỉ MAC của WAP kết nối vào, sau đó đóng cổng đó. Tương tự như vậy, có thể xác định địa chỉ IP của WAP và cố gắng để ngăn chặn chúng hoặc thực hiện tắt các cổng của switch.

CÁC BÀI THỰC HÀNH

1. Thực hành thiết lập xác thực WPA, WPA2 cho mạng WLAN

Mục đích bài thực hành: hướng dẫn cấu hình thiết bị phát mạng không dây cung cấp chức năng mã hóa, đảm bảo người dùng truy cập an toàn khi sử dụng mạng không dây và phòng chống sử dụng mạng không dây mà không được phép.

Bước 1: Kết nối máy tính với thiết bị phát sóng không dây (Access Point) qua cổng điều khiển hoặc qua địa chỉ IP mặc định.

Bước 2: Bật chức năng cấu hình.

Bước 3: Lần lượt chọn các giao thức WPA, WPA2.

Bước 4: Lưu cấu hình và thoát.

2. Thực hành thiết lập xác thực Wi-fi trong Windows Server 2008

Mục đích: Xây dựng trung tâm xác thức RADIUS Server để xác thực những người dùng nào có quyền truy cập mạng Wi-fi

Bước 1: Cài đặt Network Policy and Access Services Role

Bước 2: Cấu hình NPS với chức năng RADIUS

Bước 3: Cấu hình bộ điều khiển truy cập AP không dây

Bước 4: Cài đặt chứng chỉ CA tên máy khách

Bước 5: Cấu hình các thiết lập mạng trên máy khách

Bước 6: Kết nối và đăng nhập

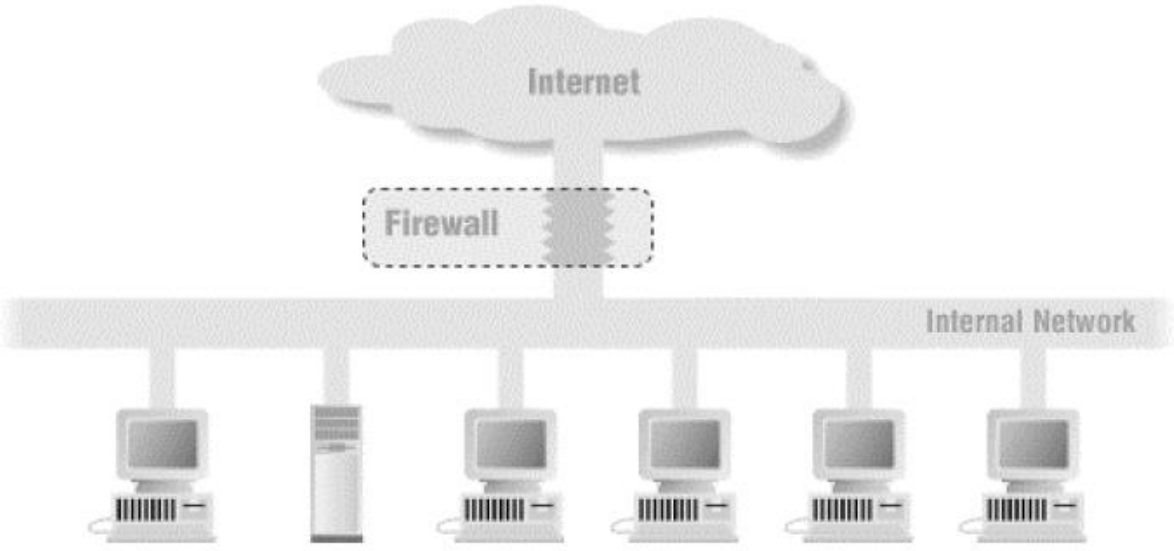
Chương 5.
TRIỂN KHAI CÔNG NGHỆ PHÒNG THỦ MẠNG

5.1. TRIỂN KHAI CÔNG NGHỆ TƯỜNG LỬA

5.1.1. Khái niệm về tường lửa

5.1.1.1 Định nghĩa

Tường lửa (*Firewall*) là một thuật ngữ dùng để mô tả những thiết bị hay phần mềm có nhiệm vụ lọc những thông tin đi vào hay đi ra một hệ thống mạng hay máy tính theo những quy định đã được thiết lập trước đó. Mục tiêu của việc sử dụng tường lửa là tạo ra những kết nối an toàn từ vùng mạng bên trong ra bên ngoài hệ thống, cũng như đảm bảo không có những truy cập trái phép từ bên ngoài vào những máy chủ và thiết bị bên trong hệ thống mạng. Để có một tường lửa đảm bảo an toàn trong hệ thống, đòi hỏi người quản trị phải có một hệ thống tường lửa bằng phần cứng hay phần mềm mạnh mẽ, uyển chuyển, cùng với những kỹ năng và kiến thức chuyên sâu để kiểm soát chúng.



Hình 5.1 – Tường lửa bảo vệ mạng LAN bên trong

5.1.1.2 Chức năng

- Xác thực người dùng khi truy cập tới nguồn tài nguyên thông tin của vùng mạng được bảo vệ bên trong. Kiểm soát tất cả các ứng dụng, dịch vụ vào ra như: web, mail, ftp, telnet, ssh, vpn, remote desktop, …
- Kiểm soát truy cập vào ra dựa vào địa chỉ IP, các cổng TCP/UDP.
- Kiểm soát và quản lý hiệu quả đường dẫn URL và định dạng tệp tin ở lớp ứng dụng. Ví dụ: cấm truy cập website nào đó, cấm tải các tệp tin định dạng .exe, .mp3, .mp4, .flv, .mkv…
- Chuyển dịch địa chỉ IP (NAT), ánh xạ các cổng TCP/UDP từ mạng ngoài vào mạng trong và ngược lại.

- Nhược điểm:

✓ Tường lửa không thể chống lại các tấn công vòng qua tường lửa.

✓ Tường lửa không thể chống lại các nguy cơ đe dọa từ bên trong.

✓ Tường lửa không thể chống lại các tấn công bởi virus, sâu mạng, mã độc hại.

5.1.1.3 Phân loại tường lửa

Trên thế giới có nhiều cách phân loại tường lửa khác nhau được trình bày sau đây:

✓ Phân loại theo nhà sản xuất: Mỗi một nhà sản xuất thì họ có các sản phẩm tường lửa khác nhau, và mức độ bảo vệ cho hệ thống mạng cũng khác nhau.

- Tường lửa cứng: Là loại tường lửa được sản xuất thành sản phẩm chuyên dụng. Người quản trị chỉ cần lắp ráp và cấu hình cho nó. Một số tường lửa cứng điển hình: Check Point, Juniper, Cisco…
- Tường lửa mềm: Là sản phẩm tường lửa được đóng thành phần mềm và cần phải có máy chủ và hệ điều hành của hãng thứ ba để cài đặt. Một số tường lửa mềm điển hình: ISA hoặc Forefont (TMG) của hãng Microsoft, ZoneAlarm của hãng CheckPoint, ESET Smart Security, Proventia Network của hãng IBM.

- ✓ Phân loại theo phạm vi sử dụng:
    - Tường lửa cá nhân: Là loại tường lửa được cài đặt tại máy tính cá nhân. Nó có chức năng kiểm soát luồng thông tin vào ra ngay tại máy tính cá nhân.
    - Tường lửa mạng: Là loại tường lửa chạy trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng hoặc các vùng mạng DMZ.
- ✓ Phân loại theo mô hình tầng mạng
    - Tầng mạng: Là loại tường lửa hoạt động ở tầng mạng theo mình hình OSI.
    - Tầng giao vận: Tường lửa cổng vòng.
    - Tầng ứng dụng: Tường lửa cổng ứng dụng.
- ✓ Phân loại theo trạng thái
    - Tường lửa có trạng thái (Stateful firewall).
    - Tường lửa phi trạng thái (Stateless firewall).

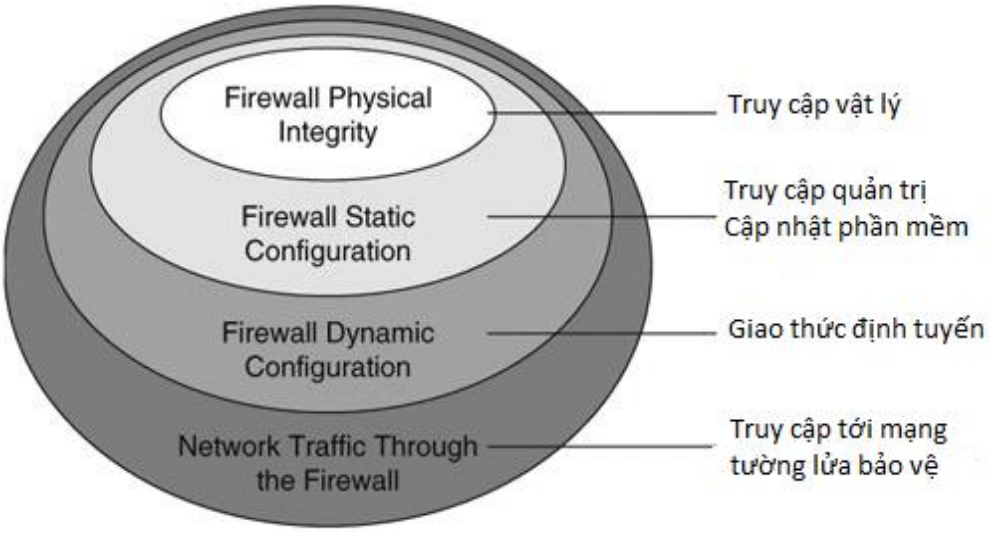
5.1.2. Tạo chính sách tường lửa

Lập chính sách bảo mật tường lửa bằng văn bản để cung cấp một lộ trình mức cao cần phải được thực hiện để đảm bảo rằng tổ chức có một chiến lược bảo mật được định hướng rõ ràng. Đó là một quan niệm sai lầm chung của một tổ chức có một chính sách bảo mật. Trong thực tế, một chính sách bảo mật tổng thể của một tổ chức thường bao gồm nhiều chính sách bảo mật riêng lẻ, được viết để giải quyết các đối tượng cụ thể, các thiết bị hoặc các vấn đề về bảo mật.

Mục tiêu của chính sách bảo mật là xác định cái gì cần được bảo vệ, người chịu trách nhiệm bảo vệ, và trong các trường hợp bảo vệ bằng cách nào. Chức năng cuối cùng thường được tách ra thành một tài liệu độc lập như lọc đầu vào, lọc đầu ra, hoặc các tài liệu về chính sách quản lý truy cập. Tóm lại, chính sách bảo mật cần được người quản trị vạch ra đơn giản và chính xác những yêu cầu cụ thể, các quy tắc, các đối tượng phải được đáp ứng, để cung

cấp một phương pháp định lượng về xác nhận khả năng bảo mật của một tổ chức.

Để đảm bảo các chính sách bảo mật tường lửa sẽ hoạt động chính xác thì phải gắn nó với các lớp bảo mật, mỗi một lớp có một phạm vi hoạt động riêng biệt. Hình 5.2 minh họa các lớp mà tường lửa bảo vệ. Như hình trình bày, tường lửa được chia thành bốn thành phần riêng biệt.



Hình 5.2 – Các lớp tường lửa bảo vệ

Tại trung tâm là lớp bảo vệ toàn vẹn tường lửa ở mức vật lý, tường lửa ở lớp này chủ yếu liên quan đến việc truy cập vật lý đến các bức tường lửa. Vì vậy, người quản trị cần phải đảm bảo rằng các chính sách bảo mật giải quyết được các vấn đề liên quan tới truy cập vật lý tới thiết bị tường lửa, chẳng hạn như kết nối tới cổng điều khiển trực tiếp của tường lửa.

Lớp tiếp theo trình bày chính sách cấu hình tĩnh tường lửa, lớp này liên quan chủ yếu đến việc truy cập vào phần mềm đã được cấu hình tĩnh của tường lửa khi đang chạy. Ở lớp này, chính sách bảo mật cần tập trung vào việc xác định các điều kiện sẽ được yêu cầu để hạn chế truy cập quản trị, bao gồm cả thực hiện cập nhật phần mềm và cấu hình tường lửa.

Lớp thứ ba là cấu hình tường lửa động, lớp này bổ sung cho cấu hình tường lửa tĩnh bằng cách liên kết với cấu hình động của tường lửa thông qua việc sử dụng các công nghệ như các giao thức định tuyến, các lệnh của giao thức phân giải địa chỉ (ARP), giao diện và trạng thái thiết bị, ghi lại hoạt

động. Mục tiêu của chính sách bảo mật ở lớp này là để xác định các yêu cầu xung quanh những loại cấu hình động sẽ được cho phép.

Lớp cuối cùng là khi đã có lưu lượng mạng đi qua tường lửa, mà thực chất là những gì mà tường lửa được sử dụng để bảo vệ tài nguyên. Lớp này có liên quan với chức năng như danh sách kiểm soát truy cập (ACL) và dịch vụ thông tin ứng dụng. Chính sách bảo mật ở lớp này có trách nhiệm xác định các yêu cầu có liên quan tới lưu lượng mạng cho phép và ngăn chặn đi qua tường lửa.

5.1.2.1 Định dạng chính sách bảo mật

Để hoàn thành các mục tiêu đã được định nghĩa phía trên, hầu hết các chính sách bảo mật phải tuân theo một định dạng nhất định hoặc bố trí và chia sẻ các yếu tố chung. Hầu hết các chính sách bảo mật được chia vào bảy phần như sau:

1. Khái quát: Phần này cung cấp một giải thích nhỏ về chính sách giải quyết những vấn đề gì.
2. Mục đích: Phần này giải thích tại sao chính sách được sử dụng.
3. Phạm vi: Phần này xác định phạm vi áp dụng chính sách và xác định những ai là người chịu trách nhiệm về chính sách.
4. Chính sách: Phần này là chính sách thực tế của nó.
5. Thực thi: Phần này xác định cách chính sách cần phải được thực thi và những ảnh hưởng nếu không tuân thủ chính sách.
6. Định nghĩa: Phần này chứa các định nghĩa về các thuật ngữ hoặc các khái niệm sử dụng trong chính sách.
7. Lịch sử sửa đổi: Phần này là nơi mà những thay đổi về chính sách được ghi chép và theo dõi.

5.1.2.2 Các chính bảo mật chung của tường lửa

Mỗi một tổ chức có các yêu cầu về bảo mật thông tin khác nhau và do đó chính sách của họ cũng khác nhau. Tuy nhiên, hầu hết cả các hệ thống mạng đều yêu cầu các chính sách bảo mật tường lửa chung như sau:

- Chính sách quản lý truy cập
- Chính sách lọc lưu lượng mạng
- Chính sách định tuyến
- Chính sách truy cập từ xa – VPN
- Chính sách giám sát, ghi lại hoạt động của tường lửa
- Chính sách vùng mạng DMZ (demilitarized zone)
- Chính sách áp dụng chung

5.1.2.3 Chính sách quản lý truy cập

Như trên được áp dụng, chính sách quản lý truy cập tồn tại để xác định phương pháp cho phép và các tiếp cận quản lý truy cập tới tường lửa. Chính sách này hướng tới giải quyết tính toàn vẹn về vật lý và lớp cấu hình tĩnh tường lửa an toàn. Chính sách quản lý truy cập cần phải xác định các giao thức quản lý cả bên ngoài và bên trong mạng sẽ được phép, cũng như người quản trị có thể kết nối tới tường lửa với các quyền tương ứng với nhiệm vụ.

Ngoài ra, chính sách quản lý truy cập cũng nên xác định các yêu cầu cho các giao thức quản lý mạng như Network Time Protocol (NTP), syslog, TFTP, FTP, Simple Network Management Protocol (SNMP), và bất kỳ giao thức nào có thể được sử dụng để quản lý và duy trì thiết bị.

5.1.2.4 Chính sách lọc lưu lượng mạng

Chính sách không xác định các nguyên tắc thực tế một tường lửa sẽ được sử dụng, chính sách lọc cần chỉ ra và xác định chính xác các loại lọc phải được sử dụng và nơi lọc được áp dụng. Chính sách này hướng tới giải quyết lớp cấu hình tĩnh của tường lửa và đặc biệt là lưu lượng mạng thông qua tường lửa. Ví dụ, một chính sách lọc tốt cần phải yêu cầu lọc cả lưu lượng vào ra đi qua tường lửa. Chính sách lọc cũng nên xác định các yêu cầu chung trong việc kết nối mạng có mức bảo mật không giống nhau và bảo mật tài nguyên. Ví dụ, với một vùng mạng DMZ, tùy thuộc vào kết nối của lưu lượng, yêu cầu lọc ở các mức độ khác nhau là cần thiết, và đó là vai trò của chính sách lọc để xác định những yêu cầu về bảo mật mạng.

5.1.2.5 Chính sách định tuyến

Chính sách định tuyến thường không phải là tài liệu chính của tường lửa. Tuy nhiên với nhiều phân vùng mạng phức tạp cũng như gia tăng sử dụng tường lửa bên trong mạng nội bộ, vì vậy mà tường lửa có thể dễ dàng trở thành một phần của định tuyến hạ tầng mạng. Chính sách định tuyến nên có một phần quy định cụ thể một tường lửa trong định tuyến hạ tầng mạng và xác định phương pháp trong đó việc định tuyến sẽ xảy ra. Chính sách này hướng tới giải quyết các lớp cấu hình tĩnh tường lửa và cấu hình động tường lửa. Trong hầu hết các trường hợp, chính sách định tuyến nên ngăn cấm một cách rõ ràng tường lửa từ việc chia sẻ bảng định tuyến mạng nội bộ với các tài nguyên mạng bên ngoài. Tương tự như vậy, chính sách định tuyến cần xác định các trường hợp trong đó các giao thức định tuyến động và định tuyến tĩnh phải thích hợp. Chính sách này cũng nên xác định bất kỳ cơ chế giao thức bảo mật cụ thể cần được thiết lập (Ví dụ, việc sử dụng các thuật toán băm để đảm bảo chỉ xác thực các nút có thể vượt qua định tuyến dữ liệu).

5.1.2.6 Chính sách truy cập từ xa – VPN

Trong lĩnh vực hội tụ ngày nay, sự tách biệt giữa tường lửa và bộ kết nối truy cập tư xa tập trung đã dần mờ đi. Hầu như các tường lửa trên thị trường có thể phục vụ kết hợp chức năng mạng riêng ảo truy cập từ xa VPN, và do đó chính sách truy cập từ xa VPN cần xác định các yêu cầu mức độ mã hóa và xác thực khi một kết nối VPN được yêu cầu. Trong một số trường hợp, chính sách VPN được kết hợp với chính sách mã hóa của tổ chức xác định các phương thức VPN tổng thể sẽ được sử dụng. Chính sách này hướng tới giải quyết lớp cấu hình tĩnh của tường lửa và lưu lượng mạng đi qua nó.

Chính sách truy cập từ xa VPN cũng cần phải xác định các giao thức bảo mật sẽ được sử dụng: Giao thức bảo mật IP (IPsec), giao thức truyền lớp hai (L2TP), giao thức truyền điểm nối điểm (PPTP). Trong hầu hết các trường hợp, IPsec nên được sử dụng dành riêng. Ví dụ, trong chính sách VPN sử dụng cho IPsec cần phải được yêu cầu sử dụng khóa chia sẻ và xác thực mở rộng với sử dụng chứng chỉ số, mật khẩu một lần, và hạ tầng khóa công khai (PKI) đầy đủ để đảm bảo an toàn cho hệ thống mạng. Tương tự như vậy,

chính sách truy cập từ xa VPN nên xác định những phương thức mà máy trạm được sử dụng (ví dụ: Microsoft VPN client, Cisco Secure VPN client…).

Cuối cùng, chính sách truy cập từ xa VPN cần phải xác định loại truy cập và tài nguyên sẽ được cung cấp cho kết nối và những kết nối sẽ được phép. Ví dụ: chính sách VPN cho phép kết nối từ mạng tới mạng (site to site) cũng như kết nối từ máy trạm tới mạng (remote client), vì vậy mà chính sách VPN phải xác định cho từng loại kết nối cụ thể sẽ được sử dụng.

5.1.2.7 Chính sách giám sát, ghi lại hoạt động của tường lửa

Một trong những yếu tố quan trọng nhất để đảm bảo tường lửa đang cung cấp mức độ đảm bảo an toàn cho hệ thống mạng là thực hiện chức năng giám sát hệ thống tường lửa. Chính sách này xác định các phương thức và mức độ giám sát sẽ được thực hiện. Ở mức tối thiểu, chính sách giám sát - ghi lại hoạt động cung cấp cơ chế theo dõi hiệu năng của tường lửa cũng như sự xuất hiện của tất cả các sự kiện liên quan đến an ninh ghi lại trạng thái hoạt động của tường lửa. Chính sách này hướng tới giải quyết lớp cấu hình tĩnh tường lửa.

Chính sách giám sát, ghi lại hoạt động của tường lửa cũng cần phải xác định luồng thông tin phải được thu thập, duy trì và báo cáo. Trong nhiều trường hợp thông tin có thể được sử dụng để xác định các yêu cầu về quản lý và giám sát các ứng dụng của bên thứ ba như CiscoWorks, NetIQ Security Manager, Kiwi Syslog Deamon.

5.1.2.8 Chính sách vùng mạng DMZ (Demilitarized zone)

Chính sách DMZ là một tài liệu trên phạm vi rộng mà định nghĩa tất cả các yếu tố không chỉ liên quan tới DMZ mà còn cả các thiết bị bên trong vùng DMZ. Mục tiêu của chính sách DMZ là để xác định các tiêu chuẩn và yêu cầu của tất cả các thiết bị và kết nối và luồng lưu lượng có liên quan đến DMZ. Chính sách này hướng tới giải quyết lớp cấu hình tĩnh tường lửa và luồng lưu lượng mạng đi qua tường lửa.

Do sự phức tạp trong môi trường vùng mạng DMZ, vì vậy chính sách này liên quan tới nhiều vấn đề bảo mật trong vùng mạng DMZ. Để giúp đảm

bảo chính sách DMZ vẫn còn chức năng và hiệu quả, ba tiêu chuẩn điển hình cần được xác định cho tất cả các thiết bị, kết nối, luồng lưu lượng mạng liên quan đến vùng DMZ:

- Trách nhiệm của chủ sở hữu
- Yêu cầu cấu hình an toàn
- Yêu cầu hoạt động và kiểm soát sự thay đổi

5.1.2.9 Chính sách áp dụng chung

Ngoài các chính sách cụ thể về tường lửa, có rất nhiều chính sách áp dụng chung cho hệ thống mạng (có ứng dụng với nhiều thiết bị) cũng nên được áp dụng cho tường lửa, bao gồm một số chính sách sau đây:

- Chính sách mật khẩu: Chính sách này nhằm đảm bảo an toàn khi người quản trị đăng nhập tới tường lửa để cấu hình, giám sát.
- Chính sách về mật mã: Chính sách này liên quan tới việc xác định tất cả các hình thức truy cập sử dụng mật mã bao gồm: Secure HTTP (HTTPs), Secure Sockets Layer (SSL), Secure Shell (SSH), IPsec/VPN.
- Chính sách ghi nhật ký: Xác định các yêu cầu ghi nhật ký của tường lửa.
- Chính sách đánh giá rủi ro: Dùng để xác định phương pháp sẽ được sử dụng để xác định các rủi ro liên quan đến tất cả thiết bị trên hệ thống, di chuyển và những thay đổi liên quan đến tường lửa và mạng vành đai nói chung.

5.1.2.10 Chính sách bảo mật cho tường lửa

Một trong những lý do chính sách bảo mật cho tường lửa được tách riêng sau các chính sách bảo mật thông thường khác là nó cũng có thể chứa hoặc thay thế các yếu tố của một số chính sách bảo mật đã đề cập ở trên. Chính sách bảo mật tường lửa (đôi khi được gọi là chính sách tường lửa) phải giải quyết tất cả các yêu cầu bảo mật cụ thể của tường lửa, như đã định nghĩa trong cấu trúc phân lớp của hình 5.1. Khi thực hiện nhiệm vụ này, chính sách tường lửa có thể bị chồng chéo, bao hàm hoặc trùng lặp tới các chính sách

trước. Ngoài ra, nếu có chính sách bảo mật khác được áp dụng cho tường lửa thì cần phải được tham chiếu tới tài liệu chứa danh sách các chính sách đã được thiết lập. Để tránh vấn đề này xảy ra cần phải xây dựng một danh sách kiểm tra dựa trên bốn lớp trong hình 5.1. Các phần sau đây bao gồm chính sách cho bốn lớp.

Đảm bảo tính toàn vẹn về vật lý cho tường lửa

Để đảm bảo chính sách bảo mật tường lửa có đầy đủ tính năng giải quyết các vấn đề bảo vệ vật lý, phải đảm bảo tuân thủ các yếu tố bảo mật sau đây:

- Xác định người được quyền cài đặt, gỡ bỏ cài đặt và di chuyển tường lửa.
- Xác định người được ủy quyền bảo trì phần cứng và thay đổi cấu hình vật lý của tường lửa.
- Xác định người được ủy quyền kết nối vật lý với tường lửa, đặc biệt là thông qua cổng điều khiển trực tiếp giao diện đăng nhập.
- Xác định các phương pháp phục hồi thích hợp trong trường hợp khi sự cố xảy ra về vật lý hoặc bằng chứng về sự tiếp cận với tường lửa.

Cấu hình tĩnh tường lửa

Để đảm bảo chính sách bảo mật tường lửa có đầy đủ chức năng giải quyết các vấn đề an toàn cấu hình tĩnh, phải đảm bảo các yếu tố sau đây là những thành phần của chính sách bảo mật:

- Xác định người được ủy quyền để đăng nhập vào tường lửa thông qua bất kỳ phương thức kết nối nào (Local hoặc Remote).
- Xác định các quyền hạn rõ ràng tương ứng với người dùng và người quản trị.
- Xác định các thủ tục để thực hiện thay đổi cấu hình và cập nhật tường lửa.
- Xác định các chính sách mật khẩu (thường kết hợp với các chính sách mật khẩu của tổ chức) cho tường lửa.

- Xác định phương thức cho khả năng đăng nhập từ xa, bao gồm xác định các vùng mạng cho phép hoặc hệ thống được phép đăng nhập từ xa (thường kết hợp với chính sách quản lý truy cập).
- Xác định các thủ tục phục hồi cho bức tường lửa trong trường hợp có sự cố xảy ra.
- Xác định các chính sách ghi lại các hoạt động của tường lửa.
- Xác định các yêu cầu mã hóa cho tường lửa (thường kết hợp với các chính sách mã hóa của tổ chức).
- Xác định phương pháp quản lý và giám sát từ xa (ví dụ, SNMP, syslog…) cho tường lửa (thường kết hợp với chính sách quản lý truy cập).

Cấu hình động cho tường lửa

Đề đảm bảo các chính sách bảo mật tường lửa giải quyết đầy đủ các vấn đề bảo mật cấu hình động, đảm bảo các yếu tố là những thành phần của chính sách bảo mật tường lửa:

- Xác định những loại tiến trình và dịch vụ nào được phép chạy trên tường lửa cũng như những mạng và thiết bị nào sẽ được truy cập tới tiến trình và dịch vụ đó.
- Xác định các giao thức định tuyến sẽ được phép và yêu cầu tính năng bảo mật tương ứng.
- Xác định cách thức tường lửa sẽ cập nhật và duy trì thông tin thời gian hệ thống.
- Xác định phương pháp để duy trì mật khẩu một lần, phương thức xác thực và thuật toán mã hóa, khóa mã.

Lưu lượng mạng đi qua tường lửa

Để đảm bảo các chính sách bảo mật tường lửa kiểm soát toàn bộ luồng lưu lượng mạng đi qua tường lửa, đảm bảo các yếu tố sau đây là những thành phần của chính sách bảo mật tường lửa:

- Xác định phương thức mà luồng lưu lượng mạng sẽ cho phép và luồng lưu lượng nào bị ngăn chặn.
- Xác định quy trình yêu cầu thay đổi và cập nhật luật cho tường lửa.
- Xác định các loại giao thức nào, các cổng và dịch vụ sẽ cho phép hoặc bị ngăn chặn.

5.1.3. Thiết lập luật và lọc gói tin

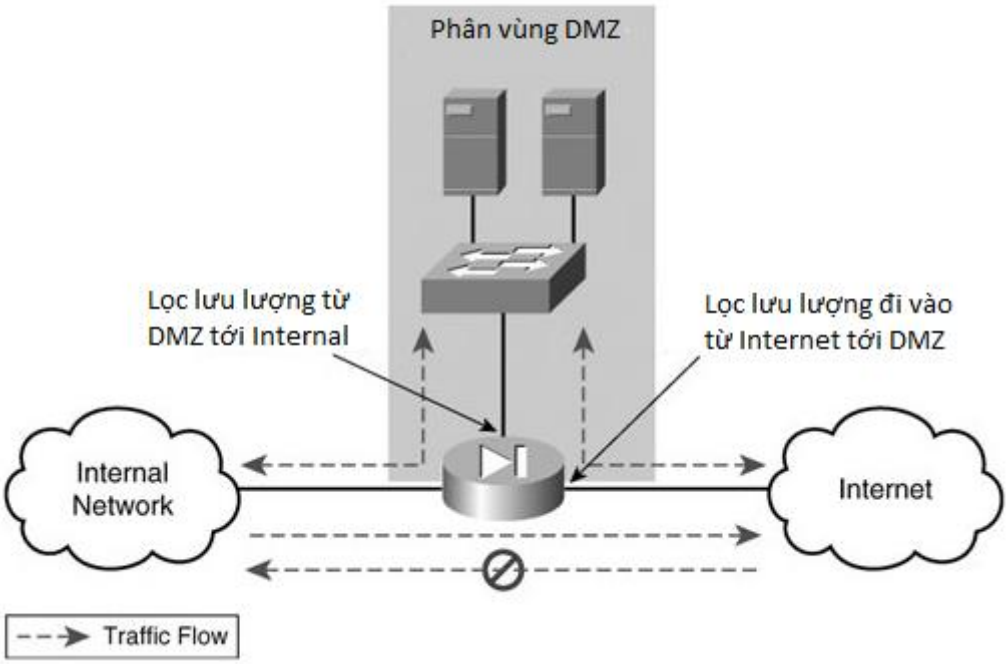
Các chính sách đã đề cập ở trên đây tập trung chủ yếu vào việc xác định các yêu cầu và kỳ vọng sự thực thi của tường lửa và các hệ thống liên quan. Sau khi các yêu cầu đã được xác định, người quản trị phải xây dựng thực sự cấu hình và các luật mà tường lửa sẽ sử dụng. Đây được coi là việc thực thi chính sách bảo mật của tường lửa, mặc dù trên thực tế các chính sách bảo mật tường lửa được xác định là sự kết hợp của các chuẩn, hướng dẫn, thủ tục so với việc thực thi chính sách vào tường lửa.

Đề đảm bảo có sự phân biệt giữa chính sách bảo mật mà xác định các yêu cầu và tập luật là xác định các quy tắc cấu hình thực tế tuân thủ các yêu cầu đã đặt ra. Nhìn chung có ba tập quy tắc cần phải thiết lập cho tường lửa:

- Tập luật lọc đầu vào
- Tập luật lọc đầu ra
- Luật quản lý truy cập

5.1.3.1 Tập luật lọc đầu vào

Tập luật lọc đầu vào được sử dụng để giới hạn luồng lưu lượng mạng đi vào một giao diện mạng (interface) hoặc từ một phân vùng mạng. Bộ lọc thường được áp dụng tới luồng lưu lượng mạng từ nguồn không tin cậy (ví dụ: Internet hoặc DMZ) tới vùng mạng được bảo vệ (mạng nội bộ - LAN, mạng DMZ). Để tiếp cận dễ dàng với bộ lọc đầu vào thì điều quan trọng là phải hiểu được một bộ lọc đầu vào liên quan đến hành động và nguồn gốc của luồng lưu lượng mạng được lọc. Ví dụ: Xem xét cấu hình của một tường lửa đơn giản với một phân vùng mạng DMZ, có thể hai bộ lọc đầu vào sẽ được áp dụng cho tường lửa này như hình sau đây:



Hình 5.3 – Hai bộ lọc đầu vào cho vùng mạng DMZ

Hình 5.3 trình bày luồng lưu lượng mạng theo các mũi tên, lưu lượng có thể đi từ Internet tới phân vùng mạng DMZ và ngược lại, từ mạng DMZ tới mạng nội bộ, từ mạng nội bộ đi được tới cả hai Internet và DMZ, nhưng các phiên khởi tạo kết nối từ mạng Internet tới mạng nội bộ bị ngăn chặn.

Trong trường hợp này hai tập luật lọc sẽ được xây dựng và áp dụng cho tường lửa. Tập luật đầu tiên sẽ điều khiển truy cập từ Internet tới mạng DMZ. Trong trường hợp này Internet được coi là mạng không tin cậy, DMZ được coi là mạng tin cậy. Tập luật thứ hai kiểm soát truy cập từ mạng DMZ tới mạng nội bộ. Trong trường hợp này mạng DMZ được coi là mạng không tin cậy, và mạng nội bộ được coi là mạng tin cậy.

Đối với hầu hết các tường lửa thương mại hiện nay, các phương pháp lọc mặc định đều có một cách tiếp cận đơn giản cho luồng lưu lượng mạng. Điều này có nghĩa là mặc định tất cả lưu lượng truy cập đến từ mạng không tin cậy đều bị từ chối, trừ trường hợp được cho phép đặc biệt.

Mặc dù đây là một trong số lớn các phương pháp cấu hình gộp, thực tế trong hầu hết tất cả các tường lửa người quản trị phải thực hiện cấu hình cho phép một số lưu lượng mạng từ mạng không tin cậy vào mạng tin cậy. Phổ biến nhất từ Internet tới mạng DMZ và từ DMZ tới mạng nội bộ.

Phương thức tiếp cận có hệ thống tới tập luật lọc đầu vào:

Phương thức tiếp cận hiệu quả nhất để thực hiện tập luật lọc là sử dụng một phương pháp tiếp cận có hệ thống để xây dựng tập luật lọc cho tường lửa. Để xây dựng hiệu quả danh sách luật lọc người quản trị nên thực hiện theo danh sách hướng dẫn dưới đây:

Bước 1. Xác định mạng nguồn (không tin cậy) và mạng đích (tin cậy) hoặc các hệ thống mà luật lọc sẽ được áp dụng.

Bước 2. Xác định các dịch vụ hoặc các ứng dụng mà tường lửa sẽ áp dụng.

Bước 3. Xác định các cổng TCP/UDP được yêu cầu bởi các dịch vụ hoặc ứng dụng.

Bước 4. Xác định các hệ thống nguồn (không tin cậy) và đích (tin cậy) mà một dịch vụ và một cổng cụ thể sẽ được áp dụng bởi tập luật của tường lửa.

Kết hợp bốn bước đầu tiên giúp người quản trị xác định những gì tập luật lọc cần cung cấp truy cập tới các dịch vụ và ứng dụng mà chính sách bảo mật tường lửa đã chỉ ra. Ngoài ra, tập luật lọc cũng được sử dụng để bảo vệ các phân vùng mạng bên trong khỏi một số tấn công như là từ chối dịch vụ, quét cổng. v.v.

Bước 5. Xác định địa chỉ mạng nguồn không nên cho phép từ mạng không tin cậy. Trong tài liệu RFC (*Request for Comments*) 1918 định nghĩa không gian địa chỉ mạng riêng (Private) là 10.0.0.0/18, 172.16.0.0/12, 192.168.0.0/16; RFC 3330 đề cập đến những địa chỉ đặc biệt như là địa chỉ Loopback – 127.0.0.0/8, địa chỉ mạng cục bộ 169.254.0.0/16; và không gian địa chỉ IP của mạng tin cậy và không gian của mọi địa chỉ IP không được gán.

Bước 6. Xây dựng và triển khai danh sách điều khiển truy cập (ACL) để áp dụng tới tập luật lọc đầu vào và sau đó áp dụng tới giao diện mạng thích hợp.

Bước 7. Giám sát ACL để xác định những kết nối nào được phép và kết nối nào nên bị ngăn chặn, và quan trọng hơn là xác định kiểu tấn công vào mạng bên trong đi qua tường lửa.

Tuân thủ những phương thức trên để đảm bảo luật lọc được hoàn chỉnh theo chính sách bảo mật tường lửa và chức năng bảo vệ tài nguyên bên trong

tường lửa. Phương thức trên có thể áp dụng tới hầu hết mọi hệ thống. Tuy nhiên có ba phạm vi chung mà luật lọc cần phải thực hiện:

- Truy cập từ Internet tới phân vùng mạng DMZ.
- Truy cập từ phân vùng mạng DMZ tới mạng nội bộ.
- Truy cập từ Internet tới mạng nội bộ.

Quản lý truy cập từ Internet tới vùng mạng DMZ

Thế giới công nghệ hiện đại như ngày nay, người quản trị có thể sử dụng công nghệ tường lửa để ngăn chặn tất cả lưu lượng mạng từ Internet, để bảo vệ hệ thống mạng trước các nguy cơ tiềm năng từ Internet. Chúng ta không sống trong một thế giới hoàn hảo, vì vậy mà rất nhiều nguy cơ xâm nhập từ Internet. Tuy nhiên nó giống như những gì đã bắt đầu với một tường lửa liên quan tới yêu cầu truy cập dựa vào Internet đã trở thành nhiều vấn đề lỗ hổng. Tất nhiên, vấn đề ở đây là lưu lượng luôn luôn được phép đi qua tường lửa, tường lửa trở nên kém hiệu quả khi đảm nhiệm chức năng là hàng rào bảo mật cho toàn bộ hệ thống.

Mặc dù không có phương pháp hoàn hảo để đảm bảo rằng những sai sót sẽ không xảy ra (thực sự, người quản trị nên lập kế hoạch và có biện pháp đáp ứng khi có sự cố về sai sót xảy ra), một trong những phương pháp giảm thiểu sai sót bằng cách thực hiện tập luật lọc cho lưu lượng từ Internet tới vùng mạng DMZ dựa vào mẫu có sẵn sau đó áp dụng xử lý ở bước bảy đã trình bày trên đây để xây dựng luật lọc hoàn thiện hơn, một số hướng dẫn thực hiện như sau:

Bước 1. Bắt đầu tập luật bằng cách thực hiện luật cấm toàn bộ. Trong nhiều trường hợp một số sản phẩm tường lửa thực hiện luật cấm toàn bộ tại vị trí cuối cùng của ACL, đó là luật để đảm bảo ngoài lưu lượng cho phép ở trên thì những lưu lượng còn lại đều bị tường lửa ngăn chặn.

Bước 2. Đánh giá các dịch vụ và các cổng tương ứng mà vùng mạng DMZ yêu cầu. Hầu hết trong các dạng tường lửa đều thực hiện đọc tập luật từ trên xuống dưới.

Bước 3. Đánh giá những địa chỉ IP nguồn và đích yêu cầu tới các dịch vụ và cổng tương ứng cần thiết để mở cho các kết nối từ Internet tới vùng mạng DMZ. Xem xét đóng tất cả những dịch vụ và cổng không cần thiết. Ví dụ, nếu hệ thống nhất định cần cung cấp dịch vụ FTP có thể đến và đi, cho phép truy cập tới máy chủ FTP với những địa chỉ cho phép từ Internet. Một dịch vụ chỉ có thể được khai thác nếu kẻ tấn công có thể tiếp cận được dịch vụ đó.

Bước 4. Xem xét tất cả các luật mà đã xây dựng trong ACL và kiểm tra sau đây:

- Các dịch vụ và cổng mà hệ thống sẽ cung cấp phải được cho phép ở tường lửa.
- Các dịch vụ và cổng mà hệ thống không cung cấp phải ngăn chặn ngay tại tường lửa.
- Luật cuối cùng là chặn tất cả.

Bước 5. Ghi lại tất cả các dòng ACL. Mặc dù điều này có vẻ như không thể vượt qua một số lượng dữ liệu sẽ được lưu trữ, tất cả các luật tuân thủ được trỏ đến sự cần thiết phải được lưu trữ đúng cách. Để giúp quản lý số lượng dữ liệu lưu trữ, hãy xem xét triển khai phần mềm quản lý của bên thứ ba như CiscoWorks hoặc chức năng quản lý bảo mật NetIQ.

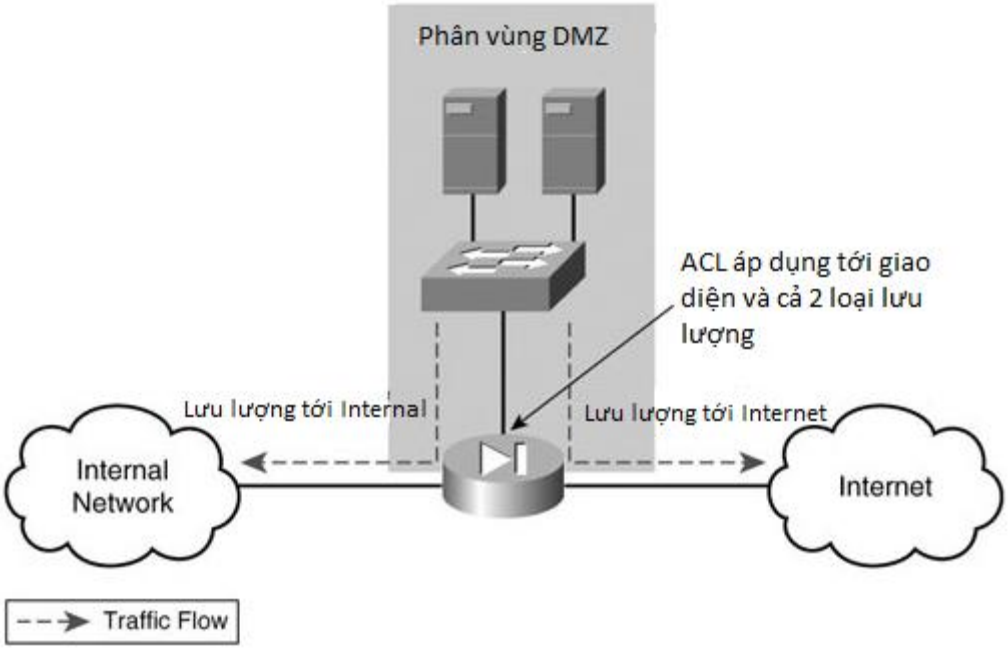
Bước 6. Áp dụng tập luật lọc phù hợp cho tường lửa để bảo vệ an toàn cho mạng bên trong.

Bước 7. Giám sát kết quả của lưu lượng truy cập được phép và bị ngăn chặn của ACL cho đến khi hệ thống mạng bên trong được đảm bảo an toàn trong quá trình hoạt động của tường lửa.

Quản lý truy cập từ mạng DMZ tới mạng nội bộ bên trong

Đây có lẽ là tập luật lọc quan trọng nhất người quản trị sẽ thực hiện bởi vì đây là những gì bảo vệ thật sự cho tài nguyên nội bộ khỏi các mối đe dọa bên ngoài. Các ứng dụng Internet ngày nay đang đòi hỏi phải tiếp cận nhiều hơn tới tài nguyên nội bộ, và một phương pháp hiệu quả nhằm giảm thiểu những rủi ro liên quan đến cấp quyền truy cập đó là thực hiện một máy chủ

trung gian trong DMZ được phép truy cập từ Internet, do đó truy cập vào dữ liệu back-end thường nằm trên mạng nội bộ.



Hình 5.4 – Lọc lưu lượng từ DMZ

Vì DMZ có một giao diện mạng duy nhất cho tất cả lưu lượng từ Internet hoặc mạng nội bộ, xây dựng và áp dụng một ACL tới giao diện mạng sẽ có chức năng hoạt động như một bộ lọc đầu vào tới mạng nội bộ và một bộ lọc để đi ra Internet. Điều này sẽ làm cho ACL phức tạp hơn khi lên kế hoạch và thực hiện.

Quản lý truy cập từ mạng Internet tới mạng nội bộ

Xây dựng một ACL để kiểm soát lưu lượng truy cập từ Internet tới mạng nội bộ có chức năng không khác nhau từ các kịch bản ACL trình bày trên đây. Điều khác nhau là gì, đó là lưu lượng sẽ đi đến từ một mạng hoàn toàn không đáng tin cậy và có khả năng tiếp cận trực tiếp với tài nguyên nội bộ. Bây giờ, phản ứng thích hợp với loại hình này thực hiện chỉ đơn giản là không cho phép nó. Trong những trường hợp đó, cần phải hoàn toàn chắc chắn về những gì tường lửa đang cho phép thông qua việc sử dụng các bộ lọc đầu vào của tường lửa.

Ngoài ra, người quản trị nên xem xét sử dụng một bức tường lửa mà có chức năng proxy cho các ứng dụng thực sự của dịch vụ đang quảng bá để đảm

bảo rằng chỉ có các loại dịch vụ hoạt động ở lớp ứng dụng muốn cho phép thực sự. Một ví dụ của việc này là Microsoft ISA Firewall sử dụng tính năng công khai ứng dụng của nó để cấp quyền truy cập tài nguyên.

5.1.3.2 Tập luật lọc đầu ra

Thực tế mà nói, tập luật lọc đầu ra gần như giống hệt với tập luật lọc đầu vào. Sự khác biệt nằm ở những gì một bộ lọc đầu ra áp dụng tới. Không giống như các bộ lọc đầu vào, bộ lọc đầu ra áp dụng cho lưu lượng đến từ một mạng tin cậy tới một mạng không tin cậy. Kết quả là, bộ lọc đầu ra thường được áp dụng trên giao diện tường lửa kết nối vào mạng nội bộ hoặc một mạng DMZ. Một cách đơn giản nghĩ đến việc các bộ lọc đi vào hoặc lọc đi ra là một bộ lọc mà lọc lưu lượng truy cập đến, và một bộ lọc thực hiện lọc lưu lượng đi ra ngoài.

Không giống như bộ lọc đi vào, nhiều bức tường lửa mặc định để cho phép tất cả lưu lượng truy cập từ mạng tin cậy tới mạng không tin cậy. Điều này đúng khi nói đến Cisco Secure PIX Firewall, trong đó sử dụng các khái niệm về mức độ bảo mật giao diện để xác định hệ thống sẽ tự động được cấu hình để cho phép lưu lượng.

Ưu điểm của loại cấu hình là các bức tường lửa có thể được cắm vào mạng, và sau đó hầu như không phải cấu hình, máy trạm nội bộ có thể truy cập tới nguồn tài nguyên bên ngoài (thường là Internet). Từ quan điểm và khả năng sử dụng đơn giản, đây là một điều tốt. Nhưng trong thực tế, đây là tường lửa có mức kiểm soát bảo mật thấp bởi vì nghĩa đơn giản là lưu lượng truy cập thậm chí mã độc hại sẽ được phép truyền theo mặc định.

Thực hiện tập luật lọc đi ra cho mạng nội bộ

Có lẽ vấn đề lớn nhất và cũng là lý do để người quản trị không thực hiện tập luật lọc đi ra cho luồng lưu lượng nội bộ của họ là luật lọc đi ra có thể là vô cùng phức tạp để có được quyền. Bộ lọc đi vào là tương đối đơn giản. Một số ít các dịch vụ và hệ thống mà người dùng sẽ cần truy cập vào, và cấu hình ACL cho phù hợp. Bởi vì hầu hết các bức tường lửa ngày nay thực hiện kiểm tra trạng thái gói tin, lưu lượng trả về cho các kết nối được phép bằng bộ lọc đi vào được tự động cho phép. Với một bộ lọc đi ra, có thể có

danh sách lớn hơn nhiều các cổng mà phải được mở ra. Mặc dù nó rất dễ dàng để giả định rằng người dùng của trong hệ thống thực sự chỉ cần truy cập Internet thông qua HTTP và HTTPS, và cũng có thể trong mạng nội bộ có những người dùng sử dụng tất cả các loại cổng để kết nối với tất cả các loại tài nguyên hợp pháp bên ngoài. Tương tự như vậy, nếu có nguồn tài nguyên trong DMZ mà người dùng cần truy cập tới, bộ lọc đi ra sẽ cần phải phù hợp với những kết nối đó.

Thực hiện tập luật lọc đi ra cho mạng DMZ

Như đã đề cập khi miêu tả về luật lọc đi vào, nếu mạng DMZ chỉ có một nhánh thì luật lọc đi vào và luật lọc đi ra có hiệu quả tương tự bởi vì tất cả các thông tin phải đi qua cùng một giao diện mạng tương tự trên bức tường lửa. Khi thực hiện phân chia ra các bộ lọc của ACL, hãy nhớ để tập trung vào lưu lượng sẽ được phép từ hệ thống trên DMZ tới các hệ thống trên Internet. Ngoài ra, phương pháp tương tự cũng được áp dụng cho lọc đi vào và lọc đi ra khác cũng được áp dụng ở đây.

5.1.3.3 Thiết lập luật truy cập để quản lý thiết bị tường lửa

Với phân loại luật lọc đi vào hoặc lọc đi ra, nhiệm vụ chính sách bảo mật tiếp theo là xem xét tập luật quản lý truy cập. Mặc dù một số tường lửa sẽ bao gồm quản lý truy cập trong việc lọc đi vào hoặc lọc đi ra thích hợp, do tính chất của luật quản lý truy cập đảm bảo truy cập được gọi ra và chú ý đặc biệt.

Điều quan trọng nhất cần nhớ về quản lý truy cập là không quan tâm đến phương pháp, những quy tắc sau cần được áp dụng:

- Giới hạn quản lý truy cập, chỉ cho phép các máy trạm quản lý cụ thể.
- Không bao giờ cho phép quản lý truy cập từ mạng không tin cậy.
- Luôn luôn sử dụng một phương pháp mã hóa để quản lý truy cập.
- Trong trường hợp không thể sử dụng một phương pháp mã hóa để quản lý (ví dụ như nhật ký hệ thống), xem xét việc thực hiện IPsec để đảm bảo lưu lượng trong khi truy cập.

Có rất nhiều phương pháp để thực hiện quản lý từ xa và ghi nhật ký của một tường lửa. Một số phương pháp phổ biến nhất như sau:

- Telnet và SSH
- SNMP
- Syslog
- TFTP và FTP
- HTTP và HTTPs

Telnet và SSH

Telnet là giao thức phổ biến cho quản lý từ xa các thiết bị tường lửa, phần lớn là do thực tế là nó hầu như là một phương pháp chuẩn thực hiện các kết nối dòng lệnh từ xa với các hệ thống dựa trên UNIX và các thiết bị mạng. Nhưng Telnet là một giao thức không được mã hóa và nên hạn chế sử dụng nếu có thể. Thay vào đó, sử dụng SSH cho các chức năng tương tự.

SSH (Secure Shell) là một giao thức mạng cho phép người quản trị làm được khá nhiều điều tương tự như Telnet, kết nối từ xa bằng dòng lệnh, nhưng với lưu lượng SSH được mã hóa và do đó một phương pháp quản lý từ xa an toàn. Ngay cả với điều này cũng không nên cấu hình SSH được phép truy cập từ một mạng không tin cậy. Mặc dù chắc chắn là thuận tiện hơn để có thể SSH vào các bức tường lửa từ nhà thay vì ngồi trực tiếp tại phòng máy chủ, để lộ SSH trên giao diện kết nối Internet đặc biệt là khi một sự cố bảo mật xảy ra. Thay vào đó, hãy xem xét thực hiện cấu hình VPN để hỗ trợ truy cập từ xa cho phép người quản trị VPN vào mạng DMZ mà từ đó họ có thể truy cập quản lý cho các bức tường lửa bằng SSH.

SNMP

SNMP (Simple Network Management Protocol) trình bày một ít của vấn đề liên quan với tường lửa. Một mặt, khó có thể bàn luận về giá trị của dữ liệu SNMP cung cấp như là thống kê hiệu suất. Mặt khác, SNMP là một giao thức truyền thống không an toàn có thể được sử dụng để hoàn tất cấu hình lại tường lửa (giả sử SNMP không trong chế độ chỉ đọc). Trong thực tế, vấn đề không an này là lý do lớn nhất mà các tổ chức quyết định vô hiệu hóa hoàn

toàn SNMP trên tường lửa của họ. Mặc dù điều này là chắc chắn có hiệu quả, nếu người quản trị muốn tận dụng SNMP thì có thể làm một số việc để đảm bảo an toàn hơn:

- Nếu SNMPv3 có sẵn trên tường lửa, sử dụng nó hơn là SNMPv1 hoặc SNMPv2c. SNMPv3 cung cấp cho việc mã hóa cũng như xác thực người dùng.
- Nếu SNMPv1 hoặc SNMPv2c được sử dụng, xem xét sử dụng IPsec để đóng gói và bảo đảm an toàn luồng lưu lượng.
- Không sử dụng cùng một chuỗi chung SNMP trên tường lửa mà đã sử dụng bất cứ nơi nào khác trong mạng. Điều này đảm bảo rằng nếu tường lửa gặp sự cố bởi một cách nào đó, các chuỗi chung là vô giá trị ở những nơi khác trong mạng.
- Nếu không kích hoạt hướng tới có ý định sử dụng SNMP để thực hiện cấu hình tường lửa, chỉ nên thực hiện SNMP trong chế độ chỉ đọc.
- Hạn chế SNMP để truy cập quản lý, chỉ sử dụng các máy trạm quản lý được chỉ định.

Syslog

Syslog (System log) khác với hầu hết các phương pháp quản lý khác là sự phục vụ như một phương thức hoạt động cho người quản trị để tương tác với tường lửa, nhật ký hệ thống chỉ đơn giản là truyền nhật ký thông tin và dữ liệu đến một máy chủ phân tích nhật ký hệ thống để xem xét, hành động và lưu trữ. Bởi vì gói tin syslog có thể chứa thông tin liên quan đến khai thác tiềm năng bảo mật, sự chú ý cần được thực hiện để đảm bảo rằng tường lửa chỉ có thể truyền dữ liệu nhật ký hệ thống đến một máy chủ syslog được chỉ định. Syslog thường được truyền đi trong một môi trường không được mã hóa trên cổng UDP 514. Do đó đảm bảo an toàn là cần thiết, và cần phải thực hiện IPsec cho thông tin liên lạc giữa các máy chủ syslog và tường lửa.

TFTP và FTP

TFTP và FTP đều được sử dụng chủ yếu cho việc sao chép tập tin vào/ra từ tường lửa và cập nhật phần mềm hệ thống hoặc cấu hình. Mặc dù

FTP cung cấp các cơ chế xác thực mà TFTP không có, cả hai giao thức truyền tải dữ liệu trong một môi trường không được mã hóa và do vậy dễ bị nghe trộm. Với thực tế là các lưu lượng truy cập thường xuyên sẽ chứa dữ liệu cấu hình, đây là một vấn đề bảo mật quan trọng.

Để đảm bảo an toàn lưu lượng TFTP và FTP, giới hạn tường lửa chỉ giao tiếp với máy chủ TFTP và FTP đã định trước. Hơn nữa, nếu có thể để đóng gói dữ liệu TFTP hay FTP trong IPsec, để đảm bảo rằng dữ liệu trong quá trình truyền được bảo vệ phù hợp.

HTTP và HTTPS

HTTP và HTTPS cả hai thường được sử dụng cho quản lý từ xa dựa trên web. Tương tự như Telnet và SSH, HTTP sử dụng một phương pháp truyền dẫn không được mã hóa (HTTPS có sử dụng mã hóa). Do đó, phải triển khai giao thức HTTPS để truy cập quản lý thông qua giao thức web.

Bản chất của HTTPS là cung cấp bảo mật cho truy cập quản lý tường lửa và phần lớn là một quá trình đảm bảo rằng các máy trạm quản lý được quy định được phép kết nối với các bức tường lửa trên HTTPS. Cũng như SSH, HTTPS cũng không nên truy cập cấu hình từ mạng không tin cậy như Internet.

5.1.4. Tường lửa ứng dụng

Nguyên lý hoạt động

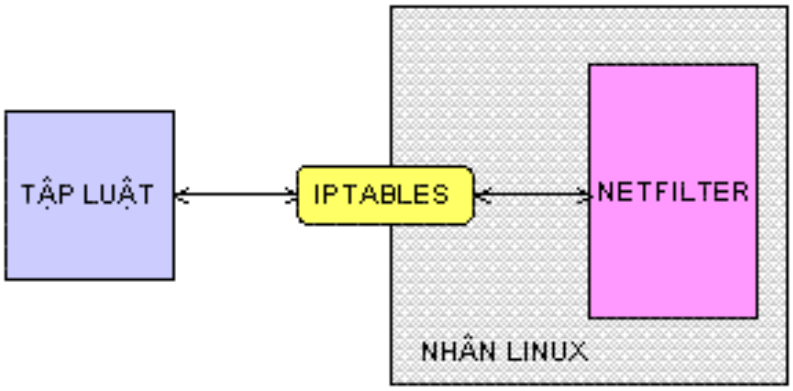
Đây là loại tường lửa được thiết kế tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service (dịch vụ đại diện). Proxy service là các bộ chương trình đặc biệt cài đặt trên gateway cho từng ứng 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 truyền thông tin qua tường lửa. Ngoài ra, proxy code có thể được 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.

Cổng ứng dụng phối hợp giữa kiểm soát truy cập mức thấp với các chức năng lớp cao (lớp 7 – lớp ứng dụng).

5.1.5. Tường lửa Iptables trên Linux

5.1.5.1 Giới thiệu về Iptables

Iptables là một tường lửa sử dụng lọc gói dữ liệu mạnh mẽ, miễn phí và có sẵn trên Linux. Netfilter/ Iptables gồm hai phần là Netfilter ở trong nhân Linux và Iptables nằm ngoài nhân. Iptables chịu trách nhiệm giao tiếp giữa người dùng và Netfilter để đẩy các luật của người dùng vào cho Netfilter xử lý. Netfilter tiến hành lọc các gói dữ liệu ở mức IP. Do Netfilter làm việc trực tiếp trong nhân, nhanh và không làm giảm tốc độ của hệ thống.



Hình 5.5 – Sơ đồ Netfilter / Iptables

5.1.5.2 chức năng của tường lửa Iptables

- Tích hợp tốt với nhân Linux, để cải thiện tốc độ xử lý gói tin và tính tin cậy của Iptables.
- Lọc tất cả các gói dữ liệu. Điều này cho phép tường lửa theo dõi mỗi một kết nối thông qua nó, dựa vào các thông số kỹ thuật (địa chỉ IP, cổng nguồn và đích) để tường lửa thực hiện các hành động đã được định sẵn.
- Lọc gói dựa trên địa chỉ MAC và các cờ trong TCP header. Điều này giúp ngăn chặn việc tấn công giả mạo gói tin, và truy cập từ mạng nội bộ đến mạng khác.

- Ghi nhật ký hệ thống cung cấp các tùy chọn điều chỉnh mức độ chi tiết của báo cáo kết quả hoạt động.
- Chuyển dịch địa chỉ mạng (NAT) tốt hơn.
- Hỗ trợ tích hợp với các chương trình web proxy như Squid.
- Ngăn chặn các kiểu tấn công từ chối dịch vụ.

5.1.5.3 Xử lý gói tin trong tường lửa Iptables

Tất cả các gói tin được kiểm tra bởi Iptables thông qua các bảng tuần tự được xây dựng (hàng đợi) để xử lý. Mỗi một hàng đợi được dành riêng xử lý cho một loại hình cụ thể các hoạt động của gói tin và được điều khiển bởi một chuỗi các hoạt động chuyển đổi / lọc gói tin thích hợp.

Tổng số có ba bảng:

- Đầu tiên là bảng Mangle có trách nhiệm cho sự thay đổi về chất lượng dịch vụ của các bit trong TCP header như là TOS (type of service), TTL (time to live), và MARK.
- Bảng thứ hai Filter chịu trách nhiệm lọc gói dữ liệu. Nó gồm có ba quy tắc nhỏ (chain) để giúp thiết lập các nguyên tắc lọc gói, bao gồm:
  - ✓ Forward chain: Lọc gói tin đến các máy chủ được bảo vệ bởi tường lửa.
  - ✓ Input chain: Lọc gói khi đi vào tường lửa.
  - ✓ Output chain: Lọc gói khi đi ra tường lửa.
- Bảng thứ ba NAT chịu trách nhiệm chuyển dịch địa chỉ mạng, gồm có hai loại:
  - ✓ Pre-routing chain: gói tin được NAT khi địa chỉ đích của gói tin cần phải được thay đổi.
  - ✓ Post-routing chain: gói tin được NAT khi địa chỉ nguồn của gói tin cần phải được thay đổi.

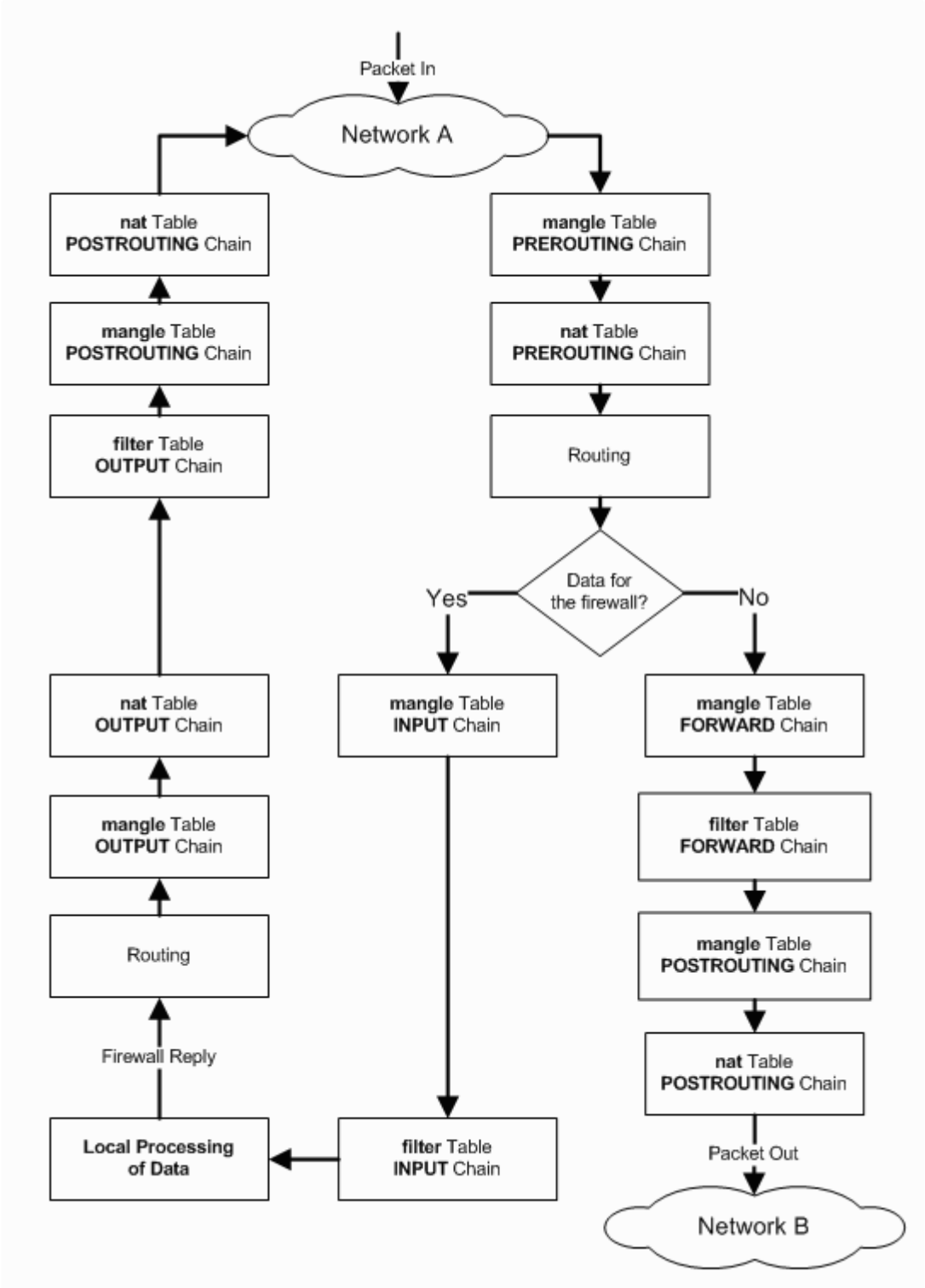
Bảng 5.1 – Xử lý các gói tin được định tuyến qua tường lửa

Loại	Chức	Quy tắc xử lý	Chức năng của Chain

bảng	năng của bảng	gói (Chain)	
Filter	Lọc gói tin	FORWARD	Lọc gói tin tới máy chủ có thể truy cập bởi NIC khác trên tường lửa.
		INPUT	Lọc gói tin đi vào tường lửa.
		OUTPUT	Lọc gói tin đi ra khỏi tưởng lửa.
NAT	Chuyển dịch địa chỉ mạng	PREROUTING	Chuyển dịch địa chỉ xảy ra trước khi định tuyến. Tạo điều kiện cho việc chuyển đổi địa chỉ IP đích để tương thích với bảng định tuyến của tường lửa. Sử dụng với NAT của địa chỉ IP đích hay DNAT.
		POSTROUTING	Chuyển dịch địa chỉ xảy ra sau khi định tuyến. Điều này có nghĩa là không cần phải sửa đổi địa chỉ IP đích của gói tin trước khi định tuyến. Được sử dụng với NAT địa chỉ IP nguồn bằng cách NAT một tới một IP hoặc nhiều tới một IP. Được gọi là NAT nguồn hay SNAT.
		OUTPUT	Chuyển dịch địa chỉ mạng cho gói tin được tạo ra bởi tường lửa.
Mangle	Chỉnh sửa TCP header	PREROUTING POSTROUTING OUTPUT INPUT FORWARD	Chỉnh sửa chất lượng dịch vụ các bit trong gói tin TCP trước khi xảy ra định tuyến.

Người quản trị cần phải chỉ rõ bảng và chain cho mỗi luật tường lửa được tạo ra. Có một ngoại lệ: Hầu hết các luật đều liên quan đến bộ lọc, vì thế giả sử rằng bất kỳ chain Iptables đã định nghĩa không có bảng thích hợp sẽ là một phần của bảng lọc. Vì vậy bảng lọc là mặc định.

Để hiểu rõ hơn về điều này, hãy xem cách các gói dữ liệu được xử lý bởi Iptables. Trong hình 5.6 một gói tin TCP từ Internet đến tại giao diện của tường lửa trên mạng A để tạo ra một kết nối dữ liệu.



Hình 5.6 – Sơ đồ đường đi của gói tin được xử lý trong Iptables

Đầu tiên các gói được kiểm tra bằng các luật trong chain PREROUTING của bảng mangle. Sau đó nó được kiểm tra bởi các luật trong chain PREROUTING của bảng NAT để xem các gói tin có yêu cầu DNAT hay không. Sau đó nó được định tuyến.

Nếu gói dữ liệu được dành cho một mạng được bảo vệ, sau đó nó được lọc theo các luật trong chain FORWARD của bảng filter, và nếu cần thiết, các gói dữ liệu phải trải qua SNAT trong chain POSTROUTING trong bảng NAT trước khi đến mạng B. Khi máy chủ đích có trả lời, các gói dữ liệu phải đi qua cùng một trình tự các bước như trên. Cả chain FORWARD và POSTROUTING có thể được cấu hình để thực hiện tính năng chất lượng dịch vụ (QoS) trong bảng mangle của, nhưng việc thiết lập này thường không được thực hiện trong môi trường SOHO.

Nếu gói dữ liệu được định hướng đi vào bên trong tường lửa, nó sẽ được kiểm tra bởi chain INPUT trong bảng mangle, và nếu gói dữ liệu qua được các kiểm tra của chain INPUT trong bảng filter, thì được đi vào các chương trình máy chủ bên trong tường lửa.

Khi tường lửa cần gửi dữ liệu ra ngoài. Gói dữ liệu sẽ được dẫn và đi qua sự kiểm tra của chain OUTPUT trong bảng mangle (nếu cần), tiếp đó là kiểm tra trong chain OUTPUT của bảng NAT để xem DNAT có cần hay không và chain OUTPUT của bảng filter sẽ kiểm tra gói dữ liệu nhằm phát hiện các gói dữ liệu không được phép gửi đi. Cuối cùng trước khi gói dữ liệu được đưa ra trở lại Internet, SNAT và QoS sẽ được kiểm tra trong chain POSTROUTING.

- **Targets và Jumps**

Targets là hành động sẽ diễn ra khi một gói dữ liệu được kiểm tra và phù hợp với môt yêu cầu nào đó. Khi một target đã được nhận dạng, gói dữ liệu cần nhảy (jump) để thực hiện các xử lý tiếp theo. Bảng sau liệt kê các targets mà Iptables sử dụng:

Bảng 5.2 – Trình bày các hành động mà tường lửa áp dụng

target	Miêu tả	Tùy chọn phổ biến nhất
ACCEPT	Iptables dừng xử lý gói dữ liệu đó và chuyển tiếp nó vào một ứng dụng cuối hoặc hệ điều hành để xử lý.	N/A

DROP	Iptables ngừng xử lý gói dữ liệu đó và gói dữ liệu bị chặn lại hoặc loại bỏ.	N/A
LOG	Thông tin của gói dữ liệu sẽ được đưa vào syslog để kiểm tra. Iptables tiếp tục xử lý gói với các luật kế tiếp.	`--log-prefix "string"` Iptables sẽ thêm vào log messange một chuỗi do người dùng định sẵn. Thông thường là để thông báo lý do vì sao gói bị bỏ.

REJECT	Tương tự như DROP, nhưng nó sẽ gửi trả lại cho phía người gửi một thông báo lỗi rằng gói đã bị chặn và loại bỏ.	`--reject-with qualifier`
		
		Tham số qualifier sẽ cho biết loại thông báo gửi trả lại. Qualifier gồm các loại sau:
		
		`icmp-port-unreachable (default)`
		`icmp-net-unreachable`
		`icmp-host-unreachable`
		`icmp-proto-unreachable`
		`icmp-net-prohibited`
		`icmp-host-prohibited`
		`tcp-reset`
		`echo-reply`

DNAT	Dùng để thực hiện chuyển dịch địa chỉ mạng đích, địa chỉ IP đích của gói dữ liệu sẽ được viết lại.	`--to-destination ipaddress` Cho Iptables những địa chỉ IP đích nên thay đổi.
SNAT	Dùng để thực hiện chuyển dịch địa chỉ mạng nguồn, viết lại địa chỉ IP nguồn của gói dữ liệu.	`--to-source <address>[-<address>][:<port>-<port>]` Xác định địa chỉ IP và cổng nguồn được sử dụng bởi SNAT.
MASQUERADE	Dùng để thực hiện chuyển dịch địa chỉ mạng nguồn. Mặc định, địa chỉ IP nguồn giống với giao diện của tường lửa.	`[--to-ports <port>[-<port>]]` Chỉ ra cụ thể phạm vi của các cổng nguồn mà cổng gốc có thể được ánh xạ.

- **Các tham số chuyển mạch quan trọng của Iptables:**

Các tham số sau sẽ cho phép Iptables thực hiện các hành động sao cho phù hợp với biểu đồ xử lý gói dữ liệu do người quản trị hoạch định sẵn.

Bảng 5.3 – Bảng các tham số chuyển mạch quan trọng của Iptables

Lệnh chuyển mạch iptables	Miêu tả

-t <-table->	Nếu không chỉ định rõ là bảng nào, thì bảng filter sẽ được áp dụng.
-j <target>	Nhảy đến một chain đích nào đó khi gói dữ liệu phù hợp với luật hiện tại.
-A	Gắn thêm một luật nào đó vào cuối một chain.
-F	Xóa hết tất cả mọi luật trong bảng đã chọn.
-p <protocol-type>	Chỉ ra giao thức áp dụng, bao gồm icmp, tcp, udp.
-s <ip-address>	Chỉ ra địa chỉ IP nguồn.
-d <ip-address>	Chỉ ra địa chỉ IP đích.
-i <interface-name>	Chỉ ra giao diện "input" khi gói dữ liệu đi vào.
-o <interface-name>	Chỉ ra giao diện "output" khi gói dữ liệu đi ra.

Để hiểu rõ thêm và các lệnh ta cùng xét một ví dụ thiết lập luật như sau:

```
iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1  -p TCP -j
ACCEPT
```

Với luật trên Iptables được cấu hình cho phép tường lửa chấp nhận các gói dữ liệu có giao thức là TCP, đến từ giao diện mạng eth0, có địa chỉ IP nguồn là bất kỳ đi đến địa chỉ 192.168.1.1 là địa chỉ IP của tường lửa (0/0 nghĩa là bất kỳ địa chỉ IP nào).

Bảng 5.4 – Các điều kiện TCP và UDP thông dụng

Switch	Desciption
-p tcp --sport <port>	Chỉ ra giao thức áp dụng TCP và cổng nguồn. Có thể là một cổng đơn lẻ hoặc một chuỗi theo định dạng: *start-port-number:end-port-number*
-p tcp --dport <port>	Chỉ ra giao thức áp dụng TCP và cổng đích. Có thể là một cổng đơn lẻ hoặc một chuỗi theo định dạng: *starting-port:ending-port*
-p tcp --syn	Sử dụng để nhận dạng một yêu cầu kết nối TCP mới. ! --syn, nghĩa là không phải là một yêu cầu kết nối mới.
-p udp --sport <port>	Chỉ ra giao thức áp dụng UDP và cổng nguồn. Có thể là một cổng đơn lẻ hoặc một chuỗi theo định dạng: *starting-port:ending-port*
-p udp --dport <port>	Chỉ ra giao thức sử dụng UDP và cổng đích. Có thể là một cổng đơn lẻ hoặc một chuỗi theo định dạng: *starting-port:ending-port*

Bảng 5.5 – Các luật mở rộng

Switch	Desciption
`-m multiport --sports <port, port>`	Cấu hình nhiều cổng TCP/UDP nguồn, mỗi cổng được phân cách bằng dấu phẩy (,). Đây là liệt kê các cổng chứ không phải là một chuỗi các cổng liền nhau.
`-m multiport --dports <port, port>`	Cấu hình nhiều cổng TCP/UDP đích, mỗi cổng được phân cách bằng dấu phẩy (,).Đây cũng là liệt kê các cổng chứ không phải là một chuỗi các cổng liền nhau.
`-m multiport --ports <port, port>`	Cấu hình đồng thời nhiều cổng TCP/UDP và được phân cách bằng dấu phẩy (,). Đây cũng là liệt kê các cổng. Không phân biệt cổng nguồn hay cổng đích.
`-m --state <state>`	Các trạng thái thường xuyên được sử dụng: **ESTABLISHED:** Gói dữ liệu là một phần của kết nối đã được thiết lập trong cả hai hướng. **NEW:** Gói dữ liệu là bắt đầu một kết nối mới. **RELATED:** Gói dữ liệu bắt đầu một kết nối phụ. Đây là một tính năng phổ biến của các giao thức như là giao thức truyền dữ liệu FTP, hoặc giao thức ICMP. **INVALID:** Gói dữ liệu không thể nhận dạng được. Điều này có thể do việc thiếu tài nguyên hệ thống hoặc lỗi ICMP không trùng với một luồng dữ liệu có sẵn.

Sử dụng chuỗi được người dùng định nghĩa

Người quản trị có thể cấu hình Iptables để có chuỗi người dùng định nghĩa. Tính năng này thường được sử dụng để giúp đơn giản quá trình xử lý gói tin. Ví dụ, thay vì sử dụng một giao thức, nên xây dựng chuỗi cho tất cả các giao thức, có thể sử dụng chuỗi để xác định loại giao thức cho gói dữ liệu và sau đó chuyển giao tiến trình thực tế cuối cùng tới một định nghĩa của người dùng, chuỗi giao thức cụ thể trong lọc bảng. Nói cách khác, có thể thay thế một chuỗi dài với một chuỗi ngắn chính trỏ tới nhiều chuỗi ngắn, qua đó rút ngắn chiều dài của tất cả các chuỗi mà gói dữ liệu đi qua. Ví dụ sáu lệnh sau giúp việc cải tiến tốc độ xử lý:

```
iptables -A INPUT -i eth0  -d 206.229.110.2 -j fast-input-
```

```
queue
iptables -A OUTPUT -o eth0 -s 206.229.110.2 -j fast-output-
queue

iptables -A fast-input-queue  -p icmp -j icmp-queue-in
iptables -A fast-output-queue -p icmp -j icmp-queue-out

iptables -A icmp-queue-out -p icmp --icmp-type echo-request \
         -m state --state NEW -j ACCEPT

iptables -A icmp-queue-in -p icmp --icmp-type echo-reply -j
ACCEPT
```

Trong đó:

Chain	Miêu tả
INPUT	Được xây dựng trong chuỗi INPUT của Iptables
OUTPUT	Được xây dựng trong chuỗi OUTPUT của Iptables
fast-input-queue	Chuỗi đầu vào dành riêng cho việc xác định các giao thức cụ thể và phân luồng các gói dữ liệu đến chuỗi giao thức cụ thể.
fast-output-queue	Chuỗi đầu ra dành riêng cho việc xác định các giao thức cụ thể và phân luồng các gói dữ liệu đến chuỗi giao thức cụ thể.
icmp-queue-out	Đầu ra dành riêng cho giao thức ICMP.
icmp-queue-in	Đầu vào dành riêng cho giao thức ICMP.

Lưu và phục hồi các đoạn mã lệnh trong Iptables

Iptables lưu nội dung các dòng lệnh cấu hình đã được nhập vào tới màn hình hoặc STOUT. Bằng cách chuyển hướng đầu ra tới một tập tin, sử dụng lệnh sau để khôi phục lại dữ liệu và trở lại iptables để cấu hình khi lệnh iptables-save được thực hiện. Khi daemon Iptables khởi động, nó kiểm tra sự tồn tại của tập tin /etc/sysconfig/iptables. Đây là tập tin mà nó sử dụng các cấu hình mặc định. Tập tin này cũng là nơi mà Iptables-save trỏ tới. Vì vậy để lưu lại cấu hình của tường lửa để nó kích hoạt tồn tại khi được khởi động, cần phải chuyển hướng đầu ra của lệnh iptables-save đối với tập tin này như sau:

```
[root@bigboy tmp]# iptables-save > /etc/sysconfig/iptables
```

Định dạng của tệp tin /etc/sysconfig/iptables là hơi khác với các đoạn mã trình bày trong chương này. Việc khởi tạo chuỗi tích hợp là tự động và chuỗi "Iptables" được bỏ qua từ các luật đã thực hiện. Đây là một ví dụ cấu hình tệp tin /etc/sysconfig/iptables để cho phép ICMP, IPsec (gói dữ liệu ESP và AH), các kết nối đã được thiết lập, và đầu vào SSH.

Không phải là một ý tưởng hay nếu chỉnh sửa đoạn mã này trực tiếp bởi vì nó luôn luôn được ghi đè bởi lệnh iptables-save và nó không lưu bất kỳ chú giải nào, mà cũng khó khăn để làm theo. Với những lý do này, người quản trị nên viết và áp dụng một đoạn mã tùy biến và sau đó sử dụng lệnh iptables-save để thực hiện những thay đổi cố định. Dưới đây là một ví dụ hướng dẫn làm thế nào để tự phục hồi cấu hình của Iptables bằng cách sử dụng lệnh iptables-restore. Trong trường hợp này, tệp tin được khôi phục lại là /etc/sysconfig/iptables.

```
[root@bigboy tmp]# iptables-restore -c <
/etc/sysconfig/iptables
```

Đôi khi đoạn mã được tạo ra để thực hiện các luật Iptables có thể bị hỏng hoặc bị mất, hoặc được kế thừa từ một hệ thống mới và không tìm thấy đoạn mã ban đầu được sử dụng để bảo vệ nó. Trong những tình huống này, có thể sử dụng các lệnh iptables-save và iptables-restore để giúp người quản trị quản lý liên tục tường lửa.

Các mô-đun (module) trong nhân Linux cần thiết để khởi động Iptables

Tường lửa Iptables yêu cầu phải tải các mô-đun nhất định trong nhân Linux để kích hoạt một số chức năng của nó. Bất cứ khi nào các loại NAT được yêu cầu thì mô-đun iptable_nat cần phải được nạp. Mô-đun ip_conntrack_ftp cần phải được thêm vào để hỗ trợ giao thức FTP và phải luôn luôn được nạp với mô-đun ip_conntrack nhằm theo dõi trạng thái kết nối TCP. Hầu hết các đoạn mã có thể sẽ theo dõi các trạng thái kết nối, vì vậy mô-đun ip_conntrack sẽ cần thiết trong mọi trường hợp. Mô-đun ip_nat_ftp cũng cần phải được nạp cho các máy chủ FTP phía sau tường lửa NAT.

Chú ý: Trong Linux tệp tin /etc/sysconfig/iptables không hỗ trợ việc tải các mô-đun. Vì vậy, chúng ta phải thêm vào những trạng thái đó vào tệp tin /etc/rc.local và chạy nó tại cuối mỗi lần khởi động lại.

Những mẫu đoạn mã trong phần này bao gồm những trạng thái được lưu trong tệp tin /etc/rc.local:

```
# File: /etc/rc.local

# Module to track the state of connections
modprobe ip_conntrack

# Load the iptables active FTP module, requires ip_conntrack
modprobe ip_conntrack_ftp

# Load iptables NAT module when required
modprobe iptable_nat

# Module required for active an FTP server using NAT
modprobe ip_nat_ftp
```

Hệ điều hành thiết lập các phòng thủ cơ bản

Người quản trị có thể cấu hình một vài thứ trên Linux trước khi triển khai các đoạn mã lệnh cho tường lửa để nâng cao khả năng phòng thủ của tường lửa để chống lại tấn công. Ví dụ, hệ điều hành Linux có một số cơ chế bảo vệ được xây dựng sẵn, nên được kích hoạt bằng cách thay đổi các tham số nhân hệ thống trong tập tin /etc/sysctl.conf.

Nâng cao khả năng khởi tạo cho tường lửa

Ngoài những thiết lập ở trên, có thêm một số bước khởi tạo nâng cao hơn tới đoạn mã của tường lửa, bao gồm cả kiểm tra đường truyền truy cập Internet từ những địa chỉ riêng RFC1918. Khởi tạo phức tạp hơn sẽ bao gồm kiểm tra các cuộc tấn công sử dụng cờ TCP không hợp lệ và định hướng gói tin broadcast.

Đoạn mã cũng sử dụng nhiều chuỗi người dùng định nghĩa để thực hiện mã ngắn hơn và nhanh hơn như các chuỗi có thể nhiều lần truy cập. Điều này loại bỏ sự cần thiết phải lặp lại các dòng lệnh tương tự.

Người quản trị có thể sử dụng nhiều biện pháp phòng thủ để bảo vệ hệ thống mạng.

Cấu hình Iptables để cho phép DNS truy cập tới tường lửa

Một tường lửa cần phải cho phép truy vấn DNS tới Internet. Đây là một chức năng cơ bản của tường lửa. Các dòng lệnh sau đây sẽ được áp dụng không chỉ với tường lửa hoạt động là một máy trạm DNS mà còn cho các tường lửa làm việc trong một bộ nhớ đệm hoặc máy chủ đóng vai trò cung cấp dịch vụ DNS.

```
#------------------------------------------------------------
---
# Allow outbound DNS queries from the FW and the replies too
#
# - Interface eth0 is the internet interface
#
# Zone transfers use TCP and not UDP. Most home networks
# / websites using a single DNS server won't require TCP
statements
#
#------------------------------------------------------------
---

iptables -A OUTPUT -p udp -o eth0 --dport 53 --sport
1024:65535 \
         -j ACCEPT

iptables -A INPUT -p udp -i eth0 --sport 53 --dport
1024:65535 \
         -j ACCEPT
```

Cấu hình Iptables cho phép giao thức HTTP và SSH truy cập tới tường lửa

Đoạn mã mẫu sau đây áp dụng cho một tường lửa mà cung cấp cùng lúc hai dịch vụ một máy chủ web được quản lý từ xa bởi người quản trị hệ thống qua các phiên SSH. Các gói dữ liệu đi vào được chỉ định dành cho các cổng 80 và 22 phải được phép, do đó đây bước đầu tiên cần phải thực hiện trong việc thiết lập một kết nối. Không cần thiết để xác định các cổng khi gói dữ liệu trả về (gói dữ liệu đi ra) cho tất cả các kết nối đã được thiết lập và đã cho phép. Các kết nối khởi tạo bởi người dùng đăng nhập vào máy chủ web sẽ bị từ chối.

Thiết lập Iptables thực hiện chức năng NAT tĩnh

Trong ví dụ này, tất cả lưu lượng tới một địa chỉ IP công cộng đặc biệt, không chỉ tới một cổng đặc biệt, được chuyển dịch tới một máy chủ đơn trên mạng con được bảo vệ. Bởi vì các bức tường lửa có nhiều địa chỉ IP (nhiều giao diện mạng), ta không thể thực hiện MASQUERADE; nó sẽ buộc giả mạo như là địa chỉ IP của giao tiếp chính. Thay vào đó, sử dụng SNAT để chỉ rõ địa chỉ IP alias được sử dụng cho các kết nối khởi tạo bởi tất cả các máy chủ khác trong mạng được bảo vệ.

Cần phải tạo ra địa chỉ IP alias cho mỗi một IP Internet cho phương pháp NAT một tới một làm việc.

5.2. TRIỂN KHAI CÔNG NGHỆ PHÁT HIỆN VÀ NGĂN CHẶN XÂM NHẬP TRÁI PHÉP

5.2.1. Thiết kế và lựa chọn hệ thống

5.2.1.1 Giới thiệu hệ thống phát hiện và ngăn chặn xâm nhập IDPS

Phát hiện xâm nhập là tiến trình theo dõi các sự kiện xảy ra trên một hệ thống máy tính hay hệ thống mạng, phân tích chúng để tìm ra các dấu hiệu "xâm nhập bất hợp pháp". Xâm nhập bất hợp pháp được định nghĩa là sự cố gắng tìm mọi cách để xâm hại đến tính toàn vẹn, tính sẵn sàng, tính có thể tin cậy hay là sự cố gắng vượt qua các cơ chế bảo mật của hệ thống máy tính hay mạng đó. Việc xâm nhập có thể là xuất phát từ một kẻ tấn công nào đó trên mạng Internet nhằm giành quyền truy cập hệ thống, hay cũng có thể là một người dùng được phép trong hệ thống đó muốn chiếm đoạt các quyền khác mà họ chưa được cấp phát. Như đã đề cập ở trên, hệ thống phát hiện xâm nhập là hệ thống phần mềm hoặc phần cứng có khả năng tự động theo dõi và phân tích để phát hiện ra các dấu hiệu xâm nhập.

Ngăn chặn xâm nhập là quá trình thực hiện phát hiện xâm nhập và cố gắng để ngăn chặn các sự cố được phát hiện ra. Hệ thống phát hiện và ngăn chặn xâm nhập (IDPS - Intrusion Detection and Prevention Systems) chủ yếu tập trung vào việc xác định sự cố có thể xảy ra, ghi lại thông tin về sự cố đó, cố gắng để ngăn chặn chúng, và lập báo cáo với quản trị hệ thống mạng.

Ngoài ra, các tổ chức sử dụng IDPS cho các mục đích khác, chẳng hạn như xác định các vấn đề với chính sách an ninh, ghi lại các mối đe dọa hiện tại và ngăn chặn các hành vi vi phạm chính sách an ninh mạng. IDPS là thành phần bổ sung cần thiết cho hạ tầng an ninh mạng của các tổ chức, công ty.

5.2.1.2 Chức năng của IDPS:

Có nhiều loại công nghệ IDPS, sự khác biệt chủ yếu là do các loại sự kiện mà chúng có thể phát hiện và các phương pháp mà chúng sử dụng để xác định sự cố. Ngoài việc giám sát và phân tích các sự kiện để xác định hoạt động không mong muốn, tất cả các loại công nghệ IDPS thường thực hiện các chức năng sau:

- Ghi lại thông tin liên quan đến các sự kiện giám sát: Thông tin thường được ghi lại và lưu ngay trên thiết bị và cũng có thể được gửi đến hệ thống máy chủ giám sát an ninh tập trung (SIEM).
- Thông báo cho nhân viên quản trị các sự kiện an ninh quan trọng: Các thông báo này được biết đến như một cảnh báo, thực hiện thông qua một số phương pháp như: e-mail, trang web, tin nhắn trên giao diện quản trị IDPS, Simple Network Management Protocol (SNMP) bẫy, tin nhắn syslog.

5.2.1.3 Các kỹ thuật phát hiện xâm nhập trái phép

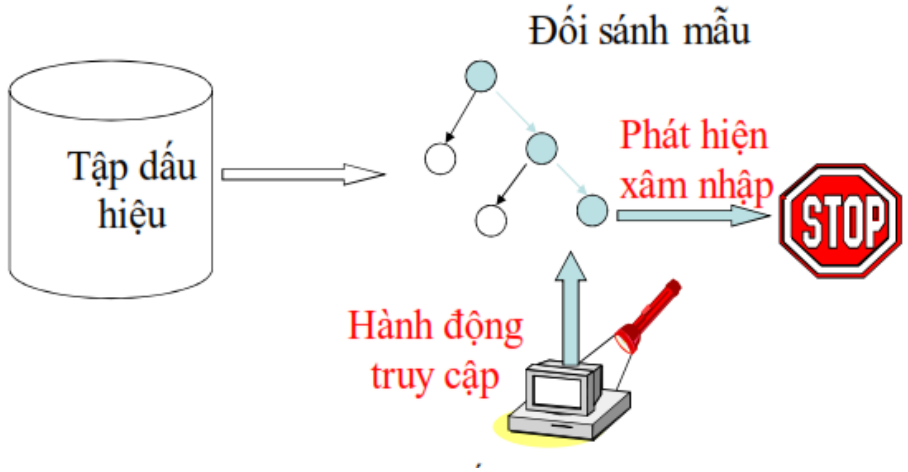
IDS sử dụng nhiều kỹ thuật khác nhau để phát hiện các hành động xâm nhập hệ thống trái phép. Những kỹ thuật cơ bản như: Dựa trên dấu hiệu, sự kiện bất thường và dựa trên mô hình. Thông thường IDS sử dụng nhiều phương pháp phát hiện xâm nhập và đôi khi cũng sử dụng phương pháp riêng lẻ hay kết hợp nhằm phát hiện chính xác các hành động xâm nhập.

- **Phát hiện dựa trên dấu hiệu:**

Dấu hiệu là một mẫu tương ứng với các đe dọa đã biết được thống kê các đặc trưng và lưu lại trên hệ thống. Hệ thống sẽ thu thập các thông tin liên quan và so sánh với các dấu hiệu tấn công được lưu trữ trong cơ sở dữ liệu để xác định xem hành động đó có nguy hiểm hay không. Ví dụ sau đây mô tả cách IDS phát hiện xâm nhập dựa vào dấu hiệu.

- Cố gắng telnet với tên người dùng “root”, điều này vi phạm chính sách an toàn của hệ thống.

- Thư điện tử có tiêu đề “Free pictures!” đính kèm file “freepics.exe” và file này có đặc điểm của mã độc hại đã biết.



Hình 5.7 - Mô tả dấu hiệu xâm nhập

Kỹ thuật này rất hiệu quả trong việc phát hiện các đe dọa đã biết nhưng lại không hiệu quả trong việc phát hiện những nguy cơ chưa được biết. Ví dụ kẻ tấn công sửa tên file thành “freepic2.exe”, thì việc tìm kiếm dấu hiệu trên với mã độc hại này sẽ không hiệu quả.

Phát hiện dựa vào dấu hiệu là một kỹ thuật đơn giản vì nó chỉ so sánh hành động hiện tại với danh sách dấu hiệu đã biết bằng cách so sánh các toán tử. Kỹ thuật này ít được dùng trong mô hình mạng lớn hay các giao thức ứng dụng bởi vì nó không thể theo dõi và hiểu được trạng thái của tất cả các thành phần phức tạp trong hệ thống. Bên cạnh đó kỹ thuật này không có khả năng ghi nhớ những yêu cầu trước đó khi có một yêu cầu hiện tại. Do đó việc phát hiện tấn công dựa trên phương pháp này có độ tin cậy không cao.

- **Phát hiện dựa trên sự bất thường:**

Phát hiện dựa vào sự bất thường là quá trình so sánh hành động được coi là bình thường với các sự kiện đang diễn ra nhằm phát hiện ra sự bất thường. Với kỹ thuật này IDS dựa vào profile miêu tả hành động bình thường của nhiều đối tượng như người dùng, máy chủ, các kết nối mạng, hay ứng

dụng. Profile này được tạo ra bằng cách giám sát các hành động thông thường trong một khoảng thời gian để đưa ra đặc điểm nổi bật của hành động đó.

Kỹ thuật này chỉ có độ chính xác cao khi IDS được gắn vào một hệ thống mạng cụ thể và có thời gian đủ lâu để học tất cả các hành động bình thường của hệ thống.

- **Kỹ thuật phát hiện dựa vào phân tích trạng thái giao thức:**

Phân tích trạng thái giao thức là quá trình phân tích hành vi của giao thức được sử dụng trên cơ sở đã biết các định nghĩa về hoạt động hợp lệ của giao thức để nhận ra hành vi tấn công. Kỹ thuật này dựa vào profile liên quan đến giao thức mà IDS hỗ trợ. "Trạng thái" trong phân tích trạng thái giao thức nghĩa là IDS có khả năng hiểu và theo dõi trạng thái của mạng, truyền tải và các giao thức ứng dụng.

Điều ngăn cản chính của phương pháp này chính là việc tập trung tài nguyên, bởi vì sự phức tạp trong quá trình phân tích và thực hiện giám sát trạng thái cho nhiều phiên làm việc đồng thời. Một vấn đề khác là phương pháp này không thể phát hiện được các tấn công có đặc trưng mà hành vi thông thường của giao thức được thừa nhận, như việc thực hiện nhiều hành động trong một khoảng thời gian ngắn như tấn công từ chối dịch vụ. Hơn nữa, chuẩn giao thức được sử dụng trong IDS có thể xung đột với cách thực hiện của giao thức hiện có trong mạng.

- **Phát hiện dựa trên mô hình:**

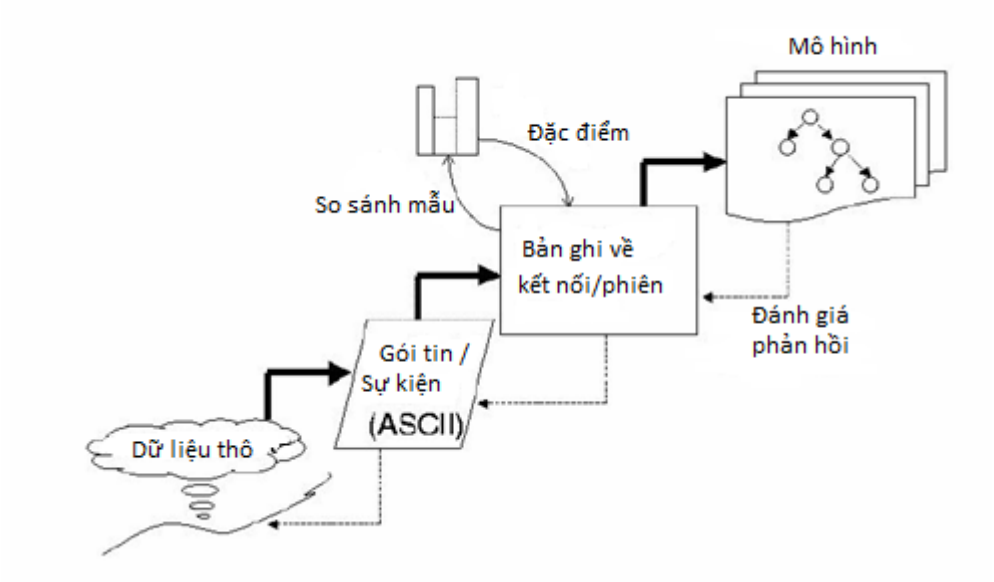
Phương pháp phát hiện dựa trên mô hình sử dụng các kỹ thuật học máy, khai phá dữ liệu, trí tuệ nhân tạo để xây dựng các mô hình, các luật phát hiện tấn công một cách tự động từ các tập dữ liệu mô phỏng tấn công. Sau đó các mô hình được sử dụng trong các hệ thống IDS để dự đoán các tấn công mới. Phương pháp này có ưu điểm là cho phép phát hiện được các tấn công mới, tuy nhiên hạn chế của nó là đưa ra nhiều cảnh báo nhầm hơn các phương pháp trên. Phát hiện nhờ quá trình tự học: Kỹ thuật này bao gồm hai bước. Khi bắt đầu thiết lập, hệ thống phát hiện tấn công sẽ chạy ở chế độ tự học và tạo ra một hồ sơ về cách cư xử của mạng với các hoạt động bình thường. Sau thời gian khởi tạo, hệ thống sẽ chạy ở chế độ làm việc, tiến hành theo dõi, phát

hiện các hoạt động bất thường của mạng bằng cách so sánh với hồ sơ đã thiết lập.

- **Ứng dụng kỹ thuật khai phá dữ liệu cho việc phát hiện xâm nhập trái phép**

Khai phá dữ liệu là một phướng pháp tiếp cận tương đối mới trong việc phát hiện xâm nhập. Khai phá dữ liệu được định nghĩa cụ thể theo "Sự khám phá ra các mẫu, các mối quan hệ, các biến đổi, những sự bất thường, những qui luật, những cấu trúc và sự kiện quan trọng mang tính chất thống kê trong dữ liệu". Trong đó tồn tại nhiều kiểu thuật toán khai phá dữ liệu khác nhau như: phân lớp, phân tích hồi quy, phân cụm, khai phá luật kết hợp…Công việc khai phá dữ liệu trong phát hiện xâm nhập trái phép là để trích lọc tri thức từ một tập dữ liệu lớn của các thông tin truy cập trên mạng, để phân tích biểu diễn nó thành mô hình phát hiện xâm nhập trái phép. Phương pháp tiếp cận này xét về việc phát hiện xâm nhập như là tiến trình phân tích dữ liệu, trong khi đó các phương pháp tiếp cận trước là những quá trình kỹ nghệ tri thức.

Phương pháp khai phá dữ liệu để phát hiện xâm nhập lần đầu tiên được thực hiện bởi MADAMID (Mining Audit Data for Automated Models for Instruction Detection: Khai phá dữ liệu được sử dụng trong mô hình tự động để phát hiện xâm nhập). Quá trình khai phá dữ liệu trong việc xây dựng những mô hình phát hiện xâm nhập. Dữ liệu thô đầu tiên được chuyển đổi thành thông tin gói dữ liệu mạng với mã ASCII mà lần lượt nó được chuyển đổi thành thông tin ở mức truy cập Những bản ghi ở mức truy cập này chứa trong đó những thuộc tính kết nối như là dịch vụ, thời gian kết nối v.v…



Hình 5.8 - Quá trình khai phá dữ liệu của việc xây dựng mô hình PHXN

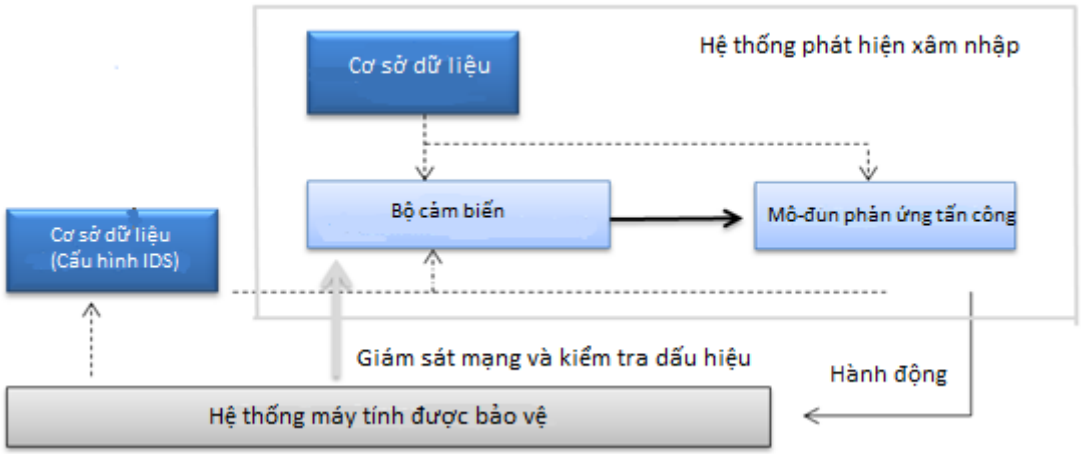
Thuật toán khai phá dữ liệu được áp dụng cho những dữ liệu này để tạo ra các mô hình phát hiện xâm nhập. Các thuật toán khai phá dữ liệu được dùng trong phương pháp này là RIPPER "Thuật toán phân lớp dựa vào luật", siêu phân lớp, thuật toán hồi qui, luật kết hợp. Các thuật toán này được áp dụng để kiểm soát dữ liệu, tính toán các mô hình mà thu thập chính xác hành vi thực tế việc xâm nhập trái phép cũng như các hoạt động bình thường.

Thuật toán RIPPER được dùng để học mô hình phân lớp để xác định diễn biến bình thường và diễn biến bất thường trong hệ thống. Kỹ thuật hồi quy và tương quan được dùng để xây dựng các mẫu liên tiếp từ các bản ghi dữ liệu thu thập. Những mẫu liên tiếp này biểu diễn lại những tổng hợp thống kê về mạng và hoạt động của hệ thống bằng cách đo lường sự tương quan giữa tính chất của hệ thống và dãy đồng loạt các sự kiện xảy ra cùng lúc. Từ các mẫu liên tiếp được xây dựng các mẫu phù hợp của các hoạt động bình thường, các mẫu xâm nhập trái phép được bổ sung tạo ra cơ sở dữ liệu học. Cơ sở dữ liệu này cho phép việc học mô hình xâm nhập hiệu quả hơn nhằm để phát hiện xâm nhập bằng các thuật toán khai phá dữ liệu khác nhau.

Phân tích và khai phá dữ liệu thu thập kết hợp với luật và thuật toán phân lớp để phát hiện ra các cuộc tấn công trên dữ liệu thu thô. Luật kết hợp được sử dụng để thu thập những tri thức cần thiết về bản chất của dữ liệu thô

chẳng hạn như thông tin về các mẫu trên từng bản ghi có thể cải thiện hiệu quả việc phân lớp. Hệ thống này có hai giai đoạn, giai đoạn huấn luyện và giải đoạn phát hiện. Trong cơ sở dữ liệu ở giai đoạn huấn luyện của các tập mẫu thường xuyên được tạo cho các mẫu tấn công miễn phí từ việc sử dụng duy nhất việc tấn công miễn phí tập dữ liệu. Điều này phục vụ như là sơ lượt lại mà các mẫu dữ liệu thường xuyên tìm thấy sau đó sẽ được so sánh. Tiếp theo một cửa số trượt, sử dụng thuật toán trực tuyến để tìm bộ mẫu thường xuyên trong kết nối D cuối cùng và so sánh chúng với những tập dữ liệu được lưu trữ trong cơ sở dữ liệu tấn công miễn phí, loại bỏ những dữ liệu được coi là bình thường. Tại giai đoạn phân lớp là chỉ được huấn luyện để học mô hình phát hiện xâm nhập. Tại giai đoạn phát hiện một thuật toán tự động được dùng để đưa ra tập mẫu mà được xem là đáng ngờ và được dùng bởi thuật toán phân lớp đã học để phân lớp các mẫu như tấn công, báo động giả hoặc không xác định. Các tấn công không xác định là những cuộc tấn công không có khả năng để phát hiện như báo động giả hoặc biết được các cuộc tấn công. Thử nghiệm phương pháp này chỉ để phát hiện các cuộc tấn công bình thường.

5.2.1.4 Kiến trúc hệ thống IDPS

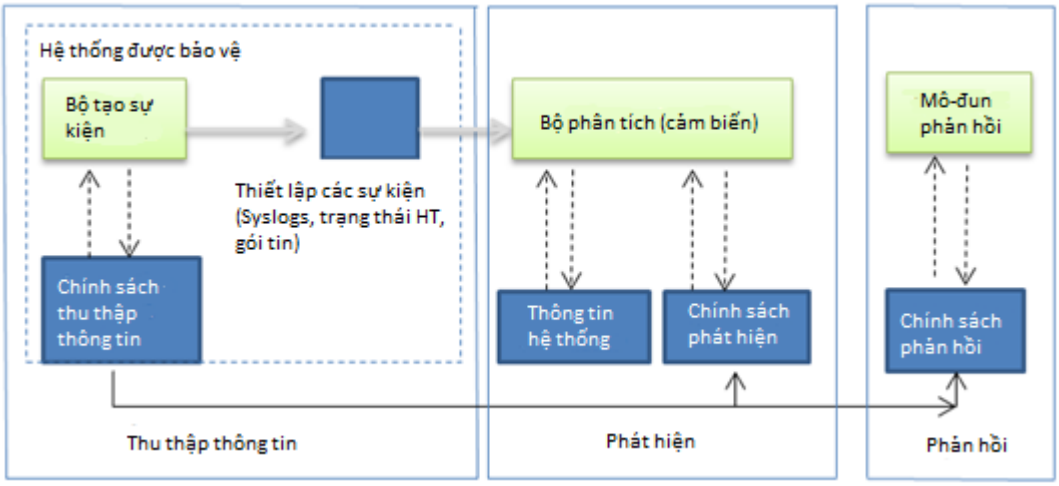


Hình 5.9 – Kiến trúc hệ thống phát hiện xâm nhập

Kiến trúc của hệ thống IDS bao gồm các thành phần chính: Thành phần thu thập gói tin (information collection), thành phần phân tích gói tin (Dectection), thành phần phản hồi (respontion) nếu gói tin đó được phát hiện

là một tấn công của tin tặc. Trong ba thành phần này thì thành phần phân tích gói tin là quan trọng nhất và ở thành phần này bộ cảm biến đóng vai trò quyết định nên chúng ta sẽ đi vào phân tích bộ cảm biến để hiểu rõ hơn kiến trúc của hệ thống phát hiện xâm nhập là như thế nào. Bộ phận phát hiện gói tin: Trong bộ phận phát hiện gói tin có một thành phần quan trọng đó là bộ cảm biến.

Bộ cảm biến được tích hợp với thành phần sưu tập dữ liệu – một bộ tạo sự kiện. Cách sưu tập này được xác định bởi chính sách tạo sự kiện để định nghĩa chế độ lọc thông tin sự kiện. Bộ tạo sự kiện (hệ điều hành, mạng, ứng dụng) cung cấp một số chính sách thích hợp cho các sự kiện, có thể là một bản ghi các sự kiện của hệ thống hoặc các gói mạng. Số chính sách này cùng với thông tin chính sách có thể được lưu trong hệ thống được bảo vệ hoặc bên ngoài. Trong trường hợp nào đó, ví dụ khi luồng dữ liệu sự kiện được truyền tải trực tiếp đến bộ phân tích mà không có sự lưu dữ liệu nào được thực hiện. Điều này cũng liên quan một chút nào đó đến các gói mạng.



Hình 5.10 – Vai trò của bộ cảm biến

Vai trò của bộ cảm biến là dùng để lọc thông tin và loại bỏ dữ liệu không tương thích đạt được từ các sự kiện liên quan với hệ thống bảo vệ, vì vậy có thể phát hiện được các hành động nghi ngờ. Bộ phân tích sử dụng cơ sở dữ liệu chính sách phát hiện cho mục này. Ngoài ra còn có các thành phần: dấu hiệu tấn công, profile hành vi thông thường, các tham số cần thiết (ví dụ: các ngưỡng). Thêm vào đó, cơ sở dữ liệu giữ các tham số cấu hình, gồm có các chế độ truyền thông với module đáp trả. Bộ cảm biến cũng có cơ sở dữ

liệu của riêng nó, gồm dữ liệu lưu về các xâm phạm phức tạp tiềm ẩn (tạo ra từ nhiều hành động khác nhau).

IDS có thể được sắp đặt tập trung (ví dụ như được tích hợp vào trong tường lửa) hoặc phân tán. Một IDS phân tán gồm nhiều IDS khác nhau trên một mạng lớn, tất cả chúng truyền thông với nhau. Nhiều hệ thống tinh vi đi theo nguyên lý cấu trúc một tác nhân, nơi các module nhỏ được tổ chức trên một host trong mạng được bảo vệ.

Vai trò của tác nhân là để kiểm tra và lọc tất cả các hành động bên trong vùng được bảo vệ và phụ thuộc vào phương pháp được đưa ra – tạo phân tích bước đầu và thậm chí đảm trách cả hành động đáp trả. Mạng các tác nhân hợp tác báo cáo đến máy chủ phân tích trung tâm là một trong những thành phần quan trọng của IDS. DIDS có thể sử dụng nhiều công cụ phân tích tinh vi hơn, đặc biệt được trang bị sự phát hiện các tấn công phân tán. Các vai trò khác của tác nhân liên quan đến khả năng lưu động và tính roaming của nó trong các vị trí vật lý. Thêm vào đó, các tác nhân có thể đặc biệt dành cho việc phát hiện dấu hiệu tấn công đã biết nào đó. Đây là một hệ số quyết định khi nói đến nghĩa vụ bảo vệ liên quan đến các kiểu tấn công mới.

Giải pháp kiến trúc đa tác nhân được đưa ra năm 1994 là AAFID (các tác nhân tự trị cho việc phát hiện xâm phạm). Nó sử dụng các tác nhân để kiểm tra một khía cạnh nào đó về các hành vi hệ thống ở một thời điểm nào đó. Ví dụ: một tác nhân có thể cho biết một số không bình thường các telnet session bên trong hệ thống nó kiểm tra. Tác nhân có khả năng đưa ra một cảnh báo khi phát hiện một sự kiện khả nghi. Các tác nhân có thể được nhái và thay đổi bên trong các hệ thống khác (tính năng tự trị). Một phần trong các tác nhân, hệ thống có thể có các bộ phận thu phát để kiểm tra tất cả các hành động được kiểm soát bởi các tác nhân ở một host cụ thể nào đó. Các bộ thu nhận luôn luôn gửi các kết quả hoạt động của chúng đến bộ kiểm tra duy nhất. Các bộ kiểm tra nhận thông tin từ các mạng (không chủ từ một host), điều đó có nghĩa là chúng có thể tương quan với thông tin phân tán. Thêm vào đó một số bộ lọc có thể được đưa ra để chọn lọc và thu thập dữ liệu.

Ngoài ra còn có 1 số điểm chú ý sau:

- Kiến trúc, vị trí đặt hệ thống IDS: tùy thuộc vào quy mô tổ chức của doanh nghiệp cũng như mục đích sử dụng hệ thống IDS của doanh nghiệp.
- Chiến lược điều khiển: là sự mô tả rõ ràng cho mỗi hệ thống IDS về việc kiểm soát, kiểm tra thông tin đầu vào đầu ra:
  - ✓ Chiến lược tập trung: là việc điều khiển trực tiếp các thao tác như kiểm tra, phát hiện, phân tích, đáp trả, báo cáo từ vị trí trung tâm.
  - ✓ Phân thành nhiều thành phần: Phát hiện, kiểm tra từ các vị trí thành phần rồi về báo cáo về vị trí trung tâm.
  - ✓ Phân phối: Mỗi vùng sẽ có những trung tâm đại diện cho trung tâm chính trực tiếp điều khiển các thao tác giám sát, kiểm tra báo cáo.

5.2.1.5 Phân loại IDPS

✓ NIDS – Hệ thống IDPS dựa trên mạng (Network IDPS)

Phần lớn các IDPS thương mại là ở dạng Network-based. N-IDPS (Network-based IDPS) thường bao gồm một tập hợp các cảm biến được đặt tại các điểm khác nhau trong mạng.

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

Được đặt giữa kết nối hệ thống mạng bên trong và mạng bên ngoài để giám sát toàn bộ lưu lượng vào ra. Có thể là một thiết bị phần cứng riêng biệt được thiết lập sẵn hay phần mềm cài đặt trên máy tính. Chủ yếu dùng để đo

lưu lượng mạng được sử dụng. Tuy nhiên có thể xảy ra hiện tượng nghẽn cổ chai khi lưu lượng mạng hoạt động ở mức cao.

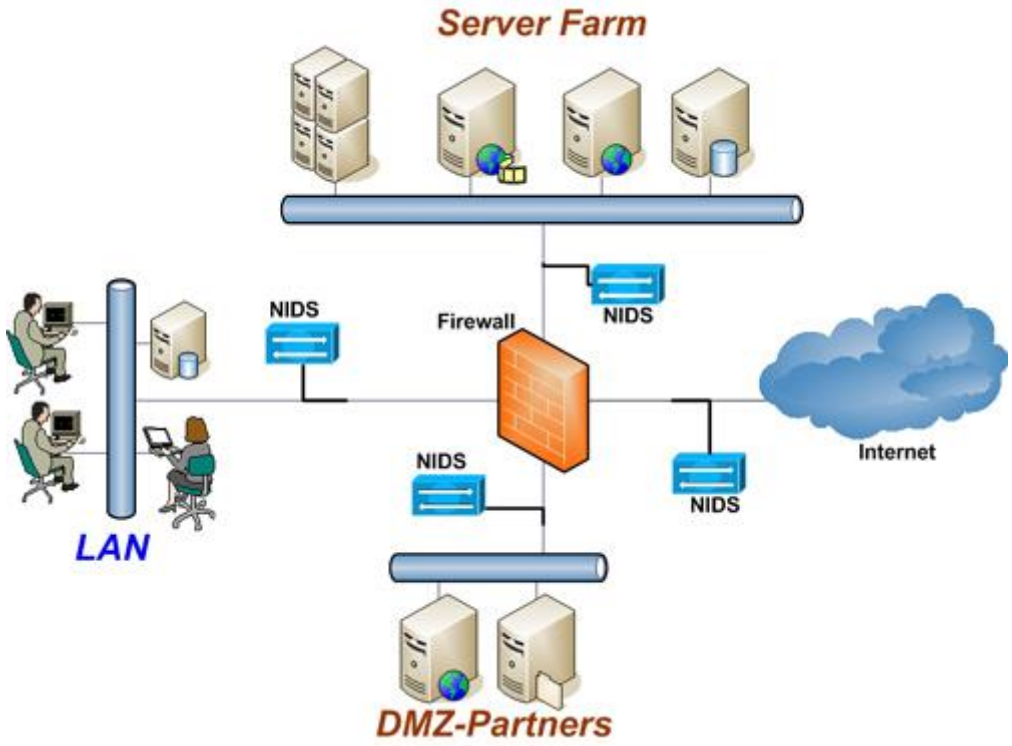
Lợi thế của NIPDS:

- Quản lý được cả một phân vùng mạng (gồm nhiều host).
- Trong suốt với người sử dụng lẫn kẻ tấn công.
- Cài đặt và bảo trì đơn giản, không ảnh hưởng tới mạng.
- Tránh DOS ảnh hưởng tới một host nào đó.
- Có khả năng xác định lỗi ở tầng Network (trong mô hình OSI).
- Độc lập với OS.

Hạn chế của NIDPS:

- Có thể xảy ra trường hợp báo động giả (false positive), tức không có xâm nhập mà NIDPS báo là có xâm nhập.
- Không thể phân tích các lưu lượng đã được mã hóa (vd: SSL, SSH, IPSec…).
- NIDPS đòi hỏi phải được cập nhật các dấu hiệu mới nhất để thực sự an toàn.
- Có độ trễ giữa thời điểm bị tấn công với thời điểm phát báo động. Khi báo động được phát ra, hệ thống có thể đã bị tổn hại.
- Không cho biết việc tấn công có thành công hay không. Một trong những hạn chế là giới hạn băng thông. Những bộ dò mạng phải nhận tất cả các lưu lượng mạng, sắp xếp lại những lưu lượng đó cũng như phân tích chúng. Khi tốc độ mạng tăng lên thì khả năng của đầu dò cũng vậy. Một giải pháp là bảo đảm cho mạng được thiết kế chính xác để cho phép sự sắp đặt của nhiều đầu dò. Khi mà mạng phát triển, thì càng nhiều đầu dò được lắp thêm vào để bảo đảm truyền thông và bảo mật tốt nhất.

Một cách mà các tin tặc cố gắng nhằm che đậy cho hoạt động của họ khi gặp hệ thống IDPS dựa trên mạng là phân mảnh những gói thông tin của họ. Mỗi giao thức có một kích cỡ gói dữ liệu giới hạn, nếu dữ liệu truyền qua mạng lớn hơn kích cỡ này thì gói dữ liệu đó sẽ được phân mảnh. Phân mảnh đơn giản chỉ là quá trình chia nhỏ dữ liệu ra những mẫu nhỏ. Thứ tự của việc sắp xếp lại không thành vấn đề miễn là không xuất hiện hiện tượng chồng chéo. Nếu có hiện tượng phân mảnh chồng chéo, bộ cảm biến phải biết quá trình tái hợp lại cho đúng. Nhiều tin tặc cố gắng ngăn chặn phát hiện bằng cách gửi nhiều gói dữ liệu phân mảnh chồng chéo. Một bộ cảm biến sẽ không phát hiện các hoạt động xâm nhập nếu bộ cảm biến không thể sắp xếp lại những gói thông tin một cách chính xác.



Hình 5.11 – Network IDS

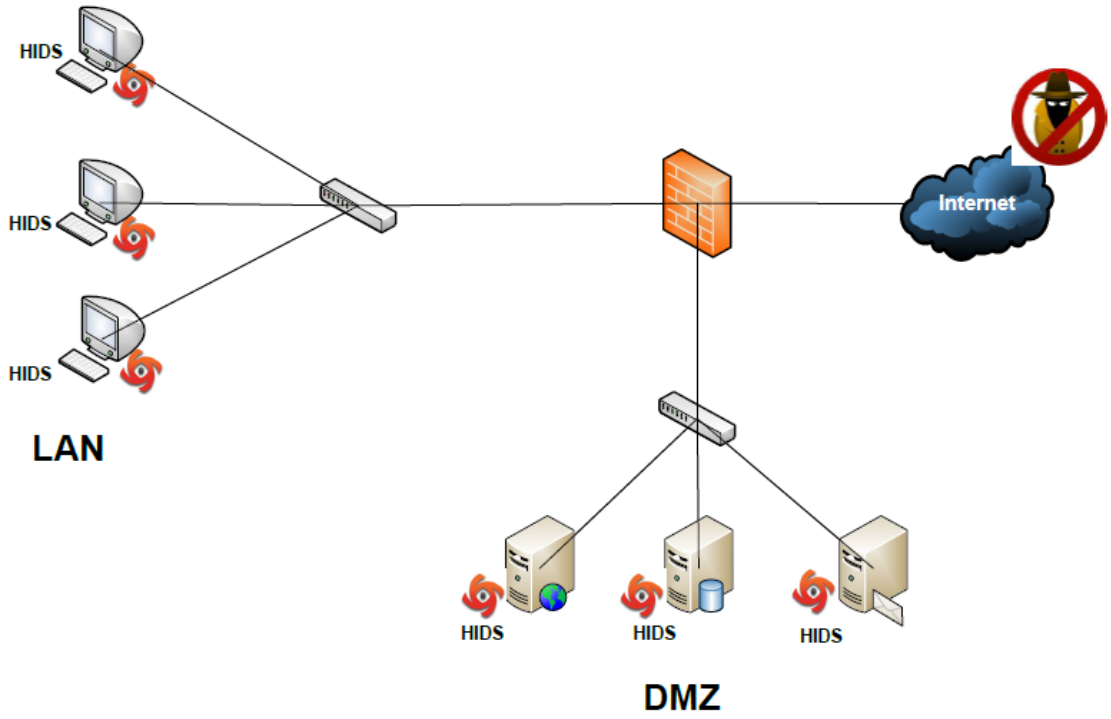
✓ Wireless:

Thực hiện giám sát lưu lượng mạng không dây và phân tích các giao thức mạng không dây để xác định hoạt động nghi ngờ liên quan đến các giao thức. Loại hình này không thể xác định hoạt động nghi ngờ trong các ứng dụng hoặc giao thức mạng lớp cao hơn (ví dụ, TCP, UDP) mà lưu lượng truy cập mạng không dây đang truyền. Loại hình này thường được triển khai trong

phạm vi mạng không dây của một tổ chức để giám sát, nhưng cũng có thể được triển khai đến các địa điểm nơi mà mạng không dây trái phép có thể xảy ra.

✓ IDPS dựa trên máy chủ (Host IDPS)

H-IDPS sử dụng các chương trình phần mềm cài đặt trên một máy chủ. H-IDPS hoạt động thu thập thông tin từ bên trong một hệ thống máy tính cá nhân như quan sát tất cả các hoạt động hệ thống, các file log và những lưu lượng mạng thu thập được.



Hình 5.12 – Host IDPS

Bằng cách cài đặt một phần mềm trên tất cả các máy tính chủ, IDPS dựa trên máy chủ quan sát tất cả những hoạt động hệ thống, như các file log và những lưu lượng mạng thu thập được. Hệ thống dựa trên máy chủ cũng theo dõi OS, những cuộc gọi hệ thống, lịch sử sổ sách (audit log) và những thông điệp báo lỗi trên hệ thống máy chủ. Trong khi những đầu dò của mạng có thể phát hiện một cuộc tấn công, thì chỉ có hệ thống dựa trên máy chủ mới có thể xác định xem cuộc tấn công có thành công hay không. Thêm nữa là, hệ thống dựa trên máy chủ có thể ghi nhận những việc mà người tấn công đã làm trên máy chủ bị tấn công (compromised host).

Không phải tất cả các cuộc tấn công được thực hiện qua mạng. Bằng cách giành quyền truy cập ở mức vật lý (physical access) vào một hệ thống máy tính, kẻ xâm nhập có thể tấn công một hệ thống hay dữ liệu mà không cần phải tạo ra bất cứ lưu lượng mạng (network traffic) nào cả. Hệ thống dựa trên máy chủ có thể phát hiện các cuộc tấn công mà không đi qua đường public hay mạng được theo dõi, hay thực hiện từ cổng điều khiển (console), nhưng với một kẻ xâm nhập có hiểu biết, có kiến thức về hệ IDPS thì hắn có thể nhanh chóng tắt tất cả các phần mềm phát hiện khi đã có quyền truy cập vật lý. Một ưu điểm khác của IDPS dựa trên máy chủ là nó có thể ngăn chặn các kiểu tấn công dùng sự phân mảnh hoặc TTL. Vì một host phải nhận và tái hợp các phân mảnh khi xử lí lưu lượng nên IDS dựa trên host có thể giám sát chuyện này.

HIDPS thường được cài đặt trên một máy tính nhất định. Thay vì giám sát hoạt động của một phân vùng mạng, HIDPS chỉ giám sát các hoạt động trên một máy tính. HIDPS thường được đặt trên các host xung yếu của tổ chức, và các máy chủ trong vùng DMZ - thường là mục tiêu bị tấn công đầu tiên. Nhiệm vụ chính của HIDPS là giám sát các thay đổi trên hệ thống, bao gồm:

- Các tiến trình.

- Các entry của Registry.

- Mức độ sử dụng CPU.

- Kiểm tra tính toàn vẹn và truy cập trên hệ thống file.

- Một vài thông số khác.

Các thông số này khi vượt qua một ngưỡng định trước hoặc những thay đổi khả nghi trên hệ thống file sẽ gây ra báo động.

Lợi thế của HIDPS:

- Có khả năng xác định người dùng liên quan tới một sự kiện.

- HIDPS có khả năng phát hiện các cuộc tấn công diễn ra trên một máy, NIDPS không có khả năng này.

- Có thể phân tích các dữ liệu mã hoá.

- Cung cấp các thông tin về host trong lúc cuộc tấn công diễn ra trên host này.

Hạn chế của HIDPS:

- Thông tin từ HIDPS là không đáng tin cậy ngay khi sự tấn công vào host này thành công.

- Khi OS bị "hạ" do tấn công, đồng thời HIDPS cũng bị "hạ".

- HIDPS phải được thiết lập trên từng host cần giám sát.

- HIDPS không có khả năng phát hiện các cuộc dò quét mạng (Nmap, Netcat…).

- HIDS cần tài nguyên trên host để hoạt động.

- HIDPS có thể không hiệu quả khi bị DOS.

- Đa số chạy trên hệ điều hành Window. Tuy nhiên cũng đã có một số chạy được trên UNIX và những hệ điều hành khác.

Vì hệ thống IDPS dựa trên máy chủ đòi hỏi phần mềm IDPS phải được cài đặt trên tất cả các máy chủ nên đây có thể là khó khăn của những nhà quản trị khi nâng cấp phiên bản, bảo trì phần mềm, và cấu hình phần mềm trở thành công việc tốn nhiều thời gian và là những việc làm phức tạp. Bởi vì hệ thống dựa trên máy chủ chỉ phân tích những lưu lượng được máy chủ nhận được, chúng không thể phát hiện những tấn công thăm dò thông thường được thực hiện nhằm chống lại một máy chủ hay là một nhóm máy chủ. Hệ thống IDPS dựa trên máy chủ sẽ không phát hiện được những chức năng quét ping hay dò cổng (ping sweep and port scans) trên nhiều máy chủ. Nếu máy chủ bị thỏa hiệp thì kẻ xâm nhập hoàn toàn có thể tắt phần mềm IDPS hay tắt kết nối của máy chủ đó. Một khi điều này xảy ra thì các máy chủ sẽ không tạo ra cảnh báo nào cả. Phần mềm IDPS phải được cài đặt trên mỗi hệ thống trên mạng nhằm cung cấp đầy đủ khả năng cảnh báo của mạng. Trong một môi trường hỗn tạp, điều này có thể là một vấn đề bởi vì phần mềm IDPS phải tương ứng nhiều hệ điều hành khác nhau. Do đó trước khi chọn một hệ thống IDPS, chúng ta phải chắc là nó phù hợp và chạy được trên tất cả các hệ điều hành.

- ✓ Phân tích hành vi mạng (Network Behavior Analysis - NBA):

NBA kiểm tra lưu lượng mạng để xác định các mối đe dọa tạo ra các luồng lưu lượng bất thường, chẳng hạn như tấn công từ chối dịch vụ (DDoS), một số hình thức của phần mềm độc hại (sâu, backdoor), và vi phạm chính sách (một hệ thống máy chủ cung cấp dịch vụ mạng tới hệ thống khác). Hệ thống NBA thường được triển khai để giám sát các luồng lưu lượng mạng nội bộ của một tổ chức, và cũng được triển khai theo dõi luồng lưu lượng giữa các mạng của tổ chức với mạng bên ngoài (ví dụ như Internet, mạng lưới các đối tác kinh doanh).

5.2.2. Triển khai hệ thống

Để triển khai hệ thống phát hiện và ngăn chặn xâm nhập người quản trị phải xác định được quy trình cần phải thực hiện đối với hệ thống mạng. Các bước cần phải thực hiện như sau:

Với hệ thống mạng được thiết kế có thiết bị phát hiện và ngăn chặn xâm nhập trước khi triển khai.

- Dựa vào môi trường thực tế của tổ chức, doanh nghiệp người quản trị lập sơ đồ hệ thống mạng phù hợp, bố trí trang thiết bị máy chủ, máy trạm, tường lửa, IDPS phù hợp với hiện trạng của tổ chức, công ty.
- Lựa chọn sản phẩm IDPS: Dựa vào hệ thống mạng lớn hay mạng nhỏ mà cần phải đầu tư trang thiết bị phù hợp, lựa chọn: thiết bị IDPS là sản phẩm thương mại hay miễn phí, số lượng cần phải đầu tư.
- Nhận biết các nguy cơ gây mất an toàn đối với hệ thống để từ đó có chính sách và triển khai phương pháp phòng chống khi có sự cố xảy ra.
- Thực hiện giám sát liện tục đối với hệ thống và thiết lập cảnh báo khi có sự cố.

Với hệ thống mạng đã được triển khai và thực hiện lắp đặt bổ sung thiết bị phát hiện và ngăn chặn xâm nhập:

- Rà soát hệ thống mạng cũng như tài sản về hệ thống mạng bao gồm: số lượng máy chủ, máy trạm, tường lửa…
- Thiết lập chính sách bảo mật sử dụng cho hệ thống phát hiện và ngăn chặn xâm nhập.

- Xem xét đầu tư trang thiết bị cho IDPS như đã trình bày ở trên.
- Nhận biết các nguy cơ gây mất an toàn và thiết lập chính sách phù hợp.
- Thực hiện triển khai lắp ráp, cài đặt và vận hành hệ thống IDPS.

5.2.3. Thiết lập an toàn cho hệ thống IDPS

Sau khi thực hiện lắp ráp, cài đặt, vận hành hệ thống phát hiện và ngăn chặn xâm nhập IDPS, người quản trị phải thực hiện giám sát và tối ưu hóa hệ thống IDPS để phát hiện và chống lại tấn công hoặc thăm dò hệ thống. Cũng như với các thành phần an toàn khác, người quản trị phải xem xét đến nhiều yếu tố là một phần của quá trình cấu hình an toàn. Các bước thực hiện sẽ phụ thuộc vào từng loại IDPS đã được cài đặt. Sau đây là các bước cấu hình an toàn cho hệ thống phát hiện xâm nhập dựa trên mạng (NIDS):

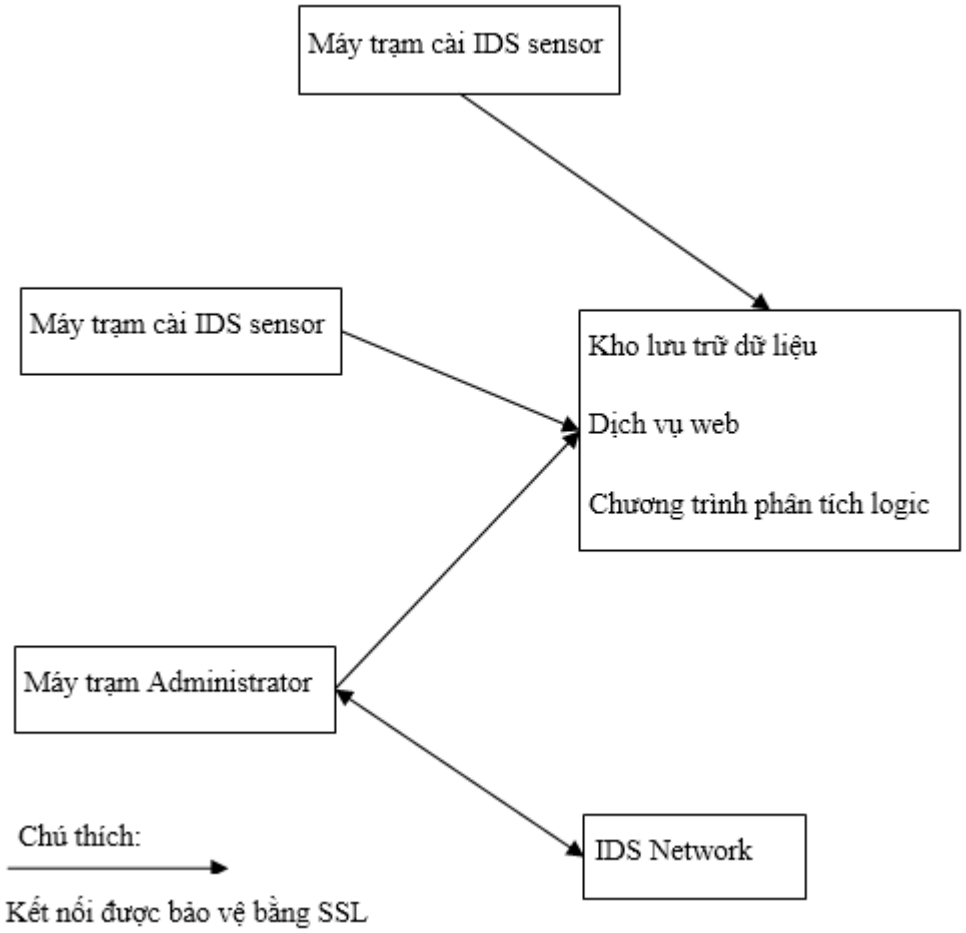
- Nếu IDPS được cài đặt dựa vào hệ điều hành của hãng thứ ba, trước tiên cần phải cấu hình an toàn cho hệ điều hành đó. Dựa vào hệ điều hành đó là Windows hay Linux mà có những phương pháp cấu hình an toàn thích hợp như đã nêu ở chương hai.
- Cấu hình an toàn cơ sở hạ tầng mạng nhằm cung cấp một môi trường an toàn cho chức năng của IDPS. Bao gồm việc phân vùng mạng, sử dụng kết hợp các thiết bị an toàn như bức tường lửa.
- Cài đặt phần mềm phát hiện xâm nhập Snort hoặc phần mềm IDS khác trên hệ thống đã được cấu hình an toàn hệ điều hành cũng như hạ tầng mạng. Tùy thuộc vào cơ sở hạ tầng mạng để lựa chọn phần mềm có năng suất cao nhất.
- Mua các thiết bị phát hiện và ngăn chặn xâm nhập chuyên dụng, những thiết bị này đã được cài đặt và cấu hình an toàn bởi nhà sản xuất, vì vậy sau khi lắp ráp thiết bị vào hệ thống chỉ việc cấu hình và chạy ứng dụng.

Đối với hệ thống phát hiện xâm nhập dựa vào máy tính yêu cầu cần phải thực hiện cài đặt và cấu hình trên hệ điều hành đã có. Để đảm bảo hệ thống không bị tổn hại, yếu tố quan trọng cần xem xét trước tiên là truy cập vật lý để điều khiển cũng như truy cập điều khiển từ xa. Nhiều hệ điều hành

cung cấp khả năng truy cập từ xa thông qua dịch vụ đầu cuối (Terminal Service), Remote Desktop, SSH. Khi truy cập từ xa để quản lý Host IDS phải chú ý đến mức độ bảo mật của các dịch vụ cung cấp. Và giám sát những lần đăng nhập không hợp lệ vào Host IDS.

Đảm bảo an toàn khi IDS hoạt động:

Kết nối truyền dữ liệu giữa các thành phần phát hiện xâm nhập và thành phần quản lý tập trung cần phải được bảo vệ cũng như kết nối giữa trình điều khiển của người quản trị với trung tâm lưu trữ. Hình 5.9 trình bày đường truyền kết nối giữa các thành phần của IDS được bảo vệ bằng SSL.



Hình 5.13 - Truyền thông giữa các thành phần của IDS được bảo vệ bằng SSL

Mục đích của việc sử dụng giao thức SSL để mã hóa luồng dữ liệu từ máy trạm cài đặt IDS tới trung tâm lưu trữ dữ liệu nhằm ngăn chặn tấn công chặn bắt và thay đổi dữ liệu.

Bảo vệ các tệp tin cấu hình:

Các tệp tin cấu hình có thể chứa mật khẩu và thông tin cấu hình nhạy cảm khác, vì vậy nó cần phải được bảo vệ. Ví dụ, nếu IDS cài đặt là Snort kết hợp với cơ sở dữ liệu là MySQL (./configure --with-mysql) tệp tin cấu hình snort.conf với các tham số:

```
output database: log, mysql, user=snort password=
PASSWORD dbname=snort host=managemet-server.domain.local
```

Trong tệp tin cấu hình snort.conf, mật khẩu lưu ở chế độ bản rõ. Đây là một điểm yếu mà người quản trị cần phải xác định để bảo vệ an toàn. Ở ví dụ trên đây khi cài đặt Snort, tệp tin snort.conf được tham chiếu khi bắt đầu quá trình cài đặt. Khi Snort đã hoạt động, thực hiện lưu trữ an toàn tệp tin này trong phạm vi an toàn, hoặc bảo vệ tệp tin bằng phương thức mã hóa.

5.3. QUẢN LÝ MÃ ĐỘC

5.3.1. Phòng chống thư rác

Thư rác hay còn gọi là SPAM là một trong những thách thức lớn nhất hiện nay mà khách hàng và các nhà cung cấp dịch vụ phải đối phó. Spam đã trở thành một hình thức quảng cáo chuyên nghiệp, phát tán virus, ăn cắp thông tin... với nhiều thủ đoạn và mánh khóe cực kỳ tinh vi. Người dùng sẽ phải mất khá nhiều thời gian để xóa những email "không mời mà đến", nếu vô ý còn có thể bị nhiễm virus, trojan, spyware ... và nặng nề hơn là mất thông tin như thẻ tín dụng, tài khoản ngân hàng qua các email dạng phishing.

5.3.1.1 Đặc điểm của thư rác

Spam (hay spam email) là thư điện tử quảng cáo hay là thư được gửi mà không có sự yêu cầu từ người nhận. Spam thường là những email vô hại và được gửi tới một số lượng lớn người nhận khác nhau. Spam được gửi với số lượng lớn có thể làm đầy hòm thư của người nhận, nên họ không nhận được các thư mới. Ngoài ra spam còn chiếm dụng băng thông, có thể gây tắc nghẽn đường truyền. Một số loại spam còn chứa nội dung lừa đảo, nhằm mục đích lừa người dùng cung cấp các thông tin cá nhân như mã số thẻ tín dụng, mật khẩu...

Để tiến hành gửi spam, người gửi (spammer) cần phải có một số lượng lớn các địa chỉ email người nhận, danh sách có thể lên đến hàng triệu. Các địa chỉ email có thể được thu thập bằng nhiều cách như: sử dụng các chương trình tự động tìm các địa chỉ email trên Internet, tấn công vào các diễn đàn để lấy trộm cơ sở dữ liệu về các thành viên, dùng phương pháp tấn công kiểu từ điển, dùng các tên thông dụng (ví dụ John, Smith, Steve,...) ghép với hàng ngàn tên miền khác nhau thành các địa chỉ đúng và có xác suất thành công rất cao.

Spam có đặc điểm là không tốn nhiều chi phí khi gửi đến một số lượng người nhận lớn, vì thế các spammer không cần sàng lọc các đối tượng nhận thư được gửi trùng lặp nhiều lần tới cùng một địa chỉ người nhận.

5.3.1.2 Các phương pháp chọn lọc Spam

Spam gây ra rất nhiều tác hại, do vậy việc phòng chống và ngăn chặn các spam là cần thiết. Hiện có nhiều công ty phần mềm cung cấp giải pháp chống spam, mỗi dòng sản phẩm có những tính năng và các ưu nhược điểm riêng, nhưng hầu hết các sản phẩm đó đều hoạt động dựa vào một số nguyên lý sau:

- Sử dụng DNS blacklist

Phương pháp sử dụng DNS black list sẽ chặn các email đến từ các địa chỉ nằm trong danh sách DNS blacklist. Có hai loại danh sách DNS Blacklist thường được sử dụng, đó là:

- ✓ Danh sách các miền gửi spam đã biết, danh sách các miền này được liệt kê và cập nhật tại địa chỉ http://spamhaus.org/sbl.
- ✓ Danh sách các máy chủ email cho phép hoặc bị lợi dụng thực hiện việc chuyển tiếp spam được gửi đi từ spammer. Danh sách này được liệt kê và cập nhật thường xuyên tại địa chỉ http://www.ordb.org. Cơ sở dữ liệu Open Relay Database này được duy trì bởi ORDB.org là một tổ chức phi lợi nhuận.

Khi một email được gửi đi, nó sẽ đi qua một số SMTP server trước khi chuyển tới địa chỉ người nhận. Địa chỉ IP của các SMTP server mà email đó

đã chuyển qua được ghi trong phần header của email. Các chương trình chống spam sẽ kiểm tra tất cả các địa chỉ IP đã được tìm thấy trong phần header của email đó sau đó so sánh với cơ sở dữ liệu DNS Blacklist đã biết. Nếu địa chỉ IP tìm thấy trong phần này có trong cơ sở dữ liệu về các DNS Blacklist, nó sẽ bị coi là spam, còn nếu không, email đó sẽ được coi là một email hợp lệ.

Phương pháp này có ưu điểm là các email có thể được kiểm tra trước khi tải xuống, do đó tiết kiệm được băng thông đường truyền. Nhược điểm của phương pháp này là không phát hiện ra được những email giả mạo địa chỉ người gửi.

- Sử dụng SURBL list

Phương pháp sử dụng SURBL phát hiện spam dựa vào nội dung của email. Chương trình chống spam sẽ phân tích nội dung của email xem bên trong nó có chứa các liên kết đã được liệt kê trong Spam URI Realtime Blocklists (SURBL) hay không. SURBL chứa danh sách các miền và địa chỉ của các spammer đã biết. Cơ sở dữ liệu này được cung cấp và cập nhật thường xuyên tại địa chỉ www.surbl.org.

Có nhiều danh sách SURBL khác nhau như sc.surbl.org, ws.surbl.org, ob.surbl.org, ab.surbl.org..., các danh sách này được cập nhật từ nhiều nguồn. Thông thường, người quản trị thường kết hợp các SURBL list bằng cách tham chiếu tới địa chỉ multi.surbl.org. Nếu một email sau khi kiểm tra nội dung có chứa các liên kết được chỉ ra trong SURBL list thì nó sẽ được đánh dấu là spam email, còn không nó sẽ được cho là một email thông thường.

Phương pháp này có ưu điểm phát hiện được các email giả mạo địa chỉ người gửi để đánh lừa các bộ lọc. Nhược điểm của nó là email phải được tải xuống trước khi tiến hành kiểm tra, do đó sẽ chiếm băng thông đường truyền và tài nguyên của máy tính để phân tích các nội dung email.

- Kiểm tra người nhận

Tấn công spam kiểu "từ điển" sử dụng các địa chỉ email và tên miền đã biết để tạo ra các địa chỉ email hợp lệ khác. Bằng kỹ thuật này spammer có thể gửi spam tới các địa chỉ email được sinh ra một cách ngẫu nhiên. Một số

địa chỉ email trong số đó có thực, tuy nhiên một lượng lớn trong đó là địa chỉ không tồn tại và chúng gây ra hiện tượng "lụt" ở các máy chủ mail.

Phương pháp kiểm tra người nhận sẽ ngăn chặn kiểu tấn công này bằng cách chặn lại các email gửi tới các địa chỉ không tồn tại trên Active Directory hoặc trên máy chủ mail server trong công ty. Tính năng này sẽ sử dụng Active Directory hoặc LDAP server để xác minh các địa chỉ người nhận có tồn tại hay không. Nếu số địa chỉ người nhận không tồn tại vượt quá một ngưỡng nào đó (do người quản trị thiết lập) thì email gửi tới đó sẽ bị coi là spam và chặn lại.

- Kiểm tra địa chỉ

Bằng cách kiểm tra địa chỉ người gửi và người nhận, phần lớn spam sẽ được phát hiện và chặn lại. Thực hiện kiểm tra địa chỉ người gửi trước khi email được tải xuống sẽ tiết kiệm được băng thông đường truyền cho toàn hệ thống.

Kỹ thuật Sender Policy Framework (SPF, www.openspf.org) được sử dụng để kiểm tra địa chỉ người gửi email. Kỹ thuật SPF cho phép chủ sở hữu của một tên miền Internet sử dụng các bản ghi DNS đặc biệt (gọi là bản ghi SPF) chỉ rõ các máy được dùng để gửi email từ miền của họ. Khi một email được gửi tới, bộ lọc SPF sẽ phân tích các thông tin trong trường "From" hoặc "Sender" để kiểm tra địa chỉ người gửi. Sau đó SPF sẽ đối chiếu địa chỉ đó với các thông tin đã được công bố trong bản ghi SPF của miền đó xem máy gửi email có được phép gửi email hay không. Nếu email đến từ một server không có trong bản ghi SPF mà miền đó đã công bố thì email đó bị coi là giả mạo.

- Chặn IP

Phương pháp này sẽ chặn các email được gửi đến từ các địa chỉ IP biết trước. Khi một email đến, bộ lọc sẽ phân tích địa chỉ máy gửi và so sánh với danh sách địa chỉ bị chặn. Nếu email đó đến từ một máy có địa chỉ trong danh sách này thì nó sẽ bị coi là spam, ngược lại nó sẽ được coi là email hợp lệ.

- Sử dụng bộ lọc Bayesian

Bộ lọc Bayesian hoạt động dựa trên định lý Bayes để tính toán xác suất xảy ra một sự kiện dựa vào những sự kiện xảy ra trước đó. Kỹ thuật tương tự như vậy được sử dụng để phân loại spam. Nếu một số phần văn bản xuất hiện thường xuyên trong các spam nhưng thường không xuất hiện trong các email thông thường, thì có thể kết luận rằng email đó là spam.

Trước khi có thể lọc email bằng bộ lọc Bayesian, người dùng cần tạo ra cơ sở dữ liệu từ khóa và dấu hiệu (như là ký hiệu $, địa chỉ IP và các miền...) sưu tầm từ các spam và các email không hợp lệ khác.

Mỗi từ hoặc mỗi dấu hiệu sẽ được cho một giá trị xác suất xuất hiện, giá trị này dựa trên việc tính toán có bao nhiêu từ thường hay sử dụng trong spam, mà trong các email hợp lệ thường không sử dụng. Việc tính toán này được thực hiện bằng cách phân tích những email gửi đi của người dùng và phân tích các kiểu spam đã biết.

Để bộ lọc Bayesian hoạt động chính xác và có hiệu quả cao, cần phải tạo ra cơ sở dữ liệu về các email thông thường và spam phù hợp với đặc thù kinh doanh của từng công ty. Cơ sở dữ liệu này được hình thành khi bộ lọc trải qua giai đoạn "huấn luyện". Người quản trị phải cung cấp khoảng 1000 email thông thường và 1000 spam để bộ lọc phân tích tạo ra cơ sở dữ liệu cho riêng nó.

- Sử dụng danh sách Black/white list

Việc sử dụng các danh sách black list, white list giúp cho việc lọc spam hiệu quả hơn.

Black list là cơ sở dữ liệu các địa chỉ email và các miền không bao giờ muốn nhận các email từ đó. Các email gửi tới từ các địa chỉ này sẽ bị đánh dấu là spam.

White list là cơ sở dữ liệu các địa chỉ email và các miền mong muốn nhận email từ đó. Nếu các email được gửi đến từ những địa chỉ nằm trong danh sách này thì chúng luôn được cho qua.

Thông thường các bộ lọc có tính năng tự học, khi một email bị đánh dấu là spam thì địa chỉ người gửi sẽ được tự động đưa vào danh sách black

list. Ngược lại, khi một email được gửi đi từ trong công ty thì địa chỉ người nhận sẽ được tự động đưa vào danh sách white list.

- Kiểm tra Header

Phương pháp này sẽ phân tích các trường trong phần header của email để đánh giá email đó là email thông thường hay là spam. Spam thường có một số đặc điểm như:

- ✓ Để trống trường From: hoặc trường To:
- ✓ Trường From: chứa địa chỉ email không tuân theo các chuẩn RFC.
- ✓ Các URL trong phần header và phần thân của message có chứa địa chỉ IP được mã hóa dưới dạng hệ hex/oct hoặc có sự kết hợp theo dạng username/password (ví dụ các địa chỉ: http://00722353893457472/hello.com,www.citibank.com@scammer.com).
- ✓ Phần tiêu đề của email có thể chứa địa chỉ email người nhận để cá nhân hóa email đó. Lưu ý khi sử dụng tính năng này với các địa chỉ email dùng chung có dạng như sales@company.com. Ví dụ khi một khách hàng phản hồi bằng cách sử dụng tính năng auto-reply với tiêu đề "your email to sales" có thể bị đánh dấu là spam. Gửi tới một số lượng rất lớn người nhận khác nhau.
- ✓ Chỉ chứa những file ảnh mà không chứa các từ để đánh lừa các bộ lọc.
- ✓ Sử dụng ngôn ngữ khác với ngôn ngữ mà người nhận đang sử dụng.

Dựa vào những đặc điểm này của spam, các bộ lọc có thể lọc chặn.

- Sử dụng tính năng Challenge/Response

Tính năng này sẽ yêu cầu người lần đầu gửi email xác nhận lại email đầu tiên mà họ đã gửi, sau khi xác nhận, địa chỉ email của người gửi được bổ sung vào danh sách White list và từ đó trở về sau các email được gửi từ địa chỉ đó được tự động cho qua các bộ lọc.

Do spammer sử dụng các chương trình gửi email tự động và họ không thể xác nhận lại tất cả các email đã gửi đi, vì thế những email không được xác nhận sẽ bị coi là spam.

Phương pháp này có hạn chế là nó yêu cầu những người gửi mới phải xác nhận lại email đầu tiên mà họ gửi. Để khắc phục nhược điểm này, người quản trị chỉ nên sử dụng phương pháp này đối với những email mà họ nghi ngờ là spam.

5.3.1.3 Phòng chống thư rác

Ngoài việc sử dụng các bộ lọc chống spam, người sử dụng cũng đóng vai trò quan trọng trong việc chống lại "đại dịch" thư rác. Bởi vậy người dùng cần tuân theo một số nguyên tắc sau:

- Luôn cập nhật các bản vá mới nhất của các phần mềm đang cài đặt trên máy.
- Đảm bảo tất cả các máy luôn được cập nhật các phần mềm chống virus và chống spam.
- Sử dụng các firewall để bảo vệ hệ thống.
- Không trả lời các email lạ không rõ nguồn gốc. Đối với các spammer, khi nhận được một trả lời từ hàng ngàn email họ gửi đi thì cũng chứng minh là phương pháp đó có hiệu quả. Ngoài ra, việc trả lời lại còn xác nhận là địa chỉ email của nạn nhân là có thực và hiện đang được sử dụng. Do vậy địa chỉ email đó sẽ "đáng giá" hơn, và các spammer sẽ gửi nhiều thư rác hơn.
- Không gửi các thông tin cá nhân (số thẻ tín dụng, mật khẩu, tài khoản ngân hàng, v.v...) trong thư điện tử. Các spammer và những kẻ lừa đảo qua mạng có thể tạo ra những trang web giả mạo các tổ chức, ngân hàng... đề nghị nạn nhân gửi mật khẩu và một số thông tin về thẻ tín dụng của nạn nhân qua email.
- Không hồi đáp email bằng cách nhấn lên từ như "loại bỏ" (remove) hoặc "ngừng đăng ký" (unsubscribe) trong dòng tiêu đề hoặc trong nội dung của thư trừ khi đây là nguồn đáng tin cậy (các email tiếp thị trực

tiếp). Đây là tiểu xảo của các spammer để người sử dụng hồi đáp lại các spam của họ. Khi nhận được hồi đáp, các spammer không những không loại bỏ địa chỉ email của nạn nhân ra khỏi danh sách mà còn gửi tới nhiều spam hơn bởi vì họ biết rằng địa chỉ email của nạn nhân hiện đang hoạt động.

- Không bao giờ bấm vào các liên kết URL hoặc địa chỉ trang web được ghi trong spam ngay cả khi nó hướng dẫn người nhận ngừng đăng ký. Điều này cũng cho người gửi biết rằng địa chỉ email của nạn nhân đang được sử dụng và có thể sẽ nhận được nhiều spam hơn.
- Hãy sử dụng hai địa chỉ email khác nhau, một địa chỉ sử dụng cho các việc riêng như bạn bè, công việc. Một địa chỉ sử dụng để đăng ký trở thành thành viên của các diễn đàn, các tổ chức... những nơi mà địa chỉ email có thể bị lạm dụng hoặc bán.
- Không nên đăng địa chỉ email ở những nơi công cộng (ví dụ như các diễn đàn, bảng tin, chat room...) nơi các spammer thường sử dụng các tiện ích để thu thập và tìm kiếm địa chỉ email.
- Sử dụng các dịch vụ email cung cấp công cụ chống spam, ví dụ như Yahoo! Mail, Gmail.
- Không bao giờ được chuyển tiếp spam cho người khác.
- Chuyển spam nhận được đến người quản trị hệ thống email. Quản trị viên sẽ thay đổi chương trình lọc để lần sau hệ thống sẽ chặn lại những email tương tự như thế.

5.3.2. Cô lập các tấn công Phishing

Phishing là loại hình thức gian lận (thương mại) trên Internet, một thành phần của Social Engineering – kỹ nghệ lừa đảo trên mạng. Nguyên tắc của Phishing là bằng cách nào đó "lừa" người dùng gửi thông tin nhạy cảm như tên, địa chỉ, mật khẩu, số thẻ tín dụng, mã thẻ ATM, số an sinh xã hội, …đến kẻ lừa đảo (scammer). Cách thực hiện chủ yếu là mô phỏng lại giao diện trang web đăng nhập (login page) của các website có thật, kẻ lừa đảo sẽ dẫn dụ nạn nhân (victim) điền các thông tin vào trang "dởm" đó rồi truyền tải

thông tin đến anh ta (thay vì đến server hợp pháp) thực hiện hành vi đánh cắp thông tin bất hợp pháp mà người sử dụng không hay biết.

Tin tặc thường đánh cắp thông tin người dùng bằng cách giả danh để giao tiếp với họ. Ví dụ như email giả danh một mạng xã hội ảo, giả danh yêu cầu thanh toán trực tuyến hay như trong trường hợp xảy ra trong ngày rồi: giả danh nhà cung cấp dịch vụ mail.

Các email này thường chuyển nạn nhân đến một trang web giả mạo giống hệt với trang web thật, làm cho họ nhầm lẫn và điền các thông tin nhạy cảm vào, kết quả là các thông tin đó rơi vào tay tin tặc.

Do cách tấn công đơn giản nhưng lại hiệu quả cao nên Phishing nhanh chóng trở thành một trong những kiểu tấn công phổ biến nhất trên mạng. Các cuộc lừa đảo được tạo ra hàng ngày bởi với mục đích chung là đánh cắp thông tin nhạy cảm của người dùng Internet.

- Các giai đoạn tấn công Phishing

- Kẻ tấn công lấy được địa chỉ Email của nạn nhân. Đây có thể đoán hoặc thu được từ nhiều nguồn khác nhau.
- Kẻ tấn công tạo một Email hợp pháp và gửi tới người nhận và yêu cầu thực hiện một số hành động.
- Người nhận mở Email, họ sẽ bị dính mã độc mà kẻ tấn công đã nhúng vào trong Email, người nhận hoàn tất một số mục thông tin hoặc là thăm website mà kẻ tấn công dùng liên kết trong Email.
- Kẻ tấn công thu hoạch được thông tin nhạy cảm của người nhận và có thể khai thác nó trong tương lai.

Các mã độc mà kẻ tấn công có thể dùng ở đây là: Worm và Trojan, Spyware và kỹ năng lừa đảo (deceit).

- Phương pháp Worm và Trojan

Trong phương pháp này, kẻ tấn công dùng phần mềm độc hại để nhúng vào trong Email và gửi cho người nhận. Cuối cùng truyền thông tin về cho kẻ tấn công qua mạng. Nó còn có thể chặn đứng sự truyền thông giữa máy tính nạn nhân với cơ quan hợp pháp. Các chương trình phòng chống virus, chương

trình phát hiện xâm nhập máy chủ và tường lửa cá nhân có thể khóa các loại tấn công này.

- Phương pháp lừa đảo (Deceit)

Trong phương pháp này kẻ tấn công sử dụng phương thức lừa đảo để dẫn dụ người nhận Email thăm website của kẻ tấn công, sau đó điền thông tin cá nhân vào trang website này. Qua đó kẻ tấn công có được thông tin nhạy cảm của người dùng.

- Phương pháp dùng phần mềm gián điệp (Spyware)

Trong phương pháp này kẻ tấn công sử dụng phầm mềm gián điệp cài vào máy tính nạn nhân thông qua Email và sau đó lấy cắp thông tin nhạy cảm của nạn nhân và gửi về cho kẻ tấn công. Spyware thường bị phát hiện bởi các chương trình chuyên dò tìm Spyware và nhiều chương trình chống virus khác.

- Các phương pháp phòng chống

- **Đối với doanh nghiệp**

Cần thiết lập chính sách bảo mật và triển khai các biện pháp bảo vệ người dùng và máy tính bên trong hệ thống mạng.

Tránh nhúng những liên kết vào Email: Các doanh nghiệp hợp pháp thường nhúng những liên kết trong Email để chuyển tới trang web của họ. Liên kết này bắt người dùng phải đăng nhập hệ thống bằng những thông tin như Username và Password**.** Kẻ tấn công lợi dụng thuận lợi này để lấy làm website giả và lấy những thông tin nhạy cảm của nạn nhân.

Tránh sử dụng Email form: Kẻ lừa đảo sử dụng những Email form để thu thập những thông tin cá nhân của người tiêu dùng. Nếu những doanh nghiệp cũng sử dụng hình thức này thì sẽ tạo ra khó khăn để người dùng phân biệt đâu là Email hình thức hợp pháp đâu là Email hình thức lừa đảo. Hình thức Email form có thể tạo đơn giản cho khách hàng khi doanh nghiệp yêu cầu thông tin người tiêu dùng. Nhưng hình thức này cũng tạo cơ hội cho kẻ lừa đảo lấy thông tin người dùng. Do vậy mà các doanh nghiệp phải thông báo tới khách là một Email hợp pháp không bao giờ chứa đựng Email form yêu cầu thông tin cá nhân.

Chữ ký số Email: Các doanh nghiệp thiết lập chính sách khi mà sự truyền thông các Email có giá trị của doanh nghiệp với khách hàng được xác thực bằng chữ ký số với khóa xác thực riêng. Khi mà nhận Email, người nhận xác thực Email bằng khóa công cộng. Xác xuất để kẻ lùa đảo tạo một chữ ký hợp lệ trên Email lừa đảo là vô cùng thấp.

Tạo số thứ tự của các Email: Các doanh nghiệp nên nhúng số thứ tự của mỗi Email. Nhờ vào số thứ tự này mà người tiêu dùng có thể xác định Email hợp lệ của doanh nghiệp.

Nhúng tên khách hàng vào Email: Đây là cách thức đơn giản nhất đối với cả doanh nghiệp và người tiêu dùng. Ví dụ: "Dear Nguyễn văn A". Cách thức này được dùng phổ biến với các doanh nghiệp trong các giao dịch với khách hàng. Nhưng trong cách thức này kẻ lừa đảo có thể tìm kiếm tên của khách hàng khi đã biết Email của họ. Ưu điểm của cách thức này là làm giảm sự thành công của các cuộc tấn công với quy mô lớn. Bởi vì kẻ lừa đảo phải sưu tập và tìm kiếm tên mỗi Email.

Sử dụng thẻ bài để xác nhận thông tin người dùng: Mục đích cuối cùng của kẻ lừa đảo là lấy thông tin của người dùng. Thường là Username và Password để truy nhập vào website hợp pháp. Nếu một người nào đó không biết những thông tin này thì các cuộc tấn công không thể thực hiện được. Do vậy mỗi doanh nghiệp cần phải cấp cho người tiêu dùng thẻ bài an toàn và yêu cầu họ sử dụng trong tất cả các giao dịch điện tử với doanh nghiệp. Như vậy sẽ đảm bảo được thông tin nhạy cảm của người dùng.

Kích hoạt các dịch vụ giám sát website: Triển khai các dịch vụ giám sát website của công ty để liên tục giám sát nội dung website.

Cài đặt phần mềm diệt virus và Spyware: Các cuộc tấn công lừa đảo thường bao gồm các phần mềm mã độc. Do vậy mà các doanh nghiệp cần phải sử dụng các phần mềm diệt virus để quét và diệt chúng, thường xuyên cập nhật thông tin virus.

- **Đối với người dùng cá nhân**

Phải luôn luôn cập nhật các bản vá lỗi cho hệ thống máy tính để tránh các kẻ tấn công lợi dụng điểm yếu, lỗ hỗng của phần mềm mà cài đặt các chương trình virus và các phần mềm gián điệp.

Cài đặt các công cụ phòng chống Phishing vào các trình duyệt web. Nó sẽ bảo vệ an toàn khi lướt web. Các thanh công cụ thông dụng hiện nay: BitDefender, Netcraft…Hiện tại thì IE 7 và 8, FireFox đều có tính năng ngăn chạn Phishing

Khi người dùng vào hộp thư (Mail). Trước khi mở một Mail nào đó thì phải xem Mail đó được gửi bởi ai. Và có đáng tin cậy hay không. Nếu thư không đáng tin cậy thì người dùng có thể xóa nó ngay mà không cần mở. Khi đã mở một thư nào đó mà trong thư có gắn các liên kết thì người dùng phải kiểm tra xem liên kết đó dẫn tới đâu. Liên kết có tin tưởng thì mới click vào liên kết đó. Chỉ khi Mail thực sự tin tưởng mới được điền thông tin nhạy cảm.

Khi được yêu cầu cung cấp thông tin quan trọng (thông tin nhạy cảm), tốt hơn hết là nên trực tiếp vào website của phía yêu cầu để cung cấp thông tin chứ không đi theo đường liên kết được gửi đến qua Email. Cẩn thận hơn thì nên email lại (không reply email đã nhận) với phía đối tác để xác nhận hoặc liên hệ với phía đối tác bằng Phone hỏi xem có chính xác là họ cần thông tin hay không.

Để phòng chống Phishing hiệu quả thì chủ yếu là từ phía người dùng phải cẩn thận trong việc sử dụng Email. Ngoài ra có hỗ trợ của một số phần mềm.

Kiểu tấn công lừa đảo qua đường Email. Tin tặc thường nhúng virus và spyware và Email. Vì vậy người dùng khi cài đặt các chương trình diệt virus thì chúng sẽ tìm kiếm, diệt và bảo vệ máy tính an toàn trước các hiểm họa Phishing.

5.3.3. Bảo vệ hệ thống khỏi Virus và Spyware

Ngày nay, khi càng nhiều máy tính được nối mạng Internet thì nguy cơ lây nhiễm virus, spyware, Trojan,… ngày càng cao với mức lây lan rất nhanh. Vì vậy, người quản trị nên thực hiện một số biện pháp dưới đây để có thể bảo vệ hệ thống mạng tránh khỏi các nguy cơ từ mạng Internet.

Cài đặt một phần mềm diệt virus hiệu quả

Nhiều người sử dụng máy tính tin tưởng các ứng dụng diệt virus miễn phí có thể bảo vệ thiết bị của họ trước virus và spyware. Tuy nhiên, các chương trình miễn phí này sẽ không cung cấp một sự bảo vệ đầy đủ cho các nguy cơ đang tăng lên hàng ngày.

Vì vậy, cần phải cài đặt các phần mềm diệt virus dành cho doanh nghiệp và chuyên nghiệp hơn trên máy tính cũng như máy chủ của mình. Các chương trình diệt virus chuyên nghiệp sẽ được cập nhật hàng ngày nhằm chống lại những nguy cơ mới tấn công vào lỗ hổng của các phần mềm và hệ điều hành. Trong số những phần mệt diệt virus này, thông dụng nhất phải kể đến Kaspersky Anti-Virus, Symantec AntiVirus Corporate Edition,…

Cài đặt phần mềm chống spyware thời gian thực

Thật là sai lầm khi nhiều người dùng máy tính nghĩ rằng một chương trình diệt virus luôn tích hợp sẵn cả bảo vệ thiết bị của họ tránh khỏi spyware và adware. Một số người khác lại nghĩ, các ứng dụng chống spyware miễn phí kết hợp với một phần mềm antivirus sẽ cung cấp khả năng bảo vệ đầy đủ cho thiết bị.

Thật không may bởi hầu hết các chương trình chống spyware miễn phí đều không cung cấp khả năng bảo vệ thiết bị theo thời gian thực để chống lại Trojan và spyware. Một vài chương trình miễn phí có thể phát hiện nguy cơ nhiễm spyware khi chúng đã lây nhiễm cho thiết bị. Trong khi đó, chương trình chống spyware chuyên nghiệp sẽ ngăn chặn việc lây nhiễm và xóa các nguy cơ này ngay từ lúc đầu.

Đảm bảo chương trình chống mã độc luôn hoạt động

Các chương trình antivirus và anti-spyware yêu cầu việc cập nhật dữ liệu và đăng ký đều đặn. Nếu không cập nhật, các chương trình chống mã độc sẽ không có khả năng bảo vệ máy tính trước các nguy cơ tấn công mới. Nhiều cuộc tấn công diễn ra chỉ trong thời gian ngắn nhưng có sức lây nhiễm 100-300 nghìn trang web mỗi ngày. Vì vậy, người dùng nên cập nhật thường xuyên cho phần mềm diệt virus và spyware cũng như chú ý đến thời điểm hết hạn đăng ký của phần mềm này.

Thực hiện quét máy tính hàng ngày

Đôi khi, virus và spyware thoát khỏi vòng kiểm soát của phần mềm bảo vệ và lây nhiễm vào thiết bị. Vì vậy, việc quét hệ thống hàng ngày sẽ giúp phát hiện và loại bỏ được mầm lây nhiễm này ra khỏi máy tính.

Vô hiệu hóa chức năng autorun

Nhiều virus tấn công vào máy tính khi các bộ nhớ ngoài được kết nối với máy tính thông qua chức năng autorun. Vì vậy, người dùng nên tắt chức năng này khi kết nối các ổ cứng ngoài, USB, thiết bị mạng,…

Để vô hiệu hóa chức năng autorun trên hệ điều hành Windows, người dùng có thể thực hiện các bước sau:

- Vào Start, Run gõ gpedit.msc rồi OK.

- Trong cửa sổ Group Policy, kích đúp vào Administrative Templates, chọn System.

- Trong khung bên phải, kích đúp vàp Turn Off Autoplay.

- Kích đúp vào Turn Off Autoplay, chọn Enabled. Trong ô Turn Off Autoplay on chọn All drives và ấn OK.

- Thoát khỏi Group Policy.

- Khởi động lại máy

Vô hiệu hóa tính năng xem trước hình ảnh trong Outlook

Khi thư điện tử chứa các hình ảnh bị nhiễm virus và ứng dụng Outlook cho phép người dùng xem trước hình ảnh trong đó thì đây là một cách khởi động cho virus lây nhiễm sang hệ thống PC người dùng. Vì vậy, để ngăn chặn việc lây nhiễm tự động, người dùng nên tắt chức năng xem trước hình ảnh trong Outlook.

Đối với các phiên bản mới của ứng dụng Microsoft Outlook sẽ không có chế tự động hiển thị hình ảnh. Nhưng nếu người dùng thay đổi các thiết lập bảo mật mặc định thì nên quay lại tắt chức năng này đi. Nếu dùng Outlook 2007, người dùng thực hiện các bước sau để tắt chức năng này: vào Tools |

Trust Center, bật Automatic Download và lựa chọn Don't Download Pictures Automatically In HTML E-Mail Messages Or RSS.

Không kích vào các đường dẫn trên email hay trong tài liệu đính kèm

Người dùng không bao giờ được kích vào các file đính kèm email trước khi dùng các ứng dụng chống mã độc dành cho doanh nghiệp để quét. Thay vì kích vào đường dẫn đính kèm email, người dùng nên truy cập vào các trang Web này bằng cách mở trình duyệt và gõ địa chỉ trang đó vào.

Lướt web thông minh

Nhiều ứng dụng chống mã độc dành cho doanh nghiệp sẽ được tích hợp ngay trên trình duyệt web để giúp chống lại việc lây nhiễm từ các ổ đĩa, hoặc dùng để lọc các cuộc tấn công. Việc làm này nhằm tránh cho người dùng bị đánh cắp thông tin mật khẩu, tài chính hay dữ liệu nhạy cảm.

Người dùng không nên gõ bất kỳ thông tin cá nhân, tài chính hay tài khoản đăng nhập vào các trang web không đáng tin cậy. Đồng thời, không mở trực tiếp các đường dẫn đính kèm email.

Sử dụng phần cứng tường lửa và hệ thống IDPS

Khi thực hiện chia sẻ máy in, truy cập tài nguyên mạng,… người dùng có thể sử dụng các phần mềm tường lừa (firewall). Tuy nhiên, không phải lúc nào phần mềm này cũng có thể chống lại được vô số các cuộc tấn công vào thiết bị kết nối mạng Internet. Vì vậy, để bảo vệ máy tính chống lại virus, sâu,… thì ngoài phần mềm tường lửa người dùng nên sử dụng thiết bị phần cứng - firewall.

5.3.4. Phòng chống sâu mạng

Sâu máy tính – Worm được hiểu như là một loại virus đặc biệt hay một chương trình độc hại. Phương thức lây lan qua mạng là khác biệt cơ bản giữa virus và sâu. Hơn nữa, sâu có khả năng lan truyền như chương trình độc lập mà không cần lây nhiễm qua tập tin. Ngoài ra, nhiều loại sâu có thể chiếm quyền kiểm soát hệ thống từ xa thông qua các "lỗ hổng" mà không cần có sự "giúp sức" nào từ người dùng. Tuy nhiên, cũng có những trường hợp ngoại lệ như sâu Happy99, Melissa, LoveLetter, Nimda…

Quá trình phát triển gồm 4 giai đoạn sau:

- ✓ Thế hệ thứ nhất: năm 1979 đến đầu những năm 1990
- ✓ Thế hệ thứ hai: đầu những năm 1990 đến 1998
- ✓ Thế hệ thứ ba: từ 1999 đến 2000
- ✓ Thế hệ thứ tư: từ 2001 đến nay

Phân loại sâu Internet

- Phân loại theo mục tiêu khám phá

Sâu máy tính muốn lây nhiễm vào một máy thì trước tiên nó phải tìm hiểu xem máy đó còn tồn tại trên mạng hay không. Một số kỹ thuật của sâu dùng để khám phá như: quét chủ động và quét thụ động. Đây chính là các loại sâu được phân loại theo mục tiêu khám phá những nạn nhân mới. Tuy vậy sâu máy tính có thể kết hợp các kỹ thuật khác nhau để đạt được hiệu quả cao nhất trong lan truyền cũng như thực hiện mục đích của sâu.

Kỹ thuật quét chủ động

Sâu Internet có thể tự động tìm kiếm các nạn nhân bằng việc quét các địa chỉ được tạo ra một cách ngẫu nhiên hay được tạo ra từ trước.

Kỹ thuật quét thụ động

Loại sâu này không tự động tìm kiếm các nạn nhân. Thay vào đó hoặc là chúng chờ cho các nạn nhân tiềm năng liên lạc với chúng hoặc lợi dụng hành vi của người sử dụng để tìm kiếm các mục tiêu mới.

- Phân loại theo phương tiện lan truyền và cơ chế phân phối

Những phương tiện lây nhiễm cũng có thể ảnh hưởng tới tốc độ và kỹ thuật ẩn nấp của một con sâu. Một con sâu có thể chủ động lây lan từ máy này sang máy khác, hoặc có thể được mang theo như là một phần của những giao tiếp bình thường.

- Tự thực hiện
- Kênh thứ hai
- Nhúng

- Phân loại theo đối tượng kích hoạt

Phương tiện kích hoạt sâu trên một máy tính lưu trữ ảnh hưởng đáng kể tới việc lây nhiễm của sâu mạng. Một vài loại sâu có thể được kích hoạt để lây nhiễm ngay lập tức, nhưng cũng có những sâu có thể phải chờ vài ngày hoặc vài tuần để được kích hoạt.

- Kích hoạt bởi con người
- Kích hoạt dựa vào hoạt động của con người
- Quy trình kích hoạt theo lịch
- Tự kích hoạt

- Phân loại theo chức năng

Ngoài mục đích lan truyền trên Internet sâu còn có thể thực hiện các mục đích khác nhau phụ thuộc vào mục tiêu của cuộc tấn công hay ý định của kẻ viết ra sâu. Các loại sâu khác nhau sẽ thực hiện nhiệm vụ khác nhau của những tin tặc.

- Tạo lưu lượng giả
- Điều khiển từ xa qua mạng Internet
- Phát tán thư rác
- Chuyển hướng trang web thông qua HTML-Proxies
- Tấn công từ chối dịch vụ DoS qua Internet
- Thu thập thông tin
- Phá hủy dữ liệu
- Điều khiển thiết bị vật lý từ xa
- Tấn công lớp vật lý
- Duy trì và cập nhật phiên bản mới

Các chu trình của sâu Internet

- Mô hình lan truyền theo kiểu bệnh dịch

Virus máy tính và sâu mạng giống như virus sinh học ở hành vi nhân bản và lây lan của chúng. Những thuật toán được phát triển cho việc nghiên cứu những bệnh truyền nhiễm có thể được điều chỉnh cho phù hợp với việc nghiên cứu virus máy tính và sự lan truyền của sâu mạng.

- ✓ Mô hình bệnh dịch cổ điển đơn giản: Trong mô hình dịch bệnh cổ điển đơn giản, mỗi máy chủ ở một trong hai trạng thái: dễ bị lây nhiễm hoặc truyền nhiễm. Mô hình giả định rằng một máy khi đã bị virus lây nhiễm, thì nó sẽ ở trạng thái truyền nhiễm mãi mãi. Chính vì vậy sự biến đổi của bất kỳ máy nào cũng chỉ có thể từ dễ bị lây nhiễm sang trạng thái truyền nhiễm.

- ✓ Mô hình bệnh dịch tổng quát Kermack-Mckendrick: Trong lĩnh vực dịch tễ học, mô hình Kermack-Mckendrick xem xét quá trình loại bỏ những máy đã bị lây nhiễm. Nó giả định rằng trong một đại dịch của một bệnh dịch truyền nhiễm, một vài máy lây nhiễm hoặc được phục hồi hoặc là chết; một máy được phục hồi từ máy đã chết, nó sẽ được miễn dịch với bệnh mãi mãi – những máy được trong trạng thái loại bỏ sau khi chúng được phục hồi hoặc chết do bệnh dịch. Do vậy mỗi máy chỉ có thể ở một trong 3 trạng thái tại mọi thời điểm: dễ bị lây nhiễm, lây nhiễm và bị loại bỏ. Bất kỳ máy nào trong hệ thống hoặc chuyển từ trạng thái "dễ bị lây nhiễm → lây nhiễm → bị loại bỏ" hoặc trong trạng thái "dễ bị lây nhiễm" mãi mãi.

- Mô hình lan truyền hai thành tố

Quá trình lan truyền thực sự của sâu trên Internet là một quá trình phức tạp. Trong phần này, bài sẽ chỉ đề cấp tới những sâu được liên tục kích hoạt. Theo cách này, một sâu trên một máy truyền nhiễm liên tục cố gắng tìm kiếm và lây nhiễm cho những máy có nguy cơ lây nhiễm, giống sự cố của sâu Code Red vào ngày 19 tháng 7 năm 2001.

Như chúng ta thấy việc lan truyền của worm là một quá trình rời rạc. Tuy nhiên để mô hình hóa lan truyền của sâu Internet thì việc sử dụng phương trình vi phân liên tục cũng cho kết quả gần đúng. Phương trình vi phân liên

tục sử dụng phù hợp cho quá trình lan truyền trên diện rộng với quy mô mạng lớn như Internet.

Quá trình loại bỏ từ máy chủ dễ bị lây nhiễm phức tạp hơn trong mô hình Kermack - McKendrick. Vào lúc bắt đầu lan truyền của sâu; hầu hết mọi người đều chưa biết về sự tồn tại của Code Red worm. Kết quả là việc loại bỏ những máy nhạy cảm là nhỏ và tăng chậm. Khi có nhiều và nhiều hơn nữa những máy tính bị nhiễm bệnh, con người đã có nhận thức về Code Red worm và tầm quan trọng của việc chống lại nó. Do đó tốc độ tiêm chủng tăng nhanh trong thời gian tiếp theo đó. Tốc độ giảm khi số lượng máy nhạy cảm co lại và hội tụ về không khi không có máy nhạy cảm nào.

Các kỹ thuật phát hiện sâu mạng

Cùng với sự phát triển của các kỹ thuật trong mô hình của sâu các kỹ thuật nhằm phát hiện và phòng chống sâu Internet cũng đã được nghiên cứu và áp dụng. Sau đây là một vài kỹ thuật phát hiện sâu mạng dựa vào việc phân tích lưu lượng truyền thông, giám sát những cổng nhạy cảm, những lỗ hổng của hệ thống và phát hiện dựa vào định danh. Những phương pháp này là những phương pháp quan trọng và cốt lõi để phát hiện tin tặc và đặc biệt là sâu Internet.

- Phân tích lưu lượng

Phương pháp phân tích lưu lượng đã được phát triển để theo dõi các tin tặc, phương pháp này cũng đã được áp dụng để thiết kế và thực hiện trong nhiều phần mềm theo dõi và giám sát hoạt động của sâu; vì vậy nó cũng đáng tin cậy.

- Giám sát những hố đen trong mạng và những cổng nhảy cảm

Hai phương pháp hiệu quả để xác định sâu mạng và theo dõi hành vi của chúng là sử dụng hệ thống giám sát hố đen và những cổng nhạy cảm. Các hệ thống này có khả năng theo dõi hành vi của sâu và ghi lại những gì quan sát được. Những phân tích dữ liệu sau đó sẽ mang lại những manh mối có giá trị như tốc độ tăng trưởng của sâu, hoặc thậm chí cả sự hiện diện của những agent mới xâm nhập vào mạng.

- Phát hiện dựa vào định danh

Mô hình phát hiện sâu mạng dựa vào định danh sử dụng cơ sở dữ liệu bao gồm các thông tin về những con sâu đã được biết đến trước đó để đối chiếu với kẻ lạ mặt xâm nhập vào hệ thống từ đó đưa ra các cảnh báo về một con sâu. Có ba loại chính của hệ thống phát hiện dựa vào định danh.

- Mô hình truyền thống trong phân tích định danh: Phân tích định danh là phương pháp phân tích nội dung của dữ liệu bị bắt để phát hiện sự hiện diện của những chuỗi đã được biết đến. Những chữ ký được lưu trữ trong cơ sở dữ liệu và đã được chỉ ra từ nội dung của những file độc hại được biết đến. Những file này thường là những chương trình thực thi được kết hợp với sâu.
- Phân tích định danh tải trọng mạng: Bởi vì sâu tồn tại thông qua các hoạt động mạng, sự hiện diện của chúng có thể được phát hiện bằng các sử dụng bộ giám sát mạng thụ động và bộ giám sát định danh tải trọng. Sâu mạng thường có những định danh đặc biệt khi chúng tấn công các máy chủ trên mạng. Bằng cách xây dựng thư viện những định danh độc hại được biết đến, một bộ giám sát mạng có thể cảnh báo cho một quản trị viên biết về sự xuất hiện của một hoạt động bất thường và của một sâu mạng.
- Phân tích định danh logfile: Nhiều sâu tấn công tất cả các máy chủ mà không có sự chọn lọc có thể bị phát hiện bằng việc triển khai các máy chủ có hệ thống an ninh tốt. Khi các con sâu đó tấn công các máy chủ đó không hề bị tổn thương; ngược lại chúng còn thu thập được thông tin về con sâu đó như: tải trọng, kích thước hay máy nguồn của sâu … tất cả các thông tin này đều được lưu trong file log của máy chủ đó. Việc phân tích những thông tin trong file log đó có thể cho chúng ta những định danh về một con sâu. Từ đó có thể cập nhật cho các máy chủ khác biết về chúng và loại trừ hay ngăn chặn những yêu cầu của các sâu.
- Phân tích định danh file: Kiểm tra nội dung của một hệ thống file chúng có thể được sử dụng để phát hiện sự có mặt của một con sâu. Bởi vì hầu hết các sâu đều thực thi nhị phân và đều nằm trên ổ đĩa của hệ thống. Đây là phương pháp phổ biến nhất được sử

dụng để tìm kiếm sâu, và cũng là cơ sở cho việc cài đặt các phần mềm antivirus. Để kiểm tra sự hiện diện của sâu, một công cụ phát hiện sâu sẽ được thực thi để quét bộ nhớ của hệ thống.

Một số mô hình phòng chống sâu mạng

Phòng chống sâu Internet là một công việc được các nhà an ninh mạng quan tâm vì thiệt hại do sâu Internet gây ra là rất lớn. Đã có nhiều nghiên cứu, đề xuất về mô hình và phương pháp để phòng chống sâu. Phần sau đây sẽ giới thiệu mô hình điển hình là "Friends Model".

- Mô hình Friends

Mô hình (được gọi là mô hình bè bạn) này dựa trên sự sẵn sàng hợp tác của các máy chủ trên giao thức được sắp xếp từ trước. Khi một con sâu được phát hiện lập tức nó sẽ được thông báo đến tất cả các máy trong mạng bởi một giao thức. Cảnh bảo này có thể được gửi đi từ một máy dò toàn cục hay từ một máy dò của một tập hợp các máy chủ tham gia hệ thống. Điều này còn phụ thuộc vào khả năng của máy dò. Mục tiêu của phương pháp này là tối đa hoá các máy chủ được bảo vệ khỏi sâu.

Một số công cụ phòng chống sâu mạng

- Công cụ Kuang

Kuang là một hệ thống dựa vào những quy tắc; nó tìm ra những mâu thuẫn trong thiết lập của các quyết định bảo vệ được thực hiện bởi người sử dụng và người quản trị của một hệ thống UNIX. Nó cho phép người quản trị hệ thống thực hiện phân tích điều gì sẽ xảy ra trong tương lai của một cấu hình bảo vệ, và trong chế độ đó nó giúp người quản lý tạo ra những quyết định bảo vệ. Công cụ Kuang ngầm định rằng khi đã truy cập được vào hệ thống thì có thể trở thành chủ nhân của hệ thống đó. Với một tập các đặc quyền ban đầu và mục tiêu cuối cùng, thệ thống này phân tích cấu hình bảo vệ và đưa ra thứ tự những bước thực hiện những công việc để đạt được những mục tiêu cuối cùng đó nếu có thể.

- Công cụ NetKuang

NetKuang là phần mở rộng của Kuang. Nó chạy trên mạng của những máy tính sử dụng UNIX và có thể tìm thấy lỗ hổng được tạo ra bởi những cấu hình hệ thống yếu kém ở mức độ mạng cho phép kẻ tấn công từ một hệ thống sang các hệ thống khác. Lỗ hổng được phát hiện bằng cách tìm kiếm dựa trên mục tiêu ban đầu; đó là trên một host và song song khi nhiều hosts được kiểm tra.

- Công cụ NOOSE

NOOSE (Networked Object-Oriented Security Examiner) là một hệ thống phân tích lỗ hổng phân tán dựa trên mô hình đối tượng. Nó kết hợp máy quét của host và của mạng, lưu trữ các kết quả vào trong mốt số lớp đối tượng. Nó có thể thu thập các lỗ hổng bảo mật từ nhiều nguồn khác nhau, bao gồm cả các kết quả đầu ra của các chương trình phân tích khác. NOOSE trình bày các thông tin về lỗ hổng như một cơ sở dữ liệu tích hợp, và dễ dàng cho việc tích hợp vào chuỗi kết của từ nhiều tài khoản và hệ thống khác.

- Các công cụ khác

Có nhiều biện pháp, công cụ của nhiều hãng khác nhau nhằm bảo mật hệ thống một cách tốt nhất. Một vài hệ thống bảo mật tốt nhất được PC World Mỹ phối hợp cùng AVTest.org thực hiện đợt "sát hạch", đánh giá vào năm 2012 là những hệ thống sau: G-DATA InternetSecurity 2012, Norton Internet Security 2012, Bitdefender Internet Security 2012, Kaspersky Internet Security 2012, Trend Micro Maximum Security 2012.

5.3.5. Bảo vệ ứng dụng Web từ các tấn công

Tin tặc tấn công vào các website của các tổ chức, đặc biệt là các doanh nghiệp thương mại điện tử chủ yếu để khai thác lỗ hổng nhằm kiểm soát website hoặc tấn công tên miền nhằm chuyển hướng người duyệt web sang một website khác. Cùng với sự gia tăng các lây nhiễm mã độc cũng như yêu cầu về thời gian và ngân sách CNTT đã đến lúc các tổ chức, doanh nghiệp cần xem xét lại chiến lược bảo vệ web của mình. Phần này giới thiệu bốn nguyên tắc cơ bản giải quyết vấn đề này, đồng thời giúp tiết kiệm thời gian và chi phí cho các tổ chức, doanh nghiệp.

Web – Môi trường tiềm ẩn nhiều rủi ro

Các trang tin thông tin điện tử giờ đây không chỉ đơn thuần là một website thông tin, quảng bá thông thường mà đã và đang chuyển thành các ứng dụng chạy trên nền web. Các ứng dụng web này được xây dựng trên nhiều thành phần và chạy trên các máy chủ khác nhau: máy chủ web, máy chủ ứng dụng và máy chủ cơ sở dữ liệu,... Tại các tổ chức, doanh nghiệp, số người sử dụng web ngày càng nhiều bởi những lợi ích mà nó mang lại, cũng như khả năng truy cập dễ dàng tới những công cụ họ cần. Tuy nhiên đây cũng là môi trường nguy hiểm, tiềm ẩn nhiều rủi ro về bảo mật.

Khi một website bị tấn công, tin tặc có thể thực hiện các mục đích như thay đổi diện mạo trang chủ, thay đổi một phần hoặc toàn bộ website hay tấn công từ chối dịch vụ, làm cho website không còn khả năng phục vụ. Các cuộc tấn công này gây nhiều tổn thất cho doanh nghiệp do uy tín có thể bị suy giảm, thông tin trong giao dịch trực tuyến hoặc giao dịch ngân hàng sai lệch, thông tin nhạy cảm như: tài khoản, thẻ tín dụng, thông tin truy nhập vào hệ thống... trong quá trình thực hiện các giao dịch trực tuyến bị đánh cắp. Một trong số các nguyên nhân dẫn đến số lỗi bảo mật trên ứng dụng web là do các website được thuê gia công thường sử dụng chung mã nguồn hoặc tận dụng các mã nguồn miễn phí trên Internet mà không được chỉnh sửa một cách đúng mức, trong khi các lỗ hổng trong các mã nguồn miễn phí này cũng được công bố trên Internet khiến cho nguy cơ bị tấn công càng cao hơn.

Lợi dụng điểm yếu này, tội phạm mạng liên tục triển khai các cuộc tấn công nhằm xâm nhập hệ thống và đánh cắp dữ liệu nhạy cảm. Trong một nghiên cứu gần đây với sự tham gia của 50 tổ chức, doanh nghiệp có 64% các doanh nghiệp là nạn nhân của một cuộc tấn công trên web trong khoảng thời gian 4 tuần. Và các cuộc tấn công dựa trên web được xem là loại hình tấn công gây tổn thất lớn thứ hai cho doanh nghiệp, sau kiểu tấn công từ chối dịch vụ, bao gồm cả thiệt hại tài chính, các vấn đề pháp lý và tuân thủ, trách nhiệm pháp lý khi làm rò rỉ dữ liệu, thiệt hại cho thương hiệu và danh tiếng và mất niềm tin của khách hàng.

Các nguy cơ đối với hệ thống web

- Nguy cơ bị tấn công từ chối dịch vụ (DoS, DDoS) làm cho hệ thống không còn khả năng phục vụ các yêu cầu chính đáng.

- Nguy cơ bị thay đổi nội dung trang web làm giảm uy tín và/hoặc bôi nhọ tổ chức.
- Nguy cơ bị kẻ xấu làm sai lệch các thông tin khi thực hiện các giao dịch điện tử trên môi trường Internet.
- Nguy cơ bị đánh cắp các thông tin nhạy cảm như: thông tin tài khoản, mật khẩu truy cập hệ thống và thông tin thẻ tín dụng,…

Bốn nguyên tắc bảo vệ hệ thống web

Vậy các tổ chức, doanh nghiệp cần làm gì để chống lại tất cả các mối đe dọa. Bốn nguyên tắc sau sẽ giúp các tổ chức, doanh nghiệp xây dựng được một hệ thống bảo vệ web toàn diện.

Nguyên tắc 1 : Giảm bớt nguy cơ bị tấn công

Để giảm bớt nguy cơ bị tấn công, các tổ chức, doanh nghiệp cần tránh các mối đe dọa rõ ràng và loại bỏ các lỗ hổng bảo mật.

Lọc các URL độc hại

Các tổ chức, doanh nghiệp có thể sử dụng các bộ lọc URL để ngăn chặn người dùng truy cập vào những trang web bị nhiễm mã độc hoặc những trang mà nhiều lần bị nhiễm mã độc hay có nội dung không phù hợp. Lọc URL giúp kiểm soát thời gian các trang web mà người dùng ghé thăm, do đó đặc biệt hiệu quả trong việc ngăn chặn các trang web mã độc mới.

Kiểm soát ứng dụng

Kiểm soát ứng dụng giúp giảm bớt rủi ro bảo mật và giúp doanh nghiệp quản lý hiệu quả hơn bằng cách ngăn chặn người dùng cài đặt các phần mềm không liên quan đến hoạt động của doanh nghiệp trên máy tính. Các ứng dụng không cần thiết và không được phép này sẽ làm tăng nguy cơ bị tấn công, bởi tin tặc có thể khai thác các lỗ hổng trong các ứng dụng như trình duyệt web, phần mềm PDF, chương trình nghe nhạc, thanh công cụ,… để đánh cắp thông tin và dữ liệu. Mặt khác, chúng làm tăng số lượng các ứng dụng CNTT mà doanh nghiệp cần quản lý và nâng cấp phần mềm.

Để ngăn chặn các cuộc tấn công mạng thì các doanh nghiệp nên chủ động thực hiện các biện pháp kiểm tra và đánh giá mức độ bảo mật cho các

ứng dụng web cũng như cải thiện chất lượng các quy trình phát triển và đảm bảo chất lượng phần mềm. Các ứng dụng web đã được "quét" cũng đã giảm thiểu lỗ hổng bảo mật rất lớn khi được kiểm thử lại.

Tuy nhiên nếu chính sách kiểm soát ứng dụng cứng nhắc cũng sẽ gây nhiều hạn chế. Do đó kiểm soát ứng dụng cần linh hoạt với các chính sách khác nhau để phù hợp cho các nhóm người dùng khác nhau.

Bản vá

Theo ước tính khoảng 90% các cuộc tấn công vào các lỗ hổng phần mềm có thể được ngăn chặn khi sử dụng bản vá. Tuy nhiên thực tế hiện nay có rất nhiều máy tính vẫn được sử dụng mà không được cài đặt các bản vá lỗi bảo mật mới nhất. Điều này đặt các tổ chức, doanh nghiệp rơi vào rủi ro nghiêm trọng bởi một loạt các mối đe dọa từ mã độc. Để ngăn chặn tin tặc khai thác các lỗ hổng, các doanh nghiệp phải tập trung vào việc rút ngắn thời gian cài đặt các bản vá kể từ khi lỗ hổng bảo mật được công bố. Trong khoảng thời gian một ngày sau khi các lỗ hổng được công bố thì các tin tặc vẫn đủ thời gian chế công cụ phá hoại trước khi những bản vá đó được cài đặt trên các hệ thống.

Một hệ thống đánh giá bản vá thông minh, chẳng hạn như tích hợp vào giải pháp bảo mật bảo vệ thiết bị đầu cuối sẽ cho biết bản vá lỗi gì là phù hợp và cần phải áp dụng, thay vì trình bày một danh sách tất cả các bản vá lỗi có sẵn.

Nguyên tắc 2 : Bảo vệ mọi nơi

Bảo vệ thiết bị đầu cuối: Một vấn đề đặt ra là khi nhân viên làm việc ngoài văn phòng có thể sẽ bị nhiễm mã độc, do đó cần kiểm soát tất cả lưu lượng truy cập vào trang web của doanh nghiệp thông qua gateway hoặc một dịch vụ SaaS. Bảo vệ tất cả người dùng sẽ trở nên dễ dàng với giải pháp bảo vệ web tích hợp vào thiết bị đầu cuối. Bằng cách này, các doanh nghiệp có thể bảo vệ trang web của họ mọi lúc, mọi nơi.

Kiểm soát thiết bị di động: Sự bùng nổ việc sử dụng thiết bị và kết nối di động trong công việc dẫn tới nhu cầu bảo mật dữ liệu tại mỗi điểm là cần thiết. Do đó, các doanh nghiệp cần thiết lập các chính sách bảo mật cho thiết

bị di động, khóa máy từ xa hoặc hủy dữ liệu nếu chúng bị mất. Điều này bao gồm đảm bảo an toàn cho các tập tin được tải cũng như việc truy cập vào các dịch vụ đám mây, cho dù từ máy tính hoặc các thiết bị di động.

Nguyên tắc 3 : Ngăn chặn các tấn công và lỗ hổng

Với sự cải tiến của các công nghệ mới, các tổ chức, doanh nghiệp thể ngăn chặn các mối đe dọa mới nhanh chóng, tức thời.

Phòng chống mã độc: Theo thời gian, mã độc không chỉ đơn thuần là các virus lây lan qua việc chép dữ liệu, mà đã tiến hóa trở thành các mã tấn công đa hình, lây lan chính bằng con đường Internet. Trong những năm gần đây, tấn công mã độc đã trở thành một trong những rủi ro an toàn thông tin số một trên thế giới và tiếp tục sẽ là điểm nóng của các năm tới. Phòng chống mã độc có thể coi là thành phần thiết yếu nhất trong một giải pháp bảo vệ web. Để đạt hiệu quả cao, hệ thống này cần có khả năng kiểm soát tất cả lưu lượng truy cập web, bao gồm các nội dung đáng tin cậy, xác định các mối đe dọa cũng như các lỗ hổng mới. Mỗi khi người dùng truy cập một trang web, các công cụ quét kiểm tra lưu lượng truy cập giúp chống khỏi nguy cơ lây nhiễm mã độc.

Bảo vệ thời gian thực hàng ngày xuất hiện thêm rất nhiều mối đe dọa mới từ web, do đó việc bảo vệ cần thực hiện liên tục trong thời gian thực.

Nguyên tắc 4: Nâng cao ý thức của nhân viên về vấn đề bảo mật

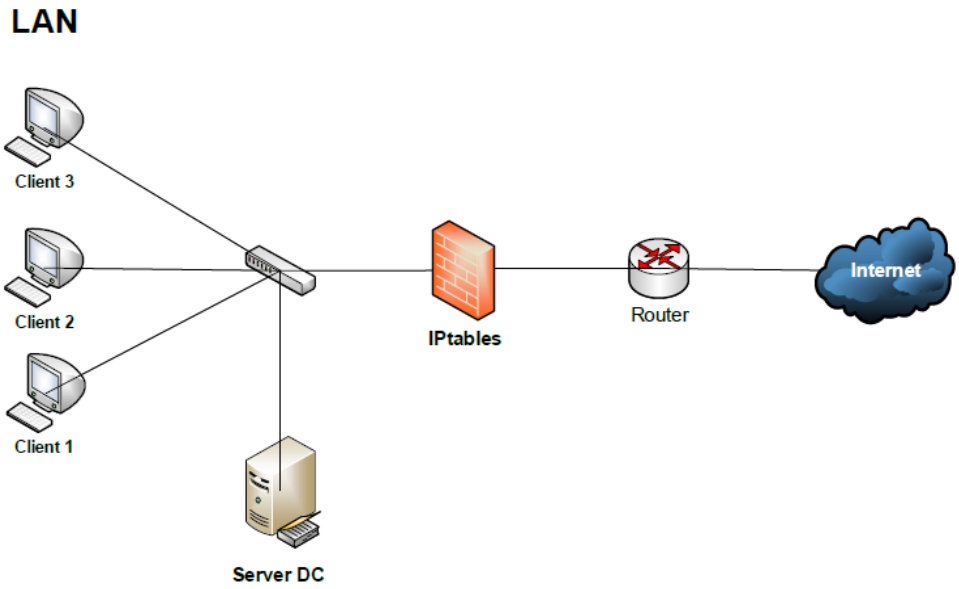
Nhân tố cần được quan tâm đầu tư đặc biệt trong tất cả các hệ thống an toàn thông tin nói chung và hệ thống bảo vệ web nói riêng là con người. Yếu tố con người trong hệ thống ATTT có thể bao gồm nhân sự vận hành và nhân sự sử dụng hệ thống thông tin. Việc đào tạo nâng cao nhận thức của nhân viên về vấn đề bảo mật sẽ đảm bảo mang lại hiệu quả cao nhất cho hệ thống bảo vệ web của doanh nghiệp, bởi nó giúp hạn chế các truy cập vào các trang web độc hại mà có thể mang lại mối đe dọa cho doanh nghiệp.

CÁC BÀI THỰC HÀNH

1. Thực hành triển khai công nghệ tường lửa Iptables

Mục đích bài thực hành: hướng dẫn kích hoạt, cấu hình tường lửa Iptables, cho phép hoạt động ở những cổng TCP/UDP cần thiết. Kiểm soát cho phép hoặc không cho phép kết nối.

Bước 1: Thiết lập mô hình mạng



Bước 2: Cài đặt máy chủ với hệ điều hành Linux (Red hat hoặc CentOS…).

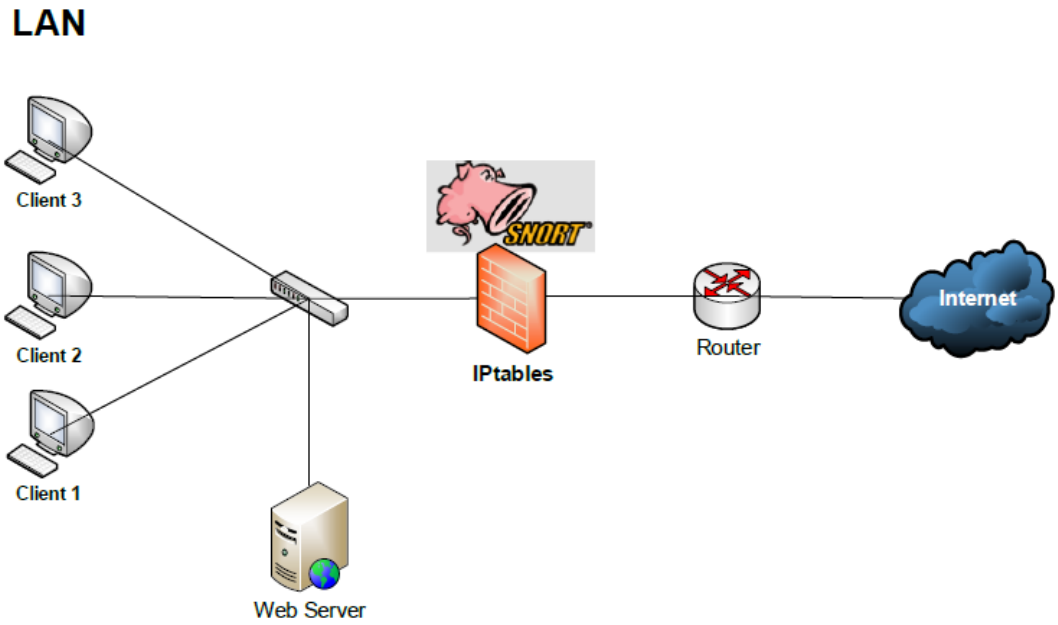
Bước 3: Kích hoạt Iptables.

Bước 4: Thiết lập luật cho Iptables cho phép người dùng bên trong mạng LAN truy cập ra Internet với các dịch vụ: mail (cổng 25, 110), dịch vụ web (cổng 80, 443), dịch vụ truyền file (cổng 20,21), dịch vụ SSH (cổng 22).

Bước 5: Từ mạng bên ngoài thực hiện tấn công từ chối dịch vụ DoS (ICMP) vào máy chủ DC. Cấu hình ngăn chặn tấn công bằng cách chặn địa chỉ IP này.

2. Thực hành triển khai công nghệ phát hiện và ngăn chặn xâm nhập sử dụng Snort và Iptables

Bước 1: Thiết lập theo mô hình mạng sau đây:



Bước 2: Trên máy chủ cài Linux kích hoạt tường lửa Iptables, cài thêm phần mềm Snort.

Bước 3: Cấu hình Snort để giám sát luồng lưu lượng vào ra từ trong và ngoài mạng.

Bước 4: Cấu hình Snort kết hợp tường lửa Iptables để phát hiện và ngăn chặn tấn công.

Bước 5: Từ bên ngoài thực hiện tấn công dò quét phát hiện máy chủ web, tấn công từ chối dịch vụ DoS HTTP vào máy chủ web.

Bước 6: Từ trang quản trị Snort kiểm tra dấu hiệu tấn công. Khi phát hiện địa chỉ IP tấn công, cấu hình Iptables để ngăn chặn địa chỉ IP này.

Chương 6.
QUẢN LÝ VÀ VẬN HÀNH AN TOÀN HỆ THỐNG

6.1. QUẢN LÝ SỰ THAY ĐỔI

Quản lý thay đổi là phương pháp tiếp cận có hệ thống về việc theo dõi và xác định sự tiến triển của hệ thống công nghệ. Sắp xếp các thay đổi đối với một hạ tầng công nghệ tập trung vào các chức năng kết quả. Các tổ chức, doanh nghiệp có nhiều giải pháp để cải tiến hoặc thay đổi trong đó có sự thay đổi về công nghệ. Đảm bảo an toàn cho hệ thống mạng là thực sự cần thiết và nó là một phần của tâm điểm về sự cải tiến và thay đổi hệ thống.

Phần này trình bày vai trò về tính bảo mật nên được thực hiện trong chương trình quản lý thay đổi. Quản lý thay đổi kết hợp một quy trình được xây dựng rõ ràng trên một khuôn khổ tùy chỉnh sử dụng tài nguyên có sẵn để phát triển hoàn chỉnh. Mục tiêu trong suốt quy trình quản lý thay đổi là duy trì khả năng bảo mật của hệ thống và mức độ rủi ro có thể chấp nhận được.

6.1.1. Xác định và phân loại các tình huống thay đổi

Không có một tình huống thể hiện sự thay đổi, do đó không thể có bất kỳ ai tiếp cận tới quản lý thay đổi. Vì vậy, sự thay đổi nên được phân loại, mỗi một loại thay đổi được ánh xạ tới một cách tiếp cận khác nhau để di chuyển nó tới quy trình quản lý sự thay đổi tương ứng. Thay đổi bảo mật có thể được xác định từ một sự thay đổi mà ảnh hưởng đến một máy tính hoặc một cá nhân để thay đổi có ảnh hưởng đến toàn bộ quá trình kinh doanh của tổ chức, vận hành của hệ thống mạng.

Cơ sở quản lý thay đổi phải nhận ra những khác biệt bằng cách trình bày các hoàn cảnh thay đổi khác nhau. Để xác định một vị trí bên trong kế hoạch quản lý thay đổi cho các loại thay đổi khác nhau về những lợi ích của việc linh hoạt, nhanh chóng của hệ thống quản lý sự thay đổi. Phát triển phạm vi rộng các quy trình quản lý thay đổi bao gồm một quá trình cho công việc nhỏ hoặc thường xuyên để ngăn chặn chúng từ những loại hình tấn công. Thực hiện quy trình quản lý thay đổi để xử lý các thay đổi theo chiều sâu sẽ thúc đẩy kiểm soát và khả năng dự đoán.

Lồng ghép các vấn đề bảo mật vào trong các hạng mục của sự thay đổi làm một thách thức. Nếu một thay đổi được coi là không quá đáng kể để đặt trong quy trình quản lý thay đổi, vậy làm thế nào các vấn đề về bảo mật được giải quyết? Câu trả lời là sự xác định, sự phân loại và bao gồm tất cả các công nghệ thay đổi vào trong một hệ thống quản lý sự thay đổi linh hoạt.

6.1.2. Phát triển kế hoạch quản lý sự thay đổi

Có một vài yếu tố của kế hoạch quản lý thay đổi là cơ bản và phù hợp với hầu hết các lý thuyết. Những nguyên tắc này có thể được mở rộng để phù hợp với hầu hết các môi trường; Nó là quá trình buộc các thành phần này với nhau để phát triển chính sách quản lý sự thay đổi. Triển khai thực hiện hoặc nâng cấp quản lý thay đổi bên trong một tổ chức

6.2. CẬP NHẬT BẢN VÁ

Trong quá trình sử dụng máy tính cài đặt Hệ điều hành Windows và 1 số phần mềm khác, người dùng có thể gặp một số lỗi của các phần mềm này. Những lỗi này sau đó được người dùng thông báo với hãng Microsoft. Microsoft sẽ tiến hành xây dựng và phát hành các gói phần mềm nhỏ giúp người dùng khắc phục những lỗi này. Những gói phần mềm này được gọi là bản vá lỗi.

Các lỗi có mức độ nghiêm trọng khác nhau. Thường các loại virus hoặc hacker sẽ dựa vào những lỗi này để xâm nhập, phá hoại hệ thống. Do đó, ngoài việc sử dụng các phần mềm ngăn chặn virus, spyware, việc cập nhật các bản vá lỗi cho máy tính cài Hệ điều hành Windows là một việc cần phải được thực hiện, nhất là đối với các máy tính có tham gia vào hệ thống mạng.

Để giúp cho người dùng dễ dàng vá các lỗi trên máy tính, hãng Microsoft cung cấp hệ thống cập nhật vá lỗi tự động thông qua giao diện Web. Người dùng có thể truy xuất vào đó thông qua công cụ đã được đính kèm sẵn trong hệ điều hành.

Tuy nhiên, việc kết nối trực tiếp từ các máy tính trong hệ thống mạng vào các máy chủ của Microsoft sẽ diễn ra rất chậm do tốc độ đường truyền

mạng ra ngoài thấp, có thể tốn rất nhiều thời gian (khoảng vài tiếng) để thực hiện công việc vá lỗi.

Để giúp tiết kiệm thời gian vá lỗi các máy tính, hệ thống mạng cục bộ nên tiến hành xây dựng một hệ thống máy chủ cục bộ giả lập nhiệm vụ máy chủ Micorsoft có tính năng cung cấp các bản vá lỗi cho các máy trạm trong hệ thống mạng.

Đồng thời, công việc vá lỗi có thể thực hiện một cách tự động mà không cần sự tương tác từ phía người dùng.

Sau đây là cách thức người dùng cài đặt công cụ hỗ trợ cập nhật vá lỗi.

6.2.1. Mục đích của việc cập nhật bản vá lỗi

- Vá các lỗi hệ điều hành
- Vá các lỗi một số phần mềm khác (như Internet Explore, Windows Media, Outlook Express, Microsoft Office, Visio, ….)
- Chống lại sự lây nhiễm virus
- Đề phòng sự tấn công của hacker.

6.2.2. Đối tượng cần phải cập nhật bản vá lỗi

Các phiên bản hệ điều hành: Microsoft Windows, Linux…

Các phiên bản phần mềm: Microsoft Office, Moriza Firefox, Internet Explorer, Adobe flash…

6.3. QUẢN LÝ CÁC SỰ CỐ AN TOÀN HỆ THỐNG

6.3.1. Xác định và phân tích sự cố

6.3.1.1 Danh mục các sự cố

Các sự cố về an toàn thông tin có thể xảy ra theo rất nhiều cách khác nhau, chính vì vậy việc hướng dẫn từng bước để xử lý toàn bộ các sự cố là điều không thể thực hiện được. Các tổ chức nên có sự chuẩn bị chung để có thể xử lý được bất kỳ loại sự cố nào đặc biệt là các sự cố thông thường xảy ra. Danh mục các sự kiện sau không phải là đầy đủ toàn bộ và cũng không cung

cấp, phân loại hoàn toàn các sự cố, nó chỉ liệt kê các phương pháp tấn công phổ biến và có thể được xem như một cơ sở để xác định các thủ tục xử lý:

- ✓ Thiết bị di động: Một cuộc tấn công có thể bắt đầu từ các thiết bị lưu trữ di động hoặc các thiết bị ngoại vi.

Ví dụ: Mã độc hại có thể lây lan vào hệ thống thông qua một bộ nhớ USB bị nhiễm từ trước.

- ✓ Chiếm dụng dung lượng/Băng thông: Một cuộc tấn công sử dụng phương pháp "Brute Force" để làm suy giảm, phá hủy hệ thống, mạng máy tính hoặc các dịch vụ.

Ví dụ: Một cuộc tấn công DDOS để làm gián đoạn sự cung cấp dịch vụ của một máy chủ, một tấn công Brute Force (Kiểu tấn công dò mật khẩu bằng cách thử tất cả mật khẩu có thể có) để chống lại cơ chế xác thực, chữ ký số …

- ✓ Web: Một cuộc tấn công từ những trang web hoặc dựa trên những ứng dụng của trang web.

Ví dụ: Sử dụng một trang web giả mạo để đánh cắp thông tin hoặc khai thác lỗ hổng bảo mật của trình duyệt nhằm cài đặt các mã độc hại lên máy tính nạn nhân

- ✓ Thư điện tử: Cuộc tấn công có thể thực hiện qua thư điện tử bằng cách đính kèm các công cụ vào thư.

Ví dụ: Đính kèm mã độc hại vào thư điện tử dưới dạng một tài liệu hoặc một liên kết đến trang web chứa mã độc hại.

- ✓ Sử dụng không đúng cách: Một số các sự cố là kết quả việc vi phạm các chính sách của tổ chức của một người dùng hợp lệ (được ủy quyền).

Ví dụ: Người dùng sau khi đăng nhập thành công đã cài một ứng dụng chia sẻ dẫn đến việc mất mát dữ liệu …

- ✓ Mất hoặc bị trộm các thiết bị: Các thiết bị máy tính hoặc thiết bị truyền thông được sử dụng bởi tổ chức bị mất cũng dẫn đến việc mất mát hoặc lộ các dữ liệu.

Ví dụ: Máy tính xách tay hoặc điện thoại của nhân viên làm việc bị mất.

6.3.1.2 Dấu hiệu nhận biết sự cố

Đối với nhiều tổ chức, công đoạn khó khăn nhất của việc ứng phó sự cố là phát hiện chính xác và có thể đánh giá được mức độ sự cố. Khả năng xác định được loại sự cố xảy ra và có thể đánh giá được mức độ và tầm quan trọng của vấn đề, điều này được kết hợp bởi 3 yếu tố:

- ✓ Sự cố có thể được phát hiện thông qua nhiều cách khác nhau, với nhiều mức rõ ràng và chi tiết. Khả năng có thể phát hiện tự động thông qua hệ thống mạng và máy chủ IDPSs, phần mềm diệt vi rút, phân tích nhật ký hoạt động. Sự cố cũng có thể được phát hiện một cách thủ công thông qua các báo cáo của người sử dụng.
- ✓ Khối lượng dấu hiệu tiềm ẩn của các sự cố thường cao. Ví dụ: Một tổ chức có thể nhận được hàng ngàn thậm chí hàng triệu cảnh báo xâm nhập mỗi ngày.
- ✓ Hiểu biết sâu: Kiến thức kỹ thuật chuyên môn và kinh nghiệm là rất cần thiết cho việc phân tích các dữ liệu liên quan đến sự cố.

Dấu hiệu của một sự cố có thể rơi vào một trong hai loại: dấu hiệu báo trước hoặc các chỉ số. Một dấu hiệu báo trước là dấu hiệu cho thấy sự cố có thể sẽ xảy ra trong tương lai. Các chỉ số là dấu hiệu cho thấy sự cố có thể sắp xảy ra hoặc đang xảy ra.

Phần lớn trong các vụ tấn công đều không xác định hoặc nhận biết được dấu hiệu báo trước từ tầm nhìn của mục tiêu. Nếu dấu hiệu báo trước được phát hiện, tổ chức có thể có cơ hội để ngăn chặn sự cố bằng cách thay đổi vị trí an ninh để tránh mục tiêu bị tấn công. Và ở mức tối thiểu, tổ chức có thể chủ động giám sát được các hoạt động liên quan đến mục tiêu. Ví dụ về một số dấu hiệu báo trước:

- Mục nhật ký của máy chủ web cho thấy được có thể trang web đó đang bị một ai đó quét để tìm các lỗ hổng bảo mật.

- Một thông báo về cách khai thác mới nhằm vào lỗ hổng bảo mật máy chủ thư điện tử của tổ chức. Một mối đe dọa từ một nhóm sẽ tấn công tổ chức.

Trong khi các dấu hiệu báo trước tương đối hiếm thì các chỉ số lại khá phổ biến. Có rất nhiều các chỉ số tồn tại nên rất khó để liệt kê một cách triệt để chúng, một số ví dụ:

- Cảm biến phát hiện xâm nhập của một mạng máy tính có thể cảnh báo khi có một tấn công lợi dụng lỗi tràn bộ đệm xảy ra đối với máy chủ cơ sở dữ liệu.
- Phần mềm diệt vi rút đưa ra cảnh báo khi phát hiện có một máy tính bị nhiễm phần mềm độc hại.
- Một quản trị viên thấy một tập tin với tên khác thường.
- Một máy chủ ghi lại sự thay đổi cấu hình trong nhật ký của nó.
- Một ứng dụng đăng nhập không thành công nhiều lần từ một hệ thống từ xa quen thuộc.
- Một quản trị mạng nhận thấy sự thay đổi khác thường của lưu lượng mạng.

6.3.1.3 Nguồn của các dấu hiệu báo trước và chỉ số

Các điểm báo và chỉ số có thể được xác định bởi nhiều nguồn khác nhau, phổ biến nhất là các phần mềm bảo mật máy tính, các bản ghi, các thông tin công khai và con người. Bảng dưới đây liệt kê các nguồn phổ biến nhất của các dấu hiệu báo trước và các chỉ số cho mỗi thể loại:

Bảng 6.1 – Các nguồn phổ biến của các dấu hiệu báo trước và chỉ số

NGUỒN	ĐẶC TẢ CHI TIẾT/ CẢNH BÁO
IDPSs	Các sản phẩm phát hiện và chống xâm nhập xác định các sự kiện đáng ngờ và ghi lại các dữ liệu cần thiết liên quan đến chúng. Bao gồm cả ngày, giờ của cuộc tấn công được phát hiện, loại tấn công, địa chỉ IP nguồn và đích, tên người dùng

	(nếu có và được biết đến). Hầu hết các sản phẩm phát hiện và chống xâm nhập đều sử dụng các dấu hiệu của tấn công để xác định các hoạt động có hại. Các dấu hiệu phải được lưu trữ cho đến lúc các cuộc tấn công mới được phát hiện. Các phần mềm này cũng có thể có các phát hiện sai lệch nên các nhà quản trị nên tự xác nhận bằng cách xem xét các dữ liệu đã ghi lại hoặc nhận các dữ liệu liên quan từ các nguồn khác.
Phần mềm chống thư rác và vi rút	Phần mềm diệt vi rút phát hiện các hình thức khác nhau của mã độc hại, tạo ra cảnh báo và ngăn chặn các mã độc hại từ máy bị nhiễm. Phần mềm diệt vi rút có thể ngăn chặn được nhiều trường hợp mã độc hại nếu các mẫu của chúng luôn được cập nhật. Phần mềm chống thư rác được sử dụng để phát hiện thư rác và ngăn cho nó không thể đến được hộp thư của người dùng. Thư rác có thể chứa phần mềm độc hại, nội dung lừa đảo và các nội dung độc hại khác vì điều đó, những cảnh báo từ phần mềm chống thư rác có thể chỉ ra các tấn công tiềm tàng.
Phần mềm kiểm tra tính toàn vẹn của tập tin	Phần mềm kiểm tra tính toàn vẹn của tập tin có thể phát hiện được những sự thay đổi quan trọng của tập tin trong suốt sự cố. Phần mềm này sử dụng thuật toán băm để kiểm tra mỗi tập tin được chỉ định. Nếu tập tin bị thay đổi thì giá trị băm ban đầu sẽ khác với giá trị băm mới. Bằng cách này các tập tin thay đổi sẽ bị phát hiện.
Dịch vụ giám sát được cung cấp bởi bên thứ ba	Dịch vụ giám sát do bên thứ ba cung cấp dựa trên yêu cầu hoặc miễn phí. Ví dụ một dịch vụ gian lận sẽ được phát hiện và thông báo cho một tổ chức nếu địa chỉ IP, tên miền … được phát hiện bởi một tổ chức khác.
	NHẬT KÝ

Nhật ký ứng dụng và các dịch vụ hệ điều hành	Nhật ký ghi lại từ hệ điều hành, các dịch vụ và các ứng dụng (đặc biệt là các dữ liệu liên quan đến kiểm toán) thường rất quan trọng khi sự cố xảy ra. Ví dụ như việc ghi lại các hoạt động và truy cập của một tài khoản. Tổ chức nên yêu cầu một mức độ cơ bản cho việc ghi lại nhật ký trên toàn hệ thống và một mức độ cao hơn cho các dữ liệu nhạy cảm. Nhật ký có thể được sử dụng cho việc phân tích thông tin về sự kiện. Tùy vào kết quả để có thể đưa ra cảnh báo về sự cố.
Nhật ký thiết bị mạng	Nhật ký có được từ các thiết bị mạng như tường lửa hoặc bộ định tuyến thường không phải là nguồn chính của các dấu hiệu báo trước và các chỉ số. Mặc dù các thiết bị này thường được cấu hình để chặn các kết nối, chúng cung cấp rất ít thông tin về bản chất của hoạt động này. Tuy nhiên chúng có thể có giá trị trong việc xác định hướng đi, lưu lượng mạng và mối liên quan giữa các sự kiện được phát hiện bởi các thiết bị khác.
	THÔNG TIN CÔNG KHAI
Thông tin về các khai thác và lỗ hổng bảo mật mới	Cập nhật các thông tin về các lỗ hổng bảo mật và cách khai thác lỗi mới có thể ngăn ngừa sự cố xảy ra và hỗ trợ được nhiều trước việc phân tích cuộc tấn công. Cơ sở lưu trữ dữ liệu lỗ hổng bảo mật quốc gia (The National Vulnerability Database – NVD) chứa các thông tin về các lỗ hổng bảo mật. Các tổ chức như US-CERT and CERT/CC định kỳ cung cấp thông tin về các mối đe dọa thông qua web, thư điện tử…
	CON NGƯỜI
Người từ trong tổ chức	Người dùng, quản trị hệ thống, quản trị mạng, nhân viên an ninh và những người khác trong tổ chức có thể báo cáo về dấu hiệu của của sự cố. Điều quan trọng là tổ chức phải xác nhận được tất cả các báo cáo đó. Một phương pháp là yêu cầu

	người cung cấp thông tin phải chắc chắn với thông tin của mình. Việc ghi lại các đánh giá này kết hợp các thông tin thu được trong suốt quá trình phân tích sự cố có thể giúp sớm phát hiện sự cố.
Người từ tổ chức khác	Các báo cáo về sự cố từ các tổ chức bên ngoài nên được xem xét một cách cẩn thận. Ví dụ như người dùng ngoài tổ chức có thể báo cáo về một tấn công đổi giao diện web hoặc về một dịch vụ nào đó không làm việc… Điều quan trọng là phải tạo được cơ chế báo cáo lại các sự cố này giúp cho người dùng có thể báo cáo lại được cho bên hỗ trợ.

6.3.1.4 Phân tích sự cố

Việc phân tích và phát hiện sự cố sẽ rất dễ dàng nếu như các báo trước và các chỉ số có được là chính xác, nhưng không phải lúc nào cũng thế. Ví dụ: hệ thống phát hiện và chống xâm nhập (IDPSs) có thể có những cảnh báo nhầm, không chính xác đối với một kết nối bình thường. Việc xác định được một mức cảnh báo lý tưởng là rất khó khăn. Tìm và phát hiện ra các sự cố an ninh thật sự trong số các cảnh báo hàng ngày đòi hỏi phải có một khả năng và kinh nghiệm tốt.

Ngay cả khi các cảnh báo là chính xác cũng không hẳn là một sự cố đã xảy ra. Một vài cảnh báo, ví dụ như lỗi của máy chủ hay việc thay đổi các tập tin quan trọng có thể xảy ra vì nhiều nguyên nhân khác bao gồm cả lỗi của người dùng. Tuy nhiên, với sự xuất hiện các cảnh báo có thể đó là việc nghi ngờ về sự cố để có thể đưa ra các hành động phù hợp. Đôi khi để xác định được sự cố cần phải có sự phối hợp giữa các nhân viên kỹ thuật, an ninh và các thông tin tìm được để có thể đưa ra một quyết định đúng.

Nhiều sự cố có thể dễ dàng phát hiện ra, ví dụ như việc thay đổi giao diện của trang web… nhưng cũng có nhiều sự cố xảy ra với các dấu hiệu không rõ ràng, ví dụ như một thay đổi nhỏ trong tập tin cấu hình hệ thống. Trong quá trình xử lý sự cố, phát hiện sự cố có thể là nhiệm vụ khó khăn nhất. Chính vì vậy, việc xây dựng một đội ngũ nhân viên giàu kinh nghiệm và thành thạo khả năng phân tích sự cố là việc rất cần thiết đối với mỗi tổ chức.

Đội ứng phó sự cố nên làm việc một cách nhanh chóng để phân tích xác nhận mỗi sự cố. Khi nhóm tin rằng sự cố đã xảy ra, phải nhanh chóng thực hiện một số phân tích ban đầu để xác định phạm vi của sự cố (chẳng hạn như hệ thống, mạng máy tính hoặc các ứng dụng bị ảnh hưởng…). Những phân tích ban đầu sẽ cung cấp cho nhóm các thông tin để ưu tiên các hoạt động tiếp theo, chẳng hạn như ngăn chặn các sự cố và phân tích sâu hơn về các tác động của sự cố.

Những đề nghị sau giúp cho việc phân tích các sự cố một cách dễ dàng và hiệu quả hơn:

- Lập hồ sơ về mạng và hệ thống: Thiết lập hồ sơ về các mức độ hoạt động dự kiến của hệ thống vì thế khi có sự thay đổi sẽ dễ dàng xác định được nguyên nhân. Nếu quá trình lưu giữ là tự động, khi có sự thay đổi (hệ thống không hoạt động theo dự kiến) thì sẽ được phát hiện và báo cáo cho quản trị viên một cách nhanh chóng.
- Hiểu rõ các hoạt động bình thường: Các thành viên trong nhóm ứng phó sự cố cần phải nghiên cứu tìm hiểu các hoạt động bình thường của hệ thống mạng để từ đó nhận biết được các hoạt động bất thường dễ dàng hơn. Không bắt buộc các thành viên đều phải có kiến thức toàn diện ở các hoạt động nhưng các thành viên nên biết sâu về một vài vấn đề nào đó cụ thể. Một cách để có thể có thêm kiến thức là thông qua việc xem các mục nhật ký hay các cảnh báo an ninh. Khi họ đã quen với các nhật ký và các cảnh báo, họ nên tập trung vào các mục không rõ nguyên nhân gây ra, đó thường là các mục quan trọng và đương nhiên cũng sẽ thú vị hơn. Việc tiến hành đánh giá nhật ký thường xuyên sẽ giúp cho các thành viên trong nhóm ứng phó sự cố luôn cập nhật được các xu hướng thay đổi và kiến thức mới. Bên cạnh đó các kết quả cũng mang lại cho các nhà phân tích một dấu hiệu đáng tin cậy của mỗi nguồn.
- Tạo một chính sách duy trì nhật ký: Thông tin liên quan đến một sự cố có thể được ghi lại ở nhiều chỗ như tường lửa, thiết bị phát hiện và chống xâm nhập và các bản ghi ứng dụng. Tạo và thực hiện một chính sách duy trì nhật ký để xác định các nhật ký có thể được duy trì trong

bao lâu có thể rất hữu ích trong việc phân tích bởi vì nhật ký cũ có thể hiển thị các hoạt động trước khi cuộc tấn công xảy ra giúp cho việc nhận biết các tấn công tương tự. Một lý do nữa là có thể sự cố xảy ra không bị phát hiện cho đến khi việc phân tích log một thời gian dài sau đó. Thời gian duy trì nhật ký tùy thuộc vào nhiều yếu tố như các chính sách và khối lượng dữ liệu.

- Sử dụng liên quan giữa các sự kiện: Bằng chứng về sự cố có thể được lưu trữ ở nhiều nơi khác nhau. Ví dụ như tường lửa có thể lưu trữ địa chỉ IP của kẻ tấn công, một ứng dụng đăng nhập có thể lưu trữ thông tin về tài khoản của kẻ đó. Một thiết bị phát hiện và chống xâm nhập có thể phát hiện và ngăn chặn một cuộc tấn công mạng đã biết trước nhưng nó lại không biết nếu như cuộc tấn công đã thành công. Các nhà phân tích cần phải kiểm tra các thông tin trong nhật ký mới có thể xác định được thông tin đó. Mối liên quan giữa các sự kiện trong các nguồn là dữ liệu quan trọng trong việc xác định sự cố.
- Đồng bộ thời gian ở tất cả các máy tính: Sử dụng giao thức như Network Time Protocol (NTP) để đồng bộ thời gian ở các máy tính trong mạng. Việc liên kết các sự kiện có thể sẽ gặp khó khăn nếu như thời gian ở các máy không giống nhau. Phải có tính nhất quán ở tem thời gian trong các sự kiện.
- Sử dụng và duy trì kiến thức cơ sở về thông tin: Kiến thức cơ bản phải bao gồm các thông tin mà đội xử lý sự cố cần tham khảo nhanh chóng trong quá trình phân tích sự cố. Mặc dù khó có thể tạo được một nền tảng kiến thức cơ bản với cấu trúc phức tạp nhưng lại đơn giản tiếp thu một cách hiệu quả. Các loại văn bản tài liệu, bảng và cơ sở dữ liệu đơn giản cung cấp cơ chế linh hoạt và nhanh chóng cho việc chia sẻ dữ liệu giữa các thành viên trong nhóm. Kiến thức cơ bản cũng nên bao gồm nhiều thông tin giải thích về sự quan trọng của các dấu hiệu báo trước và chỉ thị, ví dụ như các cảnh báo của hệ thống IDPSs, các mục nhật ký hệ điều hành hay các mã ứng dụng bị lỗi…
- Sử dụng Internet: Các công cụ tìm kiếm trên Internet cũng giúp rất nhiều cho các nhà phân tích tìm thấy các thông tin bất thường trên hệ

thống đặc biệt chức năng quét. Ví dụ: Một nhà phân tích nhận thấy có những điều bất thường trên cổng TCP 22912, ngay lập tức anh ta có thể sử dụng các từ khóa dạng như "TCP 22912", "Port 22912" để tìm kiếm thêm thông tin và tầm quan trọng cũng như các lỗi có thể khai thác được …

- Sử dụng các chương trình nghe lén "Sniffer": Đôi khi các chỉ số thu được theo cách thông thường không đem lại thông tin đầy đủ để có thể xác định được sự cố. Nếu một sự cố xảy ra, cách nhanh nhất để có thể thu được các thông tin đó là sử dụng một phần mềm nghe lén để thu thập hay quản lý lưu lượng mạng. Tuy nhiên cũng vì sự riêng tư nên việc sử dụng các phần mềm dạng này cần phải được sự cho phép của tổ chức.
- Lọc dữ liệu: Khi không có đủ thời gian để xem và phân tích tất cả các chỉ số thu được, thì ở mức tối thiểu nhất, các hoạt động đáng ngờ cần phải được điều tra. Một chiến lược khá hiệu quả là lọc và đưa ra danh sách các hoạt động có xu hướng không đáng kể hoặc là đưa ra một danh sách các hoạt động có xu hướng đáng ngờ nhất.
- Tìm kiếm những sự hỗ trợ khác: Nhiều khi nhóm ứng phó sự cố sẽ không thể xác định nguyên nhân đầy đủ và bản chất của sự cố. Lúc đó các thông tin về sự cố do các bộ phận khác cung cấp sẽ là nguồn tham khảo tốt.

6.3.1.5 Phân cấp mức độ ưu tiên đối với sự cố

Ưu tiên xử lý các sự cố có lẽ là điểm quyết định quan trọng trong quá trình xử lý sự cố. Sự cố không nên được xử lý theo kiểu gặp trước- xử lý trước (First come – first server). Thay vào đó việc xử lý cần được ưu tiên dựa vào các yếu tố lien quan, chẳng hạn như:

- Ảnh hưởng đến các chức năng: Những loại sự cố mà mục tiêu của nó là hệ thống công nghệ thông tin thường ảnh hưởng lớn đến các chức năng mà hệ thống đang cung cấp dẫn đến tác động tiêu cực cho người dùng. Đội ứng phó nên xem xét đến ảnh hưởng hiện tại của hệ thống và cả

những tác động tiêu cực trong tương lai đến hệ thống nếu như sự cố không được khắc phục.

- Thông tin về các ảnh hưởng: Khi sự cố an toàn thông tin xảy ra, tính toàn vẹn, tính bí mật và tính sẵn sàng của thông tin trong tổ chức có thể bị ảnh hưởng. Ví dụ một phần mềm độc hại có thể làm lộ các thông tin nhạy cảm của tổ chức …
- Khả năng phục hồi từ sự cố: Quy mô của sự cố và các loại tài nguyên bị ảnh hưởng sẽ quyết định thời gian và nguồn lực mà tổ chức phải bỏ ra để khôi phục lại. Trong một số trường hợp, việc phục hồi lại sẽ không có ý nghĩa (Bị lộ các thông tin bí mật, nhạy cảm …). Khi đó đội xử lý sự cố nên cân nhắc trong việc các giá trị của thông tin mang lại trước và sau khi phục hồi để quyết định ưu tiên xử lý.

Bảng sau cung cấp các mức độ ảnh hưởng khi sự cố xảy ra để các tổ chức có thể có được ưu tiên xử lý tốt nhất:

Bảng 6.2 – Mức độ ảnh hưởng đến chức năng

Mức độ	Định nghĩa.
Không	Không ảnh hưởng đến khả năng cung cấp dịch vụ của tổ chức.
Thấp	Tổ chức vẫn có thể cung cấp các dịch vụ nhưng tính hiệu quả không còn cao.
Trung bình	Tổ chức mất khả năng cung cấp các dịch vụ tới một nhóm người dùng.
Cao	Tổ chức không còn khả năng cung cấp các dịch vụ tới tất cả người dùng.

Bảng 6.3 – Mức độ ảnh hưởng đến thông tin

Mức độ	Định nghĩa
Không	Không có thông tin bị rò rỉ, thay đổi, xóa hoặc bị tổn hại
Vi phạm quyền riêng tư	Thông tin cá nhân nhạy cảm của nhân viên, quản lý … bị truy cập hoặc bị rò rỉ.

Vi phạm quyền sở hữu	Các thông tin độc quyền chưa phân loại bị rò rỉ hoặc truy cập trái phép
Mất tính toàn vẹn	Các thông tin nhạy cảm hay độc quyền bị xóa hoặc thay đổi

Bảng 6.4 – Mức độ khôi phục thông tin

Mức độ	Định nghĩa
Bình thường	Thời gian phục hồi có thể biết trước được với các nguồn lực hiện có trong tổ chức.
Bổ sung	Thời gian phục hồi có thể biết trước được với các nguồn lực bổ sung.
Mở rộng	Thời gian phục hồi không biết trước được, cần có nguồn lực bổ sung và sự giúp đỡ từ bên ngoài.
Không thể phục hồi	Không thể phục hồi từ các sự cố này (Ví dụ: các dữ liệu bí mật bị rò rỉ hoặc công khai).

Các tổ chức cũng nên thiết lập một quá trình thay đổi mức độ đối với những trường hợp đội ứng phó không kiểm soát được sự cố trong một khoảng thời gian chỉ định.

6.3.2. Hạn chế tác động của sự cố

6.3.2.1 Lựa chọn chiến lược ngăn chặn

Việc ngăn chặn là rất quan trọng, trước khi một sự cố lấn át các nguồn tài nguyên hoặc tăng thiệt hại. Hầu hết các sự cố đều yêu cầu ngăn chặn, vì vậy đó là yếu tố quan trọng hàng đầu trong quá trình xử lý từng sự cố. Một phần thiết yếu của ngăn chặn là ra quyết định (ví dụ: tắt hệ thống, ngắt kết nối từ mạng, vô hiệu hóa các chức năng nhất định). Như vậy, các quyết định là dễ dàng hơn để thực hiện nếu có những chiến lược và thủ tục được xác định có chứa sự cố. Tổ chức nên xác định những rủi ro chấp nhận được trong việc đối phó với sự cố và phát triển các chiến lược phù hợp.

Các chiến lược ngăn chặn khác nhau đối với từng loại sự cố. Ví dụ, một chiến lược ngăn chặn đối với tấn công mã độc thông qua thư điện tử sẽ khác

với một chiến lược ngăn chặn đối với tấn công từ chối dịch vụ. Mỗi tổ chức nên tạo ra các chiến lược ngăn chặn riêng cho từng loại sự cố, phải có tiêu chuẩn tài liệu rõ ràng để tạo điều kiện dễ dàng cho việc đưa ra quyết định. Tiêu chí xác định chiến lược gồm có:

- Khả năng gây thiệt hại và mất mát tài nguyên.
- Cần giữ các bằng chứng.
- Dịch vụ phải luôn sẵn sàng.
- Hiệu quả của chiến lược (Ngăn chặn được một phần hay toàn bộ sự cố).
- Thời gian cần thiết cho giải pháp.

Trong một số trường hợp, một số tổ chức trì hoãn việc ngăn chặn sự cố để họ có thể theo dõi thêm về sự cố đó nhằm mục đích thu thập chứng cứ. Khi đó, đội ứng phó sự cố nên thảo luận với bộ phận pháp lý để xác định xem điều đó là khả thi. Nếu một tổ chức biết rằng hệ thống của họ đã bị xâm nhập nhưng vẫn để cho điều đó được tiếp tục thì họ có thể sẽ phải chịu trách nhiệm khi kẻ tấn công sử dụng hệ thống mạng của họ để tấn công đến một mục tiêu khác. Chiến lược ngăn chặn chậm là khá nguy hiểm khi điều đó xảy ra. Tổ chức nếu muốn thực hiện chiến lược này thì phải chắc chắn họ có một đội ứng phó sự cố giàu kinh nghiệm có khả năng ngắt kết nối của kẻ tấn công kịp thời khi nó chưa gây ra những thiệt hại đáng kể.

6.3.2.2 Thu thập bằng chứng và xử lý

Mặc dù lý do chính để thu thập các bằng chứng là phục vụ cho việc xử lý các sự cố nhưng đôi khi điều đó cũng giúp cần thiết cho các thủ tục pháp lý. Trong trường hợp này, điều quan trọng là tài liệu về bằng chứng rõ ràng đến mức nào bao gồm cả việc hệ thống đã bị xâm nhập hay được bảo vệ. Bằng chứng nên được thu thập theo thủ tục và các quy định hiện hành. Một bằng chứng chi tiết phải bao gồm:

- Thông tin nhận dạng (Vị trí, số serri, số hiệu máy …).
- Tên, chức danh, cách thức liên lạc… của các thành viên tham gia xử lý sự cố.

- Thời gian (bao gồm cả vùng thời gian) của mỗi lần xử lý bằng chứng.
- Địa điểm nơi các bằng chứng đã được lưu trữ.

6.3.2.3 Xác định nguồn tấn công

Trong quá trình xử lý sự cố, quản trị hệ thống cần phải xác định nguồn thực hiện tấn công. Điều này mang ý nghĩa khá quan trọng nhưng đội xử lý thường tập trung vào các vấn đề ngăn chặn, xóa bỏ và phục hồi. Xác định nguồn tấn công có thể tốn nhiều thời gian và đôi lúc không mang lại kết quả. Các hoạt động sau thường được thực hiện để xác định một nguồn gốc của cuộc tấn công:

- Kiểm tra tính hợp lệ của địa chỉ IP nguồn tấn công: Những người xử lý sự cố mới thường tập trung vào địa chỉ IP của nguồn tấn công. Họ thường cố gắng để xác nhận địa chỉ đó không được giả mạo bằng cách kiểm tra kết nối tới nó. Nhưng khi địa chỉ đó không trả lời không có nghĩa nó không có thực mà có thể nó đã được cấu hình để bỏ qua các gói tin Ping hoặc Traceroute. Ngoài ra kẻ tấn công cũng có thể sử dụng một địa chỉ IP động đã được cấp cho một người dùng khác.
- Nghiên cứu về nguồn tấn công thông qua các công cụ tìm kiếm: Sử dụng một công cụ tìm kiếm để tìm các thông tin liên quan đến địa chỉ IP của nơi tấn công.
- Sử dụng cơ sở dữ liệu sự cố: Một vài nhóm nghiên cứu đã thêm các thông tin về phát hiện xâm nhập và nhật ký của tường lửa từ các tổ chức khác nhau vào một cơ sở dữ liệu sự cố chung. Một số cơ sở dữ liệu cũng cho phép mọi người tìm kiếm một hồ sơ tương ứng với một địa chỉ IP cụ thể. Đội xử lý sự cố cũng có thể sử dụng cơ sở dữ liệu đó để xem nếu như các tổ chức khác cũng có những báo cáo về các hoạt động đáng ngờ từ cùng một nguồn.
- Giám sát các kênh truyền thông có khả năng xảy ra tấn công: Đội xử lý sự cố nên giám sát các kênh truyền thông có thể được sử dụng bởi nguồn tấn công. Ví dụ như các kênh IRC …

6.3.3. Loại bỏ sự cố

Sau khi sự cố đã được ngăn chặn, việc loại bỏ các thành phần còn lại là cần thiết để có thể khắc phục hoàn toàn sự cố. Chẳng hạn như khi bị dính phần mềm độc hại thì việc xóa bỏ các thành phần lây nhiễm là điều cần thiết hay xóa các tài khoản người dùng vi phạm … Đối với một vài sự cố, có thể việc xóa là không cần thiết và khi đó họ sẽ phải khôi phục lại hệ thống. Các quản trị viên sẽ phải khôi phục lại hệ thống để có thể hoạt động bình thường và khắc phục các lỗ hổng bảo mật để ngăn chặn các sự cố tương tự có thể xảy ra. Công việc phục hồi có thể là khôi phục lại từ một bản sao lưu sạch, xây dựng lại hệ thống từ đầu hay chỉ thay thế những phần bị hư hỏng, cài đặt các bản vá lỗi, thay đổi mật khẩu, thắt chặt vành đai an ninh mạng (Tập luật tường lửa, danh sách kiểm soát truy cập….). Và đội xử lý sự cố cũng cần phải đề phòng vì khi một tài nguyên bị tấn công thành công thì khả năng nó bị tấn công lại là rất cao hoặc với cùng một cách tấn công đó nhưng kẻ tấn công lại nhắm đến mục tiêu khác trong hệ thống.

6.3.4. Bài học kinh nghiệm

Một trong những phần quan trọng nhất của việc xử lý sự cố là bài học rút ra và khả năng hoàn thiện. Mỗi thành viên đội xử lý nên phát triển để đáp ứng lại với các mối nguy hại mới, cải tiến công nghệ và rút ra các bài học kinh nghiệm. Giữ một cuộc họp về bài học kinh nghiệm giữa các bên liên quan sau mỗi khi sự cố lớn xảy ra có thể rất hữu ích cho việc cải thiện các biện pháp an ninh. Những cuộc họp như thế có thể xem xét những gì đã xảy ra, những biện pháp nào đã được đưa ra để ngăn chặn, kết qua thu được từ những biện pháp đó … Cuộc họp nên được tổ chức vào khi sự cố đã được khắc phục, những câu hỏi có thể sử dụng trong cuộc họp bao gồm:

- Những gì đã xảy ra và thời gian xảy ra vụ việc?
- Như thế nào là hành động đúng đắn của nhân viên và quản lý khi sự cố xảy ra?
- Những thông tin nào cần được thông báo sớm?
- Những hành động hay bước nào gây hạn chế sự phục hồi?
- Nhân viên và quản lý sẽ làm gì khi một sự cố tương tự xảy ra?

- Làm thế nào để chia sẻ thông tin với các tổ chức khác?
- Hành động khắc phục có ngăn ngừa được sự cố tương tự trong tương lai?
- Công cụ bổ sung hoặc nguồn lực cần thiết để phát hiện, phân tích và giảm thiểu sự cố trong tương lai?

Đối với các sự cố nhỏ thì việc phân tích sau khi sự cố xảy ra cần hạn chế ngoại trừ những sự cố được thực hiện thông qua các phương thức mới. Sau một sự cố nghiêm trọng xảy ra, tổ chức nên thực hiện một cuộc họp để đánh giá và cung cấp một cơ chế chia sẻ thông tin.

Bài học kinh nghiệm rút ra từ các sự cố cũng có ích trong việc cung cấp tư liệu để đào tạo các thành viên mới bằng cách cho họ thấy các kinh nghiệm ứng phó với sự cố. Việc cập nhật các chính sách an ninh cũng là một phần quan trọng trong bài học. Xem xét và phân tích một sự cố đã được xử lý cũng giúp nhóm loại trừ bớt những hoạt động dư thừa hoặc không chính xác trong một thủ tục nào đó.

Một hành động khác sau khi xử lý thành công sự cố là viết lại các báo cáo về sự cố đó, đây là một tài liệu giá trị để có thể sử dụng trong tương lai khi có một sự cố tương tự xảy ra.

6.3.5. Một số sự cố điển hình

6.3.5.1 Xử lý sự cố về tấn công từ chối dịch vụ

Như đã trình bày ở chương 1, tấn công từ chối dịch vụ DoS là một hoạt động mà ngăn chặn hoặc làm suy yếu quyền hợp lệ sử dụng mạng, hệ thống hoặc các ứng dụng bằng cách làm cạn kiệt tài nguyên như là CPU, bộ nhớ, băng thông, không gian lưu trữ. Một số tấn công DoS:

- Chiếm dụng tất cả băng thông mạng hiện có bằng cách tạo ra luồng lưu lượng có khối lượng lớn bất thường.
- Gửi các gói tin TCP/IP dị dạng tới một máy chủ, khi máy chủ không xử lý được dẫn đến bị ngưng trệ hoạt động.
- Gửi yêu cầu không hợp lệ tới một ứng dụng để ứng dụng đó bị sụp đổ.

- Thiết lập đồng thời nhiều phiên đăng nhập tới một máy chủ để người dùng khác không thể khởi tạo phiên đăng nhập.
- Chiếm dụng tất cả không gian đĩa hiện có bằng cách tạo ra nhiều tập tin lớn.

- Các bước cần phải chuẩn bị trước khi sự cố xảy ra

- Đàm phán với nhà cung cấp dịch vụ ISP của tổ chức để yêu cầu họ hỗ trợ kết hợp xử lý khi tấn công DoS xảy ra. Một số yêu cầu bao gồm lọc hoặc hạn chế lưu lượng (Ví dụ: ngăn chặn địa chỉ IP nguồn được xác định hoặc thiết lập giới hạn tối đa cho lưu lượng ICMP đi vào), cung cấp nhật ký (logs) của lưu lượng tấn công DoS, và giới hạn các cuộc tấn công tới tổ chức. Thiết lập rõ về thủ tục tổ chức nên làm theo khi yêu cầu sự hỗ trợ của các ISP, bao gồm theo dõi hoạt động 24/7 và sao lưu, nhiều kênh truyền thông, và phương pháp cho nhà cung cấp dịch vụ ISP để xác thực yêu cầu của tổ chức.
- Xem xét điều tra tính khả thi của việc tham gia hợp tác đối phó một cuộc tấn công DDoS phổ biến có ảnh hưởng đến nhiều tổ chức. Ví dụ, các tổ chức nhanh chóng trao đổi thông tin liên quan đến các cuộc tấn công với tổ chức ứng phó sự cố tập trung (ví dụ: VN-CERT) để các tổ chức đó có thể xây dựng một phản ứng phối hợp để tổ chức bị ảnh hưởng để thực hiện. Nhiệm vụ này cho phép các tổ chức xử lý sự cố một cách nhanh chóng và hiệu quả hơn.
- Triển khai và cấu hình phần mềm phát hiện và phòng chống xâm nhập để phát hiện luồng lưu lượng DoS. Ví dụ, phần mềm phát hiện xâm nhập mạng thường có dấu hiệu để nhận biết các loại tấn công DoS khác nhau, phần mềm phân tích hành vi mạng có thể xác định lưu lượng truy cập bất thường gây ra bởi các cuộc tấn công DoS, và phát hiện xâm nhập mạng không dây và phần mềm phòng chống có thể phát hiện các cuộc tấn công DoS dựa trên mạng không dây.
- Đàm phán về phát hiện xâm nhập với nhà cung cấp dịch vụ ISP của tổ chức đó bởi vì một số cuộc tấn công có thể tràn nhập tài nguyên ISP và thậm chí không đạt được các bộ định tuyến vành đai của tổ chức. Các

ISP có thể thực hiện giám sát lưu lượng để phát hiện các cuộc tấn công DoS lớn xảy ra trên các mạng của ISP.

- Thực hiện giám sát tài nguyên liên tục để thiết lập cơ sở cho việc sử dụng băng thông mạng và sử dụng tài nguyên máy chủ quan trọng, và ghi lại hoặc cảnh báo khi có sự chênh lệch bất thường từ thiết lập cơ sở.
- Xác định các trang web cung cấp khả năng thống kê về độ trễ giữa các ISP khác nhau và giữa các địa điểm vật lý khác nhau. Phương thức này thường được gọi là theo dõi trạng thái Internet. Khi tấn công DoS dựa trên mạng xảy ra, xử lý sự cố có thể sử dụng các trang web này để xác định xem các cuộc tấn công đang ảnh hưởng đến các tổ chức khác.
- Gặp quản trị viên mạng để đàm phán làm thế nào họ có thể hỗ trợ trong việc phân tích và thu thập các cuộc tấn công mạng DoS và DDoS. Ví dụ, các quản trị viên thiết lập ghi lại hoạt động trong quá trình tấn công. Quản trị cũng có nhiệm vụ trong việc bảo vệ bằng chứng, chẳng hạn như hỗ trợ với việc bản sao nhật ký (logs) hệ thống.
- Duy trì bản sao cục bộ (bản điện tử và bản giấy) của bất kỳ thông tin trên máy tính có liên quan trong việc xử lý sự cố DoS trong trường hợp đường truyền Internet của tổ chức hoặc kết nối mạng nội bộ bị mất.

- Phòng ngừa sự cố

- Cấu hình mạng vành đai để ngăn chặn tất cả lưu lượng đến và đi mà không được cho phép. Bao gồm:
    - Ngăn chặn sử dụng các chức năng như echo và chargen, không phục vụ cho mục đích hợp lệ và thường được sử dụng trong cuộc tấn công DoS.
    - Thực hiện lọc đầu vào và đầu ra để chặn các gói dữ liệu giả mạo cho mục đích xâm nhập.
    - Ngăn chặn lưu lượng từ dải địa chỉ IP không được gán (được gọi là BOGON Address List). Công cụ tấn công giả mạo địa chỉ IP có thể sử dụng địa chỉ chưa được gán để sử dụng Internet.

- Thiết lập quy tắc cho tường lửa và danh sách kiểm soát truy cập (ACL) thiết bị định tuyến để ngăn chặn lưu lượng đúng cách.
- Cấu hình thiết bị định tuyến vành đai không để chuyển tiếp trực tiếp gói tin broadcast.
- Hạn chế lưu lượng ICMP đến và đi, chỉ cho phép các loại và đoạn mã cần thiết.
- Chặn các kết nối gửi qua kênh IRC, dịch vụ ngang hàng và cổng nếu sử dụng dịch vụ tương ứng là không được phép.

- Thực hiện giới hạn tốc độ cho các giao thức nhất định, chẳng hạn như ICMP, vì vậy giao thức chỉ có thể sử dụng tỷ lệ phần trăm chỉ định của tổng số băng thông. Giới hạn tốc độ có thể được thực hiện ở mạng vành đai của tổ chức (ví dụ, các bộ định tuyến vành đai, tường lửa) và từ các ISP của tổ chức.
- Trên các máy tính có khả năng truy cập Internet, vô hiệu hóa tất cả các dịch vụ không cần thiết, và hạn chế việc sử dụng các dịch vụ có thể được sử dụng trong cuộc tấn công DoS (ví dụ, cấu hình máy chủ DNS không cho phép truy vấn đệ quy).
- Thực hiện thiết lập dự phòng cho các máy chủ đảm nhiệm chức năng chính (ví dụ, nhiều ISP, tường lửa, máy chủ Web).
- Đảm bảo hệ thống mạng không hoạt động hết công suất tối đa, hoặc có được dễ dàng cho một cuộc tấn công DoS tiếp nhận các tài nguyên còn lại.

6.3.5.2 Xử lý sự cố về mã độc hại

- Định nghĩa và ví dụ của sự cố

Mã độc hại là một chương trình được bí mật gắn vào các phần mềm với mục đích phá hủy dữ liệu, chạy chương trình phá hoại hoặc xâm nhập, hoặc không thỏa hiệp tính bí mật, tính toàn vẹn và tính sẵn sàng của dữ liệu của nạn nhân, các ứng dụng, hoặc hệ điều hành. Mã độc hại được thiết kế để thực hiện các chức năng bất chính mà không cần sự cho phép của người sử dụng của hệ thống. Nhiều loại mã độc hại, bao gồm virus, sâu, trojan, MMC, và

pha trộn với các hình thức tấn công. Phần mềm độc hại cũng bao gồm các công cụ tấn công như backdoor, rootkit, và keystroke logger, và cookie theo dõi sử dụng như phần mềm gián điệp.

- Các bước cần phải chuẩn bị trước khi sự cố xảy ra

Các hành động cần được thực hiện để chuẩn bị cho xử lý sự cố mã độc hại bao gồm:

- **Nhận thức cho người sử dụng tác hại mã độc hại.** Thông tin bao gồm đánh giá cơ bản của phương pháp mã độc sử dụng để nhân bản, các hiện tượng khi bi lây nhiễm. Tổ chức các buổi đào tạo người dùng thường xuyên giúp đảm bảo người dùng nhận thức được những rủi ro mà mã độc hại gây ra. Khuyến cáo người dùng về những gì họ nên làm khi xảy ra lây nhiễm (ví dụ: ngắt kết nối máy trạm từ mạng, và gọi cho bộ phận hỗ trợ) bởi vì xử lý không đúng của sự cố có thể làm cho một sự cố nhỏ tồi tệ hơn nhiều.
- **Tham khảo thông tin về nhà cung cấp Antivirus.** Người dùng có thể đăng ký danh sách gửi thư từ các nhà cung cấp chống virus cung cấp thông tin kịp thời về các mối đe dọa mã độc hại mới.
- **Triển khai hệ thống phát hiện xâm phạm dựa trên Host đến máy máy chủ, máy trạm quan trọng.** Phần mềm IDPS dựa trên Host giúp phát hiện dấu hiệu sự cố mã độc hại, chẳng hạn như thay đổi cấu hình và sửa đổi tệp tin thực thi hệ thống. Chức năng kiểm tra tính toàn vẹn tệp tin là hữu ích trong việc xác định các thành phần bị ảnh hưởng của một hệ thống.
- **Thu thập tài nguyên phân tích sự cố mã độc hại.** Các tổ chức cần có các công cụ phân tích thích hợp có sẵn trước khi một sự cố xảy ra. Danh sách cổng, tài liệu về hệ điều hành, tài liệu ứng dụng, sơ đồ mạng và danh mục các tài nguyên quan trọng, và cơ sở mạng dự kiến, hệ thống, và các hoạt động ứng dụng tất cả nên có sẵn để hỗ trợ trong việc xác định và kiểm tra sự cố.
- **Phần mềm khôi phục sự cố mã độc.** Để hỗ trợ việc phục hồi, tổ chức phải đảm bảo có sẵn các phần mềm khôi phục sự cố. Tổ chức phải đảm

bảo hoạt động ổ đĩa hệ thống khởi động và đĩa CD, các bản vá lỗi bảo mật từ các hệ điều hành và các nhà cung cấp ứng dụng và phần mềm đóng gói và bản sao lưu sạch có sẵn.

- Phòng ngừa sự cố

Các hướng dẫn sau đây cung cấp cụ thể phòng ngừa sự cố mã độc hại:

- **Sử dụng phần mềm Antivirus.** Phần mềm chống virus là một điều cần thiết để chống lại các mối đe dọa mã độc hại và hạn chế thiệt hại. Các phần mềm nên được triển khai trên tất cả các máy trong toàn công ty, và tất cả các bản sao phải được giữ hiện tại với các dấu hiệu virus mới nhất để ngăn chặn các mối đe dọa mới nhất. Phần mềm chống virus cũng nên được sử dụng cho các ứng dụng, thiết bị có thể truyền mã độc hại, chẳng hạn như email, chuyển tập tin, và các phần mềm nhắn tin. Phần mềm nên được cấu hình để thực hiện quét định kỳ của hệ thống cũng như quét theo thời gian thực của mỗi tập tin khi được tải về, mở ra, hoặc thực hiện. Phần mềm chống virus cũng nên được cấu hình để xóa bỏ, cách ly các tập tin bị nhiễm. Một số sản phẩm chống virus không chỉ tìm virus, sâu, và Trojan, và cũng kiểm tra HyperText Markup Language (HTML), ActiveX, JavaScript, và các loại mã điện thoại di động có nội dung độc hại.
- **Ngăn chặn việc cài đặt các phần mềm gián điệp.** Một số trình duyệt web có thể được cấu hình để nhắc nhở người dùng chấp thuận việc cài đặt phần mềm như trình duyệt web plug-in hoặc để ngăn chặn bất kỳ trang web cài đặt phần mềm trên máy khách. Các thiết lập này đặc biệt hữu ích để ngăn chặn việc cài đặt phần mềm gián điệp trong các trình duyệt Web. Để giảm thiểu các mối đe dọa phần mềm gián điệp, tổ chức nên sử dụng phần mềm chống virus có khả năng nhận ra các mối đe dọa phần mềm gián điệp nhằm phát hiện và gỡ bỏ tiện ích phần mềm gián điệp. Phần mềm nên được triển khai trên tất cả các hệ thống mà đạt yêu cầu là có sẵn.
- **Ngăn chặn tệp tin nghi ngờ.** Cấu hình máy chủ email và máy trạm để ngăn chặn các tệp tin đính kèm có phần mở rộng tệp tin có liên quan

đến mã độc hại (ví dụ, .pif, .vbs…), và nghi ngờ tệp tin mở rộng kết hợp (ví dụ. Txt.vbs, Htm.exe). Tuy nhiên, điều này cũng có thể vô tình chặn các hoạt động hợp lệ. Một số tổ chức thay đổi phần mở rộng tập tin đính kèm email nghi ngờ để người nhận sẽ phải lưu các tập tin đính kèm và đổi tên trước khi chạy, đó là một sự thỏa hiệp tốt trong một số môi trường giữa chức năng và an toàn.

- **Lọc thư rác.** Thư rác thường được sử dụng để lừa đảo và cung cấp phần mềm gián điệp, và đôi khi nó có chứa các loại khác của phần mềm độc hại. Sử dụng phần mềm lọc thư rác trên máy chủ email, máy trạm hoặc trên các thiết bị mạng làm giảm đáng kể số lượng thư rác đến người sử dụng, và giảm thiểu sự cố kích hoạt phần mềm mã độc hại chứa trong mail spam.
- **Hạn chế việc sử dụng các chương trình thiết yếu với khả năng truyền tệp tin.** Ví dụ như chia sẻ tệp tin ngang hàng và các chương trình âm nhạc, phần mềm tin nhắn, và IRC máy trạm và máy chủ. Các chương trình này thường được sử dụng để lây lan mã độc trong người dùng.
- **Giáo dục người sử dụng việc xử lý an toàn tệp tin đính kèm email.** Phần mềm chống virus được cấu hình để quét mỗi tệp tin đính kèm trước khi mở nó. Người dùng không nên mở tệp tin đính kèm có nghi ngờ hoặc tệp tin đính kèm không rõ nguồn gốc. Người dùng cũng không nên hoàn toàn chắc chắn nếu biết người gửi, các tập tin đính kèm không bị nhiễm. Ví dụ, người gửi có thể không biết rằng hệ thống của họ bị nhiễm mã độc hại có thể trích xuất địa chỉ email từ các tập tin và gửi bản sao của mã độc hại vào các địa chỉ. Hoạt động này tạo ra tin tưởng các email đến từ một người đáng tin cậy, tuy nhiên người ta không nhận thức được rằng họ đã được gửi đi. Người sử dụng cũng nên được giáo dục về các loại tập tin mà họ không bao giờ nên mở (ví dụ, .bat, .com, .exe, .pif, .vbs). Mặc dù nhận thức của người sử dụng các thực hành tốt nên làm giảm số lượng và mức độ nghiêm trọng của sự cố mã độc hại, các tổ chức nên cho rằng người dùng sẽ có những sai sót và lây nhiễm sang hệ thống.

- **Hạn chế mở chia sẻ Windows.** Một số sâu lây lan thông qua chia sẻ không an toàn trên máy chạy Windows. Nếu một máy trong tổ chức bị nhiễm mã độc hại, nó có thể nhanh chóng lây lan sang hàng trăm hoặc hàng ngàn máy khác trong tổ chức thông qua các chia sẻ không an toàn. Tổ chức nên thường xuyên quét tất cả các máy khi mở thư mục chia sẻ và quy định các chủ sở hữu để đảm bảo chia sẻ đúng cách. Ngoài ra, mạng vành đai phải được cấu hình để ngăn chặn lưu lượng sử dụng cổng NetBIOS đi ra và đi vào mạng của tổ chức. Hành động này sẽ ngăn chặn không chỉ máy chủ bên ngoài lây nhiễm trực tiếp từ máy chủ nội bộ thông qua chia sẻ nhưng cũng lây nhiễm mã độc bên trong lây lan sang các tổ chức khác thông qua việc mở thư mục chia sẻ.
- **Sử dụng trình duyệt web bảo mật để giới hạn mã điện thoại di động.** Tất cả các trình duyệt web cần phải có các thiết lập bảo mật để ngăn chặn ActiveX và các mã di động vô tình được tải về và cài đặt trên hệ thống cục bộ. Tổ chức nên xem xét việc thành lập một chính sách bảo mật Internet mà xác định được loại mã điện thoại di động có thể được sử dụng từ nhiều nguồn khác nhau (ví dụ, máy chủ nội bộ, máy chủ bên ngoài). Phần mềm lọc nội dung trang web cũng có thể được triển khai để giám sát hoạt động mạng liên quan đến Web và ngăn chặn một số loại mã điện thoại di động từ các địa điểm không đáng tin cậy.
- **Ngăn chặn chuyển tiếp của Email.** Sâu thư điện tử đôi khi cố gắng sử dụng các máy chủ email của tổ chức để chuyển tiếp, có nghĩa là không cho người gửi cũng như người nhận email là một phần của tổ chức. Máy chủ email cho phép chuyển tiếp có thể cung cấp sâu gửi thư hàng loạt một cách dễ dàng để phát tán. Tổ chức nên xem xét cấu hình máy chủ email của họ để ngăn chặn chuyển tiếp và ghi lại tất cả những cố gắng để chuyển tiếp thư điện tử.
- Cấu hình máy trạm thư để hoạt động an toàn hơn. Toàn bộ máy trạm email của tổ chức nên được cấu hình để tránh các hành động có thể vô tình cho phép lây nhiễm hoặc phát tán xảy ra. Ví dụ, máy trạm email không cho phép tự động mở hoặc chạy tệp tin đính kèm.

6.3.5.3 Xử lý sự cố về truy cập không xác thực

Một sự cố truy cập trái phép xảy ra khi một người truy cập vào các tài nguyên mà người đó không có ý định. Truy cập trái phép thường đạt được thông qua việc khai thác các lỗ hổng ứng dụng hoặc hệ điều hành, hoặc mua lại tên đăng nhập và mật khẩu, hoặc kỹ nghệ xã hội. Kẻ tấn công có được truy cập nhưng bị giới hạn thông qua một lỗ hổng và truy cập để tấn công leo thang đặc quyền, cuối cùng đạt được quyền truy cập cao hơn. Ví dụ về các sự cố truy cập trái phép bao gồm:

- Thực hiện một thiết lập với quyền root từ xa tới một máy chủ email.
- Thay đổi giao diện một máy chủ Web.
- Đoán hay phá mật khẩu.
- Xem hoặc sao chép dữ liệu nhạy cảm, chẳng hạn như bảng lương, thông tin y tế, và số thẻ tín dụng, mà không được phép.
- Chạy phần mềm sniffer gói tin trên một máy trạm để chặn bắt tên người dùng và mật khẩu.
- Truy cập vào một modem không có bảo mật và truy cập mạng nội bộ.
- Đăng nhập vào máy trạm không có giám sát mà cần quyền hạn.

- Các bước chuẩn bị xử lý sự cố

Một số khuyến cáo để chuẩn bị trước khi sự cố xảy ra:

- Cấu hình phần mềm IDPS dựa trên mạng và / hoặc dựa trên máy để xác định và cảnh báo về những hành vi truy cập trái phép.
- Sử dụng máy chủ lưu trữ tập trung thông tin cần thiết từ máy tính trong toàn tổ chức được lưu trữ trong một vị trí đảm bảo an toàn.
- Thiết lập các thủ tục đi kèm khi tất cả người dùng của một ứng dụng, hệ thống, miền tin cậy, hoặc tổ chức nên thay đổi mật khẩu của mình vì một sự thỏa hiệp mật khẩu. Các thủ tục cần tuân thủ chính sách mật khẩu của tổ chức.
- Khuyến cáo về xử lý sự cố truy cập trái phép với quản trị hệ thống để họ hiểu được vai trò của họ trong quá trình xử lý sự cố.

- Phòng ngừa sự cố

Sử dụng chiến lược phòng thủ nhiều lớp mạnh, với nhiều lớp bảo mật giữa người sử dụng trái phép và các tài nguyên mà đang cố gắng khai thác. Bảng sau đây liệt kê các bước hỗ trợ cho một chiến lược phòng thủ nhiều lớp.

Bảng 6.5 – Bảng phân cấp phòng thủ nhiều lớp

Hạng mục	Hành động cụ thể
An toàn mạng	• Cấu hình mạng vành đai để ngăn chặn tất cả các lưu lượng truy cập mà không được phép. • Bảo vệ toàn bộ tất cả các phương pháp truy cập từ xa, bao gồm modem và mạng riêng ảo. Một modem không đảm bảo an toàn có thể cung cấp truy cập trái phép dễ dàng với các hệ thống mạng nội bộ. Khi đảm bảo truy cập từ xa, xem xét cẩn thận độ tin cậy của các khách hàng, nếu ngoài tầm kiểm soát của tổ chức, nên giới hạn tiếp cận với các tài nguyên có thể, và hành động của họ phải được giám sát chặt chẽ. • Đặt tất cả các dịch vụ truy cập công khai trong khu vực phân đoạn mạng (DMZ). Mạng vành đai được cấu hình để máy chủ bên ngoài có thể thiết lập kết nối duy nhất tới host trên DMZ, không cho phép tới phân đoạn mạng nội bộ.
An toàn máy tính	• Thực hiện đánh giá lỗ hổng thường xuyên để xác định những rủi ro nghiêm trọng và giảm thiểu rủi ro ở mức chấp nhận. • Vô hiệu hóa tất cả các dịch vụ không cần thiết trên máy chủ. Phân chia các dịch vụ quan trọng riêng biệt để chúng chạy trên máy khác nhau. Nếu kẻ tấn công sau đó thỏa hiệp một máy chủ, truy cập ngay lập tức chỉ đạt được một dịch vụ duy nhất.

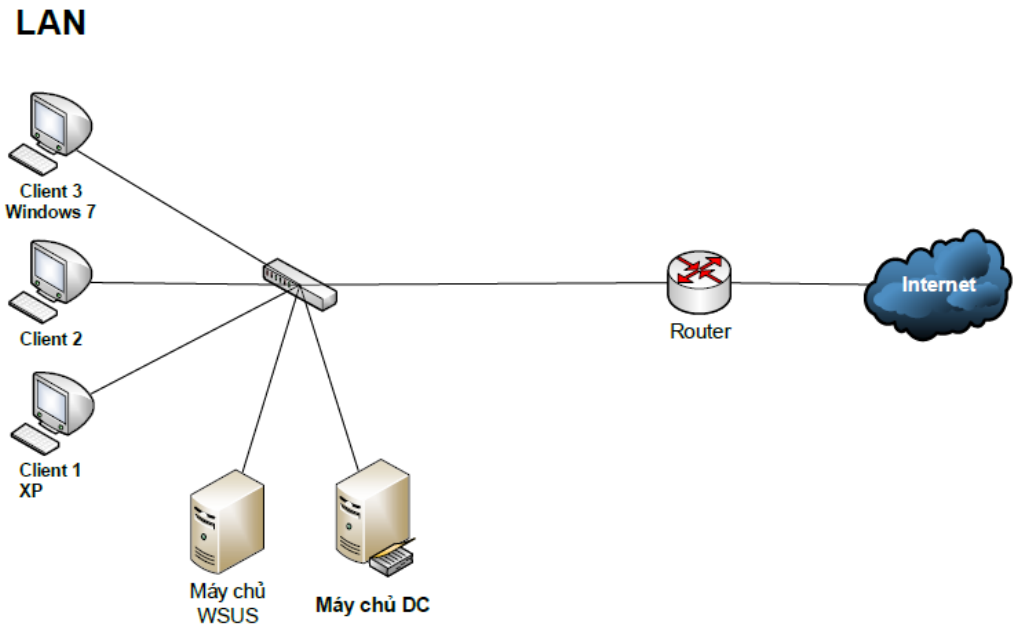
	• Chạy các dịch vụ với những đặc quyền ít nhất có thể để giảm tác động trực tiếp khi bị khai thác thành công. • Sử dụng phần mềm tường lửa host-based/personal để hạn chế tiếp xúc với cá nhân cuộc tấn công. • Hạn chế truy cập vật lý trái phép để đăng nhập vào hệ thống bằng cách yêu cầu người dùng khóa màn hình tự động khi không sử dụng và yêu cầu người dùng đăng xuất trước khi rời khỏi văn phòng. • Thường xuyên kiểm tra các thiết lập sự cho phép đối với tài nguyên quan trọng, bao gồm các tệp tin mật khẩu, cơ sở dữ liệu nhạy cảm và các trang web công cộng. Quá trình này có thể dễ dàng tự động báo cáo những thay đổi trong điều khoản trên một cách thường xuyên.
Xác thực và thẩm quyền	• Tạo ra một chính sách mật khẩu có yêu cầu sử dụng phức tạp, khó khăn để đoán mật khẩu, không chia sẻ mật khẩu, và hướng người dùng sử dụng mật khẩu khác nhau trên các hệ thống khác nhau, đặc biệt là các máy chủ bên ngoài và các ứng dụng. • Yêu cầu xác thực đủ mạnh, đặc biệt để truy cập tài nguyên quan trọng. • Tạo ra các tiêu chuẩn xác thực và ủy quyền cho nhân viên và nhà phát triển để thực hiện khi thẩm định, phát triển phần mềm. Ví dụ, mật khẩu được mã hóa mạnh mẽ sử dụng một thuật toán xác nhận FIPS 140 khi chúng được truyền hoặc lưu trữ. • Lập thủ tục dự phòng tài khoản người dùng. Phê duyệt cho các yêu cầu tài khoản mới và một quá trình định kỳ vô hiệu hóa hoặc xóa các tài khoản không còn cần thiết.
An toàn vật lý	Thực hiện các biện pháp bảo mật vật lý để hạn chế quyền truy cập vào các nguồn tài nguyên quan trọng.

CÁC BÀI THỰC HÀNH

1. Thực hành cập nhật bản vá cho hệ điều hành Windows

Mục đích bài thực hành: hướng dẫn cài đặt, cấu hình dịch vụ cập nhật bản vá WSUS của Microsoft để lấy về các bản vá hệ điều hành, dịch vụ Office từ nhà cung cấp Microsoft và cập nhật cho toàn bộ máy chủ và máy trạm trong mạng nội bộ.

Bước 1: Cài đặt mô hình



Bước 2: Tại máy chủ WSUS cài đặt phần mềm WSUS

Bước 3: Cấu hình máy chủ WSUS tự động tải về các bản vá cho hệ điều hành Windows XP và Windows 7, phần mềm Office.

Bước 4: Tại máy chủ quản lý tập trung DC tạo chính sách tự động lấy bản vá và cài đặt từ máy chủ WSUS và áp dụng cho toàn bộ máy trạm bên trong.

Bước 5: Tại máy trạm kiểm tra cập nhật bản vá.

Tài liệu tham khảo

[1] Nghị định của Chính phủ số: 90/2008/NĐ-CP về chống thư rác (Năm 2008).

[2] John Mallery. Hardening Network Security. McGraw-Hill/Osborne Media (Năm 2005).

[3] Karen Scarfone, Paul Hoffman. Guidelines on Firewalls and Firewall Policy. NIST SP 800-41 (Năm 2002).

[4] Elizabeth D. Zwicky. Building Internet Firewalls. O'Reilly & Associates (Năm 2000).

[5] Wes Noonan, Ido Dubrawsky. Cisco Press Firewall Fundamentals. Cisco Press (Năm 2006).

[6] Karen Scarfone, Peter Mell. Guide to Intrusion Detection and Prevention Systems. NIST SP 800-94 (Năm 2007).

[7] Paul Cichonski, Tom Millar. Computer Security Incident Handling Guide. NIST SP 800-61 (Năm 2012).